THE UNIVERSITY OF CALGARY

Diophantine Equations, Lucas Sequences and Pseudoprimes

by

Zhaiyu Mo

A DISSERTATION

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

December, 1993

ISBN 0-315-93948-6

Canada

Name Zhaiyu Mo

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

Mathematics

SUBJECT TERM

0	4	0	5

SUBJECT CODE

U·M·I

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS
Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION
General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0680
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0279
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523
Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0288
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS
Language
- General 0679
- Ancient 0289
- Linguistics 0290
- Modern 0291

Literature
- General 0401
- Classical 0294
- Comparative 0295
- Medieval 0297
- Modern 0298
- African 0316
- American 0591
- Asian 0305
- Canadian (English) 0352
- Canadian (French) 0355
- English 0593
- Germanic 0311
- Latin American 0312
- Middle Eastern 0315
- Romance 0313
- Slavic and East European 0314

PHILOSOPHY, RELIGION AND THEOLOGY
Philosophy 0422
Religion
- General 0318
- Biblical Studies 0321
- Clergy 0319
- History of 0320
- Philosophy of 0322

Theology 0469

SOCIAL SCIENCES
American Studies 0323
Anthropology
- Archaeology 0324
- Cultural 0326
- Physical 0327

Business Administration
- General 0310
- Accounting 0272
- Banking 0770
- Management 0454
- Marketing 0338

Canadian Studies 0385
Economics
- General 0501
- Agricultural 0503
- Commerce-Business 0505
- Finance 0508
- History 0509
- Labor 0510
- Theory 0511

Folklore 0358
Geography 0366
Gerontology 0351
History
- General 0578
- Ancient 0579
- Medieval 0581
- Modern 0582
- Black 0328
- African 0331
- Asia, Australia and Oceania 0332
- Canadian 0334
- European 0335
- Latin American 0336
- Middle Eastern 0333
- United States 0337

History of Science 0585
Law 0398
Political Science
- General 0615
- International Law and Relations 0616
- Public Administration 0617

Recreation 0814
Social Work 0452
Sociology
- General 0626
- Criminology and Penology 0627
- Demography 0938
- Ethnic and Racial Studies 0631
- Individual and Family Studies 0628
- Industrial and Labor Relations 0629
- Public and Social Welfare 0630
- Social Structure and Development 0700
- Theory and Methods 0344

Transportation 0709
Urban and Regional Planning 0999
Women's Studies 0453

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES
Agriculture
- General 0473
- Agronomy 0285
- Animal Culture and Nutrition 0475
- Animal Pathology 0476
- Food Science and Technology 0359
- Forestry and Wildlife 0478
- Plant Culture 0479
- Plant Pathology 0480
- Plant Physiology 0817
- Range Management 0777
- Wood Technology 0746

Biology
- General 0306
- Anatomy 0287
- Biostatistics 0308
- Botany 0309
- Cell 0379
- Ecology 0329
- Entomology 0353
- Genetics 0369
- Limnology 0793
- Microbiology 0410
- Molecular 0307
- Neuroscience 0317
- Oceanography 0416
- Physiology 0433
- Radiation 0821
- Veterinary Science 0778
- Zoology 0472

Biophysics
- General 0786
- Medical 0760

EARTH SCIENCES
Biogeochemistry 0425
Geochemistry 0996
Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleoecology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES
Environmental Sciences 0768
Health Sciences
- General 0566
- Audiology 0300
- Chemotherapy 0992
- Dentistry 0567
- Education 0350
- Hospital Management 0769
- Human Development 0758
- Immunology 0982
- Medicine and Surgery 0564
- Mental Health 0347
- Nursing 0569
- Nutrition 0570
- Obstetrics and Gynecology 0380
- Occupational Health and Therapy 0354
- Ophthalmology 0381
- Pathology 0571
- Pharmacology 0419
- Pharmacy 0572
- Physical Therapy 0382
- Public Health 0573
- Radiology 0574
- Recreation 0575
- Speech Pathology 0460
- Toxicology 0383

Home Economics 0386

PHYSICAL SCIENCES
Pure Sciences
Chemistry
- General 0485
- Agricultural 0749
- Analytical 0486
- Biochemistry 0487
- Inorganic 0488
- Nuclear 0738
- Organic 0490
- Pharmaceutical 0491
- Physical 0494
- Polymer 0495
- Radiation 0754

Mathematics 0405
Physics
- General 0605
- Acoustics 0986
- Astronomy and Astrophysics 0606
- Atmospheric Science 0608
- Atomic 0748
- Electronics and Electricity 0607
- Elementary Particles and High Energy 0798
- Fluid and Plasma 0759
- Molecular 0609
- Nuclear 0610
- Optics 0752
- Radiation 0756
- Solid State 0611

Statistics 0463

Applied Sciences
Applied Mechanics 0346
Computer Science 0984
Engineering
- General 0537
- Aerospace 0538
- Agricultural 0539
- Automotive 0540
- Biomedical 0541
- Chemical 0542
- Civil 0543
- Electronics and Electrical 0544
- Heat and Thermodynamics 0348
- Hydraulic 0545
- Industrial 0546
- Marine 0547
- Materials Science 0794
- Mechanical 0548
- Metallurgy 0743
- Mining 0551
- Nuclear 0552
- Packaging 0549
- Petroleum 0765
- Sanitary and Municipal 0554
- System Science 0790

Geotechnology 0428
Operations Research 0796
Plastics Technology 0795
Textile Technology 0994

PSYCHOLOGY
General 0621
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0989
Psychobiology 0349
Psychometrics 0632
Social 0451

Nom _____

Dissertation Abstracts International est organisé en catégories de sujets. Veuillez s.v.p. choisir le sujet qui décrit le mieux votre thèse et inscrivez le code numérique approprié dans l'espace réservé ci-dessous.

SUJET | CODE DE SUJET | U·M·I

Catégories par sujets

HUMANITÉS ET SCIENCES SOCIALES

COMMUNICATIONS ET LES ARTS
Architecture 0729
Beaux-arts 0357
Bibliothéconomie 0399
Cinéma 0900
Communication verbale 0459
Communications 0708
Danse 0378
Histoire de l'art 0377
Journalisme 0391
Musique 0413
Sciences de l'information 0723
Théâtre 0465

ÉDUCATION
Généralités 515
Administration 0514
Art 0273
Collèges communautaires 0275
Commerce 0688
Économie domestique 0278
Éducation permanente 0516
Éducation préscolaire 0518
Éducation sanitaire 0680
Enseignement agricole 0517
Enseignement bilingue et multiculturel 0282
Enseignement industriel 0521
Enseignement primaire. 0524
Enseignement professionnel 0747
Enseignement religieux 0527
Enseignement secondaire 0533
Enseignement spécial 0529
Enseignement supérieur 0745
Évaluation 0288
Finances 0277
Formation des enseignants 0530
Histoire de l'éducation 0520
Langues et littérature 0279
Lecture 0535
Mathématiques 0280
Musique 0522
Orientation et consultation 0519
Philosophie de l'éducation 0998
Physique 0523
Programmes d'études et enseignement 0727
Psychologie 0525
Sciences 0714
Sciences sociales 0534
Sociologie de l'éducation 0340
Technologie 0710

LANGUE, LITTÉRATURE ET LINGUISTIQUE
Langues
- Généralités 0679
- Anciennes 0289
- Linguistique 0290
- Modernes 0291

Littérature
- Généralités 0401
- Anciennes 0294
- Comparée 0295
- Médiévale 0297
- Moderne 0298
- Africaine 0316
- Américaine 0591
- Anglaise 0593
- Asiatique 0305
- Canadienne (Anglaise) 0352
- Canadienne (Française) 0355
- Germanique 0311
- Latino-américaine 0312
- Moyen-orientale 0315
- Romane 0313
- Slave et est-européenne 0314

PHILOSOPHIE, RELIGION ET THÉOLOGIE
Philosophie 0422
Religion
- Généralités 0318
- Clergé 0319
- Études bibliques 0321
- Histoire des religions 0320
- Philosophie de la religion 0322

Théologie 0469

SCIENCES SOCIALES
Anthropologie
- Archéologie 0324
- Culturelle 0326
- Physique 0327

Droit 0398
Économie
- Généralités 0501
- Commerce-Affaires 0505
- Économie agricole 0503
- Économie du travail 0510
- Finances 0508
- Histoire 0509
- Théorie 0511

Études américaines 0323
Études canadiennes 0385
Études féministes 0453
Folklore 0358
Géographie 0366
Gérontologie 0351
Gestion des affaires
- Généralités 0310
- Administration 0454
- Banques 0770
- Comptabilité 0272
- Marketing 0338

Histoire
- Histoire générale 0578
- Ancienne 0579
- Médiévale 0581
- Moderne 0582
- Histoire des noirs 0328
- Africaine 0331
- Canadienne 0334
- États-Unis 0337
- Européenne 0335
- Moyen-orientale 0333
- Latino-américaine 0336
- Asie, Australie et Océanie 0332

Histoire des sciences 0585
Loisirs 0814
Planification urbaine et régionale 0999
Science politique
- Généralités 0615
- Administration publique 0617
- Droit et relations internationales 0616

Sociologie
- Généralités 0626
- Aide et bien-âtre social 0630
- Criminologie et établissements pénitentiaires 0627
- Démographie 0938
- Études de l' individu et de la famille 0628
- Études des relations interethniques et des relations raciales 0631
- Structure et développement social 0700
- Théorie et méthodes. 0344
- Travail et relations industrielles 0629

Transports 0709
Travail social 0452

SCIENCES ET INGÉNIERIE

SCIENCES BIOLOGIQUES
Agriculture
- Généralités 0473
- Agronomie. 0285
- Alimentation et technologie alimentaire 0359
- Culture 0479
- Élevage et alimentation 0475
- Exploitation des pâturages 0777
- Pathologie animale 0476
- Pathologie végétale 0480
- Physiologie végétale 0817
- Sylviculture et faune 0478
- Technologie du bois 0746

Biologie
- Généralités 0306
- Anatomie 0287
- Biologie (Statistiques) 0308
- Biologie moléculaire 0307
- Botanique 0309
- Cellule 0379
- Écologie 0329
- Entomologie 0353
- Génétique 0369
- Limnologie 0793
- Microbiologie 0410
- Neurologie 0317
- Océanographie 0416
- Physiologie 0433
- Radiation 0821
- Science vétérinaire 0778
- Zoologie 0472

Biophysique
- Généralités 0786
- Medicale 0760

SCIENCES DE LA TERRE
Biogéochimie 0425
Géochimie 0996
Géodésie 0370
Géographie physique 0368
Géologie 0372
Géophysique 0373
Hydrologie 0388
Minéralogie 0411
Océanographie physique 0415
Paléobotanique 0345
Paléoécologie 0426
Paléontologie 0418
Paléozoologie 0985
Palynologie 0427

SCIENCES DE LA SANTÉ ET DE L'ENVIRONNEMENT
Économie domestique 0386
Sciences de l'environnement 0768
Sciences de la santé
- Généralités 0566
- Administration des hôpitaux 0769
- Alimentation et nutrition 0570
- Audiologie 0300
- Chimiothérapie 0992
- Dentisterie 0567
- Développement humain 0758
- Enseignement 0350
- Immunologie 0982
- Loisirs 0575
- Médecine du travail et thérapie 0354
- Médecine et chirurgie 0564
- Obstétrique et gynécologie 0380
- Ophtalmologie 0381
- Orthophonie 0460
- Pathologie 0571
- Pharmacie 0572
- Pharmacologie 0419
- Physiothérapie 0382
- Radiologie 0574
- Santé mentale 0347
- Santé publique 0573
- Soins infirmiers 0569
- Toxicologie 0383

SCIENCES PHYSIQUES
Sciences Pures

Chimie
- Généralités 0485
- Biochimie 487
- Chimie agricole 0749
- Chimie analytique 0486
- Chimie minérale 0488
- Chimie nucléaire 0738
- Chimie organique 0490
- Chimie pharmaceutique 0491
- Physique 0494
- PolymÇres 0495
- Radiation 0754

Mathématiques 0405
Physique
- Généralités 0605
- Acoustique 0986
- Astronomie et astrophysique 0606
- Électronique et électricité 0607
- Fluides et plasma 0759
- Météorologie 0608
- Optique 0752
- Particules (Physique nucléaire) 0798
- Physique atomique 0748
- Physique de l'état solide 0611
- Physique moléculaire 0609
- Physique nucléaire 0610
- Radiation 0756

Statistiques 0463

Sciences Appliqués Et Technologie

Informatique 0984
Ingénierie
- Généralités 0537
- Agricole 0539
- Automobile 0540
- Biomédicale 0541
- Chaleur et thermodynamique 0348
- Conditionnement (Emballage) 0549
- Génie aérospatial 0538
- Génie chimique 0542
- Génie civil 0543
- Génie électronique et électrique 0544
- Génie industriel 0546
- Génie mécanique 0548
- Génie nucléaire 0552
- Ingénierie des systèmes 0790
- Mécanique navale 0547
- Métallurgie 0743
- Science des matériaux 0794
- Technique du pétrole 0765
- Technique minière 0551
- Techniques sanitaires et municipales 0554
- Technologie hydraulique 0545

Mécanique appliquée 0346
Géotechnologie 0428
Matières plastiques (Technologie) 0795
Recherche opérationnelle 0796
Textiles et tissus (Technologie) 0794

PSYCHOLOGIE
Généralités 0621
Personnalité 0625
Psychobiologie 0349
Psychologie clinique 0622
Psychologie du comportement 0384
Psychologie du développement 0620
Psychologie expérimentale 0623
Psychologie industrielle 0624
Psychologie physiologique 0989
Psychologie sociale 0451
Psychométrie 0632

THE UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a dissertation entitled "Diophantine Equations, Lucas Sequences and Pseudoprimes" submitted by Zhaiyu Mo in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Supervisor, Dr. J.P. Jones
Department of Mathematics and Statistics

Dr. R.A. Mollin
Department of Mathematics and Statistics

Dr. P. Zvengrowski
Department of Mathematics and Statistics

Dr. R.E. Woodrow
Department of Mathematics and Statistics

Dr. Lisa Higham
Department of Computer Science

External Examiner Dr. H.C. Williams
The University of Manitoba

Date Jan 6, 1994

Abstract

In this dissertation, we study properties of Lucas sequences; specifically, properties of the sequences $X_a(n)$ and $Y_a(n)$, which are the sequences of solutions of the Pell equation $x^2 - (a^2 - 4)y^2 = 4$. Using these properties, we give definitions of some new types of Lucas pseudoprime, and hence new methods for studying primes. First we define several types of pseudoprime. Second we prove that if an integer n is one of these kinds of pseudoprime, for sufficiently many bases a, then n must be prime. Also we construct formulas for the number of incongruent bases a mod n such that n is a pseudoprime to the base a for various types of Lucas pseudoprime. In this dissertation, we also study related questions about ordinary pseudoprimes. We construct formulas for the number of incongruent bases a mod n such that n is a strong pseudoprime to the base a and the number of incongruent bases a mod n such that n is an ordinary Euler pseudoprime to the base a. Finally, returning to Lucas pseudoprimes, we show that for any odd composite integer n, the number of incongruent bases mod n to which n is an Euler Lucas pseudoprime is always less than $(n-2)/2$, less than $(n-2)/3$ if n is not a Lucas Carmichael number, and less than $(n-2)/4$ in some other cases.

Acknowledgements

The author wishes to thank his supervisor Professor James P. Jones for valuable direction and supervision in the preparation of this dissertation.. The author also wishes to acknowledge a valuable contribution from Professor Hugh C. Williams. A key idea of Professor Williams in 1987 led the author and his supervisor to theorems in Section 7. The author also wishes to thank Professor Richard A. Mollin for valuable discussions.

CONTENTS

Symbols and Abbreviations

$Y_a(n)$	the n^{th} y solution of $x^2-(a^2-4)y^2=4$
$X_a(n)$	the n^{th} x solution of $x^2-(a^2-4)y^2=4$
$\phi(n)$	Euler's ϕ function
$\epsilon_a(n)$	Jacobi symbol $((a^2-4)/n)$ $(=(\frac{a^2-4}{n}))$
$\tau_a(n)$	Jacobi symbol $((a+2)/n)$ $(=(\frac{a+2}{n}))$
$\rho_a(n)$	Jacobi symbol $((a-2)/n)$ $(=(\frac{a-2}{n}))$
$n \mid m$	n divides m
$n^e \Vert m$	m is divisible by n^e and m is not divisible by n^{e+1}
$n \nmid m$	n does not divide m
(n,m)	the greatest common divisor of n and m
$[n,m]$	the least common multiple of n and m
$n=\square$	n is a perfect square
$n\neq\square$	n is not a square
$\lfloor s \rfloor$	the largest integer less than or equal to s, the floor of s
$\lceil s \rceil$	the least integer greater than or equal to s, the ceiling of s
$rem(n,m)$	the remainder after n is divided by m
$Re(\alpha)$	the real part of a complex number α
$Im(\alpha)$	the imaginary part of a complex number α
iff	if and only if
CRT	the Chinese Remainder Theorem

Symbols and Abbreviations

$lpsp(a)$	Lucas pseudoprime to the base a	(see *p.*75)
$elpsp(a)$	Euler Lucas pseudoprime to the base a	(see *p.*75)
$slpsp(a)$	strong Lucas pseudoprime to the base a	(see *p.*75)
$slxpsp(a)$	extra strong Lucas pseudoprime to the base a	(see *p.*75)
$apsp(a)$	a-pseudoprime to the base a	(see *p.*80)
$tpsp(a)$	t-pseudoprime to the base a	(see *p.*80)
$rpsp(a)$	r-pseudoprime to the base a	(see *p.*80)
$ltpsp(a)$	Lucas t-pseudoprime to the base a	(see *p.*81)
$rapsp(a)$	r-pseudoprime and a-pseudoprime to the base a	(see *p.*81)
$sltpsp(a)$	strong Lucas t-pseudoprime to the base a	(see *p.*82)
$psp(a)$	pseudoprime to the base a	(see *p.*144)
$epsp(a)$	Euler pseudoprime to the base a	(see *p.*144)
$spsp(a)$	strong pseudoprime to the base a	(see *p.*145)
$r_a(n)$	the rank of n in the $Y_a(i)$ sequence	(see *p.*61)
$O_a(n)$	the order of a mod n	(see *p.*144)
$T_a(n)$	totient function of a mod n	(see *p.*64)

Introduction

In this dissertation, we study the properties of the sequence of solutions of the Pell equation

(i) $$x^2 - (a^2 - 4)y^2 = 4,$$

which includes the sequence of solutions of the Pell equation

(ii) $$x^2 - (a^2 - 1)y^2 = 1$$

as a special case. The sequences of solutions of the Pell equations (i) and (ii) are examples of Lucas sequences. Lucas sequences played an important role in the solution of Hilbert's tenth problem by Matijasevič in 1970. In his original proof, Matijasevič used a Lucas sequence, the sequence of Fibonacci numbers, to show that exponentiation is Diophantine definable. This solved Hilbert's tenth problem in the negative, based on previous work of M. Davis, Julia Robinson and H. Putnam. Now many modern, simplified proofs have been given. In these modern proofs the original Fibonacci sequence has been replaced by the sequence of solutions of the Pell equation (i) or (ii).

The sequence of solutions of (i) contains the sequence of solutions of (ii) as a subsequence when a is even. Hence the former sequence is more general. Following the notation of Y. Matijasevič and J. Robinson [33] [20] [21], throughout this dissertation, we denote the n^{th} x solution and the n^{th} y solution of (i) by $X_a(n)$ and $Y_a(n)$, respectively.

The sequences $X_a(n)$ and $Y_a(n)$ are equal to the Lucas functions $V_n(P,Q)$ and $U_n(P,Q)$ when $P = a$ and $Q = 1$. In general $U_n(P,Q)$ and $V_n(P,Q)$ are defined by

$$U_n(P,Q) = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad V_n(P,Q) = \alpha^n + \beta^n$$

where α and β are the roots of the polynomial $x^2 - Px + Q$ and P, Q are arbitrary but fixed coprime integers. However $Q = 1$ is not very restrictive since it is known that ([52])

$$Q^n V_n(P',1) \equiv V_{2n}(P,Q) \pmod{n}$$

$$PQ^{n-1}U_n(P',1) \equiv U_{2n}(P,Q) \pmod{n}$$

whenever $(Q,n)=1$ and $QP' = P^2 - 2Q \pmod{n}$.

We will show in §1 that $X_a(n) = V_n(a,1)$ and $Y_a(n) = U_n(a,1)$. Hence the theory of $X_a(n)$ and $Y_a(n)$ becomes a part of classical Lucas - Lehmer theory. Throughout the dissertation we are studying Lucas - Lehmer theory. However we have our own point of view, coming from logic, and we emphasize different things which are useful to us, for example, things useful in Diophantine representation. We also hope some of these things may be relevant to the possible eventual attainment of a polynomial time algorithm for primality testing.

We obtain the following new main results:

(1) We define some new types of pseudoprimes related to the sequences $X_a(n)$ and $Y_a(n)$; namely, t-pseudoprime (*tpsp*), r-pseudoprime (*rpsp*) and a-pseudoprime (*apsp*), which are consequences of Theorems 7.11 and 7.13 - 7.14, also *slxpsp*(a), an exceptionally strong kind of strong Lucas pseudoprime. We also combine these new types of pseudoprimes with certain classical ones, such as Lucas pseudoprime, Euler - Lucas pseudoprime and strong Lucas pseudoprime in order to get some stronger types of pseudoprime. For example we introduce the Lucas t-pseudoprime and strong Lucas t-pseudoprime. From Theorem 7.17 we obtain several relationships among the aforementioned new types of pseudoprime.

(2) In §11 we prove a large number of results to the effect that for an odd integer n, the primality of n is equivalent to n being a type of pseudoprime to all possible bases. See Theorems 11.22, 11.24, 11.25, 11.26, 11.27, 11.28, 11.29 and 11.31. Theorems 11.25, 11.26 are consequences of already known results on general Lucas sequences $U_n(P,Q)$ (see [51]). However the others are new, particularly those about *tpsp*'s, *rpsp*'s and *apsp*'s.

(3) In §12 and §13 we derive three formulas which count the number of incongruent bases a mod n such that n is a Lucas pseudoprime to the base a, an Euler - Lucas pseudoprime to the base a, or a strong Lucas pseudoprime to the base a (see Theorems 12.8, 12.7 12.9).

(4) In §14 we give upper bounds for $EL(n)$, the number of incongruent bases a mod n such that n is an Euler - Lucas pseudoprime to the base a. First we show that for all odd composite integers n, $EL(n) < \frac{n-2}{2}$. Then we show that in other cases we can get $EL(n) < \frac{n-2}{3}$ and $EL(n) < \frac{n-2}{4}$ for certain types of composite n. These results have some applications to primality testing, especially to probabilistic primality testing (see Theorems 14.24, 14.25, 14.26, 14.27, 14.28, 14.29).

In §1 we begin with background knowledge of general Lucas sequences, $U_n(P,Q)$, $V_n(P,Q)$. This is helpful to put the subject of the sequence of solutions of the Pell equation into perspective. Based on the discussion in §1, §2 and §3, we derive some general properties of Lucas sequences, specifically the sequences $X_a(n)$, $Y_a(n)$, their derivatives, inequalities, identities and divisibility properties. These three sections play the role of a toolbox for the later discussion. The Lucas sequence primality tests using $X_a(n)$ and $Y_a(n)$, which we shall give, can all be carried out in polynomial time, at each fixed base a. Proof of this is reviewed in §5. In §6 we give proofs

of some classical Lucas sequence results. Most results in §1 - §6 are known. Our new results mostly occur in sections 7 through 14. In §7 we define some new types of Lucas pseudoprimes and also give some examples which show that *sltpsp*(a) and *slxpsp*(a) are very strong Lucas primality tests. In §8 we show that Lucas - Lehmer's test for Mersenne primes and Fermat primes can be deduced from our *ltpsp* test. In §9 we derive many interesting results about prime powers. Some of these we need in later sections and some of these are nice on their own. In §10 we define the concept of Lucas primitive root for our sequences $X_a(n)$ and $Y_a(n)$, and show that all integers have Lucas primitive roots. Also we prove some useful results about quadratic residues and ranks. In §11 we define different kinds of Lucas - Carmichael numbers. These are Lucas analogs of ordinary Carmichael numbers. For each kind of Lucas - Carmichael defined in terms of factorization properties, we give equivalent Lucas sequence conditions. These results show that some methods of Lucas primality testing are not strong enough for primality, even if such tests are passed for all bases, e.g. the test $X_a(n) \equiv a \pmod{n}$. An example showing this is $n = 7,056,721 = 7{\cdot}47{\cdot}89{\cdot}241$ (see Theorem 11.14). However, many of the tests we mention in §7 are sufficient for primality if one of them is passed for all bases, and some are enough on fewer bases. Section 11 makes all of this clear.

In §12 and §13 we derive some formulas which count the number of incongruent bases for some kinds of ordinary pseudoprimes and Lucas pseudoprimes. These results are used in §14 to show for example that if n is composite, then there are no more than $(n-2)/2$ incongruent bases to which n is an Euler - Lucas pseudoprime. In the conclusion section, we state some open problems and conjectures.

§1. Background

In this section, we discuss the properties of general Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$. The properties discussed in this section are the basis for our later discussion about the sequence of solutions to the Pell equation

$$x^2 - (a^2-4)y^2 = 4. \tag{1.1}$$

Obviously the family of Pell equations (1.1) includes the Pell equation

$$x^2 - (a^2-1)y^2 = 1, \tag{1.2}$$

as a special case; for if we multiply by 4 we have $(2x)^2 - ((2a)^2-4)y^2 = 4$.

When a is odd in (1.1) we obtain a new family of Pell equations which are not of the form (1.2). Equation (1.1) has infinitely many solutions, just as (1.2) does. (We give a proof of this below.)

Following the notation of Y. Matijasevič and J. Robinson, the sequence of solutions of (1.1) will be denoted by $x = X_a(n)$ and $y = Y_a(n)$. These sequences are the main interest of this thesis.

When we use the Pell equation (1.1), this subject is part of the Lucas-Lehmer theory developed by E. Lucas [32] and D.H. Lehmer [26] [27]. As described by Lucas [32] it is the theory of two sequences

$$V_n = \alpha^n + \beta^n, \qquad U_n = \tfrac{\alpha^n - \beta^n}{\alpha - \beta}, \tag{1.3}$$

where α and β are the roots of the equation

$$x^2 - Px + Q = 0. \tag{1.4}$$

Here P and Q are any two nonzero integers. $D = P^2 - 4Q$ is the discriminant of (1.4). D is assumed to be nonzero, hence we always have $\alpha \neq \beta, \alpha \neq 0$ and $\beta \neq 0$. We can suppose $|\beta| \leq |\alpha|$. We have also

(1.5) $\qquad P = \alpha + \beta, \quad Q = \alpha \cdot \beta, \quad D = (\alpha - \beta)^2, \quad D = P^2 - 4Q.$

If $D > 0$, then α and β are real, in addition to $\alpha \neq \beta, \alpha \neq 0$ and $\beta \neq 0$. Also since $\alpha + \beta = P \neq 0$, we have $\alpha \neq -\beta$. Thus $\alpha \neq \pm\beta$. Hence $|\alpha| \neq |\beta|$ so we can suppose $|\beta| < |\alpha|$. We also have $\alpha/\beta \neq \pm 1$. Since α and β are real, this implies that α/β is not an n^{th} root of unity when $D > 0$. If $D \leq 0$, then $|\alpha| = |\beta|$. Hence

(1.6) $$|\alpha| = |\beta| \Leftrightarrow D \leq 0.$$

Thus when $0 < D$, α/β is not an n^{th} root of unity for any n. When $D \leq 0$, it is possible for α/β to be an n^{th} root of unity. In this case the sequences V_n and U_n become periodically zero (degenerate). This happens if $P^2 = Q, P^2 = 2Q, P^2 = 3Q$ or $P^2 = 4Q$. In these cases α/β is a $3^{rd}, 4^{th}, 6^{th}$ or 1^{st} root of unity, respectively. These are the only degenerate cases (Bundschuh and Shiue [4].) We give a proof of this.

Theorem 1.7. Let α and β be the roots of $x^2 - Px + Q$ where P and Q are nonzero integers. Then α/β is an n^{th} root of unity if and only if $P^2 = Q, P^2 = 2Q, P^2 = 3Q$ or $P^2 = 4Q$.

The proof of Theroem 1.7 will follow from several lemmas.

Lemma 1.7.1. For any positive integer n there exist integers $c_0, c_1, \cdots, c_{n-1}$ such that $2cos(n\theta)$ can be expressed as a monic polynomial in $2cos(\theta)$, with integer coefficients,

(1.7.1) $$2cos(n\theta) = (2cos(\theta))^n + c_{n-1}(2cos(\theta))^{n-1} + \cdots + c_1(2cos(\theta)) + c_0.$$

Proof. From $cos(\alpha + \beta) + cos(\alpha - \beta) = 2cos(\alpha)cos(\beta)$ with $\alpha = n\theta$ and $\beta = \theta$ we have $\qquad 2cos((n+1)\theta) = 2cos(n\theta) \cdot cos(\theta) - 2cos((n-1)\theta).$

By induction this identity implies (1.7.1). For example for $n = 2$ and $n = 3$,

$$2cos(2\theta) = 4cos^2(\theta) - 2, \qquad 2cos(3\theta) = 8cos^3(\theta) - 6cos(\theta).$$

This completes the proof of Lemma 1.7.1.

Lemma 1.7.2. If ω is a complex n^{th} root of unity, $\omega^n = 1$ and $Re(\omega)$ is a rational number, then $2Re(\omega)$ is an integer.

Proof. Suppose $\omega^n = 1$. Then $|\omega| = 1$. Hence $\omega = cos(\theta) + i \cdot sin(\theta)$ so that $Re(\omega) = cos(\theta)$ and $2Re(\omega) = 2cos(\theta)$. From $\omega^n = cos(n\theta) + i \cdot sin(n\theta)$ and $\omega^n = 1$ we have $cos(n\theta) = 1$. Hence $2cos(n\theta) = 2$, an integer. Therefore the result follows from the Lemma 1.7.1.

Lemma 1.7.3. Suppose s is rational, r is real, some root ω of $x^2 - sx + r = 0$ is also a complex n^{th} root of unity $\omega^n = 1$ and $s^2 - 4r \leq 0$. Then s is an integer.

Proof. Suppose $\omega^2 - s\omega + r = 0$. Multiply by 4 and complete the square to obtain $0 = 4\omega^2 - 4s\omega + 4r = (2\omega - s)^2 + 4r - s^2 \Rightarrow (2\omega - s)^2 = s^2 - 4r \Rightarrow s = 2Re(\omega)$. Hence the conclusion of Lemma 1.7.3 follows from Lemma 1.7.2.

Proof of Theorem 1.7. Let $D = P^2 - 4Q$. If $D > 0$, then, as mentioned, α/β cannot be an n^{th} root of 1. Consider the case $D \leq 0$. In this case $P^2 \leq 4Q$ so that $0 < Q$. Let $t = P^2/Q$ and $s = t - 2$. Then s and t are rational and since $D \leq 0$, $0 < t \leq 4$ and hence $-2 < s \leq 2$. $Q = \alpha\beta$ and $Q \neq 0$ imply $\alpha \neq 0$ and $\beta \neq 0$. Since $Q = \alpha\beta$ and $P = \alpha + \beta$, we have

$$s = \frac{\alpha}{\beta} + \frac{\beta}{\alpha}.$$

Hence α/β is a root of the polynomial $x^2 - sx + 1$. Consequently $\alpha/\beta = \omega$ where

$$\omega = \frac{s \pm i\sqrt{4 - s^2}}{2}.$$

Here $i = \sqrt{-1}$. Since $0 < t \leq 4$, if t is an integer, there are only 4 cases. When $t = 1, s = -1$ and α/β is a 3^{rd} root of unity. When $t = 2, s = 0$ and α/β is a 4^{th}

root of unity. When $t = 3, s = 1$ and α/β is a 6^{th} root of unity. When $t = 4, s = 2$ and α/β is a 1^{st} root of unity. By Lemma 1.7.3 with $r = 1$, s is an integer. Hence the conclusion of the theorem follows.

Later we will suppose $0 < D$ in addition to $P \neq 0$ and $Q \neq 0$. In this case, as we observed above, α and β are real, α/β is not an n^{th} root of unity and by (1.6) we have $|\beta| \neq |\alpha|$. Hence we can suppose $|\beta| < |\alpha|$. It is easy to see that

(1.8.) $\quad 0 < \beta \Leftrightarrow 0 < PQ. \qquad$ Also $\qquad 0 < \beta < \alpha \Leftrightarrow 0 < P$ and $0 < Q.$

We also have $1 < |\alpha/\beta|$ since $|\alpha/\beta| = |\alpha|/|\beta|$ (and $|\beta| \neq 0$ since $Q \neq 0$). Also $|\beta| < |\alpha|$ if and only if $\beta^2 < \alpha^2$. So it follows from (1.4) and (1.5) that

(1.8.1) $\qquad \beta < \alpha \quad \Leftrightarrow \quad 0 < P \quad \Leftrightarrow \quad \alpha = \frac{P+\sqrt{D}}{2}$ and $\beta = \frac{P-\sqrt{D}}{2}.$

Using (1.8.1) it is easy to see that

(1.8.2) $\qquad 0 < \beta < 1 \quad \Leftrightarrow \quad 0 < Q(P - Q - 1).$

In this thesis we will usually suppose $0 < P$. Hence the right side of (1.8.1) will hold.

Normally one may also suppose that $D \neq \square$ (D is not a perfect square). Then $\beta = \overline{\alpha}$, so that β is the conjugate of α. Hence α and β are two irrational reals and $\alpha \neq \pm\beta$. One usually also assumes $(P, Q) = 1$, but it won't be necessary here because we will later put $Q = 1$.

From the hypotheses $0 < D$, $Q \neq 0$ and $1 \leq P$, we can easily see that $1 < \alpha$ and

(1.8.3) $\qquad -1 < \beta \Leftrightarrow 0 < P + Q + 1.$

Also since $\sqrt{D} < P$ if and only if $0 < Q$, by (1.5) and (1.8.2) we have

(1.8.4) $\qquad 0 < \beta \quad \Leftrightarrow \quad 0 < Q \qquad$ and $\qquad \beta < 1 \quad \Leftrightarrow \quad Q + 1 < P.$

Consequently

(1.8.5) $\qquad 0 < \beta < 1 < \alpha \quad \Leftrightarrow \quad 0 < Q$ and $Q + 1 < P.$

In fact $|\beta| < 1$ if and only if $|Q+1| < P$. Also when $1 \leq P$ we have

(1.8.6) $-1 < \beta < 0 < 1 < \alpha \Leftrightarrow 0 < P+Q+1 < P+1$ and $1 < \beta < \alpha \Leftrightarrow P < Q+1$.

By (1.8.1) we have from $0 \leq D$ that $P \leq 2\alpha$. By (1.5) we have $\alpha\beta = Q$. It follows that $|\beta| = |\alpha\beta|/|\alpha| = |Q|/\alpha \leq 2|Q|/P$. Therefore $\beta \to 0$ as $P \to +\infty$. Consequently

$$\lim_{P \to +\infty} \frac{P - \sqrt{P^2 - 4Q}}{2} = 0. \tag{1.8.7}$$

From the assumptions $0 < D, Q \neq 0$ and $1 \leq P$, it follows that $1 \leq V_n$ and $0 \leq U_n$, as well as $0 < U_n$ for $0 < n$. Shortly we will put $Q = 1$ and suppose $2 < P$. Then we will have $2 \leq V_n$ and $n \leq U_n$. Also it will follow that $0 < \beta < 1 < \alpha$, by (1.8.5).

For any P and Q, if $\alpha \neq \beta$, the sequences U_n and V_n satisfy the Lucas identity:

$$V_n^2 - D \cdot U_n^2 = 4Q^n. \tag{1.9}$$

To prove (1.9) we shall use (1.3), (1.5), $D = (\alpha - \beta)^2$ and $\alpha\beta = Q$. We have by (1.5)

$$\begin{aligned} V_n^2 - D \cdot U_n^2 &= (\alpha^n + \beta^n)^2 - (\alpha - \beta)^2 \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 \\ &= (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2 = 4\alpha^n\beta^n = 4Q^n. \end{aligned}$$

The functions U_n and V_n satisfying the Lucas identity (1.9) can also be defined as *Lucas sequences*, that is as sequences satisfying a second order linear recurrence:

(1.10) (i) $\quad V_0 = 2, \quad V_1 = P, \quad V_{n+2} = P \cdot V_{n+1} - Q \cdot V_n,$

(ii) $\quad U_0 = 0, \quad U_1 = 1, \quad U_{n+2} = P \cdot U_{n+1} - Q \cdot U_n.$

Proof. Using (1.3) and $P = \alpha + \beta$, $Q = \alpha\beta$, we have

$$P \cdot V_{n+1} - Q \cdot V_n = (\alpha + \beta)(\alpha^{n+1} + \beta^{n+1}) - \alpha\beta(\alpha^n + \beta^n) = (\alpha^{n+2} + \beta^{n+2}) = V_{n+2}.$$

$$P \cdot U_{n+1} - Q \cdot U_n = (\alpha + \beta)\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) - \alpha\beta\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) = \left(\frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta}\right) = U_{n+2}.$$

In a similar way one can derive the *Addition Laws*, (also due to Lucas [32]),

(1.11) $$2V_{n+m} = V_n \cdot V_m + D \cdot U_n \cdot U_m,$$

(1.12) $$2Q^m V_{n-m} = V_n \cdot V_m - D \cdot U_n \cdot U_m,$$

(1.13) $$2U_{n+m} = U_n \cdot V_m + V_n \cdot U_m,$$

(1.14) $$2Q^m U_{n-m} = U_n \cdot V_m - V_n \cdot U_m.$$

As special cases of the Addition Laws, $(m = 1)$ we have

(1.11′) $$2V_{n+1} = P \cdot V_n + D \cdot U_n,$$

(1.12′) $$2Q \cdot V_{n-1} = P \cdot V_n - D \cdot U_n,$$

(1.13′) $$2U_{n+1} = P \cdot U_n + V_n,$$

(1.14′) $$2Q \cdot U_{n-1} = P \cdot U_n - V_n.$$

From (1.11) and (1.13) we can obtain the *Double Angle Formulas* (Lucas [32]).

(1.15) (i) $U_{2n} = U_n \cdot V_n$ (ii) $V_{2n} = V_n^2 - 2Q^n = D \cdot U_n^2 + 2Q^n.$

If we replace n by $n+1$ and m by n in (1.12), then we obtain the identity

$$V_{n+1} \cdot V_n - D \cdot U_{n+1} \cdot U_n = 2P \cdot Q^n.$$

From this identity we may derive

(1.16) $$U_n^2 - U_{n+1} \cdot U_{n-1} = Q^{n-1}.$$

Proof of (1.16). Using (1.12′), (1.13′) and also replacing D by $P^2 - 4$ in (1.9) we have

$$4QU_n^2 - 4Q^n = P^2U_n^2 - V_n^2 = (PU_n + V_n)(PU_n - V_n) = 2U_{n+1} \cdot 2QU_{n-1} = 4QU_{n+1} \cdot U_{n-1}.$$

Dividing both sides by $4Q$ and transposing terms we obtain (1.16).

Replacing n by $n+1$ in (1.16) and U_{n+2} by $P \cdot U_{n+1} - Q \cdot U_n$ in (1.10) (ii) we obtain

(1.17) $$U_{n+1}^2 - P \cdot U_{n+1} \cdot U_n + Q \cdot U_n^2 = Q^n.$$

From (1.14″), (1.12″) and (1.15) we have the identities

(1.18) $$P \cdot U_n^2 - 2Q \cdot U_n \cdot U_{n-1} = U_{2n},$$

(1.19) $$P \cdot V_n^2 - 2Q \cdot V_n \cdot V_{n-1} = DU_{2n}.$$

By induction using (1.10) (*ii*), (1.14′) and (1.15) with n replaced by $n+1$ one can obtain (1.20) and from it, by (1.9), obtain (1.21).

(1.20) $$U_{n+1}^2 - Q \cdot U_n^2 = U_{2n+1},$$

(1.21) $$V_{n+1}^2 - Q \cdot V_n^2 = D \cdot U_{2n+1}.$$

By adding and substracting Addition Equations (1.11) - (1.14) one obtains the Lucas *Product Formulas*

(1.22) $$V_{n+m} + Q^m \cdot V_{n-m} = V_n \cdot V_m,$$

(1.23) $$U_{n+m} + Q^m \cdot U_{n-m} = U_n \cdot V_m,$$

(1.24) $$V_{n+m} - Q^m \cdot V_{n-m} = D \cdot U_n \cdot U_m,$$

(1.25) $$U_{n+m} - Q^m \cdot U_{n-m} = V_n \cdot U_m.$$

Now let $i = n+m, j = n-m$ so that $n = (i+j)/2$ and $m = (i-j)/2$. Then from (1.22) - (1.25) we obtain the Lucas *Half Angle Formulas*,

(1.26.1) $$V_i + Q^{\frac{i-j}{2}} V_j = V_{(i+j)/2} \cdot V_{(i-j)/2},$$

(1.26.2) $$V_i - Q^{\frac{i-j}{2}} V_j = D \cdot U_{(i+j)/2} \cdot U_{(i-j)/2},$$

(1.26.3) $$U_i + Q^{\frac{i-j}{2}} U_j = U_{(i+j)/2} \cdot V_{(i-j)/2},$$

(1.26.4) $$U_i - Q^{\frac{i-j}{2}} U_j = V_{(i+j)/2} \cdot U_{(i-j)/2}.$$

As a special case, if we put $i = n, j = 1$ and use $V_1 = P, U_1 = 1$, then we obtain

(1.27.1) $$V_n + Q^{\frac{n-1}{2}} P = V_{(n+1)/2} \cdot V_{(n-1)/2},$$

(1.27.2) $$V_n - Q^{\frac{n-1}{2}} P = D \cdot U_{(n+1)/2} \cdot U_{(n-1)/2},$$

(1.27.3) $$U_n + Q^{\frac{n-1}{2}} = U_{(n+1)/2} \cdot V_{(n-1)/2},$$

(1.27.4) $$U_n - Q^{\frac{n-1}{2}} = V_{(n+1)/2} \cdot U_{(n-1)/2}.$$

Identities (1.11′) - (1.14′) can be combined into the following. Suppose $\epsilon = \pm 1$,

(1.28) (i) $$2Q^{\frac{1+\epsilon}{2}}V_{n-\epsilon} = PV_n - \epsilon DU_n,$$

(ii) $$2Q^{\frac{1+\epsilon}{2}}U_{n-\epsilon} = -\epsilon V_n + PU_n,$$

(iii) $$2Q^{\frac{1-\epsilon}{2}}V_{n+\epsilon} = PV_n + \epsilon DU_n,$$

(iv) $$2Q^{\frac{1-\epsilon}{2}}U_{n+\epsilon} = \epsilon V_n + PU_n.$$

Assuming $0 < D$, by induction on n, using (1.10) (i) (ii) and Addition Laws (1.11′) (1.13′), one obtains

(1.29) $$\left(\frac{V_1 + \sqrt{D}U_1}{2}\right)^n = \frac{V_n + \sqrt{D}U_n}{2}.$$

Proof. $n = 0$. $\left(\frac{V_1+\sqrt{D}U_1}{2}\right)^0 = 1 = \frac{2+\sqrt{D}\cdot 0}{2} = \frac{V_0+\sqrt{D}U_0}{2}$.

Assume (1.29) holds for n. For $n+1$, using (1.10) (i),(ii), (1.11′) and (1.13′)

$$\left(\frac{V_1 + \sqrt{D}U_1}{2}\right)^{n+1} = \left(\frac{V_1 + \sqrt{D}U_1}{2}\right)\left(\frac{V_1 + \sqrt{D}U_1}{2}\right)^n = \left(\frac{V_1 + \sqrt{D}U_1}{2}\right)\left(\frac{V_n + \sqrt{D}U_n}{2}\right)$$

$$= \frac{V_1V_n + \sqrt{D}V_1U_n + \sqrt{D}U_1V_n + DU_1U_n}{4} = \frac{PV_n + \sqrt{D}PU_n + \sqrt{D}V_n + DU_n}{4}$$

$$= \frac{PV_n + DU_n + \sqrt{D}(PU_n + V_n)}{4} = \frac{2V_{n+1} + \sqrt{D}\cdot 2U_{n+1}}{4} = \frac{V_{n+1} + \sqrt{D}\cdot U_{n+1}}{2}.$$

We give next a proof by induction that, at least in the cases $Q + 1 < P$ and $Q = \pm 1$, all solutions of the Lucas identity (1.9) are given by the Lucas sequences (1.10) (i) and (ii). For this we will use the following lemma.

Lemma 1.30. Suppose $D = P^2 - 4Q$, $Q+1 < P$ and $Q = \pm 1$. Suppose $V^2 - DU^2 = 4Q^i$ for some i, $0 \leq V$ and $1 < U$. If $Q = +1$, then $V \leq PU, (P-2)U < V$ and $DU \leq PV$. If $Q = -1$, then $PU \leq V < (P+2)U$ and $PV \leq DU$.

Proof. Suppose $V^2 - DU^2 = 4Q^i$, $0 \leq V$ and $1 < U$. Since $1 < U$ we have $|V^2/U^2 - D| = 4|Q|^i/U^2 = 4/U^2 \leq 1$ which implies $|V/U - \sqrt{D}| < 1/\sqrt{D}$. Hence

$$\sqrt{D} - \frac{1}{2\sqrt{D}} \leq \frac{V}{U} \leq \sqrt{D} + \frac{1}{2\sqrt{D}}. \tag{1.30'}$$

If $Q = +1$, then $P - 2 < D/P$ so the inequalities $V \leq PU, (P-2)U < V$ and $DU \leq PV$ are equivalent to $D/P \leq V/U \leq P$ which follows from (1.30') since it is easy to see that

$$Q = +1 \text{ and } 2 < P \quad \Rightarrow \quad \frac{D}{P} < \sqrt{D} - \frac{1}{2\sqrt{D}} \text{ and } \sqrt{D} + \frac{1}{2\sqrt{D}} < P.$$

If $Q = -1$, then when $P = 1$ or $P = 2$, we have $P+2 < D/P$ so that the inequalities $PU \leq V \leq (P+2)U$ and $PV \leq DU$ are implied by the inequality $P \leq V/U \leq P+2$ which follow from (1.30') since $P \leq \sqrt{D} - 1/(2\sqrt{D})$ and $\sqrt{D} + 1/(2\sqrt{D}) < P + 2$. If $Q = -1$ and $2 < P$, then $D/P < P + 2$ so that the $PU \leq V < (P+2)U$ and $PV \leq DU$ are implied by $P \leq V/U \leq D/P$ which follows from (1.30') and the observation that

$$Q = -1 \text{ and } 2 < P \quad \Rightarrow \quad P < \sqrt{D} - \tfrac{1}{2\sqrt{D}} \text{ and } \sqrt{D} + \tfrac{1}{2\sqrt{D}} < \tfrac{D}{P}.$$

Theorem 1.31 Suppose $D = P^2 - 4Q$, $Q + 1 < P$ and $Q = \pm 1$. Suppose further that $0 \leq V$, $0 \leq U$. Then $V^2 - DU^2 = 4Q^i$ for some i if and only if it is possible to find a nonnegative integer n such that $V = V_n$, $U = U_n$, also when $Q = -1$, we have $n \equiv i \pmod 2$.

Proof. Sufficiency follows from (1.9).

To show the existence of n, we will use induction on U (Fermat's method of descent). First suppose $U = 0$ and $0 \leq V$. Then

$$V^2 - DU^2 = 4Q^i \;\Rightarrow\; V^2 = 4Q^i \;\Rightarrow\; |V|^2 = 4 \;\Rightarrow\; V = 2$$

so that we may take $n = 0$. If $U = 1$ and $0 \leq V$, then when i is even and $Q = -1$

$$V^2 - DU^2 = 4Q^i \implies V^2 - P^2 + 4Q = 4Q^i \implies V^2 - P^2 = 0 \text{ or } V^2 - P^2 = 8.$$

If $V^2 - P^2 = 0$, then $V = P$ and we may take $n = 1$. If $V^2 - P^2 = 8$, then $P = 1$ and $V = 1$ or $V = 3$. Hence we may take $n = 0$ or $n = 2$.

Suppose $1 < U, 0 \leq V, V^2 - DU^2 = 4Q^i$ and the statement holds for all pairs (V', U') such that $0 \leq U' < U$ and $0 \leq V'$. Put $V' = (PV - DU)/(2Q)$ and put $U' = (-V + PU)/(2Q)$. From $V^2 - DU^2 = 4Q^i, Q = \pm 1$ and $D \equiv P \pmod 2$, we can see that U' and V' are integers. Also $0 \leq U' < U$ and $0 \leq V'$ by Lemma 1.30. Further

$$\begin{aligned} V'^2 - DU'^2 &= (PV - DU)^2/(4Q^2) - D(PU - V)^2/(4Q^2) \\ &= (P^2V^2 - DP^2U^2 + DV^2 - D^2U^2)/(4Q^2) = (P^2 - D)(V^2 - DU^2)/(4Q^2) \\ &= (P^2 - D)4Q^i/(4Q^2) = 4Q4Q^i/(4Q^2) = 4Q^{i-1}. \end{aligned}$$

Thus $V'^2 - DU'^2 = 4Q^{i-1}$. By the induction hypothesis there exists a nonnegative integer n such that $V' = V_{n-1}$ and $U' = U_{n-1}$. From $P^2 - D = 4Q$ one obtains $V = (P \cdot V' + D \cdot U')/2$ and $U = (V' + P \cdot U')/2$. Hence $V = (P \cdot V_{n-1} + D \cdot U_{n-1})/2 = (V_1 V_{n-1} + DU_1 U_{n-1})/2 = V_n$ by Addition Law 1.11. Also $U = (V_{n-1} + P \cdot U_{n-1})/2 = (U_1 V_{n-1} + V_1 U_{n-1})/2 = U_n$ by Addition Law 1.13. Therefore the result holds for U.

The equation corresponding to identity (1.17),

$$y^2 - Pxy + Qx^2 = Q^n \tag{1.32}$$

has a property similar to the Lucas equation (1.9). If $|Q| = 1$, then all solutions to (1.32) are given by $x = U_n, y = U_{n+1}$ where U_n and U_{n+1} are defined by (1.10) (*ii*).

Theorem 1.33 Suppose $Q = \pm 1$. Then $0 \leq x$, $0 \leq y$ and $y^2 - Pxy + Qx^2 = Q^i$ for some i if and only if it is possible to find a nonnegative integer n such that $x = U_n, y = U_{n+1}$ and $n \equiv i \pmod 2$ if $Q = -1$.

Proof. ($\Leftarrow$). By identity (1.17). ($\Longrightarrow$). Suppose $y^2 - Pxy + Qx^2 = Q^i$ for some i, x and y satisfying $0 \leq x$ and $0 \leq y$. Put $V = 2y - Px$. Then $y = (Px+V)/2$. Substitute this y into $y^2 - Pxy + Qx^2 = Q^i$ to obtain $(Px+V)^2/4 - P(Px+V)x/2 + Qx^2 = Q^i$. This equation is equivalent to $(Px + V)^2 - 2P(Px + V)x + 4Qx^2 = 4Q^i$ which simplifies to $V^2 - P^2x^2 + 4Qx^2 = 4Q^i$ which then becomes $V^2 - (P^2 - 4Q)x^2 = 4Q^i$. By Theorem 1.31 there exists n such that $V = V_n$ and $x = U_n$. Hence from identity (1.13′) we have $2y = Px + V = PU_n + V_n = 2U_{n+1}$ which implies $y = U_{n+1}$. Hence $x = U_n$ and $y = U_{n+1}$.

The solutions of the Pell equation $x^2 - (a^2 - 1)y^2 = 1$ do not satisfy the Lucas equation (1.9). However the solutions of the Pell equation $x^2 - (a^2 - 4)y^2 = 4$ satisfy (1.9) and when a is even contain the solutions for $x^2 - (a^2 - 1)y^2 = 1$ as a subsequence. Hence we put $P = a$ and $Q = 1$.

From (1.5) with $a = P, d = D$ and $Q = 1$, we have $\beta = \alpha^{-1}$ and $\alpha - \beta = \sqrt{d} = \sqrt{a^2 - 4}$. Then the Lucas equation (1.9) becomes the Pell equation (1.1):

$$V_n^2 - (a^2 - 4)U_n^2 = 4. \tag{1.34}$$

Hence the sequence of the solutions to the Pell equation (1.1), denoted by $X_a(n)$ and $Y_a(n)$, are $Y_a(n) = U_n$ and $X_a(n) = V_n$. That is

$$X_a(n)^2 - (a^2 - 4)Y_a(n)^2 = 4. \tag{1.35}$$

Also $$x^2 - (a^2 - 4)y^2 = 4 \Leftrightarrow \exists n[x = X_a(n) \text{ and } y = Y_a(n)].$$

From (1.29), we have

$$\frac{X_a(n) + Y_a(n)\sqrt{a^2 - 4}}{2} = \left(\frac{a + \sqrt{a^2 - 4}}{2}\right)^n. \tag{1.36}$$

(1.36) shows that the algebraic integer $\alpha = (a+\sqrt{d})/2$, called the *generator*, generates

all solutions for (1.35). Its conjugate, $\beta = \overline{\alpha}$ is its inverse, $\beta = \alpha^{-1}$. Thus

$$\frac{a-\sqrt{a^2-4}}{2} = \left(\frac{a+\sqrt{a^2-4}}{2}\right)^{-1}. \tag{1.37}$$

Taking the conjugate of the both sides of (1.36) we get

$$\frac{X_a(n)-Y_a(n)\sqrt{a^2-4}}{2} = \left(\frac{a-\sqrt{a^2-4}}{2}\right)^{n}. \tag{1.38}$$

This shows that $X_a(n)$ and $Y_a(n)$ can be defined also by $\beta = \overline{\alpha} = \alpha^{-1} = a-\sqrt{a^2-4}$, i.e. by the conjugate of the generator. Next we prove

$$\frac{X_a(nm)+Y_a(nm)\sqrt{a^2-4}}{2} = \left(\frac{X_a(n)+Y_a(n)\sqrt{a^2-4}}{2}\right)^{m}. \tag{1.39}$$

Proof. Replace n by nm in (1.36) to get

$$\frac{X_a(nm)+Y_a(nm)\sqrt{d}}{2} = \left(\frac{a+\sqrt{d}}{2}\right)^{nm} = \left(\left(\frac{a+\sqrt{d}}{2}\right)^{n}\right)^{m} = \left(\frac{X_a(n)+Y_a(n)\sqrt{d}}{2}\right)^{m}.$$

Adding and subtracting equations (1.36) and (1.38) we obtain

$$X_a(n) = \alpha^n + \overline{\alpha}^n = \left(\frac{a+\sqrt{a^2-4}}{2}\right)^{n} + \left(\frac{a-\sqrt{a^2-4}}{2}\right)^{n}, \tag{1.40}$$

$$Y_a(n) = \frac{1}{\sqrt{d}}(\alpha^n - \overline{\alpha}^n) = \frac{1}{\sqrt{a^2-4}}\left[\left(\frac{a+\sqrt{a^2-4}}{2}\right)^{n} - \left(\frac{a-\sqrt{a^2-4}}{2}\right)^{n}\right]. \tag{1.41}$$

The equations may also be written in the form

$$X_a(n) = \alpha^n + \alpha^{-n} = \alpha^n\left(1+\alpha^{-2n}\right) = \alpha^n\left(1+\frac{1}{\alpha^{2n}}\right), \tag{1.42}$$

$$Y_a(n) = \frac{1}{\sqrt{d}}\left(\alpha^n - \alpha^{-n}\right) = \frac{\alpha^n}{\sqrt{d}}\left(1-\alpha^{-2n}\right) = \frac{\alpha^n}{\sqrt{d}}\left(1-\frac{1}{\alpha^{2n}}\right). \tag{1.43}$$

Hence we have also

$$X_a(n) = \left(\frac{a+\sqrt{d}}{2}\right)^{n}\left(1+\frac{1}{(\frac{a+\sqrt{d}}{2})^{n}}\right), \tag{1.44}$$

$$(1.45) \qquad Y_a(n) = \frac{1}{\sqrt{d}}\left(\frac{a+\sqrt{d}}{2}\right)^n \left(1 - \frac{1}{(\frac{a+\sqrt{d}}{2})^n}\right),$$

The functions $X_a(n)$ and $Y_a(n)$ can also be defined for negative values of n. This is useful in identities involvings $\pm$ signs. Lucas [32] gave the following as definitions

$$(1.46) \qquad X_a(-n) = X_a(n), \qquad Y_a(-n) = -Y_a(n).$$

Proof. Using (1.42) and (1.43) we have

$$X_a(-n) = \alpha^{-n} + \alpha^n = \alpha^n + \alpha^{-n} = X_a(n).$$

$$Y_a(-n) = \frac{1}{\sqrt{d}}\left(\alpha^{-n} - \alpha^{-(-n)}\right) = \frac{1}{\sqrt{d}}\left(\alpha^{-n} - \alpha^n\right) = -\frac{1}{\sqrt{d}}\left(\alpha^n - \alpha^{-n}\right) = -Y_a(n).$$

The functions $X_a(n)$ and $Y_a(n)$ may also be defined in a natural way for negative values of a. The following relations will be used in the later sections.

$$(1.47) \qquad X_{-a}(n) = (-1)^n X_a(n), \qquad Y_{-a}(n) = -(-1)^n Y_a(n).$$

Proof. Replacing a by $-a$ in (1.40) and (1.41) we have

$$\begin{aligned} X_{-a}(n) &= \left(\frac{-a+\sqrt{d}}{2}\right)^n + \left(\frac{-a-\sqrt{d}}{2}\right)^n \\ &= (-1)^n\left(\frac{a-\sqrt{d}}{2}\right)^n + (-1)^n\left(\frac{a+\sqrt{d}}{2}\right)^n = (-1)^n X_a(n), \end{aligned}$$

$$\begin{aligned} Y_{-a}(n) &= \frac{1}{\sqrt{d}}\left(\left(\frac{-a+\sqrt{d}}{2}\right)^n - \left(\frac{-a-\sqrt{d}}{2}\right)^n\right) \\ &= \frac{(-1)^n}{\sqrt{d}}\left(\left(\frac{a-\sqrt{d}}{2}\right)^n - \left(\frac{a+\sqrt{d}}{2}\right)^n\right) = (-1)^n(-Y_a(n)). \end{aligned}$$

Here $\sqrt{d} = \sqrt{a^2-4}$ remains unchanged when a is replaced by $-a$. Thus (1.47) is proved.

Our main interest in this thesis is the sequence of the solutions for the Pell equation (1.1). Hence we usually let $Q = 1$. The above is only included to explain

how our theory of the Pell equation (1.1) fits into the classical Lucas - Lehmer theory of Lucas [32] and Lehmer [26].

The following Jacobi symbols will play a special role,

$$\epsilon = \left(\frac{d}{n}\right) = \left(\frac{a^2-4}{n}\right), \qquad \rho = \left(\frac{a-2}{n}\right), \qquad \tau = \left(\frac{a+2}{n}\right). \tag{1.46}$$

When it is necessary to specify what a is or what n is, we use ϵ_a, ρ_a, τ_a or $\epsilon_a(n)$ $\rho_a(n)$, and $\tau_a(n)$ to denote these Jacobi symbols.

§2. Derivatives and inequalities

In this section, we derive formulas for the derivatives and some inequalities for Lucas sequences. These derivatives will actually be used and together with the identities which we derive in the next section play important roles in the later sections. For the derivatives, we shall begin with the general sequences, V_n and U_n. We shall consider derivatives with respect to P. V_n and U_n are polynomials in P and Q. So if Q is held constant, then, for fixed n, V_n and U_n are polynomials in P. Consequently they have derivatives with respect to P. Let $V_n' = dV_n/dP$ and $U_n' = dU_n/dP$ denote these derivatives. We will show

Theorem 2.1. (i) $V_n' = n \cdot U_n$ and (ii) $DU_n' = nV_n - PU_n$.

Proof. (i) and (ii) hold for $n = 0$. Assume they hold for n. We shall use (1.10′), (1.12′) and $D' = 2P$.

$$\begin{aligned} 2V_{n+1}' &= \frac{d}{dP}(2V_{n+1}) = \frac{d}{dP}(PV_n + DU_n) = V_n + PV_n' + 2PU_n + DU_n' \\ &= V_n + P(nU_n) + 2PU_n + nV_n - PU_n \quad \text{(by the induction hypothesis)} \\ &= V_n + P(nU_n) + PU_n + nV_n = (n+1)(PU_n + V_n) \\ &= (n+1)2U_{n+1} = 2(n+1)U_{n+1}. \quad \text{(by (1.12′))} \end{aligned}$$

Thus $V_{n+1}' = (n+1)U_{n+1}$. Hence (i) holds for $n+1$. Similarly

$$\begin{aligned} 2DU_{n+1}' &= D\frac{d}{dP}(2U_{n+1}) = D\frac{d}{dP}(PU_n + V_n) \quad \text{(by (1.12′))} \\ &= D(U_n + PU_n' + V_n') = DU_n + PDU_n' + DV_n' \\ &= DU_n + P(nV_n - PU_n) + nDU_n \quad \text{(by induction hypothesis and (i))} \\ &= DU_n + nPV_n - P^2U_n + nDU_n \end{aligned}$$

$$= (n+1)PV_n + (n+1)DU_n - P^2U_n - PV_n$$

$$= (n+1)(PV_n + DU_n) - P(PU_n + V_n)$$

$$= (n+1)2V_{n+1} - P\cdot 2U_{n+1}. \quad \text{(by (1.10') and (1.12') again)}$$

This shows that $DU'_{n+1} = (n+1)V_{n+1} - PU_{n+1}$.

Thus (i) and (ii) are proven.

If we put $P = a$, $Q = 1$ and write $D = d$, then we have

Corollary 2.2. $X'_a(n) = nY_a(n)$ and $dY'_a(n) = nX_a(n) - aY_a(n)$.

Corollary 2.3. $(Y'_a(n), Y_a(n)) \mid 2(n, Y_a(n))$.

Proof. Let $k = (Y'_a(n), Y_a(n))$. Then $k \mid Y'_a(n)$ and $k \mid Y_a(n)$. By 2.2, $k \mid nX_a(n)$. Hence $k \mid (nX_a(n), Y_a(n))$. Since $X_a(n)^2 - dY_a(n)^2 = 4$, $(X_a(n), Y_a(n)) \mid 2$. Therefore $k \mid 2(n, Y_a(n))$.

Next we mention some inequalities for the sequences X_a and Y_a.

Suppose $2 < a$, $d = a^2 - 4$, and $\alpha = (a + \sqrt{d})/2$. Then $a < 2\alpha < 2a$. Since $\overline{\alpha} = \alpha^{-1}$, we have $0 < 1/a < \overline{\alpha} < 2/a < 1$ and also $1 < a - 1 < \sqrt{d} < \alpha < a < 2\sqrt{d}$. Further,

$$0 < 1/\sqrt{d} < \sqrt{2/d} < 2/a < a - \sqrt{d} < 2/\sqrt{d} < 2/(a-1) \leq 3/a \leq 1. \tag{2.4}$$

Next we will use $x^2 = dy^2 + 4$ and $d = a^2 - 4$ to prove that for $a > 2$, $n \geq 1$,

$$dY_a(n)^2 < \alpha^{2n} - 1. \tag{2.5}$$

From (1.43) we have $\sqrt{d}Y_a(n) = \alpha^n(1 - \alpha^{-2n})$. If we square both sides of this equation and use the inequality $(1-x)^2 < 1 - x$ (which holds for $0 < x < 1$, then we get $dY_a(n)^2 = \alpha^{2n}(1 - \alpha^{-2n})^2 < \alpha^{2n}(1 - \alpha^{-2n}) = \alpha^{2n} - 1$. Hence (2.5) holds for $2 < a$ and $1 \leq n$.

From $x^2 = dy^2 + 4$ and $d = a^2 - 4$ one can show that for $a > 2$ and $n > 0$

$$\frac{X_a(n)}{a} < Y_a(n) < \frac{X_a(n)}{\sqrt{d}} < \frac{X_a(n)}{a-1} \leq \frac{X_a(n)}{2}. \tag{2.6}$$

From (2.5) we also have $dY_a(n)^2 < 2\alpha^{2n}$ and hence $\sqrt{d}Y_a(n) < \alpha^n$. It is not difficult to see that for $2 < a$, $3 \leq n$:

$$\frac{1}{a}(a-1)^{n-1} < \frac{1}{a}\left(\frac{a+\sqrt{d}}{2}\right)^n < \frac{X_a(n)}{a} < Y_a(n) < \frac{1}{\sqrt{d}}\left(\frac{a+\sqrt{d}}{2}\right)^n < a^{n-1}. \tag{2.7}$$

Here we need the assumption $3 \leq n$ only for the rightmost inequality. For most of the others it is sufficient to suppose only $2 < a$ and $1 \leq n$. For example for $\sqrt{d} \cdot Y_a(n)^2 < \alpha^n$ this is enough. For the leftmost inequality we can suppose $2 \leq n$. This inequality is easy to prove for $n = 2$. The rightmost inequality, for which we need to assume $n = 3$, can be proved by using $a^3 + \sqrt{d}^3 \leq 2a^2\sqrt{d}$ to show that $\alpha^3 < a^2\sqrt{d}$ holds for $2 < a$. For n greater than these values the rightmost (and leftmost) inequalities can be proved by induction using $a - 1 < \alpha < a$.

Lemma 2.8. For $2 < a$ and $1 \leq n$,

(i) $(a-1)^{n+1} < X_a(n+1) < a^{n+1}$, (ii) $(a-1)^n < Y_a(n+1) < a^n$,

(iii) $n < a \Rightarrow a^n < X_a(n+1) \leq a^{n+1}$, (iv) $n < a \Rightarrow a^{n-1} < Y_a(n+1) \leq a^n$,

Most of these inequalities follow from (2.6). The left side of the first inequality (i) $(a-1)^{n+1} < X_a(n+1)$, is slightly stronger than what would follow directly from (2.6). It is most easily derived by induction using the Lucas Equations for $X_a(n)$ and $Y_a(n)$ (see (1.8) and (1.9) or (3.10) and (3.11) below). In the proofs of inequalities (iii) and (iv), which hold when $n < a$, we use the elementary inequality $0 \leq x \leq 1 \Rightarrow 1 - nx \leq (1-x)^n$. Put $x = 1/a$. Since $1 + n \leq a$, we have $a^{n-1} = a^n/a \leq a^n(1 - n/a) \leq a^n(1 - 1/a)^n = (a-1)^n$.

Lemma 2.9. For all n, we have the following inequalities

(i) If $2 < a$, then $2Y_a(n-1) < \alpha Y_a(n-1) < Y_a(n)$,

(ii) If $2 < a$, then $Y_a(n)+Y_a(n-1) < 2Y_a(n) < \sqrt{d}Y_a(n) < X_a(n)$,

(iii) If $3 < a$, then $2Y_a(n-1) + 2Y_a(n) < X_a(n)$,

(iv) If $2 < a$, then $X_a(n-2) + 2X_a(n-1) < X_a(n)$,

(v) For $2 \leq a$, $a \leq b \Rightarrow X_a(n) \leq X_b(n)$, $Y_a(n) \leq Y_b(n)$,

(vi) For $2 \leq a$, $2 \leq X_a(n)$ and $n \leq Y_a(n)$.

Proof. $2 < a \Rightarrow 2 < \alpha \Rightarrow 2Y_a(n-1) < \alpha Y_a(n-1) < Y_a(n)$. This last inequality, $\alpha Y_a(n-1) < Y_a(n)$, follows from (1.43) since $1 < \alpha$. For the proof of the second inequality, (ii), we use (2.6). We have $\sqrt{d}Y_a(n) < X_a(n)$ and $2 < a$ implies that $2 < \sqrt{5} \leq \sqrt{a^2-4} = \sqrt{d}$. Inequality (iii) follows from (i), (2.5) and the implication $3 < a \Rightarrow 3 < \sqrt{d}$. Thus $X_a(n) > \sqrt{d}Y_a(n) > 3Y_a(n) = Y_a(n)+2Y_a(n) > 2Y_a(n-1)+Y_a(n)$. Hence $2Y_a(n-1) + 2Y_a(n) < X_a(n)$. To prove (iv) from (2.7), it is enough to show $(a + a\alpha)/\sqrt{d} \leq \alpha^2$. Using $a - 1 < \sqrt{d} < \alpha < a$, one sees that when $3 < a$, this inequality follows from $a(a+1) < a^3$. For $Y_a(n)$ inequality (v) follows from (1.45) since α and $\alpha/\sqrt{d}$ are increasing functions of a for $a \geq 2$. For $X_a(n)$ inequality (v) can be deduced from inequality (v) for $Y_a(n)$ and (1.35). If $a \leq b$, then $X_a(n)^2 = (a^2-4)Y_a(n)^2+4 \leq (b^2-4)Y_b(n)^2+4 = X_b(n)^2$. Finally, inequality (vi) follows from inequality (v) by taking $b = a$ and $a = 2$ in (v).

§3. Identities

We list some of the identities which hold for the sequences X_a and Y_a. Most of these identities were known to Lucas and Lehmer. Many will be directly used in later discussion. Some are not used directly. However we list them for possible use in the future.

These identities have an algebraic interpretation as equations which hold for polynomials in $Z[a]$. See (3.10.1) and (3.11.1) below and (4.13.1) - (4.13.3) in the next section.

In these identities many $\pm$ signs occur. In this connection recall that $X_a(n)$ and $Y_a(n)$ are defined for negative values of n by (1.46) $X_a(-n) = X_a(n)$ and $Y_a(-n) = -Y_a(n)$.

From (1.36) and $4\alpha^{n+m} = 2\alpha^n \cdot 2\alpha^m$ and $4\alpha^{n-m} = 2\alpha^n \cdot 2\alpha^{-m}$ we have

$$2X_a(n \pm m) + 2Y_a(n \pm m)\sqrt{d} = (X_a(n) + Y_a(n)\sqrt{d})(X_a(m) \pm Y_a(m)\sqrt{d}). \tag{3.1}$$

Taking rational and irrational parts of (3.1), we get the *Addition Equations.*

$$2X_a(n \pm m) = X_a(n)X_a(m) \pm dY_a(n)Y_a(m), \tag{3.2}$$

$$2Y_a(n \pm m) = Y_a(n)X_a(m) \pm X_a(n)Y_a(m). \tag{3.3}$$

Here the $\pm$ signs correspond. Putting $m = n$ in these equations, taking the signs to be $+$ and using (1.1) we obtain the Lucas [32] *Double Angle Formulas.*

$$X_a(2n) = X_a(n)^2 - 2 = dY_a(n)^2 + 2, \tag{3.4}$$

$$Y_a(2n) = X_a(n)Y_a(n). \tag{3.5}$$

The following identities were also known to Lucas [32]. We will call them *Periodicity Equations.*

(3.6) $$X_a(m \pm 2n) = X_a(n)X_a(m \pm n) - X_a(m),$$

(3.7) $$Y_a(m \pm 2n) = X_a(n)Y_a(m \pm n) - Y_a(m).$$

Proof. Multiply the left side by 2, then expand by (3.2), (3.3), (3,4) and (3.5),

$$\begin{aligned}
2X(m \pm 2n) &= X(m)X(2n) \pm dY(m)Y(2n) \\
&= X(m)(X(n)^2 - 2) \pm dY(m)X(n)Y(n) \\
&= X(n)X(m)X(n) \pm dX(n)Y(m)Y(n) - 2X(m) \\
&= X(n)[X(m)X(n) \pm dY(m)Y(n)] - 2X(m) \\
&= X(n)2X(m \pm n) - 2X(m) \\
&= 2[X(n)X(m \pm n) - X(m)]. \qquad \text{(3.6) is proved.} \\
2Y(m \pm 2n) &= Y(m)X(2n) \pm X(m)Y(2n) \\
&= Y(m)(X(n)^2 - 2) \pm X(m)X(n)Y(n) \\
&= X(n)Y(m)X(n) \pm X(n)X(m)Y(n) - 2Y(m) \\
&= X(n)[Y(m)X(n) \pm X(m)Y(n)] - 2Y(m) \\
&= X(n)2Y(m \pm n) - 2Y(m) \\
&= 2[X(n)Y(m \pm n) - Y(m)]. \qquad \text{(3.7) is proved.}
\end{aligned}$$

Note that since (3.1) - (3.5) hold algebraically as statements about polynomials in a, (3.6) and (3.7) must also hold as statements about polynomials.

Putting $m=1$ in the Addition Equations and using $X_a(1)=a$ and $Y_a(1)=1$ we get

(3.8) $$2X_a(n+1) = aX_a(n) + dY_a(n), \quad 2Y_a(n+1) = aY_a(n) + X_a(n),$$

(3.9) $$2X_a(n-1) = aX_a(n) - dY_a(n), \quad 2Y_a(n-1) = aY_a(n) - X_a(n).$$

Formulas (3.8) and (3.9) tell us how to obtain $Y_a(n-1)$ from $Y_a(n)$ and $X_a(n-1)$ from $X_a(n)$, without knowing n. This is because we can get $X_a(n)$ from $Y_a(n)$ (and

$Y_a(n)$ from $X_a(n)$) by (1.35). Thus (3.8) and (3.9) prove that the Y_a and X_a sequences are each polynomial time retraceable (see §5).

From (3.8), (3.9) and $d = a^2 - 4$ we have

(3.8.1) $\quad 2X_a(n) = aX_a(n+1) - dY_a(n+1), \qquad 2Y_a(n) = -X_a(n+1) + aY_a(n+1),$

(3.9.1) $\quad 2X_a(n) = aX_a(n-1) + dY_a(n-1), \qquad 2Y_a(n) = X_a(n-1) - aY_a(n-1).$

Adding corresponding pairs of equations (3.8) and (3.9) and replacing n by $n+1$ we obtain the *Lucas second order recurrence equations*:

(3.10) $(i) \quad X_a(0) = 2, \qquad X_a(1) = a, \qquad X_a(n+2) = aX_a(n+1) - X_a(n).$

$(ii) \quad Y_a(0) = 0, \qquad Y_a(1) = 1, \qquad Y_a(n+2) = aY_a(n+1) - Y_a(n).$

The Lucas equations can be used to prove the following, for fixed n,

$X_a(n)$ *is a polynomial in* a *of degree* n.

$Y_a(n)$ *is a polynomial in* a *of degree* $n-1$.

The sequnces X_a and Y_a are not yet defined for $a = 0, 1$, or 2. When $a = 0$, the defining equation (1.1) is $x^2 + 4y^2 = 4$. When $a = 1$ (1.1) is $x^2 + 3y^2 = 4$. When $a = 2$ (1.1) is $x^2 = 4$. We shall define functions X_0, X_1, X_2, Y_0, Y_1 and Y_2 giving solutions to these equations simply by following the Lucas equations. That is we define

(3.11) $\quad X_0(n) = 0 \quad$ (n odd), $\qquad Y_0(n) = (-1)^{\frac{n-1}{2}} \quad$ (n odd),

$\qquad X_0(n) = 2(-1)^{\frac{n}{2}} \quad$ (n even), $\qquad Y_0(n) = 0 \quad$ (n even),

(3.12) $\qquad X_1(3i) = 2(-1)^i, \qquad Y_1(3i) = 0$

$\qquad X_1(3i \pm 1) = (-1)^i, \qquad Y_1(3i \pm 1) = \pm(-1)^i,$

(3.13) $\qquad X_2(n) = 2, \qquad Y_2(n) = n.$

Observe that these functions are periodic. X_0 is $2, 0, -2, 0 \pmod 4$, Y_0 is $0, 1, 0, -1 \pmod 4$, X_1 is $2, 1, -1, -2, -1, 1 \pmod 6$ and Y_0 is $0, 1, 1, 0, -1, -1 \pmod 6$.

X_0, Y_0 and Y_1 are degenerate Lucas sequences since they are periodically 0. However the Lucas Equations (3.10) and (3.11) hold for them, as well as for X_1, X_2 and Y_2. In fact all the identities (3.2) - (3.9) hold for these functions since the Lucas equations can be used to derive the Addition Equations. Defining equation (1.1) also holds. Throughout this thesis we therefore allow $a = 0, a = 1$ and $a = 2$.

By means of (1.46) and (1.47) we can also extend the definitions of the functions X_0, X_1, X_2, Y_0, Y_1 and Y_2 so that they are defined on negative n and for negative values of a. Below we consider $a = -1$ and $a = -2$. We shall also need the following simple properties of the X_1 and Y_1 functions.

Lemma 3.14 If $(n, 6) = 1$, then $X_1(n) = 1$ and $Y_1(n) = \left(\frac{-3}{n}\right) \equiv n \pmod 6$.

If $3 \mid n$, then $X_1(n) = 2(-1)^{n/3}$ and $Y_1(n) = 0$.

Proof. From Definition 3.12, X_1 and Y_1 can be seen to be periodic with period 6. If $(n, 6) = 1$, then $n = 6j \pm 1$ so that $X_1(6j \pm 1) = 1$ and $Y_1(6j \pm 1) = \pm 1$. From the theory of quadratic residues it is known that if $(n, 6) = 1$, then $(-3/n) \equiv n \pmod 6$. In other words, if $n = 6j \pm 1$, then $(-3/n) = \pm 1$. Consequently $(-3/n) = Y_1(n)$.

Adding and subtracting pairs of Addition Equations (3.2) (3.3) we get the Lucas [32] *Product Formulas*:

$$X_a(n+m) + X_a(n-m) = X_a(n) \cdot X_a(m), \tag{3.15}$$

$$X_a(n+m) - X_a(n-m) = dY_a(n) \cdot Y_a(m), \tag{3.16}$$

$$Y_a(n+m) + Y_a(n-m) = Y_a(n) \cdot X_a(m), \tag{3.17}$$

$$Y_a(n+m) - Y_a(n-m) = X_a(n) \cdot Y_a(m). \tag{3.18}$$

Letting $i = n + m$ and $j = n - m$ so that $n = (i + j)/2$ and $m = (i - j)/2$, the product formulas give us the *Half Angle Formulas*:

$$X_a(i) + X_a(j) = X_a\left(\frac{i+j}{2}\right) \cdot X_a\left(\frac{i-j}{2}\right), \tag{3.19}$$

$$X_a(i) - X_a(j) = dY_a\left(\frac{i+j}{2}\right) \cdot Y_a\left(\frac{i-j}{2}\right), \tag{3.20}$$

$$Y_a(i) + Y_a(j) = Y_a\left(\frac{i+j}{2}\right) \cdot X_a\left(\frac{i-j}{2}\right), \tag{3.21}$$

$$Y_a(i) - Y_a(j) = X_a\left(\frac{i+j}{2}\right) \cdot Y_a\left(\frac{i-j}{2}\right). \tag{3.22}$$

Putting $i = n$, $j = 1$, using $X_a(1) = a$ and $Y_a(1) = 1$, we have the special cases,

$$X_a(n) + a = X_a\left(\frac{n+1}{2}\right) \cdot X_a\left(\frac{n-1}{2}\right), \tag{3.19$'$}$$

$$X_a(n) - a = dY_a\left(\frac{n+1}{2}\right) \cdot Y_a\left(\frac{n-1}{2}\right), \tag{3.20$'$}$$

$$Y_a(n) + 1 = Y_a\left(\frac{n+1}{2}\right) \cdot X_a\left(\frac{n-1}{2}\right), \tag{3.21$'$}$$

$$Y_a(n) - 1 = X_a\left(\frac{n+1}{2}\right) \cdot Y_a\left(\frac{n-1}{2}\right). \tag{3.22$'$}$$

Replacing i by $2i$ and j by $2j$, equations (3.19) - (3.22) can be rewritten in the form

$$X_a(2i) + X_a(2j) = X_a(i+j) \cdot X_a(i-j), \tag{3.23}$$

$$X_a(2i) - X_a(2j) = dY_a(i+j) \cdot Y_a(i-j), \tag{3.24}$$

$$Y_a(2i) + Y_a(2j) = Y_a(i+j) \cdot X_a(i-j), \tag{3.25}$$

$$Y_a(2i) - Y_a(2j) = X_a(i+j) \cdot Y_a(i-j). \tag{3.26}$$

Letting $i = n$ and $j = 1$ in (3.23) - (3.26) and using (3.4) and (3.5), we get the identities

$$X_a(n)^2 + d = X_a(n+1) \cdot X_a(n-1), \tag{3.27}$$

$$Y_a(n)^2 - 1 = Y_a(n+1) \cdot Y_a(n-1), \tag{3.28}$$

$$Y_a(2n) + a = Y_a(n+1) \cdot X_a(n-1), \tag{3.29}$$

(3.30) $$Y_a(2n) - a = X_a(n+1) \cdot Y_a(n-1).$$

Identities (3.27) and (3.28) were known to Lucas [32]. As a corollary we obtain

(3.28′) $$Y_a(n+1) \cdot Y_a(n-1) = (Y_a(n)+1) \cdot (Y_a(n)-1).$$

Multiplying (3.19′) and (3.20′) together and using (3.5) and (3.28') we obtain

(3.29′) $$(X_a(n)+a) \cdot (X_a(n)-a) = d(Y_a(n)+1) \cdot (Y_a(n)-1).$$

If we replace n by $n+1$ and m by n in Addition Equations (3.2) - (3.3) and take the sign $-$, then the result is

(3.31) $$X_a(n+1) \cdot X_a(n) - dY_a(n+1) \cdot Y_a(n) = 2a,$$

(3.32) $$Y_a(n+1) \cdot X_a(n) - X_a(n+1) \cdot Y_a(n) = 2.$$

Using (3.8) (3.9) and (1.35) one may verify the following identities.

(3.33) $$X_a(n+1)^2 - a \cdot X_a(n+1) \cdot X_a(n) + X_a(n)^2 = -d,$$

(3.34) $$Y_a(n+1)^2 - a \cdot Y_a(n+1) \cdot Y_a(n) + Y_a(n)^2 = 1.$$

Applying (3.31) and (3.32) to (3.33) and (3.34) we get

(3.35) $$X_a(n+1)^2 + X_a(n)^2 - adY_a(n+1) \cdot Y_a(n) = a^2+4,$$

(3.36) $$dY_a(n+1)^2 + dY_a(n)^2 - aX_a(n+1) \cdot X_a(n) = -d-8.$$

Using (3.8) and (1.35) it is easy to show that

(3.37) $$X_a(n+1)^2 - dX_a(n) \cdot Y_a(n+1) - X_a(n)^2 = -d,$$

(3.38) $$Y_a(n+1)^2 - X_a(n) \cdot Y_a(n+1) - Y_a(n)^2 = -1.$$

Applying (3.32) to these we have

(3.39) $$X_a(n+1)^2 - dX_a(n+1) \cdot Y_a(n) - X_a(n)^2 = d,$$

(3.40) $$Y_a(n+1)^2 - X_a(n+1) \cdot Y_a(n) - Y_a(n)^2 = 1.$$

Taking $m = 1$ in (3.6) and (3.7) and using (1.46) it is easy to show that

(3.41) $$X_a(2n \pm 1) = X_a(n) \cdot X_a(n \pm 1) - a,$$

(3.42) $$Y_a(2n \pm 1) = X_a(n) \cdot Y_a(n \pm 1) + 1.$$

Here the signs $\pm$ correspond. Applying (3.42) to (3.37) and (3.38) or directly from (1.20) and (1.21) we obtain the following identities of Lucas [32] which can also be found in Smorynski [48].

(3.43) $$dY_a(2n+1) = X_a(n+1)^2 - X_a(n)^2,$$

(3.44) $$Y_a(2n+1) = Y_a(n+1)^2 - Y_a(n)^2.$$

As a corollary

(3.43′) $$dY_a(n) = X_a\left(\frac{n+1}{2}\right)^2 - X_a\left(\frac{n-1}{2}\right)^2,$$

(3.44′) $$Y_a(n) = Y_a\left(\frac{n+1}{2}\right)^2 - Y_a\left(\frac{n-1}{2}\right)^2.$$

Applying (3.41) to (3.33) and (3.36) we get

(3.45) $$aX_a(2n+1) = X_a(n+1)^2 + X_a(n)^2 + 2a^2 - 4,$$

(3.46) $$aX_a(2n+1) = dY_a(n+1)^2 + dY_a(n)^2 + 2a^2 + 4.$$

Replacing n by $(n-1)/2$ in (3.45) and (3.46) gives

(3.45′) $$aX_a(n) = X_a\left(\frac{n+1}{2}\right)^2 + X_a\left(\frac{n-1}{2}\right)^2 + 2a^2 - 4,$$

(3.46′) $$aX_a(n) = dY_a\left(\frac{n+1}{2}\right)^2 + dY_a\left(\frac{n-1}{2}\right)^2 + 2a^2 + 4.$$

By applying (3.8) and (1.35) to (3.45) and (3.44), we get

(3.47) $$2X_a(2n+1) = aX_a(n)^2 - 2a + dX_a(n)Y_a(n),$$

(3.48) $$2Y_a(2n+1) = dY_a(n)^2 + 2 + aX_a(n)Y_a(n),$$

(3.48.1) $$2Y_a(i \pm j) = X_a(j)(Y_a(i) \pm Y_a(j)) \pm Y_a(j)(X_a(i) - X_a(j)).$$

Identities (3.43) and (3.44) are the case $m = 1$ of more general identities of Lucas [32].

(3.49) $$X_a(n+m)^2 - X_a(n)^2 = dY_a(2n+m) \cdot Y_a(m),$$

(3.50) $$Y_a(n+m)^2 - Y_a(n)^2 = Y_a(2n+m)\cdot Y_a(m).$$

Replacing n by j and m by $i-j$ in (3.49) and (3.50) we obtain

(3.49.1) $$X_a(i)^2 - X_a(j)^2 = dY_a(i+j)\cdot Y_a(i-j),$$

(3.50.1) $$Y_a(i)^2 - Y_a(j)^2 = Y_a(i+j)\cdot Y_a(i-j).$$

Putting $i = nm$ and $j = m$ in (3.23) and (3.26) and using (3.4), (3.5) we obtain four identities, the first two of which, (3.51) and (3.52) were known to Lucas [32].

(3.51) $$X_a(nm)^2 + dY_a(m)^2 = X_a(nm+m)\cdot X_a(nm-m),$$

(3.52) $$Y_a(nm)^2 - Y_a(m)^2 = Y_a(nm+m)\cdot Y_a(nm-m),$$

(3.53) $$Y_a(2nm) - Y_a(2m) = X_a(nm+m)\cdot Y_a(nm-m),$$

(3.54) $$Y_a(2nm) + Y_a(2m) = Y_a(nm+m)\cdot X_a(nm-m).$$

Corresponding to identity (3.34) we have the Diophantine equation $x^2-axy+y^2=1$. Like the Lucas equation $x^2-dy^2=4$ this equation completely defines the Y_a sequence. For $x \geq 0$ and $y \geq 0$ we have $x^2 - axy + y^2 = 1$ if and only if $(\exists n)[y = Y_a(n)$ and $x = Y_a(n+1)]$. (See Theorem 1.33 for the proof of this.)

We prove next

(3.55) If $1 \leq k$ odd, $$Y_a(kn) - kY_a(n) = dY_a(n)\sum_{i=0}^{\frac{k-1}{2}} Y_a(ni)^2.$$

Proof. The identity will be proved by induction on k. First multiply both sides of the identity by 2. It holds for $k = 1$, because then both sides equal 0. Assume the identity holds for k. We will show that it holds for $k+2$.

As k increases from k to $k+2$, twice the left side (3.55) increases by the amount:

$$\begin{aligned} & 2[Y((k+2)n) - (k+2)Y(n)] - 2[Y(kn) - kY(n)] \\ = \; & 2Y(kn+2n) - 2Y(kn) - 4Y(n) \\ = \; & Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 4Y(n) \qquad \text{(by (3.3))} \end{aligned}$$

$$
\begin{aligned}
&= X(kn)Y(n)X(n) + [X(2n)-2]Y(kn) - 4Y(n) && \text{(by (3.5))}\\
&= Y(n)X(kn)X(n) + dY(n)^2Y(nk) - 4Y(n) && \text{(by (3.4))}\\
&= Y(n)[X(nk)X(n) + dY(nk)Y(n)] - 4Y(n)\\
&= Y(n)\cdot 2X(nk+n) - 4Y(n) && \text{(by (3.2))}\\
&= 2Y(n)[X(nk+n)-2]\\
&= 2Y(n)\left[dY\left((nk+n)/2\right)^2\right] && \text{(by (3.4))}\\
&= 2dY(n)Y\left((nk+n)/2\right)^2
\end{aligned}
$$

This is also the increase in twice the right side of (3.55) as k changes to $k+2$.

(3.56) If $2 \le k$ even, $\quad Y_a(kn) - \frac{k}{2}Y_a(2n) = dY_a(n)\sum_{i=0}^{\frac{k-2}{2}} Y_a(ni)Y_a(ni+n).$

Proof. The identity will be proved as before by induction on k. First multiply both sides of the identity by 2. It holds for $k=2$ because then both sides equal 0. Assume the identity holds for k. We will show that it holds for $k+2$.

As k increases from k to $k+2$, twice the left side (3.56) increases by the amount:

$$
\begin{aligned}
&2[Y((k+2)n) - \frac{k+2}{2}Y(2n)] - 2[Y(kn) - \frac{k}{2}Y(2n)]\\
&= 2Y(kn+2n) - 2Y(kn) - 2Y(2n)\\
&= Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 2Y(2n) && \text{(by (3.3))}\\
&= Y(2n)[X(kn)-2] + Y(kn)[X(2n)-2]\\
&= Y(n)X(kn)[X(kn)-2] + Y(nk)dY(n)^2 && \text{(by (3.4))}\\
&= Y(n)X(n)dY(k/2\cdot n)^2 + dY(k/2\cdot n)X(k/2\cdot n)Y(n)^2 && \text{(by (3.5))}\\
&= dY(n)Y(k/2\cdot n)[Y(k/2\cdot n)X(n) + X(k/2\cdot n)Y(n)]\\
&= dY(n)Y(k/2\cdot n)[2Y(k/2\cdot n+n)] && \text{(by (3.3))}
\end{aligned}
$$

$$= \; 2dY(n)Y(k/2\cdot n)Y(k/2\cdot n+n)$$

This is also the increase in twice the right side of (3.56) as k changes to $k+2$.

From the Product Formulas (3.16) and (3.18) we have

$$dY_a(n)Y_a(2in) \;=\; X_a((2i+1)n) \;-\; X_a((2i-1)n), \tag{3.57}$$

$$Y_a(n)X_a(2in) \;=\; Y_a((2i+1)n) \;-\; Y_a((2i-1)n). \tag{3.58}$$

When we sum (3.57) and (3.58) for $i = 1, 2, \ldots, m$, they telescope giving

$$dY_a(n)\sum_{i=1}^{m} Y_a(2in) \;=\; X_a(2mn+n) \;-\; X_a(n), \tag{3.59}$$

$$Y_a(n)\sum_{i=1}^{m} X_a(2in) \;=\; Y_a(2mn+n) \;-\; Y_a(n). \tag{3.60}$$

Applying (3.20) and (3.22) to (3.57) and (3.58) we have

$$dY_a(n)\sum_{i=1}^{m} Y_a(2in) \;=\; dY_a(mn+n)\cdot Y_a(mn), \tag{3.61}$$

$$Y_a(n)\sum_{i=1}^{m} X_a(2in) \;=\; X_a(mn+n)\cdot Y_a(mn). \tag{3.62}$$

The next group of identities which hold for $\epsilon = \pm 1$ we call the ϵ *identities*, where ϵ can be ± 1. The first set (3.68) - (3.71) can be proved from (3.8) and (3.9) by considering the cases $\epsilon = \pm 1$. The other identites can be derived in a similar way.

$$2X_a(n+\epsilon) \;=\; aX_a(n) \;+\; \epsilon dY_a(n), \tag{3.68}$$

$$2Y_a(n+\epsilon) \;=\; \epsilon X_a(n) \;+\; aY_a(n), \tag{3.69}$$

$$2X_a(n-\epsilon) \;=\; aX_a(n) \;-\; \epsilon dY_a(n), \tag{3.70}$$

$$2Y_a(n-\epsilon) \;=\; -\epsilon X_a(n) \;+\; aY_a(n), \tag{3.71}$$

$$2X_a(n) \;=\; aX_a(n+\epsilon) \;-\; \epsilon dY_a(n+\epsilon), \tag{3.72}$$

$$2Y_a(n) \;=\; -\epsilon X_a(n+\epsilon) \;+\; aY_a(n+\epsilon), \tag{3.73}$$

$$2X_a(n) \;=\; aX_a(n-\epsilon) \;+\; \epsilon dY_a(n-\epsilon), \tag{3.74}$$

$$2Y_a(n) = \epsilon X_a(n-\epsilon) + aY_a(n-\epsilon), \tag{3.75}$$

$$2X_a(n+\epsilon) = (a^2-2)X_a(n-\epsilon) + \epsilon adY_a(n-\epsilon), \tag{3.76}$$

$$2Y_a(n+\epsilon) = \epsilon aX_a(n-\epsilon) + (a^2-2)Y_a(n-\epsilon), \tag{3.77}$$

$$2X_a(n-\epsilon) = (a^2-2)X_a(n+\epsilon) - \epsilon adY_a(n+\epsilon), \tag{3.78}$$

$$2Y_a(n-\epsilon) = -\epsilon aX_a(n+\epsilon) + (a^2-2)Y_a(n+\epsilon). \tag{3.79}$$

For $\epsilon = \pm 1$. When n is odd, all quantities below are integers.

$$2X_a\left(\frac{n+\epsilon}{2}\right) = aX_a\left(\frac{n-\epsilon}{2}\right) + \epsilon dY_a\left(\frac{n-\epsilon}{2}\right), \tag{3.80}$$

$$2Y_a\left(\frac{n+\epsilon}{2}\right) = aY_a\left(\frac{n-\epsilon}{2}\right) + \epsilon X_a\left(\frac{n-\epsilon}{2}\right), \tag{3.81}$$

$$2X_a\left(\frac{n-\epsilon}{2}\right) = aX_a\left(\frac{n+\epsilon}{2}\right) - \epsilon dY_a\left(\frac{n+\epsilon}{2}\right), \tag{3.82}$$

$$2Y_a\left(\frac{n-\epsilon}{2}\right) = aY_a\left(\frac{n+\epsilon}{2}\right) - \epsilon X_a\left(\frac{n+\epsilon}{2}\right). \tag{3.83}$$

For $\epsilon = \pm 1$ and n odd, we have from (3.19′) - (3.22′)

$$X_a(n) + a = X_a\left(\frac{n+\epsilon}{2}\right) \cdot X_a\left(\frac{n-\epsilon}{2}\right), \tag{3.84}$$

$$X_a(n) - a = dY_a\left(\frac{n+\epsilon}{2}\right) \cdot Y_a\left(\frac{n-\epsilon}{2}\right), \tag{3.85}$$

$$Y_a(n) + \epsilon = Y_a\left(\frac{n+\epsilon}{2}\right) \cdot X_a\left(\frac{n-\epsilon}{2}\right), \tag{3.86}$$

$$Y_a(n) - \epsilon = X_a\left(\frac{n+\epsilon}{2}\right) \cdot Y_a\left(\frac{n-\epsilon}{2}\right). \tag{3.87}$$

From (3.4) and (3.5) with n replaced by $(n-\epsilon)/2$ and $(n+\epsilon)/2$ we obtain the following identities. $(n-\epsilon)/2$ and $(n+\epsilon)/2$ are both integers when $\epsilon=\pm 1$ and n is odd.

$$X_a(n-\epsilon) = X_a\left(\frac{n-\epsilon}{2}\right)^2 - 2 = dY_a\left(\frac{n-\epsilon}{2}\right)^2 + 2, \tag{3.88}$$

$$Y_a(n-\epsilon) = X_a\left(\frac{n-\epsilon}{2}\right) \cdot Y_a\left(\frac{n-\epsilon}{2}\right), \tag{3.89}$$

$$X_a(n+\epsilon) = X_a\left(\frac{n+\epsilon}{2}\right)^2 - 2 = dY_a\left(\frac{n+\epsilon}{2}\right)^2 + 2, \tag{3.90}$$

$$Y_a(n+\epsilon) = X_a\left(\frac{n+\epsilon}{2}\right) \cdot Y_a\left(\frac{n+\epsilon}{2}\right). \tag{3.91}$$

$(n-\epsilon)/4$ and $(n+\epsilon)/4$ are integers when $4 \mid (n-\epsilon)$ or $4 \mid (n+\epsilon)$.

$$X_a\left(\frac{n-\epsilon}{2}\right) = X_a\left(\frac{n-\epsilon}{4}\right)^2 - 2 = dY_a\left(\frac{n-\epsilon}{4}\right)^2 + 2, \tag{3.92}$$

$$Y_a\left(\frac{n-\epsilon}{2}\right) = X_a\left(\frac{n-\epsilon}{4}\right) \cdot Y_a\left(\frac{n-\epsilon}{4}\right), \tag{3.93}$$

$$X_a\left(\frac{n+\epsilon}{2}\right) = X_a\left(\frac{n+\epsilon}{4}\right)^2 - 2 = dY_a\left(\frac{n+\epsilon}{4}\right)^2 + 2, \tag{3.94}$$

$$Y_a\left(\frac{n+\epsilon}{2}\right) = X_a\left(\frac{n+\epsilon}{4}\right) \cdot Y_a\left(\frac{n+\epsilon}{4}\right). \tag{3.95}$$

By (1.35), (3.28′) and (3.29′) we have

$$(X_a(n)+2)(X_a(n)-2) = d \cdot Y_a(n)^2, \tag{3.96}$$

$$X_a(n)^2 + d = X_a(n+\epsilon) \cdot X_a(n-\epsilon), \tag{3.97}$$

$$X_a(n)^2 - a^2 = d(Y_a(n)^2 - 1), \tag{3.98}$$

$$(X_a(n)+a) \cdot (X_a(n)-a) = d \cdot (Y_a(n)+\epsilon) \cdot (Y_a(n)-\epsilon). \tag{3.99}$$

From (3.53) and (3.54) for any $\epsilon = \pm 1$

$$Y_a(2nm) - \epsilon Y_a(2m) = X_a(nm+\epsilon m) \cdot Y_a(nm-\epsilon m). \tag{3.100}$$

Hence by (3.5)

$$X_a(nm)Y_a(nm) - \epsilon X_a(m)Y_a(m) = X_a(nm+\epsilon m) \cdot Y_a(nm-\epsilon m). \tag{3.101}$$

From (1.14′) and (1.12′) we have

$$aY_a(n) - 2Y_a(n-1) = X_a(n), \qquad aX_a(n) - 2X_a(n-1) = dY_a(n). \tag{3.106}$$

By induction on n one can prove

$$(a-2)\sum_{i=1}^{n} Y_a(i) = Y_a(n+1) - Y_a(n) - 1, \tag{3.107}$$

$$(a-2)\sum_{i=1}^{n} X_a(i) = X_a(n+1) - X_a(n) + a - 2. \tag{3.108}$$

Also by induction on n we have

$$d\sum_{i=1}^{n} Y_a(2i) = 2Y_a(2n+2) - aY_a(2n+1) - a, \tag{3.109}$$

$$d\sum_{i=1}^{n} Y_a(2i+1) = 2Y_a(2n+2) - 2Y_a(2n+1) - 2, \tag{3.110}$$

$$d\sum_{i=1}^{n} X_a(2i) = 2X_a(2n+2) - aX_a(2n+1) + d, \tag{3.111}$$

$$d\sum_{i=1}^{n} X_a(2i+1) = aX_a(2n+2) - 2X_a(2n+1). \tag{3.112}$$

Theorem 3.113. If $(n,6)=1$, then $X_1(n) = 1$ and $Y_1(n) = (-3/n) \equiv n \pmod 6$.
If $3|n$, then $X_1(n) = 2(-1)^{n/3}$ and $Y_1(n) = 0$.

Proof. If $(n,6)=1$, then $n=6j\pm1$ so that $X_1(6j\pm1)=1$ and $Y_1(6j\pm1)=\pm1$. From the theory of quadratic residues it is know that if $(n,6)=1$, then $(-3/n) \equiv n \pmod 6$. In other words, if $n = 6j \pm 1$, then $(-3/n) = \pm1$. Consequently $(-3/n) = Y_1(n)$.

§4. Divisibility properties

In this section we derive some divisibility properties of the sequences $X_a(n)$ and $Y_a(n)$. Many of these divisibility properties are known. We believe the following to be new: Lemma 4.36 and Theorem 4.50, 4.52 and their generalization, Theorem 4.61. The following divisibility properties may possibly be new or at least the proofs are new: Lemma 4.23, Lemma 4.24 and Lemma 4.37. Also the proof of 4.56 is new.

From the fact that for fixed n the functions $X_a(n)$ and $Y_a(n)$ are polynomials in a, one obtains the *Congruence Rules*:

$$(4.1) \qquad X_a(n) \equiv X_b(n) \pmod{a-b}, \qquad Y_a(n) \equiv Y_b(n) \pmod{a-b}.$$

Congruence Rule (4.1) is due to Julia Robinson [33]. In these congruences b can also be negative. Equations (1.47) can be proved by induction from the Lucas Equations (3.10) and (3.11). Thus we have also the Congruence Rules

$$(4.2) \qquad X_a(n) \equiv (-1)^n X_b(n) \pmod{a+b}, \quad Y_a(n) \equiv (-1)^{n-1} Y_b(n) \pmod{a+b}.$$

From this it follows that if $a \equiv \pm b \pmod{n}$, then for any k,

$$(4.2.1) \qquad X_a(k) \equiv \pm X_b(k) \pmod{n}, \text{ and } Y_a(k) \equiv \pm Y_b(k) \pmod{n}.$$

The Congruence Rules (4.1), (4.2) and (4.2.1) also hold when a or b is 0, 1 or 2. If we substitute these values 0, 1 and 2 into (4.1) and (4.2) and use Definitions (3.12) - (3.14) for X_0, X_1, X_2, Y_0, Y_1 and Y_2 we then obtain the *special congruence rules.*

$$(4.3) \qquad X_a(n) \equiv 2 \pmod{a-2}, \qquad Y_a(n) \equiv n \pmod{a-2},$$

$$(4.4) \qquad X_a(n) \equiv 2(-1)^n \pmod{a+2}, \qquad Y_a(n) \equiv n(-1)^{n+1} \pmod{a+2},$$

$$(4.5) \qquad X_a(2i) \equiv 2(-1)^i \pmod{a}, \qquad Y_a(2i) \equiv 0 \pmod{a},$$

$$(4.6) \qquad X_a(2i+1) \equiv 0 \pmod{a}, \qquad Y_a(2i+1) \equiv (-1)^i \pmod{a}.$$

(4.7) PARITY LEMMA If $Y_a(n)$ is even, then $X_a(n)$ is even and $X_a(n) \equiv 2 \pmod 4$.

$$X_a(n) \equiv a \cdot rem(n^2,3) \pmod 2, \quad Y_a(n) \equiv rem(n^2,3) + an + n \pmod 2.$$

When a is even: For all n, $X_a(n) \equiv 0 \pmod 2$ and $Y_a(n) \equiv n \pmod 2$. Also

$Y_a(n)$ even $\Leftrightarrow$ n even $\Rightarrow X_a(n) \equiv 2 \pmod 4 \Leftrightarrow Y_a(n) \equiv a[(-1)^{n/2}-1]/2 \pmod 4$.

$Y_a(n)$ odd $\Leftrightarrow$ n odd $\Rightarrow X_a(n) \equiv a \pmod 4 \Leftrightarrow Y_a(n) \equiv n \pmod 4$.

When a is odd: For all n, $X_a(n) \equiv Y_a(n) \equiv rem(n^2,3) \pmod 2$. Also

$Y_a(n)$ even $\Leftrightarrow X_a(n)$ even $\Leftrightarrow X_a(n) \equiv 2 \pmod 4 \Leftrightarrow Y_a(n) \equiv 0 \pmod 4 \Leftrightarrow 3 \mid n$.

$Y_a(n)$ odd $\Leftrightarrow X_a(n)$ odd $\Leftrightarrow (3,n) = 1$.

Proof. By induction on n, using (3.10) and (3.11).

Lemma 4.8. For any a, $(X_a(n), 2Y_a(n)) \mid 2$, $\quad (X_a(n)-2, X_a(n)+2) \mid 4$.

$$(X_a(n), X_a(n+1)) \mid 2, \quad (Y_a(n), Y_a(n+1) = 1.$$

a is even $\Leftrightarrow (X_a(n), X_a(n+1)) = 2$. a is odd $\Leftrightarrow (X_a(n), X_a(n+1)) = 1$.

When a is even: $2 \mid n \Leftrightarrow (X_a(n), Y_a(n)) = 2 \Rightarrow (X_a(n)-2, X_a(n)+2) = 4$.

When a is odd: $3 \mid n \Leftrightarrow (X_a(n), Y_a(n)) = 2 \Leftrightarrow (X_a(n)-2, X_a(n)+2) = 4$.

If $a \equiv 2 \pmod 4$, then $X_a(n) \equiv 2 \pmod 4$ and $(X_a(n)-2, X_a(n)+2) = 4$.

If $a \equiv 0 \pmod 4$, then $X_a(n) \equiv 1+(-1)^n \pmod 4$ and $(X_a(n)-2, X_a(n)+2) = 3+(-1)^n$.

Proof. $(X_a(n), 2Y_a(n)) \mid 2$ follows from (4.7) and defining equation (1.35), $X_a(n)^2 - dY_a(n)^2 = 4$. $(Y_a(n), Y_a(n+1)) = 1$ follows from identity (3.34). For the proof of $(X_a(n), X_a(n+1)) \mid 2$, we note that identity (3.33) implies that when a prime $p \mid X_a(n+1)$ and $p \mid X_a(n)$, then $p^2 \mid d$. Then $X_a(n)^2 - dY_a(n)^2 = 4$ implies $p^2 \mid 4$ so that $p \mid 2$. Hence $(X_a(n), X_a(n+1)) \mid 2$. Proofs of the other statements are similar.

(4.9) PERIODICITY CONGRUENCES Let m and n be natural numbers and i any integer. Then

$$X_a(2n \pm m) \equiv -X_a(m) \pmod{X_a(n)}, \quad Y_a(2n \pm m) \equiv \mp X_a(m) \pmod{X_a(n)},$$
$$X_a(4n \pm m) \equiv X_a(m) \pmod{X_a(n)}, \quad Y_a(4n \pm m) \equiv \pm Y_a(m) \pmod{X_a(n)},$$
$$X_a(4ni \pm m) \equiv X_a(m) \pmod{X_a(n)}, \quad Y_a(4ni \pm m) \equiv \pm Y_a(m) \pmod{X_a(n)},$$
$$X_a(2ni \pm m) \equiv (-1)^i X_a(m) \pmod{X_a(n)}, \quad Y_a(2ni \pm m) \equiv (-1)^i Y_a(m) \pmod{X_a(n)},$$
$$X_a(4ni \pm 2n \pm m) \equiv -X_a(m) \pmod{X_a(n)}, \quad Y_a(4ni \pm 2n \pm m) \equiv \mp Y_a(m) \pmod{X_a(n)}.$$

Proof. The first two congruences follow directly from the Periodicity Equations, (3.6) and (3.7). The other congruences follow from the first two using the Periodicity Equations and induction on i. The $\pm$ signs correspond. They depend essentially on the number of multiples of $2n$, and also of course follow the signs on m.

Lemma 4.10. The following congruences hold both number theoretically and algebraically.

$$(i) \qquad Y_a(nk) \equiv 0 \pmod{Y_a(n)},$$
$$(ii) \qquad X_a(2nk) \equiv 2 \pmod{Y_a(n)},$$
$$(iii) \qquad 2X_a(2nk \pm r) \equiv 2X_a(r) \pmod{Y_a(n)},$$
$$(iv) \qquad 2Y_a(2nk \pm r) \equiv \pm 2Y_a(r) \pmod{Y_a(n)},$$
$$(v) \qquad 2X_a(2nk + n \pm r) \equiv X_a(n)X_a(r) \pmod{Y_a(n)},$$
$$(vi) \qquad X_a(n)^2 \equiv 4 \pmod{Y_a(n)^2},$$
$$(vii) \qquad 2Y_a(2nk + n \pm r) \equiv \pm X_a(n)Y_a(r) \pmod{Y_a(n)},$$
$$(viii) \qquad X_a(n)^{2j+i} \equiv 4^j X_a(n)^i \pmod{Y_a(n)^2}$$

Proof. We prove Congruence (i) by induction on k using Periodicity Equation (3.7).

The statement holds trivially for $k = 0$ and $k = 1$. Assume it holds for k and $k+1$. Then

$$\begin{aligned} Y(n(k+2)) &= Y(nk+2n) = X(n)Y(nk+n) - Y(nk) \\ &= X(n)Y(n(k+1)) - Y(nk) \equiv 0 \pmod{Y(n)}. \end{aligned}$$

Congruence (ii) follows from (i) and Double Angle Formula (3.4) by replacing n by nk in (3.4). Congruence (iii) follows directly from (i) and (ii) and Addition Equation (3.2). Congruence (iv) follows from $(i), (ii)$ and Addition Equation (3.3). Congruence (v) follows from (iii) (with r replaced by $n+r$) and Addition Equation (3.2). Congruence (vii) follows from (iv) (with r replaced by $n+r$) and Addition Equation (3.3). Congruence (vi) is evident from defining equation (1.35). Congruence $(viii)$ follows trivially from (vi).

Now we can establish the divisibility properties of the sequences X_a, Y_a.

DIVISION THEOREM 4.11. (Lucas [32]). We have the following divisibilities which hold also algebraically

$$n \mid m \Leftrightarrow Y_a(n) \mid Y_a(m). \quad (2 \le a) \tag{4.11}$$

$$n \mid m \text{ and } m/n \text{ is odd} \Leftrightarrow X_a(n) \mid X_a(m). \quad (2 < a) \tag{4.12}$$

Proof. If $a = 2$, $Y_a(n) = n$. Hence (4.11) holds. Suppose $2 < a$. For (4.11).

$\Rightarrow$. Suppose $n \mid m$. Let $m = nk$. Then by Lemma 4.10 (i) $Y_a(n) \mid Y_a(m)$.

$\Leftarrow$. Suppose $Y_a(n) \mid Y_a(m)$. Write m in the form $m = 2nk \pm r$ with $0 \le r < n$. By Lemma 4.10 (iv) we have $0 \equiv 2Y(m) = 2Y(2nk \pm r) \equiv \pm 2Y(r) \pmod{Y(n)}$. Hence $Y(n) \mid 2Y(r)$. From $0 \le r < n$, it follows that $0 \le 2Y(r) \le 2Y(n-1) < Y(n)$ using the inequality in Lemma (2.9) (i). Therefore we have $0 \le 2Y(r) < Y(n)$ and $Y(n) \mid 2Y(r)$ which implies $r = 0$. Hence $m = 2nk$ so that $n \mid m$.

For the proof of (4.12) in the direction $\Rightarrow$, suppose $n \mid m$ and m/n is odd. From the Periodicity Congruences (4.9)

$X(2n(2i)+n) = X(4ni+n) \equiv X(n) \equiv 0 \pmod{X(n)}$ and

$X(2n(2i+1)+n) = X(4ni+2n+n) \equiv -X(n) \equiv 0 \pmod{X(n)}$.

Hence for $j = 2i$ or $j = 2i+1$, $X(2nj+n) \equiv 0 \pmod{X(n)}$. Equivalently $X(n(2j+1)) \equiv 0 \pmod{X(n)}$. Hence $X(n) \mid X(n(2j+1))$. This proves that for any odd k, $X(n) \mid X(nk)$.

For the proof of (4.12) in the direction $\Leftarrow$, suppose $X(n) \mid X(m)$. We can write $m = 2nk \pm r$ with $0 < r \leq n$. By the Periodicity Congruences (4.9) we have $0 \equiv X(m) = X(2nk \pm r) \equiv (-1)^k X(r) \pmod{X(n)}$. Hence $X(n) \mid X(r)$. If $0 < r < n$, then $X(r) < X(n)$. Consequently $r = n$ and $m = 2nk \pm n = (2k \pm 1)n$ so that $n \mid m$ and m/n is odd.

Divisibility statements (4.11) and (4.12) can be interpreted algebraically as statements about divisibility of polynomials in $Z[a]$. As a result of this we have

Corollary 4.13. If $k \mid n$, then there exists a polynomial $Q(a)$, depending on n and k, with integer coefficients and degree $n-k$, such that $Y_a(n) = Y_a(k) \cdot Q(a)$.

Lemma 4.14. Suppose $n \equiv r \pmod{m}$ and $Y_a(m)$ is even. Then $Y_a(n) \equiv Y_a(r) \pmod{2}$.

Proof. From the Parity Lemma 4.7. Consider separately the cases a even and a odd.

Lemma 4.15. $n \equiv r \pmod{m} \Rightarrow (Y_a(n), Y_a(m)) = (Y_a(r), Y_a(m))$.

Proof. By symmetry it is enough to show that $(Y_a(n), Y_a(m)) \mid (Y_a(r), Y_a(m))$. Trivially $(Y_a(n), Y_a(m)) \mid Y_a(m)$. Hence we need only show $(Y_a(n), Y_a(m)) \mid Y_a(r)$. Let $k = (Y_a(n), Y_a(m))$. Let $n = r \pm qm$, then $\pm qm = n - r$. By the Division Theorem

4.11 and Addition Equation (3.3) we have

$$Y_a(m)) \mid Y_a(qm) \text{ and } \pm 2Y_a(qm)) = Y_a(n)X_a(r)) - X_a(n)Y_a(r).$$

Since $k \mid Y_a(m)$, we have

(*) $\qquad k \mid Y_a(n)$ and $2k \mid Y_a(n)X_a(r) - X_a(n)Y_a(r)$.

Case 1. $Y_a(m)$ or $Y_a(n)$ is odd. In this case k must be odd and $(X_a(n), 2Y_a(n)) \mid 2$ implies $(k, X_a(n)) = 1$ so that $k \mid Y_a(r)$ by (*).

Case 2. $Y_a(m)$ and $Y_a(n)$ are both even. In this case by Lemma 4.14 $Y_a(r)$ must be even. Hence $X_a(n)$ and $X_a(r)$ are even by the Parity Lemma 4.7. Hence from (*) we have

$$k \mid Y_a(n) \text{ and } k \mid Y_a(n) \cdot \frac{X_a(r)}{2} - \frac{X_a(n)}{2} \cdot Y_a(r).$$

But now we have $(X_a(n), 2Y_a(n)) = 2$ which implies $(X_a(n)/2, Y_a(n)) = 1$ so that $(k, X_a(n)/2) = 1$ since $k \mid Y_a(n)$. It follows that $k \mid Y_a(r)$. This completes the proof.

GCD THEOREM 4.16. (Lucas [32]). For all $a \geq 2$,

(i) $\qquad (Y_a(n), Y_a(m)) = Y_a(\,(n,m)\,)$,

(ii) $\qquad$ If n and m are odd, then $(X_a(n), X_a(m)) = X_a(\,(n,m)\,)$.

Proof. We show that $(Y_a(n), Y_a(m)) = Y_a(\,(n,m)\,)$. Suppose $m < n$. We will apply Lemma 4.15 to the equations arising in the Euclid Algorithm for (n,m). Let the sequence of remainders in the Euclid Algorithm be $0 = r_n < r_{n-1} < \cdots < r_1 < m < n$ where $r_{n-1} = (n,m)$. Suppose the equations are

$$n = mq_1 + r_1, \qquad m = r_1q_2 + r_2, \qquad r_1 = r_2q_3 + r_3,$$

$$r_2 = r_3q_4 + r_4, \cdots \quad r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad r_{n-2} = r_{n-1}q_n + r_n.$$

By applying Lemma 4.15 $n+1$ times to these equations we have

$$\begin{aligned}(Y_a(n),Y_a(m)) &= (Y_a(m),Y_a(r_1)) = (Y_a(r_1),Y_a(r_2)) = \cdots = (Y_a(r_{n-2}),Y_a(r_{n-1}))\\ &= (Y_a(r_{n-1}),Y_a(r_n)) = (Y_a(r_{n-1}),Y_a(0)) = Y_a(r_{n-1}) = Y_a((n,m)).\end{aligned}$$

The last equality is due to $r_{n-1} = (n,m)$. Hence $(Y_a(n),Y_a(m)) = Y_a((n,m))$.

Theorem 4.16 (ii) can be derived in a similar way from (4.12) (McDaniel [36]); (ii) also holds under slightly more general hypotheses, that $n/(n,m)$ and $m/(n,m)$ are odd.

Corollary 4.17. $(Y_a(n),Y_a(m))=1 \Leftrightarrow (n,m)=1$. Also $[Y_a(n),Y_a(m)]\,|\,Y_a([n,m])$.

Proof. The first statement follows from the GCD theorem. For the second, from the Division Theorem, we have $Y_a(n) \mid Y_a([n,m])$ and $Y_a(m) \mid Y_a([n,m])$. Therefore $[Y_a(n),Y_a(m)] \mid Y_a([n,m])$.

REMARK. $[Y_a(n),Y_a(m)] < Y_a([n,m])$ is possible, e.g., let $a=3, n=4$ and $m=6$.

Corollary 4.18. Suppose $a \geq 2$. Then $n \mid m$ implies $Y_a(n) \cdot Y_a(m) \mid Y_a(n \cdot m)$.

Corollary 4.19. Let $\epsilon = \pm 1$. Then

n odd $\Rightarrow$ $(Y_a(n+\epsilon),Y_a(n-\epsilon)) = a$,

n even $\Rightarrow$ $(Y_a(n+\epsilon),Y_a(n-\epsilon)) = 1$.

Proof. By the GCD Theorem. If n is odd, then $(n+\epsilon, n-\epsilon) = 2$ and $Y_a(2) = a$. If n is even, then $(n+\epsilon, n-\epsilon) = 1$ and $Y_a(1) = 1$.

Corollary 4.20. If n is odd, then $(Y_a((n+\epsilon)/2), Y_a((n-\epsilon)/2)) = 1$.

Corollary 4.21. If $(n,2a) = 1$ and $\epsilon = \pm 1$, then $n \mid Y_a(n \pm \epsilon) \Rightarrow (n, Y_a(n \mp \epsilon)) = 1$.

Lemma 4.21.1. If n is odd and $d = a^2 - 4$, then $(d,n) = (a+2,n)(a-2,n)$.

Proof. It is known that $((a+2)(a-2),n) \mid (a+2,n)(a-2,n)$. Therefore $(d,n) \mid (a+2,n)(a-2,n)$. But $((a+2,n),(a-2,n)) = 1$ as n is odd.

Theorem 4.22. (*i*) $2n \mid m \Leftrightarrow X_a(n) \mid Y_a(m)$,

(*ii*) $X_a(2kn) \equiv \pm 2 \pmod{X_a(n)}$,

(*iii*) $(X_a(n), X_a(2kn)) \mid 2$.

Proof. Put $m = 0$ in the Periodicity Congruences 4.9.

Lemma 4.23. If k is odd, $Y_a(nk) \equiv kY_a(n) \pmod{Y_a(n)^3}$.

Lemma 4.24. If k is even, $Y_a(nk) \equiv \frac{k}{2}X_a(n)Y_a(n) \pmod{Y_a(n)^3}$.

Proof. By identities (3.55) and (3.56).

Lemma 4.25. If k is odd, $X_a(nk) \equiv k(-1)^{\frac{k-1}{2}}X_a(n) \pmod{X_a(n)^2}$.

Lemma 4.26. If k is even, $X_a(nk) \equiv 2(-1)^{\frac{k}{2}} \pmod{X_a(n)^2}$.

Proof. Induction on k. The congruences hold for $k = 1$ and $k = 2$. Suppose Congruence (4.25) holds for an odd k and Congruence (4.26) holds for $k+1$. Consider $k+2$ (which is odd). Using the induction hypothesis and Periodicity Equation (3.6) we have

$$X(n(k+2)) = X(nk+2n) = X(n)X(nk+n) - X(nk) = X(n)X(n(k+1)) - X(nk)$$
$$\equiv X(n)2(-1)^{(k+1)/2} - k(-1)^{(k-1)/2}X(n) = X(n)(k+2)(-1)^{(k+1)/2} \pmod{X(n)^2}.$$

Hence (4.25) holds for $k+2$. Suppose next that k is even and that (4.26) holds for $k+1$. Using Periodicity Equation (3.6) again we get

$X(n(k+2)) = X(nk+2n) = X(n)X(n(k+1)) - X(nk) \equiv$

$X(n)(\pm 1)(k+1)X(n) - X(nk) \equiv -X(nk) \equiv -2(-1)^{k/2} = 2(-1)^{(k+2)/2} \pmod{X(n)^2}$.

Hence (4.26) holds for $k+2$. Both congruences are proved.

Lemma 4.27. For all a and all n, $\quad Y_a(n)^2 | Y_a(nY_a(n))$.

Proof. Replacing k by $Y(n)$ in Lemmas 4.23 and 4.24 we get the two congruences

$$(i)\ Y(nY(n)) \equiv Y(n)^2 \pmod{Y(n)^3}, \quad (ii)\ Y(nY(n)) \equiv \frac{X(n)}{2} Y(n)^2 \pmod{Y(n)^3}.$$

where the (i) holds when $Y(n)$ is odd and (ii) holds when $Y(n)$ is even. If k is even, by the Parity Lemma 4.7 then $X(n)$ is even, so the right side of (ii) is an integer. Hence (i) and (ii) imply that $Y(n)^2 \mid Y(nY(n))$ holds in any case.

First Step Down Lemma 4.28. $\quad nY_a(n) \mid m \Leftrightarrow Y_a(n)^2 \mid Y_a(m) \quad (2 \leq a)$.

Proof. $\Rightarrow$. Suppose $nY(n) \mid m$. Then $Y(nY(n)) \mid Y(m)$ by the Division Theorem. From Lemma 4.27 we have $Y(n)^2 | Y(nY(n))$; thus, $Y(n)^2 | Y(m)$.

$\Leftarrow$. For the converse suppose $Y_a(n)^2 \mid Y_a(m)$. Certainly $Y_a(n) \mid Y_a(m)$. Hence by the Division Theorem $n \mid m$. Let $m = nk$. Then we are given $Y(n)^2 \mid Y(nk)$.

Case 1. k odd. Lemma 4.23 $\Rightarrow Y(n)^2 | kY(n)$ so $Y(n) | k$. So $nY(n) | nk$ or $nY_a(n) | m$.

Case 2. k even. Lemma 4.24 implies $Y_a(nk) \equiv (1/2)X_a(n)Y_a(n)k \pmod{Y_a(n)^3}$. Then $Y(n)^2 \mid Y(nk)$ implies $Y(n) \mid (1/2)X(n)k$. From Lemma 4.8 $(Y(n), X(n)) \mid 2$. Hence if $Y(n)$ is odd, then $Y(n) \mid k$. If $Y(n)$ is even, by Parity Lemma 4.7 then $X(n) \equiv 2 \pmod 4$. Hence $(Y(n), (1/2)X(n)) = 1$ so that again $Y(n) \mid k$. Hence $nY_a(n) | nk$ and therefore $nY_a(n) | m$.

Corollary 4.28.1. $\quad Y_a(n) \mid k \Leftrightarrow Y_a(n)^2 \mid Y_a(nk). \quad (2 \leq a)$.

Second Step Down Lemma 4.29. For $2 < a$ and $1 \leq n$.

$$Y_a(k) \equiv \pm Y_a(m) \pmod{X_a(n)} \quad \Leftrightarrow \quad k \equiv \pm m \pmod{2n}.$$

Proof. $\Leftarrow$. Suppose $k = 2nj \pm m$ where j is an integer. When j is even, $j = 2i$ we have by the Periodicity Congruences 4.9 $Y(k) = Y(4ni \pm m) \equiv \pm Y(m) \pmod{X(n)}$. When j is odd, $j = 2i \pm 1$, we have $Y(k) = Y(4ni + 2n \pm m) \equiv \mp Y(m) \pmod{X(n)}$. So $Y(k) \equiv \pm Y(m) \pmod{X(n)}$ in any case. (Since j can be any integer there is no correspondence between $\pm$ signs.)

$\Rightarrow$. Suppose $Y(k) \equiv \pm Y(m) \pmod{X(n)}$. Choose k' such that $0 \leq k' \leq n$ and $k \equiv \pm k' \pmod{2n}$. Choose m' such that $0 \leq m' \leq n$ and $m \equiv \pm m' \pmod{2n}$. Then there exist integers i and j such that $k = 2ni \pm k'$ and $m = 2nj \pm m'$. Using the Periodicity Congruences we get $Y(k') = Y(2ni \pm k) \equiv \pm Y(k) \equiv \pm Y(m) = \pm Y(2nj \pm m') \equiv \pm Y(m') \pmod{X(n)}$. Hence $Y(k') \equiv \pm Y(m') \pmod{X(n)}$. Thus it follows that $X(n) \mid |Y(k') \mp Y(m')|$. If $k' \neq m'$, then from inequality (ii) in Lemma 2.9, $Y(n-1) + Y(n) < X(n)$. This implies $0 < |Y(k') \mp Y(m')| \leq Y(k') + Y(m') \leq Y(n-1) + Y(n) < X(n)$, a contradiction. Hence $k' = m'$. Therefore $k \equiv \pm m \pmod{2n}$.

In the following lemma there is also no correspondence between the $\pm$ signs.

Lemma 4.30. For $4 \leq a$, $2Y_a(k) \equiv \pm 2Y_a(m) \pmod{X_a(n)} \Leftrightarrow k \equiv \pm m \pmod{2n}$.

Proof. $\Leftarrow$. The result follows from Lemma 4.29.

$\Rightarrow$. Suppose $2Y_a(k) \equiv \pm 2Y_a(m) \pmod{X_a(n)}$. As before choose $m' \leq n$ and $k' \leq n$ such that $k \equiv \pm k' \pmod{2n}$ and $m \equiv \pm m' \pmod{2n}$. Proceed as in the proof of Lemma 4.29 and multiply the congruences by 2. One obtains finally $X_a(n) \mid 2Y_a(k') \pm 2Y_a(m')$. At this point we use inequality 2.9 (iii), $2Y_a(n-1) \pm 2Y_a(n) < X_a(n)$ to conclude that $k' = m'$.

(4.31) $2X_a(nk \pm r) \equiv 2X_a(r) \pmod{Y_a(n)}$, for k even,

(4.32) $2X_a(nk \pm r) \equiv X_a(n)X_a(r) \pmod{Y_a(n)}$, for k odd.

Proof. The first congruence, which holds for k even, is a consequence of (4.10) (iii). The second congruence, which holds for k odd, is a consequence of (4.10) (v).

We also have, from (4.10) (iv) and (4.10) (vii),

(4.34) $2Y_a(nk \pm r) \equiv \pm 2Y_a(r) \pmod{Y_a(n)}$, for k even,

(4.35) $2Y_a(nk \pm r) \equiv \pm X_a(n)Y_a(r) \pmod{Y_a(n)}$, for k odd.

Lemma 4.36. Suppose p is an odd number and $\epsilon = \pm 1$. Then for all $j \geq 1$,

(1) $2X_a\left(\frac{p^{j+1}-\epsilon^{j+1}}{2}\right) \equiv X_a\left(\frac{p^j-\epsilon^j}{2}\right) X_a\left(\frac{p-\epsilon}{2}\right) \left(\mathrm{mod}\ Y_a\left(\frac{p^j-\epsilon^j}{2}\right)\right)$,

(2) $2Y_a\left(\frac{p^{j+1}-\epsilon^{j+1}}{2}\right) \equiv \epsilon^j X_a\left(\frac{p^j-\epsilon^j}{2}\right) Y_a\left(\frac{p-\epsilon}{2}\right) \left(\mathrm{mod}\ Y_a\left(\frac{p^j-\epsilon^j}{2}\right)\right)$,

(3) $2X_a\left(\frac{p^{j+1}+\epsilon^{j+1}}{2}\right) \equiv X_a\left(\frac{p^j-\epsilon^j}{2}\right) X_a\left(\frac{p+\epsilon}{2}\right) \left(\mathrm{mod}\ Y_a\left(\frac{p^j-\epsilon^j}{2}\right)\right)$,

(4) $2Y_a\left(\frac{p^{j+1}+\epsilon^{j+1}}{2}\right) \equiv \epsilon^j X_a\left(\frac{p^j-\epsilon^j}{2}\right) Y_a\left(\frac{p+\epsilon}{2}\right) \left(\mathrm{mod}\ Y_a\left(\frac{p^j-\epsilon^j}{2}\right)\right)$.

Proof. By (4.32) and (4.35) with $n = (p^j - \epsilon^j)/2$ and $k = p$. For (1) and (2) let $r = \epsilon^j(p-\epsilon)/2$. $nk + r = (p^j - \epsilon^j)p/2 + \epsilon^j(p-\epsilon)/2 = (p^{j+1} - \epsilon^{j+1})/2$. For (3) and (4), put $r = \epsilon^j(p+\epsilon)/2$. $nk + r = (p^j - \epsilon^j)p/2 + \epsilon^j(p+\epsilon)/2 = (p^{j+1} + \epsilon^{j+1})/2$. Use also (1.46), $X_a(\epsilon^j(p-\epsilon)/2) = X_a((p-\epsilon)/2)$ and $Y_a(\epsilon^j(p-\epsilon)/2) = \epsilon^j Y_a((p-\epsilon)/2)$.

We give next a Step Down Lemma for the X_a sequence:

Lemma 4.37. For $2<a$, $X_a(k) \equiv \pm X_a(m) \pmod{X_a(n)} \Leftrightarrow k \equiv \pm m \pmod{2n}$.

Proof. $\Leftarrow$. Suppose $k = 2ni \pm m$. Then from (4.9), we have $X(k) = X(2ni \pm m) \equiv (-1)^i X(m) \equiv \mp X(m) \pmod{X(n)}$. So $X(k) \equiv \pm X(m) \pmod{X(n)}$.

$\Rightarrow$. Suppose $X(k) \equiv \pm X(m) \pmod{X(n)}$. Choose k' such that $0 \leq k' \leq n$ and $k \equiv \pm k' \pmod{2n}$. Choose m' such that $0 \leq m' \leq n$ and $m \equiv \pm m' \pmod{2n}$. Then there exist integers i and j such that $k = 2ni \pm k'$ and $m = 2nj \pm m'$. Using the Periodicity Congruences 4.9 we get $X(k') = X(2ni \pm k) \equiv \pm X(k) \equiv \pm X(m) = \pm X(2nj \pm m') \equiv \mp X(m') \pmod{X(n)}$ so $X(k') \equiv \pm X(m') \pmod{X(n)}$. Hence $X(n) \mid |X(k') \mp X(m')|$. We claim that $k' = m'$. If one of k' and m' equals n, say $k' = n$, then $X(k') \equiv \pm X(m') \pmod{X(n)}$ would imply that $X(m') \equiv 0 \pmod{X(n)}$, so $X(n) \mid X(m')$. Hence it must be that $m' = n$ therefore $k' = m'$ in this case. Next we suppose $k' \leq n-1$ and $m' \leq n-1$. If $k' \neq m'$, then $k' \leq n-2$ or $m' \leq n-2$ so that by Lemma 2.9 (iv), $0 < |X(k') \mp X(m')| \leq X(k') + X(m') \leq X(n-2) + X(n-1) < X(n)$. This would contradict $X(n) \mid |X(k') \pm X(m')|$. Hence again $k' = m'$. The claim is proved. Therefore $k \equiv \pm m \pmod{2n}$.

Theorem 4.50.

$$
\begin{aligned}
&(i) && X_{a+k}(n) &&\equiv X_a(n) + knY_a(n) && \pmod{k^2},\\
&(ii) && X_{a-k}(n) &&\equiv X_a(n) - knY_a(n) && \pmod{k^2},\\
&(iii) && dY_{a+k}(n) &&\equiv knX_a(n) + (d-ak)Y_a(n) && \pmod{dk^2},\\
&(iv) && dY_{a-k}(n) &&\equiv -knX_a(n) + (d+ak)Y_a(n) && \pmod{dk^2}.
\end{aligned}
$$

From Corollary 2.2, $X'_a(n) = nY_a(n)$ and $dY'_a(n) = nX_a(n) - aY_a(n)$, it is easy to see that Theorem 4.50 is equivalent to the following theorem. Hence we shall prove

Theorem 4.52. For any integer k,

(i) $X_{a+k}(n) \equiv X_a(n) + kX'_a(n) \pmod{k^2}$,

(ii) $X_{a-k}(n) \equiv X_a(n) - kX'_a(n) \pmod{k^2}$,

(iii) $Y_{a+k}(n) \equiv Y_a(n) + kY'_a(n) \pmod{k^2}$.

(iv) $Y_{a-k}(n) \equiv Y_a(n) - kY'_a(n) \pmod{k^2}$.

Proof. (ii) is obtainable from (i) and (iii) is obtainable from (iv) by replacing k by $-k$. Hence we need only prove (i) and (iii). Taking derivatives of both sides of identities (3.10) and (3.11), we have

(*) $X'_a(n+2)=X_a(n+1)+aX'_a(n+1)-X'_a(n)$, $Y'_a(n+2)=Y_a(n+1)+aY'_a(n+1)-Y'_a(n)$.

Now we use induction on n. For $n=0$ or $n=1$, congruences (i) and (iii) become identities.

Suppose (i) and (iii) hold for n and $n+1$. Consider the case $n+2$ for (i):

$$X_{a+k}(n+2)-X_a(n+2)=(a+k)X_{a+k}(n+1)-X_{a+k}(n)-(aX_a(n+1)-X_a(n))$$

$$= a(X_{a+k}(n+1)-X_a(n+1))-(X_{a+k}(n)-X_a(n))+kX_{a+k}(n+1)$$

$$\equiv akX'_a(n+1)-kX'_a(n)+kX_{a+k}(n+1) \quad \text{(by the induction hypothesis)}$$

$$= akX'_a(n+1)-kX'_a(n)+kX_{a+k}(n+1)-kX_{a+k}(n+1)+kX_{a+k}(n+1)$$

$$\equiv k(aX'_a(n+1)-X'_a(n))+k^2X'_a(n+1)+kX_a(n+1) \quad \text{(by the induction hypothesis)}$$

$$\equiv k(aX'_a(n+1)+X_a(n+1)-X'_a(n))+0=kX'_a(n+2) \pmod{k^2} \quad \text{(by(*))}.$$

Hence (i) is proved by induction. Consider the case $n+2$ for (iii):

$$Y_{a+k}(n+2)-Y_a(n+2)=(a+k)Y_{a+k}(n+1)-Y_{a+k}(n)-(aY_a(n+1)-Y_a(n))$$

$$= a(Y_{a+k}(n+1)-Y_a(n+1))-(Y_{a+k}(n)-Y_a(n))+kY_{a+k}(n+1)$$

$$\equiv akY'_a(n+1)-kY'_a(n)+kY_{a+k}(n+1) \quad \text{(by the induction hypothesis)}$$

$$= akY'_a(n+1)-kY'_a(n)+kY_{a+k}(n+1)-kY_{a+k}(n+1)+kY_{a+k}(n+1)$$

$$\equiv k(aY'_a(n+1)-Y'_a(n))+k^2Y'_a(n+1)+kY_a(n+1) \quad \text{(by the induction hypothesis)}$$

$$\equiv k(aY'_a(n+1)+Y_a(n+1)-Y'_a(n))+0=kY'_a(n+2) \pmod{k^2} \quad \text{(by(*))}.$$

Thus (iii) is proved.

Later we shall see how to generalize Theorem 4.52, and at the same time find a

simple proof of Hensel's Lemma. Theorem 4.52 holds for $X_a(n)$ and $Y_a(n)$ simply because they are polynomials in a. We shall show

Theorem 4.61 . Let $f(x)$ be a polynomial in Z[x]. For any integers a and b,

(4.61) $$f(b) - f(a) \equiv (b-a)f'(a) \pmod{(b-a)^2}.$$

Proof. Let $f(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$,

so that $f'(x) = c_k k x^{k-1} + c_{k-1}(k-1)x^{k-2} + \cdots + c_1$. Hence

$$(*) \qquad \frac{f(b)-f(a)}{b-a} = c_k\left(\frac{b^k-a^k}{b-a}\right) + c_{k-1}\left(\frac{b^{k-1}-a^{k-1}}{b-a}\right) + \cdots + c_1\left(\frac{b-a}{b-a}\right).$$

From the geometric series we have

$$(**) \qquad \frac{b^j-a^i}{b-a} = b^{j-1} + b^{j-2}a^1 + \cdots + b^2a^{j-3} + b^1a^{j-2} + a^{j-1}.$$

Here there are j terms in the sum. Since $b \equiv a \pmod{b-a}$, $(**)$ implies

$$\frac{b^j-a^i}{b-a} \equiv a^{j-1} + a^{j-2}a^1 + \cdots + a^2a^{j-3} + a^1a^{j-2} + a^{j-1} = ja^{j-1} \pmod{b-a}.$$

Hence from $(*)$

$$\frac{f(b)-f(a)}{b-a} \equiv c_k k a^{k-1} + c_{k-1}(k-1)a^{k-2} + \cdots + c_2 2a + c_1 = f'(a) \pmod{b-a}.$$

Therefore $f(b) - f(a) \equiv (b-a)f'(a) \pmod{(b-a)^2}$, establishing the theorem.

From Theorem 4.61, we can rewrite Theorem 4.52 in the form

Corollary 4.62. For any n and any a and b,

(i) $$X_b(n) - X_a(n) \equiv (b-a)X_a'(a) \pmod{(b-a)^2},$$

(ii) $$Y_b(n) - Y_a(n) \equiv (b-a)Y_a'(a) \pmod{(b-a)^2}.$$

Theorem 4.61 can also be used to prove Hensel's Lemma without using Taylor's Theorem. As we shall need Hensel's Lemma later, we give this proof here.

Definition 4.64. A solution a of $f(x) \equiv 0 \pmod{p^e}$ is called *nonsingular* if both $f(a) \equiv 0 \pmod{p^e}$ and $f'(a) \not\equiv 0 \pmod{p}$.

Suppose $0 \leq a < p^e$ and a is a solution of $f(x) \equiv 0 \pmod{p^e}$. We say a *lifts* to a solution b of $f(x) \equiv 0 \pmod{p^{e+1}}$ if $f(b) \equiv 0 \pmod{p^{e+1}}$ and $b \equiv a \pmod{p^e}$.

Note that a lifts to b is equivalent to saying there is a (unique) t such that $b = a + tp^e$ and $f(b) \equiv 0 \pmod{p^{e+1}}$. If $0 \leq a < p^{e+1}$ and $0 \leq b < p^{e+1}$, then we can also suppose $0 \leq t < p$.

Theorem 4.65. (Hensel's Lemma [15]). Suppose $f(x)$ is a polynomial in Z[x] and a is a nonsingular solution of $f(x) \equiv 0 \pmod{p^e}$. Then a lifts to a unique solution b of $f(x) \equiv 0 \pmod{p^{e+1}}$.

Proof. Suppose a is a nonsingular solution of $f(x) \equiv 0 \pmod{p^e}$. Hence $f(a)/p^e$ is an integer and $p \nmid f'(a)$. Therefore $f'(a)x \equiv -f(a)/p^e \pmod{p}$ has a unique solution $t \bmod p$. Hence

$$(*) \qquad tf'(a) \equiv -f(a)/p^e \pmod{p} \text{ and } 0 \leq t < p.$$

Let $b = a + tp^e$. To prove the theorem we now need only to show that b is a solution of $f(x) \equiv 0 \pmod{p^{e+1}}$. By Theorem 4.61 with $b = a + tp^e$, we have $f(b) = f(a + tp^e) \equiv f(a) + tp^e f'(a) \pmod{(tp^e)^2}$. Since $e \geq 1$, $2e \geq e + 1$. Hence

$f(b) \equiv f(a) + tp^e f'(a) \pmod{p^{e+1}}$. Therefore by $(*)$

$f(b)/p^e \equiv f(a)/p^e + tf'(a) \equiv f(a)/p^e - f(a)/p^e = 0 \pmod{p}$.

Thus $f(b) \equiv 0 \pmod{p^{e+1}}$. The theorem is proved.

REMARK. Suppose $p \mid f'(a)$. If $f(a) \equiv 0 \pmod{p^{e+1}}$, then a lifts to p different values of $b \bmod p^e$. If $f(a) \not\equiv 0 \pmod{p^{e+1}}$, then a lifts to no values of b.

For the proof of the remark, suppose $p \mid f'(a)$ and $f(a) \equiv 0 \pmod{p^{e+1}}$, then all values of t, $0 \leq t < p$ satisfy the congruence $tf'(a) \equiv -f(a)/p^e \pmod{p}$. Note that $f(a + tp^e) \equiv 0 \pmod{p^{e+1}} \Leftrightarrow tf'(a) \equiv -f(a)/p^e \pmod{p}$ as shown in the proof of Theorem 4.65. Therefore all such t satisfy $f(a + tp^e) \equiv 0 \pmod{p^{e+1}}$. Suppose $p \mid f'(a)$ and $f(a) \not\equiv 0 \pmod{p^{e+1}}$. Then note that we have $f(a+tp^e) \equiv 0 \pmod{p^{e+1}}$ $\Leftrightarrow$ $f(a) + tp^e f'(a) \equiv 0 \pmod{p^{e+1}} \Leftrightarrow f(a) + 0 \equiv 0 \pmod{p^{e+1}}$, which implies $f(a) \equiv 0 \pmod{p^{e+1}}$. This contradicts the assumption $f(a) \not\equiv 0 \pmod{p^{e+1}}$. Hence no t satisfies $f(a+tp^e) \equiv 0 \pmod{p^{e+1}}$. It follows that there is no b such that $f(b) \equiv 0 \pmod{p^{e+1}}$ and $b \equiv a \pmod{p^e}$.

Corollary 4.68. Suppose $f(x) \in Z[x]$. If $f(x) \equiv 0 \pmod{p^e}$ has exactly n solutions mod p^e and that they are all nonsingular, then $f(x) \equiv 0 \pmod{p^{e+1}}$ has exactly n solutions mod p^{e+1} and they are all nonsingular.

§5. Computational complexity of $X_a(n)$ and $Y_a(n)$

In this section we consider the computational complexity of computing the sequences $X_a(n)$ and $Y_a(n)$. We show that the four functions $X_a(n)$, $Y_a(n)$, $rem(X_a(n), m)$ and $rem(Y_a(n), m)$ are computable in polynomial time (a theorem of Lehmer [29], Lehmer, Selfridge and Brillhart [5]). We present a proof of this and give an upper bound on the degree of the polynomial.

To estimate exactly the amount of time required to carry out an algorithm on an input n it is necessary to know the amount of time required to perform one bit operation. Since this depends on the size of words, capacity of the registers and computer architecture, we will estimate the time complexity of our algorithms in terms of the number of bit operations. By a *bit operation* we understand a single addition, subtraction or multiplication of two numbers consisting of one binary digit, (1 bit, 0 or 1). We shall also include as a bit operation division by 2 or right shift.

When estimating the number of bit operations needed to perform an algorithm on an input n, we will use the binary length of n as a measure of the size of n. By the *length* of n we mean the number of digits base 2. This number, which will be denoted by $||n||$, is essentially $log(n)$. More precisely,

$$||n|| = \lfloor log_2(n) + 1 \rfloor. \tag{5.0}$$

With respect to this measure of size of n, a function f is said to be *computable in polynomial time* if there exists a constant c, such that f is computable in $O(||n||^c)$ bit operations. It is customary to refer to this by saying that f is computable in time $O(||n||^c)$.

It is known that multiplication of two n-bit integers can actually be carried out in time $O(||n||^c)$ where $c = log_2(3) = 1.585\cdots < 2$. ([23]) However, in estimating the complexity of the algorithms below, we will assume that the ordinary school algorithms are used for the elementary arithmetical operations. More precisely, we will suppose that the number of steps needed in the basic operations is as follows:

Number of steps needed to *add* or *subtract* two integers a and $b \leq n : O(||n||)$.

Number of steps needed to *multiply* two integers a and $b \leq n : O(||n||^2)$.

Number of steps needed to *divide* two integers a and $b \leq n : O(||n||^2)$.

Number of steps needed to *divide* an integer $a \leq n$ by $2 : O(||n||)$.

Number of steps needed to obtain the *integer part of the square root* of $a : O(||n||^3)$.

Number of steps needed for the *remainder* after a is divided by b, $a, b \leq n : O(||n||^3)$.

Number of steps needed to compute the *GCD* of a and $b \leq n : O(||n||^3)$.

Number of steps needed to obtain a^c *mod* b, $a, b, c \leq n : O(||n||^3)$.

Number of steps needed to compute the *Jacobi symbol* $(a/b), a, b \leq n : O(||n||^3)$.

The estimate for the time to obtain the GCD of a and b is based on Lamé's Theorem about the Euclidean Algorithm. Lamé's Theorem says that the number of divisions in the Euclidean Algorithm is $\leq 5||n||$ where $||n||$ is the decimal length of n and $n = max(a, b)$. In other words, $O(||n||)$. Each division costs $O(||n||^2)$. Hence $O(||n||^3)$ bit operations are sufficient.

The estimate of $O(||n||^3)$ for the time required to compute the remainder $rem(a^k, m)$, where $k \leq n$, $a \leq n$ and $m \leq n$, is based on the estimate of $O(||n||)$ for addition and $O(||n||^2)$ for multiplication. Using the repeated squaring algorithm (Lehmer [23]), the number of bit operations is proportional to $||k|| \cdot ||n||^2$. Since

$||a^k|| \approx k||a||$, the time to compute a^k mod m is

$$O(||k|| \cdot ||a||^2) + O(||m||^2) = O(||n||^3) + O(||n||^2) = O(||n||^3).$$

About the complexity of $X_a(n)$ and $Y_a(n)$ we will prove:

Theorem 5.1. The functions $rem(X_a(n), m)$ and $rem(Y_a(n), m)$ are computable in polynomial time. There is an algorithm to compute $rem(X_a(n), m)$ and $rem(Y_a(n), m)$ in $O((||a||+||n||+||m||)^3)$ bit operations. The functions $X_a(||n||)$ and $Y_a(||n||)$ are also computable in polynomial time. There is an algorithm to compute $X_a(||n||)$ and $Y_a(||n||)$ in $O((||n|| + ||a||)^3)$ bit operations.

Proof. We first sketch a proof for the case a even and m odd. This will use only identities (5.2) - (5.5) below. In the case when a is odd there is a small problem with division by 2, (see (5.6) and (5.7)). We can get around it when m is odd (by adding m occasionally), but when m is even, we will need identities (5.6) - (5.9) below.

The final claim of the theorem, that the functions $X_a(||n||)$ and $Y_a(||n||)$ are computable in polynomial time, follows from the first claim since if $rem(X_a(n), m)$ and $rem(Y_a(n), m)$ are computable in polynomial time $O((||a|| + ||n|| + ||m||)^3)$, we can put

$$m = a^{||n||}$$

in this result. Since $X_a(||n||) \leq a^{||n||}$ and $Y_a(||n||) \leq a^{||n||}$, (which follow from the inequality (2.8 (i) (ii)), we have

$$X_a(||n||) = rem(X_a(||n||), a^{||n||}) \quad \text{and} \quad Y_a(||n||) = rem(Y_a(||n||), a^{||n||})$$

because both sides are less than the modulus.

Hence it will be enough to prove the first part, that $rem(X_a(||n||), m)$ and $rem(Y_a(||n||), m)$ are computable in polynomial time, $O((||a||+||n||+||m||)^3)$. Initially the algorithm will be based on the following identities.

$$(5.2)\quad X_a(2n) = X_a(n)^2 - 2, \qquad \text{(doubling)}$$

$$(5.3)\quad X_a(2n+1) = \frac{1}{2}\left(aX_a(n)^2 - 2a + dX_a(n)Y_a(n)\right) = aX_a(2n) + dY_a(2n), \qquad \text{(sidestep)}$$

$$(5.4)\quad Y_a(2n) = X_a(n)Y_a(n), \qquad \text{(doubling)}$$

$$(5.5)\quad Y_a(2n+1) = \frac{1}{2}\left(dY_a(n)^2 + 2 + aX_a(n)Y_a(n)\right) = X_a(2n) + aY_a(2n). \qquad \text{(sidestep)}$$

Identity (5.2) is (3.4), (5.3) is (3.47), (5.4) is (3.5) and (5.5) is (3.48). In identities (5.3) and (5.5) there is an indicated division by 2. With (5.3) note that $aX_a(n)^2 + dX_a(n)Y_a(n)$ is always even because it is divisible by $aX_a(n) + dY_a(n)$, which is even by (3.8). Hence the division by 2 can be carried out. Similarly, in connection with (5.5), $dY_a(n)^2 + aX_a(n)Y_a(n)$ is even, being divisible by $dY_a(n) + aX_a(n)$. So the indicated division by 2 can again be carried out.

We define functions $V_a(c, x, y)$ and $U_a(c, x, y)$ by

$$(5.6)\quad V_a(c,x,y) = \begin{cases} x^2 - 2, & (\text{mod } m), \text{ if } c \text{ is even,} \\ \lfloor (ax^2 - 2a + dxy)/2 \rfloor, & (\text{mod } m), \text{ if } c \text{ is odd.} \end{cases}$$

$$(5.7)\quad U_a(c,x,y) = \begin{cases} x \cdot y, & (\text{mod } m), \text{ if } c \text{ is even,} \\ \lfloor (dy^2 + 2 + axy)/2 \rfloor, & (\text{mod } m), \text{ if } c \text{ is odd.} \end{cases}$$

$V_a(c, x, y)$ and $U_a(c, x, y)$ are functions of m as well as a, c, x and y. We have $V_a(c, x, y) < m$ and $U_a(c, x, y) < m$. Hence $V_a(c, x, y)$ and $U_a(c, x, y)$ are computable in polynomial time. The time would be $O((||a|| + ||c|| + ||x|| + ||y|| + ||m||)^2)$ bit operations.

Given n, put $l = ||n||$. We define a decreasing sequence, $b_i, (i = 0, 1, \cdots, l)$, by

$b_0 = n$ and $b_{i+1} = \lfloor b_i/2 \rfloor$, $i = 0, 1, \cdots, l-1$. Eventually $b_{l-1} = 1$ and $b_l = 0$. We also define an increasing sequence (reversed sequence) c_i, $i = 0, 1, \cdots, l$, by $c_i = b_{l-i}$. Then $c_0 = 0, c_1 = 1, \cdots, c_l = n$.

Define sequences x_i and y_i, $i = 0, 1, \cdots, l$, by $x_0 = 2$ and $y_0 = 0$, and for $i = 0, 1, \cdots, l-1$ by

$$x_{i+1} = V_a(c_{i+1}, x_i, y_i), \qquad y_{i+1} = U_a(c_{i+1}, x_i, y_i). \tag{5.8}$$

We will show by induction that

$$x_i \equiv X_a(c_i) \pmod{m} \quad \text{and} \quad y_i \equiv Y_a(c_i) \pmod{m}, \ (i = 0, \cdots, l). \tag{5.9}$$

It will follow that $x_l \equiv X_a(n) \pmod{m}$ and $y_l \equiv Y_a(n) \pmod{m}$ since $c_l = n$.

As an example, suppose we want to determine $rem(X_a(n), m)$ and $rem(Y_a(n), m)$ where $n = 21$. Since $21 = 10101_2$ in binary, we have $||n|| = 5$. Then $b_0 = 21$, $b_1 = 10, b_2 = 5, b_3 = 2, b_4 = 1, b_5 = 0$. Consequently $c_0 = 0, c_1 = 1, c_2 = 2, c_3 = 5$, $c_4 = 10, c_5 = 21$. Thus (5.8) and (5.9) imply:

$$x_1 = V_a(c_1, x_0, y_0) \equiv V_a(1, X_a(0), Y_a(0)) \equiv X_a(1) \pmod{m},$$

$$x_2 = V_a(c_2, x_1, y_1) \equiv V_a(2, X_a(1), Y_a(1)) \equiv X_a(2) \pmod{m},$$

$$x_3 = V_a(c_3, x_2, y_2) \equiv V_a(5, X_a(2), Y_a(2)) \equiv X_a(5) \pmod{m},$$

$$x_4 = V_a(c_4, x_3, y_3) \equiv V_a(10, X_a(5), Y_a(5)) \equiv X_a(10) \pmod{m},$$

$$x_5 = V_a(c_5, x_4, y_4) \equiv V_a(21, X_a(10), Y_a(10)) \equiv X_a(21) \pmod{m},$$

and

$$y_1 = U_a(c_1, x_0, y_0) \equiv U_a(1, X_a(0), Y_a(0)) \equiv Y_a(1) \pmod{m},$$

$$y_2 = U_a(c_2, x_1, y_1) \equiv U_a(2, X_a(1), Y_a(1)) \equiv Y_a(2) \pmod{m},$$

$$y_3 = U_a(c_3, x_2, y_2) \equiv U_a(5, X_a(2), Y_a(2)) \equiv Y_a(5) \pmod{m},$$

$$y_4 = U_a(c_4, x_3, y_3) \equiv U_a(10, X_a(5), Y_a(5)) \equiv Y_a(10) \pmod{m},$$

$$y_5 = U_a(c_5, x_4, y_4) \equiv U_a(21, X_a(10), Y_a(10)) \equiv Y_a(21) \pmod{m}.$$

To prove that $x_5 \equiv X_a(21) \pmod{m}$ and $y_5 \equiv Y_a(21) \pmod{m}$ and more generally that $x_n \equiv X_a(c_l) \pmod{m}$ and $y_n \equiv Y_a(c_l) \pmod{m}$, we have to prove that (5.9) holds for all i. The induction step is the following lemma.

Lemma 5.10. Suppose a is even and m is odd. Let x_i and y_i be defined by $x_0 = 2, y_0 = 0$. Suppose x_i and y_i are integers and $x_{i+1} = V_a(c_{i+1}, x_i, y_i)$, and $y_{i+1} = U_a(c_{i+1}, x_i, y_i)$ $(i = 0, \cdots, l-1)$. If $x_i \equiv X_a(c_i) \pmod{m}$ and $y_i \equiv Y_a(c_i) \pmod{m}$, then x_{i+1} and y_{i+1} are integers and $x_{i+1} \equiv X_a(c_{i+1}) \pmod{m}$ and $y_{i+1} \equiv Y_a(c_{i+1}) \pmod{m}$.

Proof. Induction on i. Suppose $x_i \equiv X_a(c_i) \pmod{m}$ and $y_i \equiv Y_a(c_i) \pmod{m}$. There are two cases to consider, according as c_{i+1} is even or odd.

Case 1: c_{i+1} is even. Then $c_{i+1} = 2c_i$.

$x_{i+1} = V_a(c_{i+1}, x_i, y_i) = V_a(2c_i, x_i, y_i) = x_i^2 - 2 \equiv X_a(c_i)^2 - 2 = X_a(2c_i) = X_a(c_{i+1}) \pmod{m}$.

$y_{i+1} = U_a(c_{i+1}, x_i, y_i) = U_a(2c_i, x_i, y_i) = x_i y_i \equiv X_a(c_i) Y_a(c_i) = Y_a(2c_i) = Y_a(c_{i+1}) \pmod{m}$.

Case 2. c_{i+1} is odd. Then $c_{i+1} = 2c_i + 1$. a and d are even so x_{i+1} and y_{i+1} are integers.

$$\begin{aligned} 2x_{i+1} &= 2V_a(c_{i+1}, x_i, y_i) = 2V_a(2c_i + 1, x_i, y_i) = ax_i^2 - 2a + dx_i y_i \\ &\equiv aX_a(c_i)^2 - 2a + dX_a(c_i)Y_a(c_i) = 2X_a(2c_i + 1) = 2X_a(c_{i+1}) \pmod{m}. \end{aligned}$$

$$\begin{aligned} 2y_{i+1} &= 2U_a(c_{i+1}, x_i, y_i) = 2U_a(2c_i + 1, x_i, y_i) = dy_i^2 + 2 + ax_i y_i \\ &\equiv dY_a(c_i)^2 + 2 + aX_a(c_i)Y_a(c_i) = 2Y_a(2c_i) = 2Y_a(c_{i+1}) \pmod{m}. \end{aligned}$$

Since $(m, 2) = 1$, we have $x_{i+1} \equiv X_a(c_{i+1}) \pmod{m}$ and $y_{i+1} \equiv Y_a(c_{i+1}) \pmod{m}$.

Since $x_0 = 2$ and $y_0 = 0$ and $c_0 = 0$, we have $x_0 = X_a(c_0)$ and $y_0 = Y_a(c_0)$. Hence $x_0 \equiv X_a(c_0) \pmod{m}$ and $y_0 \equiv Y_a(c_0) \pmod{m}$. Therefore by induction and Lemma 5.10 it follows that $x_n \equiv X_a(c_l) \pmod{m}$ and $y_n \equiv Y_a(c_l) \pmod{m}$.

This procedure works when a is even and m is odd. When a is odd or m is even, there is a problem with division by 2. We obtain only $rem(2Y_a(k), m)$ and $rem(2X_a(k), m)$ at each stage. To get $rem(Y_a(k), m)$ and $rem(X_a(k), m)$ we have to calculate $rem(2Y_a(k), 2m)$ and $rem(2X_a(k), 2m)$ somehow, using other identities. For example the above algorithm fails in the cases when $a = 4, n = 3, m = 8$, or when $a = 3, n = 3, m = 8$ or if $a = 3, n = 4$ and $m = 7$.

When a is even and m is odd, it may be possible to modify (5.6) and (5.7) by occasionally adding m when some intermediate quantity is odd and we wish it were even so we could divide it by 2. Possibly for odd m the above algorithm could be modified and made to work, for all a.

In general when a is odd or m may be even one should use a slightly different algorithm described below and based on identities (5.11) - (5.14). These identities provide a general algorithm which works in all cases. A small price is to be paid however. With the old algorithm based on identities (5.2) - (5.5), it was simpler to prove correctness. It was also enough to store pairs at each stage. The new algorithm based on identities (5.11) - (5.14) requires storage of quadruples.

We will use the following equations, (5.11) - (5.14). (For their derivation see identities (3.4), (3.5), (3.41) and (3.42).):

$$X_a(2n) = X_a(n)^2 - 2, \tag{5.11}$$

$$X_a(2n+1) = X_a(n) \cdot X_a(n+1) - a. \tag{5.12}$$

$$Y_a(2n) = X_a(n) Y_a(n), \tag{5.13}$$

$$Y_a(2n+1) = X_a(n) \cdot Y_a(n+1) - 1. \tag{5.14}$$

With equations (5.11) - (5.14), instead of storing pairs of variables such as (x, y)

in two copies, (x, y) and (x', y'), we will store a quadruple of variables (x, y, x', y') (fortunately not in two copies).

The algorithm for computing $rem(Y_a(k), m)$ and $rem(X_a(k), m)$ using (5.11) - (5.14) begins as before by computation of the sequence b_i (or sequences b_i and c_i), $i = 0, 1, \cdots, l$, where again $l = \lfloor log_2(n) + 1 \rfloor$ is the length of n. One then initializes the variables x, y, x', y' by setting them to $x = 2, x' = a, y = 0$, and $y' = 1$. One lets i run from 1 to l, and, in accordance with (5.11) - (5.14), modifies $x, x'y, y'$ as follows, depending on c_i:

When c_i is even, we put

(5.15) $$y' = x \cdot y' - 1, \quad y = x \cdot y, \quad x' = x \cdot x' - a, \quad x = x \cdot x - 2,$$

When c_i is odd, we put

(5.16) $$y = x \cdot y' - 1, \quad y' = x' \cdot y', \quad x = x \cdot x' - a, \quad x' = x' \cdot x' - 2.$$

Continue this. After exiting the loop, the values of x and y are $X_a(n)$ and $Y_a(n)$ respectively. Normally we compute (5.15) and (5.16) mod m. In this case we have $x \equiv X_a(n) \pmod{m}$ and $y \equiv Y_a(n) \pmod{m}$.

Many modifications and simplifications are possible. For example, we need not store the actual values of the sequence b_i. It is of course enough to store only the remainders mod 2 of these values. Also the second sequence c_i is not needed. One can equally well test whether b_{l-i} is even or odd and let i run from $l - 1$ to 0.

What is the computation time for this algorithm? Using the standard algorithms for arithmetic mentioned above, the cost is $O(||n||^3)$ bit operations. $O(||n||)$ operations are needed initially to obtain the sequence b_i. We then have $l = ||n||$ evaluations of the functions $V_a(c_i, x, y)$ and $U_a(c_i, x, y)$, where x and y are always of size $< ||m||$. Using the estimate $O(||m||^2)$ for the additions, subtractions and

multiplications of numbers of size $\leq ||m||$, we find that $O(||n|| \cdot ||m||^2) = O(||n||^3)$ bit operations are sufficient in total.

§6. Laws of apparition and repetition

In this section, we study some classical properties of primes and Lucas sequences. Many of these properties were known to E. Lucas [31] [32] and D.H. Lehmer [26] [27]. Based on the results in this section, various kinds of Lucas pseudoprimes will be defined in §7. First we give the definition of ranks.

Definition 6.0. Let n be a positive integer. The rank of apparition of n in the sequence Y_a is the least positive integer r such that $n \mid Y_a(r)$. We denote the rank of n by $r_a(n)$.

We first prove that the rank exists.

Lemma 6.1. Suppose $a \geq 2$. For any positive n the rank $r_a(n)$ exists.

Proof. Suppose a positive integer n is given. By (1.35) or (1.36) we know that the equation $x^2 - dy^2 = 4$ has infinitely many solutions if $d \neq \square$. Hence $x^2 - (a^2-4)n^2y^2 = 4$ has infinitely many solutions since $(a^2-4)n^2 \neq \square$. Let x, y be a nontrivial solution of $x^2 - (a^2-4)n^2y^2 = 4$, i.e. $y > 0$. Then $X = x, Y = ny$ is a nontrivial solution of the equation $X^2 - (a^2-4)Y^2 = 4$. By (1.35) there exists a $k > 0$ such that $Y = Y_a(k)$. Hence there is a $k > 0$ such that $ny = Y_a(k)$ and therefore $n \mid Y_a(k)$. Choosing the least such positive k we get the rank of n.

Lemma 6.2. For any n, (i) $a \equiv \pm b \pmod{n} \Rightarrow r_a(n) = r_b(n)$; (ii) $r_a(n) = r_{-a}(n)$.

Proof. (i) By Congruence Rules (4.2.1), for all k, we have
$a \equiv \pm b \pmod{n} \Rightarrow Y_a(k) \equiv \pm Y_b(k) \pmod{n}$. Hence for all k, $n \mid Y_a(k) \Leftrightarrow n \mid Y_b(k)$.
(ii) By (1.47) $Y_a(k) = (-1)^{k+1} Y_{-a}(k)$. Hence $r_a(n) = r_{-a}(n)$.

Lemma 6.3. For all m, n and $a \geq 2$, $r_a(m) \mid n \Leftrightarrow m \mid Y_a(n)$.

Proof.($\Rightarrow$). If $r_a(m) \mid n$, then $Y_a(r_a(m)) \mid Y_a(n)$ by the Division Theorem 4.11. But by definition we have $m \mid Y_a(r_a(m))$. Hence $m \mid Y_a(n)$.

($\Leftarrow$). Suppose $m \mid Y_a(n)$. Let $r = r_a(m)$. Write $n = rq + s$ where $0 \leq s < r$. By the Addition Law (3.3), $2Y_a(s) = 2Y_a(n - rq) = Y_a(n)X_a(rq) - X_a(n)Y_a(rq)$. Then $m \mid Y_a(r)$ and $Y_a(r) \mid Y_a(rq)$ imply $m \mid Y_a(rq)$. Hence $m \mid 2Y_a(s)$. We claim that $m \mid Y_a(s)$. If m is odd this is obvious. Suppose m is even. Then by Parity Lemma 4.7 $Y_a(n)$ is even and hence $X_a(n)$ is even. Also $m \mid Y_a(rq)$ implies that $Y_a(rq)$ is even. Again by the Parity Lemma $X_a(rq)$ is even. Therefore from above, we have

$$Y_a(s) = Y_a(n)(X_a(rq)/2) - (X_a(n)/2)Y_a(rq) \equiv 0 - 0 = 0 \pmod{m}.$$

Since $0 \leq s < r$ and r is the rank of m, we have $s = 0$. Hence $n = rq$ so that $r \mid n$. The lemma is proved.

Corollary 6.4. For any n, m and $a \geq 2$ if $m \mid n$, then $r_a(m) \mid r_a(n)$.

Proof. If $m \mid n$, then $m \mid Y_a(r_a(n))$ since $n \mid Y_a(r_a(n))$. So by Lemma 6.3 $r_a(m) \mid r_a(n)$.

Theorem 6.5. Law of Repetition for primes. (Lucas [32] Lehmer [27].) Let p be any prime, $2 \leq a$ and $0 \leq j$. Then

(i) For any $k,\ 1 \leq i, \qquad p^i \mid Y_a(n) \Rightarrow p^{i+j} \mid Y_a(nkp^j)$,

(ii) For $(k,p) = 1,\ 1 \leq i, \qquad p^i \| Y_a(n) \Rightarrow p^{i+j} \| Y_a(nkp^j)$.

Proof. (i) and (ii) follow by induction on i from

(i') For any $k,\ 1 \leq i, \qquad p^i \mid Y_a(n) \Rightarrow p^{i+1} \mid Y_a(nkp)$,

(ii') For $(k,p) = 1,\ 1 \leq i, \qquad p^i \| Y_a(n) \Rightarrow p^{i+1} \| Y_a(nkp)$.

We can prove (i') and (ii') by using (4.23) when k is odd and (4.24) when k is even,

k odd $\Rightarrow Y_a(nkp) \equiv kp \cdot Y_a(n) \pmod{Y_a(n)^3}$,

k even $\Rightarrow Y_a(nkp) \equiv \frac{1}{2}kp \cdot X_a(n)Y_a(n) \pmod{Y_a(n)^3}$.

This completes the proof.

Lemma 6.6. Suppose p is an odd prime, $(p,d)=1$, $1 \leq e < c$ and $0 \leq f$. Then

$$p^e \,|\, Y_a(r_a(p^c)) \Rightarrow r_a(p^{e+f}) \,|\, p^f \cdot r_a(p^c), \quad p^e \,||\, Y_a(r_a(p^c)) \Rightarrow r_a(p^{e+f}) = p^f \cdot r_a(p^c).$$

Proof. $(p,d)=1 \Rightarrow (p, r_a(p))=1$. (See Corollary 6.12.1.) The first is by the Law of Repetition 6.5 with $k=1$ and $n = r_a(p^c)$. For the second we use $(p, r_a(p))=1$ to show first $r_a(p^c) = r_a(p^e)$. Then by the Law of Repetition, we obtain $r_a(p^{e+f}) = p^f \cdot r_a(p^c)$.

Lemma 6.7. Suppose $p > 3$ and $(p,d) = 1$. If $r_a(p^2) = ps$, then for all $e \geq 0$, $r_a(p^{e+1}) = p^e s$. Conversely if there exists e, $1 \leq e$ and $r_a(p^{e+1}) = p^e s$, then $r_a(p^2) = ps$ and $r_a(p) = s$.

Proof. Since $p^2 \,|\, Y_a(ps)$, we have $p \,|\, Y_a(ps)$ and so $r_a(p) \,|\, ps$. It follows that $r_a(p) \,|\, s$ since $(r_a(p), p) = 1$. By the Law of Repetition 6.5 $p \,|\, Y_a(r_a(p))$ implies $p^2 \,|\, Y_a(p \cdot r_a(p))$ so that $r_a(p^2) \,|\, p \cdot r_a(p)$. But $r_a(p^2) = ps$. Hence $ps \,|\, p \cdot r_a(p)$ and therefore $s \,|\, r_a(p)$. Consequently $r_a(p) = s$. Then we have $r_a(p) = s$ and $r_a(p^2) = ps$. It follows that $r_a(p^3) = p^2 s$ since $p \,||\, Y_a(s) \Rightarrow p^2 \,||\, Y_a(ps) \Rightarrow p^3 \,||\, Y_a(p^2 s)$, etc., by the Law of Repetition. Therefore $p^{e+1} \,||\, Y_a(p^e s)$ and $r_a(p^{e+1}) = p^e s$ for all $e \geq 0$. The converse may be proved by induction. The lemma has the following generalization.

Lemma 6.7.1. Suppose $p > 3$, $(p,d) = 1$ and $1 \leq c$. $r_a(p^{c+1}) = ps$ implies that $\forall e \geq 0 \, [r_a(p^{c+e}) = p^e s]$. Conversely if there exists e, $1 \leq e$ and $r_a(p^{c+e}) = p^e s$, then $r_a(p^{c+1}) = ps$ and for all $1 \leq i \leq c$, $r_a(p^i) = s$.

How large is the rank of n? The rank of an arbitrary integer is very hard to calculate. To estimate the rank we will define a function $T_a(n)$ such that $r_a(n) \mid T_a(n)$ (analogous to Euler's ϕ fuction). T_a is called the *totient.*

Definiton 6.8. The totient of n corresponding to a, written $T_a(n)$, is defined by:

$T_a(1) = 1$. $T_a(2) = 2$ if a is even, $T_a(2) = 3$ if a is odd.

For an odd prime p, we define

$T_a(p) = p$ if $p \mid a^2-4$ and $T_a(p) = (p-\epsilon)/2$ if $(p,(a^2-4)) = 1$ where $\epsilon = \left(\frac{a^2-4}{p}\right)$.

For all primes p (including $p = 2$),

$T_a(p^{e+1}) = T_a(p) \cdot p^e$

$T_a(p_1^{e_1} \cdots p_k^{e_k}) = [\, T_a(p_1^{e_1}), \cdots, T_a(p_k^{e_k}) \,]$.

We will see later that for each integer n, $n \mid Y_a(T_a(n))$. With this, we shall prove some lemmas and theorems of Lehmer.

Lemma 6.9. Suppose n is odd, $a \geq 2$ and $d = a^2 - 4 \neq \square$. Then

$$(6.9)\quad 2^{n-1}X_a(n) = \binom{n}{1} a^1 d^{\frac{n-1}{2}} + \binom{n}{3} a^3 d^{\frac{n-3}{2}} + \cdots + \binom{n}{n-2} a^{n-2} d^1 + \binom{n}{n} a^n d^0.$$

Proof. From the identity (1.36) we have

$$\frac{X_a(n) + Y_a(n)\sqrt{a^2-4}}{2} = \left(\frac{a+\sqrt{a^2-4}}{2}\right)^n = 2^{-n}(a+\sqrt{d})^n.$$

This implies $2^{n-1}X_a(n) + 2^{n-1}Y_a(n)\sqrt{d} = (a+\sqrt{d})^n$. Expanding $(a+\sqrt{d})^n$ by the Binomial Theorem and equating rational parts we obtain

$$2^{n-1}X_a(n) = \sum_{i=0,\, i\ odd}^{n} \binom{n}{i} a^i \sqrt{d}^{n-i} = \sum_{j=0}^{(n-1)/2} \binom{n}{2j+1} a^{2j+1} d^{(n-2j-1)/2}.$$

Lemma 6.9.1. Suppose n is odd, $a > 2$ and $d = a^2 - 4 \neq \square$. Then

$$(6.9.1)\quad 2^{n-1}Y_a(n) = \binom{n}{0} a^0 d^{\frac{n-1}{2}} + \binom{n}{2} a^2 d^{\frac{n-3}{2}} + \cdots + \binom{n}{n-3} a^{n-3} d^1 + \binom{n}{n-1} a^{n-1} d^0.$$

Proof. By solving for $2^{n-1}Y_a(n)$ instead of $2^{n-1}X_a(n)$ in the expansion of $(a+\sqrt{d})^n$ we get

$$2^{n-1}Y_a(n) = \sum_{i=0,\, i\ even} \binom{n}{i} a^i \sqrt{d}^{n-i-1} = \sum_{j=0}^{(n-1)/2} \binom{n}{2j} a^{2j} \sqrt{d}^{n-2j-1},$$

after dividing by $\sqrt{d}$. This proves the lemma.

Using such expansions D.H. Lehmer proved the following theorems.

Theorem 6.10. (Lehmer [27]). Suppose n is an odd prime, $0 < d$ and $d \neq \square$. Then $X_a(n) \equiv a \pmod{n}$.

Proof. If $a=0$ or $a=1$, the theorem follows from (3.12), (3.14) and Lemma 3.13. If $a=2$, the conclusion follows from $X_2(n)=2$. Assume $a>2$, then $0 < d$ and $d \neq \square$. Hence we may apply Lemma 6.9. Since n is prime, $n \mid \binom{n}{k}$ holds for all k such that $1 \leq k \leq n-1$. Then by Lemma 6.9 we have

$$2^{n-1}X_a(n) \equiv \binom{n}{n} a^n d^0 = a^n \pmod{n}.$$

Now applying Fermat's Theorem, $2^{n-1} \equiv 1 \pmod{n}$ and $a^n \equiv a \pmod{n}$, we have $X_a(n) \equiv a^n \equiv a \pmod{n}$, which proves the theorem.

REMARK. The proof generalizes to any Lucas sequence. If V_n and U_n are defined by (1.8), (1.9) and $A \neq 0$, $B \neq 0$, $0 < D = A^2 - 4B \neq \square$ and n is an odd prime, then $V_n \equiv A \pmod{n}$.

Theorem 6.11. (Lehmer [27]) If n is an odd prime, $(n,d) = 1$ and $d = a^2 - 4 \neq \square$, then $Y_a(n) \equiv \epsilon_a \pmod{n}$.

Proof. If $a = 0$ or $a = 1$, then the result follows from (3.12), (3.14) and Lemma 3.13. If $a = 2$, then the condition $(n,d) = 1$ does not hold. Assume $a > 2$, then $0 < d = a^2 - 4 \neq \square$. Hence we may apply Lemma 6.9.1. Since n is prime,

$n \mid \binom{n}{k}$ holds for all k such that $1 \leq k \leq n-1$. Then by Lemma 6.9 we have $2^{n-1}Y_a(n) \equiv \binom{n}{0} a^0 d^{\frac{n-1}{2}} = d^{\frac{n-1}{2}} \pmod{n}$.

Applying Fermat's Theorem $2^{n-1} \equiv 1 \pmod{n}$ and Euler's Criterion $d^{\frac{n-1}{2}} \equiv (d/n) = \epsilon \pmod{n}$, we obtain $Y_a(n) \equiv d^{\frac{n-1}{2}} \equiv \epsilon \pmod{n}$ which proves the theorem.

This proof generalizes to any Lucas sequence V_n and U_n defined by (1.10) (i) (ii). If $P \neq 0$, $Q \neq 0$, $0 < D \neq \square$, $(n, D) = 1$ and n is an odd prime, then $U_n \equiv \epsilon \pmod{n}$ where $\epsilon = (D/n)$ and $D = P^2 - 4Q$.

REMARK. The converses of Theorem 6.10 and Theorem 6.11 do not hold. Also $X_a(n) \equiv a \pmod{n}$ and $Y_a(n) \equiv \epsilon_a \pmod{n}$ are independent of each other, even when $(n, 2ad) = 1$. As examples we may take $n = 115 = 5 \cdot 23$, $a = 41$ or take $n = 119 = 7 \cdot 17$, $a = 6$.

The following theorem was also known to D.H. Lehmer.

Theorem 6.12. If n is an odd prime, $(n, d) = 1$ and $d = a^2 - 4$ and $\epsilon = (d/n)$, then we have $Y_a(n - \epsilon) \equiv 0 \pmod{n}$. Furthermore, we have $Y_a((n - \epsilon)/2) \equiv 0 \pmod{n}$.

Proof. By identity (3.71) and Theorems 6.10, 6.11:

$$2Y_a(n - \epsilon) = -\epsilon X_a(n) + aY_a(n) \equiv -\epsilon a + a\epsilon = 0 \pmod{n}.$$

Hence $Y_a(n - \epsilon) \equiv 0 \pmod{n}$. By (3.89) and (3.84)

$$X_a\left(\frac{n-\epsilon}{2}\right) Y_a\left(\frac{n-\epsilon}{2}\right) = Y_a(n - \epsilon) \equiv 0 \pmod{n} \quad \text{and}$$

$$X_a\left(\frac{n-\epsilon}{2}\right) X_a\left(\frac{n+\epsilon}{2}\right) = X_a(n) + a \equiv a + a = 2a \pmod{n}.$$

If $(n, a) = 1$, then the second congruence implies $(n, X_a((n - \epsilon)/2)) = 1$. Hence the first congruence implies $n \mid Y_a((n - \epsilon)/2)$. If $n \mid a$, then

$$\epsilon = (-4/n) = (-1/n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv -1 \pmod 4 \end{cases}$$

Hence $n \equiv \epsilon \pmod 4$ so that $(n-\epsilon)/2$ is even. Then by the Division Theorem and since $a = Y_a(2)$ and $n \mid a$, it follows that $n \mid Y_a((n-\epsilon)/2)$. This completes the proof.

Corollary 6.12.1. If p is an odd prime, $(p,d) = 1$ and $\epsilon = (d/p)$, then $r_a(p) \mid (p-\epsilon)/2$. and $r_a(p^e) \mid p^{e-1}(p-\epsilon)/2$. Hence $(p, r_a(p)) = 1$.

Proof. The conclusion $r_a(p) \mid (p-\epsilon)/2$ follows from Theorem 6.12. And the conclusion $r_a(p^e) \mid p^{e-1}(p-\epsilon)/2$ follows from Theorem 6.12 and the Law of Repetition 6.5.

Lemma 6.13. Suppose p is an odd prime, $(p,s) = 1$, $1 < s$ and $1 \le i < e$. Then

(i) $r_a(p^e) = s \Rightarrow s \mid (p-\epsilon)/2$ for some $\epsilon = \pm 1$,

(ii) $r_a(p^e) = s \Rightarrow r_a(p) = s$,

(iii) $r_a(p^e) = s \Rightarrow r_a(p^i) = s$,

(iv) $r_a(p) = s$ and $p^e \| Y_a(p^i s) \Rightarrow r_a(p^e) = p^i s$,

(v) $(r_a(p^e), p) = 1 \Rightarrow r_a(p^e) = r_a(p^i) = r_a(p)$,

(vi) $r_a(p) = s \Rightarrow r_a(p^e) = p^j s$ for some j, $1 \le j < e$.

Proof. (i) follows from Corollary 6.12.1 and the GCD Theorem 4.16. To prove (ii), suppose $r_a(p^e) = s$. Put $r = r_a(p)$. Then $r \mid s$ by Corollary 6.4.1. $p \mid Y_a(r)$ implies $p^e \mid Y_a(p^{e-1}r)$ by the Law of Repetition. Hence $s \mid p^{e-1}r$. But $(p,s) = 1$. Hence $s \mid r$. Since $r \mid s$, this implies $r = s$. Proofs of (iii) and (vi) are similar. (v) is a restatement of (iii) and (ii). For (iv), consider two cases according as $i = 0$ or $i \ge 1$. If $i = 0$, the implication is trivial. If $i \ge 1$, then we have $p^e \not| Y_a(p^{i-1}s)$, by the Law of Repetition.

Lemma 6.14. If p is a prime and $p \mid d$, then $p \mid Y_a(p)$. More generally, if $p^e \mid n$ and $p \mid d$, then $Y_a(n) \equiv 0 \pmod{p^e}$.

Proof. Suppose p is an odd prime, $p \mid d$ where $d = a^2 - 4$ and $p^e \mid n$. Then since $d = (a+2)(a-2)$ and $(a+2, a-2) \mid 4$, $p \mid a-2$ or $p \mid a+2$. By (4.2.1) $a \equiv \pm 2 \pmod{p^e}$ implies $Y_a(p) \equiv \pm Y_2(p) = \pm p \equiv 0 \pmod{p}$. Hence $p \mid Y_a(p)$. Then by the Law of Repetition $p^e \mid Y_a(p^e)$. By the Division Theorem $p^e \mid n \Rightarrow Y_a(p^e) \mid Y_a(n)$. Hence $p^e \mid Y_a(n)$.

REMARK. It can be shown that if $p \mid d$ and $p > 3$, then $r_a(p^e) = p^e$. The proof uses the fact that if p is prime , $p > 3$ and $p \mid d$, then $2^{p-1} Y_a(p) \equiv p a^{p-1} \pmod{p^2}$. This congruence can be derived from Theorem 6.11.

The Lemma 6.14 also holds when $p = 2$. Suppose $p = 2$, $2 \mid d$ and $2^e \| n$ where $1 \leq e$. In this case $2 \mid d$ and $d = (a+2)(a-2)$ implies $2 \mid a$. Hence by the Law of Repetition, $2^e \mid Y_a(2^e)$. By the Division Theorem $2^e \mid n \Rightarrow Y_a(2^e) \mid Y_a(n)$. Hence $2^e \mid Y_a(n)$.

Corollary 6.14.1. Suppose $0 \leq i < e$, $1 < s$, $(p, s) = 1$ and $r_a(p^e) = p^i s$. Then $(p, a^2 - 4) = 1$.

Proof. Suppose $(p, a^2 - 4) > 1$. Then $p \mid a^2 - 4$. Put $n = p^e$ in Lemma 6.14 which implies that $r_a(p^e) \mid p^e$. Since $r_a(p^e) = p^i s$, we then have $s \mid p^e$. This contradicts the hypothesis that $1 < s$, $(p, s) = 1$. Hence $(p, a^2 - 4) = 1$.

Theorem 6.15. $n \mid Y_a(T_a(n))$. Equivalently $r_a(n) \mid T_a(n)$.

Proof. Let $n = p_1^{e_1} \cdots p_k^{e_k}$. If $(p_i, a^2 - 4) = 1$, by Theorem 6.12, $p \mid Y_a((p_i - \epsilon_i)/2)$. Since in this case, $T_a(p_i) = (p_i - \epsilon)/2$, $p_i \mid Y_a(T_a(p_i))$. Then by the Law of Repetition 6.5, for $1 \leq i \leq k$, $p_i^{e_i} \mid Y_a\left(p_i^{e_i - 1} \frac{p_i - \epsilon_i}{2}\right) = Y_a(T_a(p_i^{e_i}))$. So we have

$p_i^{e_i} \mid Y_a([T_a(p_1^{e_1}),\cdots,T_a(p_k^{e_k})]) = Y_a(T_a(n))$. Hence $n \mid Y_a(T_a(n))$. If $p_i \mid a^2-4$, then by Lemma 6.14, $p_i \mid Y_a(p_i)$. Since in this case $T_a(p_i) = p_i$ and $p_i \mid Y_a(T_a(p_i))$, by the Law of Repetition 6.5, we have $p_i^{e_i} \mid Y_a(p_i^{e_i})$, i.e. $p_i^{e_i} \mid Y_a(T_a(p_i^{e_i}))$. Hence $p_i^{e_i} \mid Y_a([T_a(p_1^{e_1}),\cdots,T_a(p_k^{e_k})]) = Y_a(T_a(n))$. Since this holds for each $p_i^{e_i} \mid n$, we then have $n \mid Y_a(T_a(n))$. This proves the theorem in either case.

Corollary 6.15.1. Let p be an odd prime. Then $(p, a^2-4) = 1$ if and only if

$$r_a(p^e) \mid p^{e-1}((p-\epsilon_a(p))/2).$$

Lemma 6.16. Suppose $2 \le k$, $\delta_i = \pm 1$, $3 \le m_i$ and $m_i \ne m_j$ for $i \ne j$. Then

$$\prod_{i=1}^{k}\left(\frac{m_i-\delta_i}{2}\right) < \frac{(\prod_{i=1}^{k} m_i)-1}{2}. \tag{6.16}$$

Proof. Induction on k. To make the notation simple let LHS denote $\prod_{i=1}^{k}((m_i-\delta_i)/2)$ and RHS denote $((\prod_{i=1}^{k} m_i)-1)/2$. For case $k=2$,

$$\text{LHS} = \frac{m_1-\delta_1}{2}\,\frac{m_2-\delta_2}{2} = \frac{m_1m_2-m_1\delta_2-m_2\delta_1+\delta_1\delta_2}{4} \le \frac{m_1m_2+m_1+m_2+1}{4}.$$

$$\text{RHS} = \frac{m_1m_2-1}{2}.$$

$$\text{RHS} - \text{LHS} \ge \frac{m_1m_2-1}{2} - \frac{m_1m_2+m_1+m_2+1}{4} = \frac{m_1m_2-(m_1+m_2+3)}{4} > 0.$$

Hence (6.16) holds for $k=2$. Suppose (6.16) holds for $k \ge 2$. Consider $k+1$.

$$\text{LHS} = \frac{m_{k+1}-\delta_{k+1}}{2}\prod_{i=1}^{k}\left(\frac{m_i-\delta_i}{2}\right) < \frac{m_{k+1}-\delta_{k+1}}{2}\,\frac{(\prod_{i=1}^{k} m_i)-1}{2}$$

$$= \frac{m_{k+1}\prod_{i=1}^{k} m_i - m_{k+1} - \delta_{k+1}\prod_{i=1}^{k} m_i + \delta_{k+1}}{4} = \frac{\prod_{i=1}^{k+1} m_i - m_{k+1} - \delta_{k+1}(\prod_{i=1}^{k} m_i - 1)}{4}$$

$$\le \frac{\prod_{i=1}^{k+1} m_i - m_{k+1} + \prod_{i=1}^{k} m_i - 1}{4} \le \frac{2\prod_{i=1}^{k+1} m_i - 4}{4} = \frac{\prod_{i=1}^{k+1} m_i - 2}{2} = \text{RHS}.$$

Hence (6.16) holds for $k+1$. The lemma is proved.

Theorem 6.17. Suppose n is odd. Then n is prime $\Leftrightarrow (n-\epsilon)/2 = T_a(n)$ and also n is prime $\Leftrightarrow (n-\epsilon)/2 \mid T_a(n)$, where $\epsilon = ((a^2-4)/n)$.

Proof. ($\Rightarrow$) By definition of $T_a(n)$.

($\Leftarrow$) Suppose n is not prime. Case (1). $n = p^e$ with $e \geq 2$. Then

$$T_a(n) = p^{e-1}\frac{p-\epsilon(p)}{2} \neq \frac{p^e-\epsilon(p^e)}{2}, \text{ also } \frac{p^e-\epsilon(p^e)}{2} \nmid p^{e-1}\frac{p-\epsilon(p)}{2}.$$

Case (2). $n = p_1^{e_1}\dots p_k^{e_k}$ where $k \geq 2$. Then using Lemma 6.16 we have

$$T_a(n) = [T_a(p_1^{e_1}),\dots,T_a(p_k^{e_k})] = \left[p_1^{e_1-1}\frac{p_1-\epsilon_1(p_1)}{2},\dots,p_k^{e_k-1}\frac{p_k-\epsilon_k(p_k)}{2}\right]$$

$$= p_1^{e_1-1}\cdots p_k^{e_k-1}\left[\frac{p_1-\epsilon_1}{2},\dots,\frac{p_k-\epsilon_k}{2}\right] \leq p_1^{e_1-1}\cdots p_k^{e_k-1}\prod_{i=1}^{k}\left(\frac{p_i-\epsilon_i}{2}\right)$$

$$< p_1^{e_1-1}\cdots p_k^{e_k-1}\frac{(\prod_{i=1}^k p_i)-1}{2} = \frac{(\prod_{i=1}^k p_i^{e_i})-p_1^{e_1-1}\cdots p_k^{e_k-1}}{2} \leq \frac{n-1}{2} \leq \frac{n-\epsilon(n)}{2}.$$

Hence $T_a(n) \neq (n-\epsilon)/2$ and $(n-\epsilon)/2 \nmid T_a(n)$. This completes the proof.

Theorem 6.18. Suppose $(n, 2a(a^2-4)) = 1$ and $\epsilon = ((a^2-4)/n)$. If $(n-\epsilon)/2 \mid r_a(n)$ or $(n-\epsilon)/2 = r_a(n)$, then n is prime.

Proof. Suppose $(n-\epsilon)/2 \mid r_a(n)$ or $(n-\epsilon)/2 = r_a(n)$. By Theorem 6.15 $r_a(n) \mid T_a(n)$. Hence $(n-\epsilon)/2 \mid T_a(n)$. By Theorem 6.17 this implies that n is prime.

Lemma 6.19. Suppose $(n, 2a(a^2-4)) = 1$, $\epsilon = ((a^2-4)/n)$, $4 \mid n-\epsilon$ and $n-\epsilon = 2^e$ for some e. Then $Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod{n}$ and $Y_a\left(\frac{n-\epsilon}{4}\right) \not\equiv 0 \pmod{n} \Rightarrow n$ is prime.

Proof. By assumption we are given $r_a(n) \mid (n-\epsilon)/2$ and $r_a(n) \nmid (n-\epsilon)/4$. Since $(n-\epsilon)/2$ is a power of 2, $r_a(n) = (n-\epsilon)/2$. Then by Lemma 6.11, n is a prime.

Lemma 6.20. Suppose n is odd, $\epsilon = \pm 1$ and $4 \mid n-\epsilon$. Then

$$Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod{n} \text{ and } (n, Y_a\left(\frac{n-\epsilon}{4}\right)) = 1 \quad \Leftrightarrow \quad n \mid X_a\left(\frac{n-\epsilon}{4}\right).$$

Proof. ($\Leftarrow$). By identity (3.93) $Y_a((n-\epsilon)/2) = Y_a((n-\epsilon)/4)X_a((n-\epsilon)/4)$, and also by coprimality of $Y_a((n-\epsilon)/4)$ and $X_a((n-\epsilon)/4)$.

($\Rightarrow$). By identity (3.93).

Lemma 6.21. Suppose $(n, 2a(a^2-4)) = 1, \epsilon = ((a^2-4)/n), 4 | n-\epsilon$ and $n-\epsilon = 2^e$ for some e. Then $n \mid X_a\left(\frac{n-\epsilon}{4}\right) \Leftrightarrow$ n is prime and $r_a(n) = \frac{n-\epsilon}{2}$.

Proof. ($\Rightarrow$). By (3.93) and Lemma 6.13, n is prime and $r_a(n) = (n-\epsilon)/2$.

($\Leftarrow$). By identity (3.93) $Y_a((n-\epsilon)/2) = Y_a((n-\epsilon)/4)X_a((n-\epsilon)/4)$ we have $n \mid X_a\left(\frac{n-\epsilon}{4}\right)$.

Lemma 6.22. Suppose $(n, 6) = 1$. If $p^2 \mid n$ for some prime p, then it is possible to find at least two a such that $2 < a < n-2, (n, a(a^2-4)) = 1$, and $p | r_a(p^2)$, (actually $r_a(p^2) = 3p$ and hence $r_a(p^{e+1}) = 3p^e$ for all $e \geq 0$). For such an a we have the following:

$$Y_a(n)^2 \not\equiv 1 \pmod{p^2}, \qquad Y_a(n \pm 1) \not\equiv 0 \pmod{p^2},$$
$$Y_a((n \pm 1)/2) \not\equiv 0 \pmod{p^2}, \quad Y_a((n-1)/2) \not\equiv 0 \pmod{p^2},$$
$$Y_a((n+1)/2) \not\equiv 0 \pmod{p^2}, \quad Y_a((n \pm 1)/2)^2 \not\equiv 1 \pmod{p^2},$$
$$X_a(n)^2 \not\equiv a^2 \pmod{p^2}, \qquad X_a((n \pm 1)/2)^2 \not\equiv a^2 \pmod{p^2}.$$

Proof. Suppose $(n, 6) = 1$, $p^2 | n$ and p is prime. Let j be the product of the other primes dividing n (1 if there are none). Put $a = jp \pm 1$. Then $a-2 = jp-1$ and $a+2 = jp+3$ or $a-2 = jp-3$ and $a+2 = jp+1$. Since $(n, 3) = 1$, we have $(a+2, n) = 1$ and $(a-2, n) = 1$. Hence $(a^2-4, n) = 1$ so that $(n, a(a^2-4)) = 1$. Then $Y_a(3) = a^2 - 1 = (jp \pm 1)^2 - 1 = j^2p^2 \pm 2jp = jp(jp \pm 2)$. Hence we have $r_a(p) = 3$ so that $r_a(p^2) = 3p$ by the Law of Repetition. Therefore $p \mid r_a(p^2)$ and also $r_a(p^{e+1}) = 3p^e$.

Suppose $p^2 \mid Y_a(n \pm 1)$ or $p^2 \mid Y_a(n)^2 - 1$. Then from (3.28) we would have $Y_a(n-1)Y_a(n+1) = Y_a(n)^2-1 \equiv 0 \pmod{p^2}$. By the GCD Theorem the two terms on the left are not both divisible by p, since $(n+1, n-1) = 2$, $Y_a(2) = a$ and $(p, a) = 1$.

Consequently $p^2 \mid Y_a(n \pm 1)$. Hence $r_a(p^2) \mid n \pm 1$. But $p \mid r_a(p^2)$. Hence $p \mid n \pm 1$, contradicting $p|n$. Thus $Y_a(n \pm 1)^2 \not\equiv 0 \pmod{p^2}$ and $Y_a(n)^2 \not\equiv 1 \pmod{p^2}$.

To show $X_a(n)^2 \not\equiv a^2 \pmod{p^2}$ and $X_a((n \pm 1)/2)^2 \not\equiv a^2 \pmod{p^2}$, we will use (3.28′) and (3.99). By (3.99) we have that if $X_a((n \pm 1)/2)^2 \equiv a^2 \pmod{p^2}$, then $p^2 \mid Y_a(\frac{n\pm1}{2} \pm 1)$. Hence $r_a(p^2) \mid \frac{n\pm1}{2} \pm 1$. Since $p \mid r_a(p^2)$, it follows that $p \mid \frac{n\pm1}{2} \pm 1$ which contradicts $p|n$. The proof for $X_a(n)^2 \not\equiv a^2 \pmod{p^2}$ is the same.

Lemma 6.23. SQUAREFREE LEMMA. Suppose $(n, 6) = 1$. If any one of the following congruences holds for all a, $1 \leq a < n$ such that $(n, a(a^2 - 4)) = 1$, then n is squarefree:

(1) $Y_a^2(n) \equiv 1 \pmod{n}$, (2) $Y_a(n-1) \equiv 0 \pmod{n}$,

(3) $Y_a(n+1) \equiv 0 \pmod{n}$, (4) $Y_a(n \pm 1) \equiv 0 \pmod{n}$,

(5) $Y_a((n-1)/2) \equiv 0 \pmod{n}$, (6) $Y_a((n+1)/2) \equiv 0 \pmod{n}$,

(7) $Y_a((n \pm 1)/2) \equiv 0 \pmod{n}$, (8) $Y_a((n \pm 1)/2)^2 \equiv 1 \pmod{n}$,

(9) $X_a(n)^2 \equiv a^2 \pmod{n}$, (10) $X_a((n \pm 1)/2)^2 \equiv a^2 \pmod{n}$.

Proof. It follows directly from Lemma 6.22.

In the following theorem we give several equivalent congruences.

Theorem 6.24. Let $d = a^2 - 4$. For $(n, 2ad) = 1$ and $\epsilon = (d/n)$, the following statements are equivalent:

(*i*) $X_a(n) \equiv a \pmod{n}$ and $Y_a(n) \equiv \epsilon \pmod{n}$,

(*ii*) $X_a(n+\epsilon) \equiv a^2 - 2 \pmod{n}$ and $Y_a(n+\epsilon) \equiv a\epsilon \pmod{n}$,

(*iii*) $X_a(n-\epsilon) \equiv 2 \pmod{n}$ and $Y_a(n-\epsilon) \equiv 0 \pmod{n}$,

(*iv*) $$Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod{n},$$

$$(v) \qquad 2X_a\left(\frac{n+\epsilon}{2}\right) \equiv aX_a\left(\frac{n-\epsilon}{2}\right) \pmod{n},$$

$$(vi) \qquad 2Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \epsilon X_a\left(\frac{n-\epsilon}{2}\right) \pmod{n},$$

$$(vii) \qquad aY_a\left(\frac{n+\epsilon}{2}\right) \equiv \epsilon X_a\left(\frac{n+\epsilon}{2}\right) \pmod{n},$$

$$(viii) \quad X_a(n+\epsilon) \equiv a^2-2 \pmod{n} \quad \text{and} \quad X_a(n-\epsilon) \equiv 2 \pmod{n},$$

$$(ix) \quad Y_a(n+\epsilon) \equiv a\epsilon \pmod{n} \quad \text{and} \quad Y_a(n-\epsilon) \equiv 0 \pmod{n}.$$

Proof. (i) $\Rightarrow$ (ii). By (3.68) we have $2X_a(n+\epsilon) = aX_a(n) + \epsilon dY_a(n) \equiv aa + \epsilon d\epsilon = a^2 + d = 2a^2 - 4 (\text{mod } n)$. Hence $X_a(n+\epsilon) \equiv a^2 - 2 (\text{mod } n)$. And by (3.69) we have $2Y_a(n+\epsilon) = \epsilon X_a(n) + aY_a(n) \equiv \epsilon a + a\epsilon = 2a\epsilon (\text{mod } n)$. Hence $Y_a(n+\epsilon) \equiv a\epsilon (\text{mod } n)$.

(ii) $\Rightarrow$ (iii). By (3.78) we have $2X_a(n-\epsilon) = (a^2-2)X_a(n+\epsilon) - \epsilon adY_a(n+\epsilon) \equiv (a^2-2)(a^2-2) - \epsilon ad\epsilon a = a^4 - 4a^2 + 4 - a^2(a^2-4) = 4 \pmod{n}$. Hence $X_a(n-\epsilon) \equiv 2 \pmod{n}$. By (3.79) we have $2Y_a(n-\epsilon) = -\epsilon aX_a(n+\epsilon) + (a^2-2)Y_a(n+\epsilon) \equiv -\epsilon a(a^2-2) + (a^2-2)a\epsilon = 0 \pmod{n}$. Thus $Y_a(n-\epsilon) \equiv 0 \pmod{n}$.

(iii) $\Rightarrow$ (iv). Since $X_a^2\left(\frac{n-\epsilon}{2}\right) = X_a(n-\epsilon) + 2 \equiv 2 + 2 = 4 \pmod{n}$, we have $(n, X_a((n-\epsilon)/2)) = 1$. Then $Y_a((n-\epsilon)/2)X_a((n-\epsilon)/2) = Y_a(n-\epsilon) \equiv 0 \pmod{n}$ implies that $Y_a((n-\epsilon)/2) \equiv 0 \pmod{n}$.

(iv) $\Rightarrow$ (i). By identities (3.85) and (3.87).

To finish the proof of 6.24, (iv) $\Leftrightarrow$ (v) follows from (3.80), (iv) $\Leftrightarrow$ (vi) follows from identity (3.81), (iv) $\Leftrightarrow$ (vii) follows from (3.83) and (viii) $\Leftrightarrow$ (ii) follows from (3.76) and (3.77). The proof is complete.

REMARK. That *(i)* - *(iv)* are equivalent does not need the hypothesis that $(n, a) = 1$.

Corollary 6.25. If n is an odd prime and $(n, d) = 1$, then n satisfies all the congruences in Theorem 6.24.

§7. Pseudoprimes related to the sequences $X_a(n)$ and $Y_a(n)$

In this section, we introduce several types of pseudoprimes related to the sequences $X_a(n)$ and $Y_a(n)$ and set forth the relationships among them. Some of these kinds of pseudoprimes are classical, like Lucas pseudoprimes (*lpsp*), Euler Lucas pseudoprimes (*elpsp*) and strong Lucas pseudoprimes (*slpsp*); some are new, like t - pseudoprimes (*tpsp*), a - pseudoprimes (*apsp*), r - pseudoprimes (*rpsp*) and extra strong Lucas pseudoprime (*slxpsp*).

A. Rotkiewicz [46] considered an odd composite number n to be a pseudoprime if n divided $U_{n-\epsilon}$ where U_k is defined by (1.10) (ii). Accordingly we will call a number n satisfying $Y_a(n-\epsilon_a) \equiv 0 \pmod{n}$, a Lucas pseudoprime in the sense of Rotkiewicz, or simply a Lucas pseudoprime. Normally we would suppose either $(n,(a^2-4))=1$ or $(n,a(a^2-4))=1$. However $(n,a^2-4)=1$ is implied by $Y_a(n-\epsilon_a(n)) \equiv 0 \pmod{n}$.

The congruences $Y_a(n-\epsilon_a(n)) \equiv 0 \pmod{n}$ and $Y_a(n) \equiv \epsilon_a(n) \pmod{n}$ are not equivalent. The example $n=77$ and $a=6$ shows that $Y_a(n-\epsilon_a) \equiv 0 \pmod{n}$ does not imply $Y_a(n) \equiv \epsilon_a \pmod{n}$. The example $n=115$ and $a=41$ shows that $Y_a(n) \equiv \epsilon_a \pmod{n}$ does not imply $Y_a(n-\epsilon_a) \equiv 0 \pmod{n}$. We will use the condition $Y_a(\frac{n-\epsilon_a}{2}) \equiv 0 \pmod{n}$, which is stronger than both of them. This condition is equivalent to the notation of Euler Lucas pseudoprime, *elpsp*, as defined by Baillie and Wagstaff [2]. There is another condition in turn stronger than this one, namely strong Lucas pseudoprime, *slpsp*, [2].

Suppose $n = u2^t + \epsilon_a$ is an odd prime, where u is odd and $(n,a^2-4)=1$. Applying Double Angle Formula (3.5) $t-1$ times to $Y_a(n-\epsilon_a)$, one obtains

$$(7.0)\quad 0 \equiv Y_a(n-\epsilon) = X_a\left(\frac{n-\epsilon}{2}\right) Y_a\left(\frac{n-\epsilon}{2}\right) = X_a\left(\frac{n-\epsilon}{2}\right) X_a\left(\frac{n-\epsilon}{4}\right) Y_a\left(\frac{n-\epsilon}{4}\right) =$$
$$\cdots = X_a\left(\frac{n-\epsilon}{2}\right) X_a\left(\frac{n-\epsilon}{4}\right) X_a\left(\frac{n-\epsilon}{8}\right) \cdots X_a\left(\frac{n-\epsilon}{2^t}\right) Y_a\left(\frac{n-\epsilon}{2^t}\right) \pmod{n}.$$

Hence one of the following conditions must be satisfied:

$$(i)\ \ (\exists i)\left[1 \le i \le t \text{ and } n \mid X_a\left(\frac{n-\epsilon}{2^i}\right)\right] \quad \text{or} \quad (ii)\ \ n \mid Y_a\left(\frac{n-\epsilon}{2^t}\right).$$

This condition gives a stronger primality test when $n \equiv \epsilon_a \pmod 4$.

Now we formalize the definitions used throughout this thesis. In the following d denotes $a^2 - 4$ and ϵ denotes the Jacobi symbol (d/n).

Definition 7.1. n is a *lpsp*(a) if $(n, 2d) = 1$ and $Y_a(n-\epsilon) \equiv 0 \pmod n$.

Definition 7.2. n is an *elpsp*(a) if $(n, 2d) = 1$ and $Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod n$.

Definition 7.3. Suppose $n = u2^t + \epsilon_a$ with u odd. Then n is a strong Lucas pseudoprime to the base a, *slpsp*(a), if $(n, 2d) = 1$ and n satisfies one of the following conditions:

$$(i)\ \ (\exists i)\left[1 \le i \le t \text{ and } n \mid X_a\left(\frac{n-\epsilon}{2^i}\right)\right] \quad \text{or} \quad (ii)\ \ n \mid Y_a\left(\frac{n-\epsilon}{2^t}\right).$$

From (3.96) $(X_a(k)+2)(X_a(k)-2) = dY_a(k)^2$ with k replaced by $(n-\epsilon)/2^t$, we can strengthen the condition 7.3 (ii) to get the following stronger type of pseudoprimes.

Definition 7.4. Suppose $n = u2^t + \epsilon_a$ with u odd. Then n is an extra strong Lucas pseudoprime to the base a, *slxpsp*(a), if $(n, 2d) = 1$ and n satisfies one of the following conditions:

$$(i)\qquad (\exists i)\left[1 \le i \le t \text{ and } n \mid X_a\left(\frac{n-\epsilon}{2^i}\right)\right] \quad \text{or}$$

$$(ii)\qquad n \mid Y_a\left(\frac{n-\epsilon}{2^t}\right) \text{ and } X_a\left(\frac{n-\epsilon}{2^t}\right) \equiv \pm 2 \pmod n.$$

Clearly $slxpsp(a) \Rightarrow slpsp(a)$. However the example, $n = 143$ and $a = 12$, shows that $slpsp(a) \not\Rightarrow slxpsp(a)$. By the Double Angle Formula, it is easy to see that $elpsp(a) \Rightarrow lpsp(a)$. The implication $slpsp(a) \Rightarrow elpsp(a)$ is due to Baillie and Wagstaff [2].

Theorem 7.5. (Baillie and Wagstaff [2]) n is a $slpsp(a) \Rightarrow n$ is an $elpsp(a)$. Further, If $n = u2 + \epsilon_a$ and u is odd, then n is a $slpsp(a) \Leftrightarrow n$ is an $elpsp(a)$.

Proof. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is a $slpsp(a)$. Let $n = u2^t + \epsilon_a(n)$ with u odd. Then $n \mid Y_a(u)$ or for some s, $0 \leq s \leq t-1$, $n \mid X_a(u2^s)$. Since $Y_a(u)$ and $X_a(u2^s)$ $(s \leq t-2)$ are factors of $Y_a(u2^{t-1}) = Y_a((n-\epsilon_a)/2)$, to show that n is $elpsp(a)$ we need only show that $n \nmid X_a(u2^{t-1})$. If $n \mid X_a(u2^{t-1})$, then for all $p_i \mid n$, $r_a(p_i) \mid u2^t$ and $r_a(p_i) \nmid u2^{t-1}$. This shows $2^t \| r_a(p_i)$ for all i $(i = 1,\ldots,k)$. However by Theorem 6.12 we have $2r_a(p_i) \mid p_i - \epsilon_a(p_i)$. Thus $p_i \equiv \epsilon_a(p_i) \pmod{2^{t+1}}$ $(i = 1,\ldots,k)$. Therefore

$$n = \prod_{i=1}^{k} p_i^{e_i} \equiv \prod_{i=1}^{k} \epsilon_a(p_i)^{e_i} = \epsilon_a(n) \pmod{2^{t+1}}$$

which contradicts our assumption $2^t \| n - \epsilon_a(n)$. Thus $n \nmid X_a(u2^{t-1})$ and hence n is an $elpsp(a)$. The second statement is true because $(n-\epsilon_a)/2$ is odd and then condition (ii) of Definiton 7.3 holds. Hence $slpsp(a) \Leftrightarrow elsps(a)$ in this case.

From Theorem 7.5, we have the following corollary.

Corollary 7.5.1. Suppose $n = u2^t + \epsilon_a(n)$ with u odd. Then n is $slpsp(a)$ if one of the following conditions holds:

$$(i)\ \ (\exists i)\left[2 \leq i \leq t \text{ and } n \mid X_a\left(\frac{n-\epsilon}{2^i}\right)\right] \quad \text{or} \quad (ii)\ \ n \mid Y_a\left(\frac{n-\epsilon}{2^t}\right).$$

Lemma 7.6. Suppose n is odd and a prime power. Then n is a *elpsp*(a) if and only if n is a *slpsp*(a).

Proof. By Theorem 7.5 we only need prove the implication $\Rightarrow$. Suppose $n = p^e$ and n is *elpsp*(a). Write $n = 2^t u + \epsilon$ where u is odd, $s \geq 1$ and $\epsilon = (d/p)$. Since $(X_a(\frac{n-\epsilon}{2^i}), X_a(\frac{n-\epsilon}{2^j})) \mid 2$ when $i \neq j$ and $(X_a(\frac{n-\epsilon}{2^i}), Y_a(\frac{n-\epsilon}{2^i})) \mid 2$ for all $i \leq t$, by (7.0) we have $p^e \mid X_a((n-\epsilon)/2^i)$ for some i or $p^e \mid Y_a((n-\epsilon)/2^t)$. Hence n is *slpsp*(a) by Definition 7.3.

The aforementioned are some classical types of Lucas pseudoprimes (except for *slxpsp*). Next we define some new types of pseudoprimes connected with the Lucas sequences X_a and Y_a. These are based on the binomial expansion and the identity

$$4(a \pm 2)\left(\frac{a + \sqrt{a^2 - 4}}{2}\right) = (a \pm 2 + \sqrt{a^2 - 4})^2. \tag{7.7}$$

Raising both sides of the identity to the n^{th} power, we obtain

$$4^n(a \pm 2)^n \left(\frac{a + \sqrt{a^2 - 4}}{2}\right)^n = (a \pm 2 + \sqrt{a^2 - 4})^{2n}. \tag{7.7.1}$$

Putting $d = a^2 - 4$ and applying (1.36) we have

$$4^n(a \pm 2)^n \left(\frac{X_a(n) + Y_a(n)\sqrt{d}}{2}\right) = (a \pm 2 + \sqrt{d})^{2n}. \tag{7.7.2}$$

Expanding the right side of (7.7.2) by the binomial theorem and solving respectively for $X_a(n)$ and $Y_a(n)$:

$$4^n(a \pm 2)^n X_a(n) = 2\sum_{i=0}^{n} \binom{2n}{2i} (a \pm 2)^{2n-2i} d^i. \tag{7.8}$$

$$4^n(a \pm 2)^n Y_a(n) = 2(a \pm 2)\sum_{i=1}^{n} \binom{2n}{2i-1} (a \pm 2)^{2n-2i} d^{i-1}. \tag{7.9}$$

These two equations will be used to prove the following theorems.

Theorem 7.10. If p is a prime, $(p, 2d) = 1$, $\epsilon_a = \left(\frac{d}{p}\right)$, $\tau_a = \left(\frac{a+2}{p}\right)$ and $\rho_a = \left(\frac{a-2}{p}\right)$, then

$$2X_a\left(\frac{p+1}{2}\right) \equiv \rho_a(a-2) + \rho_a\epsilon_a(a+2) \pmod{p}. \tag{7.10}$$

Proof. Put $n = (p+1)/2$ in (7.8). Then $p \left| \binom{p+1}{2i} \right.$ for each i, $1 \leq i \leq (p-1)/2$. Thus $p \mid \binom{p+1}{2i}$ holds for all i unless $i = 0$ or $i = (p+1)/2$. Hence (7.8) implies

$$4^{\frac{p+1}{2}}(a \pm 2)^{\frac{p+1}{2}} X_a\left(\frac{p+1}{2}\right) \equiv 2(a \pm 2)^{p+1} + 2d^{\frac{p+1}{2}} \pmod{p}.$$

Applying Euler's Criterion and Fermat's Theorem we obtain

$$4(a \pm 2)^{\frac{p-1}{2}}(a \pm 2) X_a\left(\frac{p+1}{2}\right) \equiv 2(a \pm 2)^2 + 2\epsilon_a d \pmod{p}.$$

Since $d = (a+2)(a-2)$ we may divide by $2(a \pm 2)$ to obtain

$$2(a \pm 2)^{\frac{p-1}{2}} X_a\left(\frac{p+1}{2}\right) \equiv (a \pm 2) + \epsilon_a(a \mp 2) \pmod{p}.$$

Multiplying by $(a \pm 2)^{\frac{p-1}{2}}$ and replacing $(a \pm 2)^{\frac{p-1}{2}}$ by ρ_a or τ_a we obtain (7.10). The theorem is proved.

Theorem 7.11. If p is an odd prime, $(p, d) = 1$, $\epsilon_a = \left(\frac{d}{p}\right)$ and $\tau_a = \left(\frac{a+2}{p}\right)$, then

$$X_a\left(\frac{p-\epsilon_a}{2}\right) \equiv 2\tau_a \pmod{p}. \tag{7.11}$$

Proof. Let $\rho_a = ((a-2)/p)$. Then $\epsilon_a = \tau_a\rho_a$.

First suppose $\epsilon = -1$. Then $p + 1 = p - \epsilon$. Hence from Theorem 7.10 we have

$$2X_a\left(\frac{p-\epsilon_a}{2}\right) = 2X_a\left(\frac{p+1}{2}\right) \equiv \rho(a-2) + \rho(-1)(a+2) = -4\rho = 4\epsilon\rho = 4\tau \pmod{p}.$$

Hence (7.11) holds in this case.

Next suppose $\epsilon = 1$. By Theorem 7.10 and (3.80),

$$aX_a\left(\frac{p-\epsilon}{2}\right) \equiv 2X_a\left(\frac{p+\epsilon}{2}\right) = 2X_a\left(\frac{p+1}{2}\right) \equiv \rho(a-2)+\rho 1(a+2) = 2\rho a = 2\epsilon\rho a = 2\tau a \pmod{p}.$$

If $(p, a) = 1$, divide both sides of the congruence by a to get (7.11) in this case also. If $p \mid a$, the result can be proved from Definition 3.12 and (4.1). See Theorem 7.25.

Theorem 7.12. If p is a prime, $(p, 2d) = 1, \epsilon_a = \left(\frac{d}{p}\right)$ and $\rho_a = \left(\frac{a-2}{p}\right)$, then

$$2Y_a\left(\frac{p+1}{2}\right) \equiv \rho_a(\epsilon_a + 1) \pmod{p}. \tag{7.12}$$

Proof. Put $n = (p+1)/2$ in (7.9). Then $p \mid \binom{p+1}{2i-1}$ for each i, $2 \le i \le (p-1)/2$. That is $p \mid \binom{p+1}{2i-1}$ for all i except $i = 1$ and $i = (p+1)/2$. Hence from (7.9) and $p + 1 \equiv 1 \pmod{p}$ we obtain

$$4^{\frac{p+1}{2}}(a-2)^{\frac{p+1}{2}}Y_a\left(\frac{p+1}{2}\right) \equiv 2(a-2)^p + 2(a-2)d^{\frac{p-1}{2}} \pmod{p}.$$

Dividing by $a - 2$ and applying Fermat's Theorem to obtain $(a-2)^{p-1} \equiv 1 \pmod{p}$ and $2^{p+1} \equiv 4 \pmod{p}$, we have

$$4(a-2)^{\frac{p-1}{2}}Y_a\left(\frac{p+1}{2}\right) \equiv 2 + 2d^{\frac{p-1}{2}} \pmod{p}.$$

Next apply Euler's Criterion and Fermat's Theorem to obtain

$$4\rho_a Y_a\left(\frac{p+1}{2}\right) \equiv 2 + 2\epsilon_a \pmod{p}.$$

Multiplying by ρ_a and dividing by 2, using $\rho_a^2 = 1$, we obtain (7.12).

Theorem 7.13. If p is prime, $(p, 2d) = 1, \epsilon_a = \left(\frac{d}{p}\right)$ and $\rho_a = \left(\frac{a-2}{p}\right)$, then

$$Y_a\left(\frac{p+\epsilon_a}{2}\right) \equiv \rho_a \pmod{p}. \tag{7.13}$$

Proof. For $\epsilon = \epsilon_a = 1$ or $\epsilon = \epsilon_a = -1$ this can be deduced from Theorem 7.12, (3.81) and Corollary 6.23.

$$2Y_a\left(\frac{p+\epsilon}{2}\right) = \epsilon X_a\left(\frac{p-\epsilon}{2}\right) \equiv \epsilon 2\epsilon\rho = 2\rho \pmod{p}.$$

Theorem 7.14. If p is prime, $(p, 2d) = 1, \epsilon_a = \left(\frac{d}{p}\right)$ and $\tau_a = \left(\frac{a+2}{p}\right)$, then

$$X_a\left(\frac{p+\epsilon_a}{2}\right) \equiv a\tau_a \pmod{p}. \tag{7.14}$$

Proof. This can be deduced from Theorem 7.13, (3.83).

$$X_a\left(\frac{p+\epsilon}{2}\right) = \epsilon\epsilon X_a\left(\frac{p+\epsilon}{2}\right) \equiv \epsilon a Y_a\left(\frac{p+\epsilon}{2}\right) \equiv \epsilon a\rho = a\tau \pmod{p}.$$

As before, the conditions expressed by Theorems 7.11, 7.13 and 7.14 are not equivalent. Hence we can define some new types of pseudoprimes.

Definition 7.15. Suppose $(n, 2d) = 1$ and $d = (a^2-4)$, $\epsilon_a = (d/n)$, $\rho_a = ((a-2)/n)$ and $\tau_a = ((a+2)/n)$.

$$X_a\left(\frac{n-\epsilon_a}{2}\right) \equiv 2\tau_a \pmod{n} \Leftrightarrow n \text{ is } t\text{-pseudoprime to base } a,\ tpsp(a),$$
$$X_a\left(\frac{n+\epsilon_a}{2}\right) \equiv a\tau_a \pmod{n} \Leftrightarrow n \text{ is } a\text{-pseudoprime to base } a,\ apsp(a),$$
$$Y_a\left(\frac{n+\epsilon_a}{2}\right) \equiv \rho_a \pmod{n} \Leftrightarrow n \text{ is } r\text{-pseudoprime to base } a,\ rpsp(a).$$

These concepts are all independent each other and also independent of $lpsp(a)$, $elpsp(a)$ and $slpsp(n)$.

n is a $slpsp(a)$ does not imply n is a $tpsp(a)$, $rpsp(a)$ or $apsp(a)$. For example put $n = 17\cdot19 = 323$ and $a = 3$, $n = 5\cdot 7 = 35$ and $a = 6$ or $n = 5\cdot11 = 55$ and $a = 21$.

n is a $rpsp(a)$ does not imply n is a $lpsp(a)$, $tpsp(a)$ or $apsp(a)$. For example put $n = 11\cdot13 = 143$ and $a = 3$, or $n = 71\cdot73 = 5183$ and $a = 3$.

n is a $tpsp(a)$ does not imply n is a $lpsp(a)$, $rpsp(a)$ or $apsp(a)$. For example put $n = 7^2 = 49$ and $a = 3$, or $n = 7^2\cdot23 = 1127$ and $a = 3$.

n is an $apsp(a)$ does not imply n is a $lpsp(a)$, $tpsp(a)$ or $rpsp(a)$. For example put $n = 11\cdot13 = 143$ and $a = 7$, or $a = 19$.

However, we will show that if $(n,a)=1$ in addition to $(n,d)=1$, then any two of $lpsp(a)$, $tpsp(a)$, $rpsp(a)$ and $apsp(a)$ together imply all others. Also the same holds for the group of $elpsp(a)$, $tpsp(a)$, $rpsp(a)$ and $apsp(a)$. Although $elpsp(a)$ implies $lpsp(a)$, these two groups are equivalent. Namely, any two in the former group imply any one in the latter group. i.e. $lpsp(a)$ together with $tpsp(a)$ imply $elpsp$. Hence we can define the following stronger pseudoprimes.

Definition 7.16. If $(n,2d)=1$, n is a $lpsp(a)$ and n is a $tpsp(a)$, then we say n is an Lucas t-pseudoprime to the base a, $ltpsp(a)$. If n is a $rpsp(a)$ and n is an $apsp(a)$, then we say n is an $rapsp(a)$.

Theorem 7.17. Suppose $(n,2ad)=1$, then n is an $ltpsp(a)$ if and only if

(o)	$Y_a(\frac{n-\epsilon}{2}) \equiv 0 \pmod n$	and	$X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau_a \pmod n$,
(i)	$Y_a(n-\epsilon) \equiv 0 \pmod n$	and	$X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau_a \pmod n$,
(ii)	$Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod n$	and	$Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a \pmod n$,
(iii)	$Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a \pmod n$	and	$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a \pmod n$,
(iv)	$Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod n$	and	$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a \pmod n$,
(v)	$X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau_a \pmod n$	and	$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a \pmod n$,
(vi)	$Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a \pmod n$	and	$Y_a(n) \equiv \epsilon_a \pmod n$,
(vii)	$Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a \pmod n$	and	$X_a(n) \equiv a \pmod n$,
$(viii)$	$X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau_a \pmod n$	and	$Y_a(n) \equiv \epsilon \pmod n$,
(ix)	$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a \pmod n$	and	$X_a(n) \equiv a \pmod n$,
(x)	$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a \pmod n$	and	$Y_a(n) \equiv \epsilon_a \pmod n$.

Proof. Here (i) is the definition of $ltpsp(a)$. From $\tau = \rho\epsilon$ and identities (3.80) - (3.91) and Theorem 6.22 it is easy to see that conditions (ii) - (x) are all necessary.

To show that (o) is necessary, we use the Double Angle formula and the condition $X_a((n-\epsilon)/2) \equiv 2\tau_a \pmod{n}$ to get $Y_a((n-\epsilon)/2) \equiv 0 \pmod{n}$. For the sufficiency proof we observe that $(o) \Rightarrow (i)$ is trivial. Then $(ii) \Rightarrow (i)$ by (3.81). $(iii) \Rightarrow (i)$ by (3.82) and (3.83). $(iv) \Rightarrow (i)$ by (3.80). $(v) \Rightarrow (i)$ by (3.80). $(vi) \Rightarrow (ii)$ by (3.87) and (1.1). $(vii) \Rightarrow (ii)$ by (3.85). $(viii) \Rightarrow (vi)$ by (3.87). $(ix) \Rightarrow (v)$ by (3.84). Finally $(x) \Rightarrow (ix)$ by (3.87) and (3.85).

Corollary 7.17.1. Suppose $(n, 2d) = 1$. n is *ltpsp*$(a) \Rightarrow$ *elpsp*(a). Also n is an *ltpsp*(a) if and only if n is a *rapsp*(a).

Proof. Directly from the three ϵ - identities (3.80) - (3.83).

REMARK. That the conditions (o), (i), (ii), (vi) and $(viii)$ are equivalent does not need $(n, a) = 1$.

From Theorem 7.17, n is a *ltpsp*(a) implies n is an *elpsp*(a). However n is a *ltpsp*(a) does not imply n is a *slpsp*(a) $(n = 385, a = 6)$. Also we already saw that n is a *slpsp*(a) does not imply n is a *ltpsp*(a) $(n = 35, a = 6)$.

We next define a stronger type of pseudoprime condition:

Definition 7.18. Suppose n is odd and $(n, d) = 1$ where $d = a^2 - 4$. n is said to be a strong Lucas t-pseudoprime to the base a if n is both a *slpsp*(a) and a *tpsp*(a) (written as *sltpsp*(a)).

By Theorem 7.17, we have

Theorem 7.19. Suppose $n > 1$, n odd and $(n, ad) = 1$. If n is *sltpsp*(a), then n is *slpsp*(a), *elpsp*(a), *lpsp*(a), *apsp*(a), *rpsp*(a) and *tpsp*(a).

Next we will discuss some general properties of pseudoprimes. We will show that for all odd integers $n > 3$, there always exist 3 trivial incongruent bases such that n is a *sltpsp*(a). First we need a lemma.

Lemma 7.20. Suppose n is odd, $(n,d)=1$ where $d=a^2-4$, $\epsilon_a=(d/n)$, $\rho_a=((a-2)/n)$ and $\tau_a=((a+2)/n)$. Then the Jacobi symbols ρ_a, τ_a and ϵ_a satisfy

(i) $(-1)^{\frac{n-1}{2}}(-1)^{\frac{n-\epsilon_a}{2}}\rho_a = \tau_a$, (ii) $(-1)^{\frac{n-1}{2}}(-1)^{\frac{n-\epsilon_a}{2}}\tau_a = \rho_a$,

(iii) $\tau_{-a} = (-1)^{\frac{n-\epsilon_a}{2}}\tau_a$, (iv) $\rho_{-a} = (-1)^{\frac{n-\epsilon_a}{2}}\rho_a$,

(v) $\tau_{-3} = (-1/n) = (-1)^{\frac{n-1}{2}}$, (vi) $\rho_1 = (-1/n) = (-1)^{\frac{n-1}{2}}$,

(vii) $\tau_{-a} = \rho_1\rho_a$, $(viii)$ $\rho_{-a} = \rho_1\tau_a$.

Proof. Trivial since $\epsilon_a = \rho_a \cdot \tau_a$ and $\epsilon_a = (-1/n)(-1)^{\frac{n-\epsilon_a}{2}}$.

Theorem 7.21. Suppose n is odd and $a \equiv b \pmod{n}$. Then

n is an *lpsp*(a) $\Leftrightarrow$ n is an *lpsp*(b), n is an *elpsp*$(a) \Leftrightarrow n$ is an *elpsp*(b),

n is a *tpsp*(a) $\Leftrightarrow$ n is a *tpsp*(b), n is a *rpsp*$(a) \Leftrightarrow n$ is a *rpsp*(b),

n is an *apsp*(a) $\Leftrightarrow$ n is an *apsp*(b), n is a *slpsp*$(a) \Leftrightarrow n$ is a *slpsp*(b),

n is a *slxpsp*(a) $\Leftrightarrow$ n is a *slxpsp*(b).

Proof. Suppose $a \equiv b \pmod{n}$. Then $\epsilon_a = \epsilon_b, \tau_a = \tau_b$ and $\rho_a = \rho_b$. The conclusion then follows from the Congruence Rule (4.1).

Theorem 7.22. Suppose n is odd and $a \equiv -b \pmod{n}$. Then

n is an *lpsp*(a) $\Leftrightarrow$ n is an *lpsp*(b), n is an *elpsp*$(a) \Leftrightarrow n$ is an *elpsp*(b),

n is a *tpsp*(a) $\Leftrightarrow$ n is a *tpsp*(b), n is a *rpsp*$(a) \Leftrightarrow n$ is a *rpsp*(b),

n is an *apsp*(a) $\Leftrightarrow$ n is an *apsp*(b), n is a *slpsp*$(a) \Leftrightarrow n$ is a *slpsp*(b),

n is a *slxpsp*(a) $\Leftrightarrow$ n is a *slxpsp*(b).

Proof. Since $a \equiv -b \pmod{n}$, $\epsilon_a = ((a^2-4)/n) = (((-b)^2-4)/n) = ((b^2-4)/n) = \epsilon_b$. Since $n \mid a+b$, Congruence Rule (4.2.1) implies that for any k,

$$(*) \qquad Y_a(k) \equiv (-1)^{k-1} Y_b(k) \pmod{n}.$$

Putting $k = (n-\epsilon)$ and $k = (n-\epsilon)/2$ respectively, then this congruence implies n is *lpsp*(a) if and only if n is *lpsp*(b) and n is *elpsp*(a) if and only if n is *elpsp*(b). Also by (4.2.1) we have for any k,

$$(**) \qquad X_a(k) \equiv (-1)^k X_b(k) \pmod{n}.$$

This together congruence $(*)$ shows that n is *slpsp*(a) if and only if n is *slpsp*(b). To show n is *tpsp*(a) if and only if n is *tpsp*(b), we use Lemma 7.20 (*iii*). To show n is *rpsp*(a) if and only if n is *rpsp*(b), we use Lemma 7.20 (*iv*) and $(-1)^{n-1}=1$. To show n is *apsp*(a) if and only if n is *apsp*(b), we use Lemma 7.20 (*iii*) and $(-1)^n=-1$.

If we put $b = n-a$ or $b = -a$ in Theorem 7.22, then we obtain the following two corollaries as special cases:

Corollary 7.23. Suppose $n > 1$ is odd. Then

$$n \text{ is an } lpsp(a) \Leftrightarrow n \text{ is an } lpsp(n-a), \quad n \text{ is an } elpsp(a) \Leftrightarrow n \text{ is an } elpsp(n-a),$$

$$n \text{ is a } tpsp(a) \Leftrightarrow n \text{ is a } tpsp(n-a), \quad n \text{ is an } rpsp(a) \Leftrightarrow n \text{ is an } rpsp(n-a),$$

$$n \text{ is an } apsp(a) \Leftrightarrow n \text{ is an } apsp(n-a), \quad n \text{ is a } slpsp(a) \Leftrightarrow n \text{ is a } slpsp(n-a),$$

$$n \text{ is a } slxpsp(a) \Leftrightarrow n \text{ is a } slxpsp(n-a).$$

Corollary 7.24. Suppose $n > 1$ is odd. Then

$$n \text{ is an } lpsp(a) \Leftrightarrow n \text{ is an } lpsp(-a), \quad n \text{ is an } lpsp(a) \Leftrightarrow n \text{ is an } lpsp(-a),$$

$$n \text{ is a } tpsp(a) \Leftrightarrow n \text{ is a } tpsp(n-a), \quad n \text{ is an } rpsp(a) \Leftrightarrow n \text{ is an } rpsp(-a),$$

$$n \text{ is an } apsp(a) \Leftrightarrow n \text{ is an } apsp(-a), \; n \text{ is a } slpsp(a) \Leftrightarrow n \text{ is a } slpsp(-a),$$

$$n \text{ is a } slxpsp(a) \Leftrightarrow n \text{ is a } slxpsp(-a).$$

Theorem 7.25. For all odd $n > 1$, n is an $sltpsp(0)$ and $slxpsp(0)$. Hence n is $slpsp(0)$, $apsp(0)$, $rpsp(0)$ and $tpsp(0)$.

Proof. Suppose n is odd. $\epsilon_0 = ((0^2-4)/n) = (-4/n) = (-1/n) = \pm 1$. Put $n = u2^t + \epsilon_0$ where u is odd. To show n is $slxpsp(0)$, note that $u = (n-\epsilon_0)/2^t$ is odd. Hence by Definition 3.12, $X_0(u) = 0 \equiv 0 \pmod{n}$ so that n is $slxpsp(0)$ by (7.4) (i). Therefore n is $slpsp(0)$.

For the proof that n is a $tpsp(0)$ we shall use $(2/n) = (-1)^{(n^2-1)/8}$, known from the theory of quadratic residues. Since $\tau_0 = ((0+2)/n) = (2/n)$, we need to show that $X_0((n-\epsilon_0)/2) \equiv 2(2/n) \pmod{n}$. For this we consider 4 cases:

$$n \equiv 1 \pmod 8 \Rightarrow \epsilon = +1, \tau = +1, (n-\epsilon)/2 \equiv 0 \pmod 4 \Rightarrow X_0((n-\epsilon)/2) = +2,$$

$$n \equiv 3 \pmod 8 \Rightarrow \epsilon = -1, \tau = -1, (n-\epsilon)/2 \equiv 2 \pmod 4 \Rightarrow X_0((n-\epsilon)/2) = -2,$$

$$n \equiv 5 \pmod 8 \Rightarrow \epsilon = +1, \tau = -1, (n-\epsilon)/2 \equiv 2 \pmod 4 \Rightarrow X_0((n-\epsilon)/2) = -2,$$

$$n \equiv 7 \pmod 8 \Rightarrow \epsilon = -1, \tau = +1, (n-\epsilon)/2 \equiv 0 \pmod 4 \Rightarrow X_0((n-\epsilon)/2) = +2.$$

Thus n is a $tpsp(0)$. This proves the theorem.

Using the Congruence Rule, we have the following corollary:

Corollary 7.26. If $a \equiv 0 \pmod{n}$, then n is an $sltpsp(a)$ and $slxpsp(a)$. Hence n is $slpsp(a)$, $apsp(a)$, $rpsp(a)$ and $tpsp(a)$.

Lemma 7.27. If $(n,6)=1$, $a \equiv \pm 1 \pmod{n}$ and $\epsilon=(d/n)$, then $n \equiv \epsilon \pmod{6}$.

Proof. Since $(n,6)=1$, and $a \equiv \pm 1 \pmod{n}$, $d=a^2-4 \equiv (\pm 1)^2-4=-3 \pmod{n}$. Hence $\epsilon = (d/n) = (-3/n)$. From the theory of quadratic residues it is known that $(-3/n) = 1$ if $n \equiv 1 \pmod{6}$ and $(-3/n) = -1$ if $n \equiv -1 \pmod{6}$. Hence $\epsilon = (-3/n) \equiv n \pmod{6}$.

Theorem 7.28. If $(n,6)=1$ and $a \equiv \pm 1 \pmod{n}$, then n is *sltpsp*(a) and *slxpsp*(a).

Proof. By Corollary 7.24, we need only to prove the theorem for case $a \equiv 1 \pmod{n}$. Put $n=u2^t+\epsilon$ where u is odd. For the proof that n is *slxpsp*(a), by Lemma 7.27, we have $6 \mid n-\epsilon$ and then $3 \mid n-\epsilon$. Thus $3 \mid (n-\epsilon)/2^t$. Hence by (3.13) we have $Y_a((n-\epsilon)/2^t) \equiv Y_1((n-\epsilon)/2^t) = 0 \pmod{n}$ and $X_a((n-\epsilon)/2^t) \equiv X_1((n-\epsilon)/2^t) = \pm 2 \pmod{n}$. By 7.4 (ii) these two congruences show that n is *slxpsp*(a). Therefore n is *slpsp*(a).

The proof that n is *tpsp*(a) is similar to the one used to prove Theorem 7.25. We consider the cases $n \equiv \pm 1 \pmod{12}$, where $(3/n) = 1$, and $n \equiv \pm 5 \pmod{12}$, where $(3/n) = -1$.

The Theorems 7.25, 7.28 show that for any odd integer n, $(n,6)=1$, there always exist at least 3 bases, $a = 0$, $a = 1$ and $a = n-1$, in a complete residue system mod n, for which n passes all the types of pseudoprime tests discussed above. These three bases are the so called the *trivial bases.* Hence when we test the primality of any odd integer n, these 3 bases may always be omitted.

How well do *sltpsp*(a) and *slxpsp*(a) work in primality testing? We looked at all integers up to 2.5×10^9 and found only three composite integers which can pass

an *sltpsp*(a) test for all three values $a = 3, 4, 5$. These three composite integers are $79,398,901 = 6301 \cdot 12601$, $133,800,661 = 109 \cdot 541 \cdot 2269$ and $579,606,301 = 109 \cdot 541 \cdot 9829$. They all fail to pass the *sltpsp*(a) test with $a = 6$. In fact, we have not found any composite number which is an *sltpsp*(a) for consecutive values of a for $a = 3, 4, 5$ and 6 so far. However, for the *ltpsp*(a) test, up to 2.5×10^9, there are 11 composites which are *ltpsp*(a) for $a = 3, 4, 5$, some of them are even *ltpsp*(a) for $a = 3, 4, 5, 6, 7, 8$, e.g. $140,384,161 = 6841 \cdot 20521$. Also we found that under 2.5×10^9 no composite integer can pass the *slxpsp*(a) test for $a = 3, 4, 5$.

§8. Mersenne numbers and Fermat numbers

In this section we will show that for Mersenne numbers and Fermat numbers, their primality is equivalent to that they are *ltpsp*(a) for some fixed bases a. We also relate other classical Lucas-Lehmer tests for Mersenne numbers and Fermat numbers to our new tests by using X_a and Y_a. Hence we give a new proof from Thereom 5.1 for the classical result that the primality of Mersenne numbers and Fermat numbers can be decided in polynomial time (see Corollary 8.2 and Corollary 8.4).

Suppose n is an integer of the form $n = 2^t - 1$, $t \geq 2$. If n is a prime, then it is called a Mersenne prime. Clearly, if n is prime, then t is prime. Also we have $n \equiv 1 \pmod 3$, $n \equiv 3 \pmod 4$, and $n \equiv -1 \pmod 8$.

To test the primality of $n = 2^t - 1$, there are many positive integers a such that for the Jacobi symbols $\epsilon = ((a^2 - 4)/n)$ and $\tau = ((a + 2)/n)$, we have $\epsilon = -1$ and $\tau = -1$, e.g. $a = 4$ or $a = 10$.

If $a = 4$, then $a^2 - 4 = 12$. Since $n \equiv 1 \pmod 3$, and $n \equiv 3 \pmod 4$, we have $\epsilon = (12/n) = (3/n)(4/n) = (3/n) = -(n/3) = -(1/3) = -1$. So $\epsilon = -1$. Since $n \equiv -1 \pmod 8$, $\tau = ((4+2)/n) = (6/n) = (2/n)(3/n) = (+1)(-1) = -1$. So $\tau = -1$.

If $a = 10$, then $a^2 - 4 = 96$. Since $n \equiv 1 \pmod 3$, and $n \equiv -1 \pmod 8$, we have $\epsilon = (96/n) = (16/n)(6/n) = (2/n)(3/n) = (+1)(-(n/3)) = -(1/3) = -1$. Also $\tau = ((10+2)/n) = (12/n) = (4/n)(3/n) = (+1)(-1) = -1$. Hence $\epsilon = \tau = -1$.

Thus if $n = 2^t - 1$, $t \geq 2$ and t is odd, then we can take $a = 4$ or $a = 10$ and it will be the case that $(n, 2(a^2 - 4)) = 1$ and $\epsilon = \tau = -1$. There exist also other a such that $\epsilon = -1$ and $\tau = -1$. With such an a the X_a and Y_a sequences can be used to give criteria for primality of n. The Lucas sequences X_a and Y_a can also be used

to give a quick proof of the Lucas - Lehmer test for primality of Mersenne numbers $2^t - 1$.

Theorem 8.1. (Mersenne primes.) Suppose $n = 2^t - 1$, $t \geq 2$ and t is odd, $(n, a(a^2-4)) = 1$, $\epsilon_a = -1$ and $\tau_a = -1$. Then each of the following conditions is necessary and sufficient for primality of n.

(o) $\quad n$ is an $ltpsp(a)$,

(i) $\quad X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau = -2 \pmod{n}$ and $Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod{n}$,

(ii) $\quad X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau = -a \pmod{n}$ and $Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho = 1 \pmod{n}$,

(iii) $\quad X_a\left(\frac{n-\epsilon}{4}\right) \equiv 0 \pmod{n}$,

(iv) $\quad r_a(n) = \frac{n-\epsilon}{2}$.

Proof. Since $\epsilon = -1$, $n - \epsilon = n - (-1) = n + 1 = 2^t$, so $n - \epsilon$ is a power of 2.

Sufficiency. Suppose any one of $(o) - (iv)$ holds. We will show that n is prime. If (iv) holds, then n is prime by Theorem 6.11. By Lemma 6.21, (iii) implies (iv). By (3.93), (3.92) and $\tau = -1$, (i) implies (iii), and so (o) or (ii) is also sufficient by Theorem 8.17 (i) and 8.17 (iii).

Necessity. Suppose n is prime. Then n is $ltpsp(a)$. Hence (o), (i) and (ii) hold. By (3.93) (i) implies (iii) and by Lemma 6.21 (iii) implies (iv). Therefore (iii) and (iv) are also necessary.

Corollary 8.2. (Lucas [32] - Lehmer [28] Test). For $t > 2$, t odd, $n = 2^t - 1$ is prime if and only if $n \mid s_{t-1}$ where s_k is defined by $s_1 = 4, s_{k+1} = s_k^2 - 2$.

Proof. We shall use Theorem 8.1 with $a=4$. Since $\epsilon=-1$, $(n-\epsilon)/4=(n+1)/4=2^{t-2}$. By Theorem 8.1, n is prime if and only if $n \mid X_a((n+1)/4)$. Hence n is prime if and only if $n \mid X_a(2^{t-2})$. Thus it suffices to show

(8.2) $\qquad s_k = X_4(2^{k-1}), \qquad$ for all $k \geq 1$.

(8.2) can be proved by induction on k. If $k = 1$, then $s_1 = 4 = X_4(1) = X_4(2^0) = X_4(2^{1-1})$. Suppose (8.2) holds for k. Then by (3.4) $s_{k+1} = s_k^2 - 2 = X_4^2(2^{k-1}) - 2 = X_4(2 \cdot 2^{k-1}) = X_4(2^k) = X_4(2^{k+1-1})$. Hence (8.2) is proved.

Let n be an integer of the form $n = 2^t + 1$, $4 | t$. Then $n \equiv 2 \pmod 3$, $n \equiv 1 \pmod 8$, $n \equiv 2 \pmod 5$ and if n is a prime, then t is a power of 2. Such primes are called Fermat primes, and such numbers are called Fermat numbers.

For testing primality of a Fermat number n, there exist many positive integers a such that for the Jacobi symbols $\epsilon = ((a^2 - 4)/n)$ and $\tau = ((a + 2)/n)$, we have $\epsilon = +1$ and $\tau = -1$, e.g. we can take $a = 8$ or $a = 12$.

If $a = 8$, then $a^2 - 4 = 60 = 4 \cdot 3 \cdot 5$. Since $n \equiv 2 \pmod 3$, $n \equiv 1 \pmod 8$ and $n \equiv 2 \pmod 5$, we have $\epsilon = (60/n) = (3/n)(4/n)(5/n) = (3/n)(5/n) = (n/3)(n/5) = (2/3)(2/5) = (-1)(-1) = 1$. Also since $n \equiv 1 \pmod 8$ and $a = 8$, $\tau = ((8 + 2)/n) = (10/n) = (2/n)(5/n) = (+1)(5/n) = (+1)(-1) = -1$. So $\tau = -1$.

If $a = 12$ and t is a power of 2, then $n = 2^t + 1 \equiv 3, 5 \pmod 7$. Both 3 and 5 are nonresidues mod 7, so $(7/n) = (n/7) = -1$. Thus when $a = 12$, $\epsilon = ((12^2 - 4)/n) = (140/n) = (4/n)(5/n)(7/n) = -(5/n) = -(n/5) = -(2/5) = -(-1) = +1$ and $\tau = ((12+2)/n) = (14/n) = (2/n)(7/n) = (+1)(-1) = -1$. Hence $\epsilon = +1$ and $\tau = -1$.

Thus if $n = 2^t + 1$, $t \geq 4$ and t is a power of 2, then we can take $a = 8$ or $a = 12$ and it will be the case that $(n, 2(a^2 - 4)) = 1$ and $\epsilon = 1$, $\tau = -1$. There exist also other a such that $\epsilon = 1$ and $\tau = -1$. We will show that any such a can be used to formulate a criterion for primality of n in terms of the sequences $X_a(n)$ and $Y_a(n)$.

Theorem 8.3. (Fermat primes.) Suppose $n = 2^t + 1$, $t \geq 4$ and t is a power of 2, $(n, (a^2-4)) = 1$, $\epsilon = 1$ and $\tau = -1$. Then each of the following conditions is necessary and sufficient for primality of n.

(o) n is an $ltpsp(a)$,

(i) $X_a\left(\frac{n-\epsilon}{2}\right) \equiv 2\tau = -2 \pmod{n}$ and $Y_a\left(\frac{n-\epsilon}{2}\right) \equiv 0 \pmod{n}$,

(ii) $X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau = -a \pmod{n}$ and $Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho = -1 \pmod{n}$,

(iii) $X_a\left(\frac{n-\epsilon}{4}\right) \equiv 0 \pmod{n}$,

(iv) $r_a(n) = \frac{n-\epsilon}{2}$.

Proof. Since $\epsilon = +1$, $n - \epsilon = n - 1 = 2^t$, so $n - \epsilon$ is a power of 2. Hence the same proof as for Theorem 8.1 will establish the theorem here.

Corollary 8.4. (Lucas [32] - Lehmer [28] Test) For $t \geq 4$, t is a power of 2, we have $n = 2^t + 1$ is prime if and only if $n \mid s_{t-1}$ where s_k is defined by $s_1 = 8$, $s_{k+1} = s_k^2 - 2$.

Proof. We shall use Theorem 8.3 with $a=8$. Since $\epsilon=1$, $(n-\epsilon)/4=(n-1)/4=2^{t-2}$. By Theorem 8.3, n is prime if and only if $n \mid X_a((n-1)/4)$. Hence n is prime if and only if $n \mid X_a(2^{t-2})$. Thus it suffices to show

$$s_k = X_8(2^{k-1}), \qquad \text{for all } k \geq 1. \tag{8.4}$$

One can prove (8.4) by a similar induction procedure as in the proof of (8.2).

§9. Prime powers

In this section we collect together results about p^e as an *elpsp*(a), *rpsp*(a), *apsp*(a) and *tpsp*(a). Some results in this section will be used in the later sections. Throughout p denotes an odd prime.

Lemma 9.1. For any $e \geq 0$ and all a such that $(p, 2d) = 1$, $Y_a\left(\frac{p^e - \epsilon_a(p)^e}{2}\right) \equiv 0 \pmod{p}$.

Proof. Certainly $p - \epsilon_a(p) \mid p^e - \epsilon_a(p)^e$. Hence if $k = (p^e - \epsilon_a(p)^e)/(p - \epsilon_a(p))$, then k will be an integer and $p^e - \epsilon_a(p)^e = k \cdot (p - \epsilon_a(p))$. This implies $(p^e - \epsilon_a(p)^e)/2 = k \cdot (p - \epsilon_a(p))/2$. Consequently by Lemma 6.17 and Lemma 4.10 (i) we have $Y_a((p^e - \epsilon_a(p)^e)/2) = Y_a(k \cdot (p - \epsilon_a(p))/2) \equiv 0 \pmod{p}$.

Lemma 9.2. Suppose p is an odd prime and $(p, d) = 1$. Then for any $j \geq 0$,

(i) $X_a(p^j) \equiv a \pmod{p}$ and (ii) $Y_a(p^j) \equiv \epsilon_a(p)^j \pmod{p}$.

Proof. Suppose $(p, d) = 1$.

Case 1: $\epsilon_a(p)^j = +1$. Then by Lemma 9.1, (i) holds by (3.20′), (ii) holds by (3.22′).

Case 2: $\epsilon_a(p)^j = -1$. Then by Lemma 9.1, (i) holds by (3.20′), (ii) holds by (3.21′).

Lemma 9.3. Let p be an odd prime and suppose $(p, ad) = 1$. The following are equivalent:

(i) p^e is an *elpsp*(a), (ii) $X_a(p^e) \equiv a \pmod{p^e}$, (iii) $Y_a(p^e) \equiv \epsilon_a(p)^e \pmod{p^e}$, (iv) $X_a(p^e)^2 \equiv a^2 \pmod{p^e}$, (v) $Y_a(p^e)^2 \equiv 1 \pmod{p^e}$, (vi) $Y_a(p^e \pm 1) \equiv 0 \pmod{p^e}$.

Proof. If (i) holds, then (ii), (iii), (iv), (*v*) and (vi) hold by Theorem 6.24 with $n = p^e$. Conversely suppose (ii), (iii), (iv) or (*v*) holds. Then by (1.35) or (3.99) with $n = p^e$, $(X_a(p^e) + a)(X_a(p^e) - a) = d(Y_a(p^e) + 1)(Y_a(p^e) - 1) \equiv 0 \pmod{p^e}$.

It is obvious that $(Y_a(p^e)+1,\ Y_a(p^e)-1) \mid 2$ and $(X_a(p^e)+a, X_a(p^e)-a) \mid 2a$. Since $(p, ad) = 1$ and p^e is a prime power, we have $Y_a(p^e) \equiv \pm 1 \pmod{p^e}$ and $X_a(p^e) \equiv \pm a \pmod{p^e}$. But by Lemma 9.2, $Y_a(p^e) \equiv \epsilon_a(p)^e \pmod{p}$ and $X_a(p^e) \equiv a \pmod{p}$. Hence (ii) and (iii) hold. Consequently (iv) and (v) hold. By Theorem 6.22, (i) holds. Finally, suppose (vi) holds. Then by (3.96) with $n = p^e$, (v) holds. Hence (i) holds.

Lemma 9.4. Suppose $(p, 2d) = 1$. Then

p^e is an *elpsp*$(a) \Leftrightarrow Y_a\left(\frac{p-\epsilon_a(p)}{2}\right) \equiv 0 \pmod{p^e}$.

Proof. $\Rightarrow$. Suppose $(p, 2d) = 1$ and that p^e is an *elpsp*(a). Since $\epsilon_a(p^e) = \epsilon_a(p)^e$, from the definition of *elpsp*(a) we have $p^e \mid Y_a((p^e - \epsilon_a(p)^e)/2)$. Hence $r_a(p^e) \mid (p^e - \epsilon_a(p)^e)/2$. This implies $(r_a(p^e), p) = 1$. But by Theorem 6.12, $r_a(p^e) \mid p^{e-1}(p - \epsilon_a(p))/2$. Since $(r_a(p^e), p) = 1$, this implies $r_a(p^e) \mid (p - \epsilon_a(p))/2$. Consequently by Lemma 6.4 we have $p^e \mid Y_a(p - \epsilon_a(p))/2$.

$\Leftarrow$. Suppose $(p, 2d) = 1$ and $p^e \mid Y_a((p - \epsilon_a(p))/2)$. Trivially $p - \epsilon_a(p) \mid p^e - \epsilon_a(p)^e$. Hence $(p - \epsilon_a(p))/2 \mid (p^e - \epsilon_a(p)^e)/2$. From the Division Theorem 4.11, we then have $Y_a((p - \epsilon_a(p))/2) \mid Y_a((p^e - \epsilon_a(p)^e)/2)$. Hence $p^e \mid Y_a(p^e - \epsilon_a(p)^e)/2)$. Thus p^e is *elpsp*(a).

Corollary 9.5. If $(p, 2d) = 1$ and p^e is *elpsp*(a), then for all $j \geq 0$

$Y_a\left(\frac{p^j - \epsilon_a(p)^j}{2}\right) \equiv 0 \pmod{p^e}$.

Proof. We have $p - \epsilon_a(p) \mid p^j - \epsilon_a(p)^j$. Hence if we put $k = (p^j - \epsilon_a(p)^j)/(p - \epsilon_a(p))$, then k will be an integer and we will have $p^j - \epsilon_a(p)^j = k \cdot (p - \epsilon_a(p))$. This implies $(p^j - \epsilon_a(p)^j)/2 = k \cdot (p - \epsilon_a(p))/2$. Consequently by Lemma 9.4 and Lemma 4.10 (i) we have $Y_a((p^j - \epsilon_a(p)^j)/2) = Y_a(k \cdot (p - \epsilon_a(p))/2) \equiv 0 \pmod{p^e}$.

Theorem 9.6. Suppose p is prime, $(p, 2ad) = 1$ and p^e is *elpsp*(a). Then for all $k \geq 0$ and all $j \geq 0$, we have

(i) $X_a(p^{j+k}) \equiv X_a(p^j) \pmod{p^{e+j}}$ and (ii) $Y_a(p^{j+k}) \equiv \epsilon_a(p)^k Y_a(p^j) \pmod{p^{e+j}}$.

Proof. Let $\epsilon = \epsilon_a(p)$. By (3.49.1) and (3.50.1) with i replaced by p^{j+k} and j by p^j, we have

(iii) $X_a(p^{j+k})^2 - X_a(p^j)^2 = dY_a(p^j(p^k+1)) \cdot Y_a(p^j(p^k-1))$, and

(iv) $Y_a(p^{j+k})^2 - Y_a(p^j)^2 = Y_a(p^j(p^k+1)) \cdot Y_a(p^j(p^k-1))$.

By Lemma 9.4, $p^e \mid Y_a((p-\epsilon)/2)$. Also since $p - \epsilon \mid p^k - \epsilon^k$ and $\epsilon^k = \pm 1$, we have $p - \epsilon \mid p^k \pm 1$. Hence $(p-\epsilon)/2 | p^k \pm 1$. Therefore by the Division Theorem 4.11

$$Y_a\left(\frac{p-\epsilon}{2}\right) | Y_a(p^k+1) \text{ or } Y_a\left(\frac{p-\epsilon}{2}\right) | Y_a(p^k-1).$$

Since $p^e | Y_a((p-\epsilon)/2)$, from the Law of Repetition 6.5 we get

$p^{j+e} | Y_a(p^j(p^k+1))$ or $p^{j+e} | Y_a(p^j(p^k-1))$.

By (iii) and (iv) this implies

$$X_a(p^{j+k})^2 \equiv X_a(p^j)^2 \pmod{p^{e+j}} \text{ and } Y_a(p^{j+k})^2 \equiv Y_a(p^j)^2 \pmod{p^{e+j}}.$$

Since p^{e+j} is a prime power and $(p, a) = 1$, Lemma 9.2 implies

$$X_a(p^{j+k}) \equiv \pm X_a(p^j) \pmod{p^{e+j}} \text{ and } Y_a(p^{j+k}) \equiv \pm \epsilon_a(p)^k Y_a(p^j) \pmod{p^{e+j}}.$$

Consequently by Lemma 9.2,

$$X_a(p^{j+k}) \equiv X_a(p^j) \pmod{p^{e+j}} \text{ and } Y_a(p^{j+k}) \equiv \epsilon_a(p)^k Y_a(p^j) \pmod{p^{e+j}}.$$

Corollary 9.7. Suppose $(p, 2ad) = 1$ and p^e is an *elpsp*(a). Then for all $n \geq j$ and all $m \geq j$, $X_a(p^n) \equiv X_a(p^m) \pmod{p^{e+j}}$.

Proof. By Theorem 9.6, $n \geq j$ and $m \geq j$, $X_a(p^n) \equiv X_a(p^j) \equiv X_a(p^m) \pmod{p^{e+j}}$.

Theorem 9.8. Suppose $(p, 2ad) = 1$. Then the following are equivalent:

(i) p^e is an *elpsp*(a), (ii) $X_a(p) \equiv a \pmod{p^e}$, (iii) $Y_a(p) \equiv \epsilon_a(p) \pmod{p^e}$,

(iv) $X_a(p)^2 \equiv a^2 \pmod{p^e}$, (v) $Y_a(p)^2 \equiv 1 \pmod{p^e}$, (vi) $Y_a(p \pm 1) \equiv 0 \pmod{p^e}$.

Proof. Suppose $(p, 2ad) = 1$ and (i) holds. Then (ii) holds by identity (3.85) (with $n = p$) and Lemma 9.4. Also (iii) holds by identity (3.87) (with $n = p$ and $\epsilon = \epsilon_a(p)$) and Lemma 9.4. Obviously (ii) $\Rightarrow$ (iv) and (iii) $\Rightarrow$ (v). (i) $\Rightarrow$ (vi). So (i) $\Rightarrow$ all the others. Suppose $(p, 2ad) = 1$ and (ii), (iii), (iv) or (v) holds. By (3.99) with $n = p$ and $\epsilon = \epsilon_a(p)$, $\quad (X_a(p) + a)(X_a(p) - a) = d(Y_a(p) + \epsilon_a(p))(Y_a(p) - \epsilon_a(p)) \equiv 0 \pmod{p^e}$.

Clearly $(Y_a(p) + 1, Y_a(p) - 1) \mid 2$ and $(X_a(p) + a, X_a(p) - a) \mid 2a$. Since $(p, ad) = 1$ and p^e is a prime power, $X_a(p) \equiv \pm a \pmod{p^e}$ and $Y_a(p) \equiv \pm\epsilon_a(p) \pmod{p^e}$. But by Theorems 6.10 and 6.11, $X_a(p) \equiv a \pmod{p}$ and $Y_a(p) \equiv \epsilon_a(p) \pmod{p}$.

Therefore (ii) and (iii) hold. Now by identities (3.85) and (3.87) with $n = p$, we have $Y_a\left(\frac{p+\epsilon_a(p)}{2}\right) Y_a\left(\frac{p-\epsilon_a(p)}{2}\right) \equiv 0 \pmod{p^e}$ and $X_a\left(\frac{p+\epsilon_a(p)}{2}\right) Y_a\left(\frac{p-\epsilon_a(p)}{2}\right) \equiv 0 \pmod{p^e}$.

But by Corollary 4.20 and Theorem 6.12 $(p, Y_a((p+\epsilon_a(p))/2)) = 1$. Also since $(p, a) = 1$ we have $(p, X_a((p+\epsilon_a(p))/2)) = 1$ and $X_a((p+\epsilon_a(p))/2)^2 = X_a(p+\epsilon_a(p))+2 \equiv a^2-2+2 = a^2 \pmod{p}$, by Theorem 6.24 (ii) and identity (3.90) with $n = p$ and $\epsilon = \epsilon_a(p)$. Hence (i) holds. Finally, suppose (vi) holds. Then by (3.96) with $n = p$, (v) holds. Hence (i) holds.

Corollary 9.9. Suppose $(p, 2d) = 1$. Then p^e is an *elpsp*(a) if and only if

$$(\forall k \geq 0)[X_a(p^k) \equiv a \pmod{p^e}].$$

Proof. $\Leftarrow$. Let $k = e$ and apply Lemma 9.3 or let $k = 1$ and use Theorem 9.8.

$\Rightarrow$. Suppose p^e is an *elpsp*(a). Put $j = 0$ in Theorem 9.6.

Corollary 9.10. Suppose $(p, 2d) = 1$, $c \leq e$ and p^e is an *elpsp*(a). Then p^c is an *elpsp*(a).

Proof. By Theorem 9.8 (ii), $X_a(p) \equiv a \pmod{p^e}$ implies $X_a(p) \equiv a \pmod{p^c}$.

Lemma 9.11. If $n \leq m$ and $b \equiv a \pmod{p^m}$, then $X_b(p^n) \equiv X_a(p^n) \pmod{p^{m+n}}$.

Proof. Suppose $n \leq m$ and $b = a \pm jp^m$. By Theorem 4.50 (i) (ii), with $k = jp^m$,

$$X_b(p^n) = X_{a \pm jp^m}(p^n) \equiv X_a(p^n) \pm jp^m p^n \cdot Y_a(p^n) \pmod{p^{2m}}.$$

Since $n \leq m$, we have $m + n \leq 2m$. Hence $X_b(p^n) \equiv X_a(p^n) \pmod{p^{m+n}}$.

Lemma 9.12. If $(p, 2ad) = 1$, p^i is *elpsp*(a) and $b = X_a(p)$, then $b \equiv a \pmod{p^i}$ and p^{i+1} is *elpsp*(b).

Proof. Suppose $1 \leq i$, p^i is *elpsp*(a) and $b = X_a(p)$. By Theorem 9.8, $X_a(p) \equiv a \pmod{p^i}$. Hence $b \equiv a \pmod{p^i}$. By Lemma 9.11 with $n = 1$ and $m = i$, we have $X_b(p) \equiv X_a(p) = b \pmod{p^{i+1}}$. Consequently by Theorem 9.8, p^{i+1} is an *elpsp*(b).

Theorem 9.13. If p^e is an *elpsp*(a), p^e is an *elpsp*(b) and $a \equiv b \pmod{p}$, then $a \equiv b \pmod{p^e}$.

Proof. Suppose $1 \leq e$, $(p, a^2 - 4) = 1$, p^e is *elpsp*(a), p^e is *elpsp*(b) and $a \equiv b \pmod{p}$. We shall show by induction on i that $a \equiv b \pmod{p^i}$ for every i, $(i = 1, \ldots, e)$. $i = 1$ is given. Suppose $a \equiv b \pmod{p^i}$ where $1 \leq i < e$. Then $i + 1 \leq e$. We show that $a \equiv b \pmod{p^{i+1}}$. By Lemma 9.11 with $n = i + 1$ and $m = e$, $X_b(p^{i+1}) \equiv X_a(p^{i+1}) \pmod{p^{e+i+1}}$. Hence $X_b(p^{i+1}) \equiv X_a(p^{i+1}) \pmod{p^{i+1}}$. By Corollary 9.10, p^e is *elpsp*(a) implies p^{i+1} is *elpsp*(a) and p^e is *elpsp*(b) implies p^{i+1} is *elpsp*(b). Therefore by Lemma 9.3 (ii) we have $X_a(p^{i+1}) \equiv a \pmod{p^{i+1}}$ and

$X_b(p^{i+1}) \equiv b \pmod{p^{i+1}}$. Hence $b \equiv X_b(p^{i+1}) \equiv X_a(p^{i+1}) \equiv a \pmod{p^{i+1}}$. Thus $b \equiv a \pmod{p^{i+1}}$. This proves the theorem for case $i+1$ and so the theorem is proved.

Lemma 9.14. If $(n, 2d)=1$ and n is an $elpsp(a)$, then $(n, Y_a'\left(\frac{n-\epsilon_a(n)}{2}\right))=1$.

Proof. Suppose $(n, 2d) = 1$ and n is an $elpsp(a)$. Put $k = (n-\epsilon_a(n))/2$. Then $(n,k)=1$ and $n \mid Y_a(k)$. By Lemma 4.8, $(n, X_a(k))=1$. By Corollary 2.2, $dY_a'(k) = kX_a(k)-aY_a(k)$. Hence if $p \mid n$ and $p \mid Y_a'(k)$, then we would have $p \mid Y_a(k)$ and $p \mid kX_a(k)$, a contradiction.

Theorem 9.15. If $(p, a^2-4) = 1$, then there exists a unique $b \mod p^e$ such that p^e is $elpsp(b)$ and $b \equiv a \pmod{p}$.

Proof. Suppose $(p, a^2-4) = 1$. Put $a_1 = a$. Then p is $elpsp(a_1)$. By Lemma 9.12, if $a_2 = X_{a_1}(p)$, then p^2 is $elpsp(a_2)$ and $a_2 \equiv a_1 \pmod{p^1}$. If we put $a_3 = X_{a_2}(p)$, then p^3 is $elpsp(a_3)$ and $a_3 \equiv a_2 \pmod{p^2}$. Continuing, if we put $a_4 = X_{a_3}(p)$, then p^4 is $elpsp(a_4)$ and $a_4 \equiv a_3 \pmod{p^3}$. Etc. Finally if we put $a_e = X_{a_{e-1}}(p)$, then p^e is $elpsp(a_e)$ and $a_e \equiv a_{e-1} \pmod{p^{e-1}}$. Thus if $b = a_e$, then p^e is $elpsp(b)$. To show b is unique mod p^e, suppose there is another b_1, $b_1 = b + kp^i$, $(k,p) = 1$ and p^e is $elpsp(b_1)$. Notice that $\epsilon_b = \epsilon_{b_1}$, we denote them by ϵ and then by Theorem 4.52 we have

$$Y_{b_1}\left(\frac{p^e-\epsilon^e}{2}\right) \equiv Y_b\left(\frac{p^e-\epsilon^e}{2}\right) + kp^iY_b'\left(\frac{p^e-\epsilon^e}{2}\right) \pmod{p^{i+1}}.$$

Since p^e is $elpsp(b)$ and $elpsp(b_1)$, we obtain

$$kp^iY_b'\left(\frac{p^e-\epsilon^e}{2}\right) \equiv 0 \pmod{p^{i+1}},$$

which implies $p \mid k$ since $p \nmid Y_b'\left(\frac{p^e-\epsilon^e}{2}\right)$. This contradicts $(k,p) = 1$. Hence b is unique. This completes the proof.

Theorem 9.16. For any odd prime p, the number of incongruent bases a mod p^e, such that $(p, a^2-4) = 1$ and p^e is an $elpsp(a)$, is $p-2$.

Proof. By Theorems 9.13 and 9.15, there is a 1-1 correspondence between the sets

$D = \{a : 0 \leq a < p,\ a \neq 2,\ a \neq p-2\}$ and

$D' = \{b : 0 \leq b < p^e,\ (p, b^2-4) = 1$ and p^e is an $elpsp(b)\}$.

This correspondence is given by the remainder function, $f(b) = rem(b,\ a)$.

Corollary 9.17. Suppose $p \mid a$. Then p^e is an $elpsp(a) \Leftrightarrow p^e \mid a$.

Proof. Suppose p^e is an $elpsp(a)$. By Theorem 7.25 p^e is an $elpsp(0)$. Hence we can apply Theorem 9.13, $a \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p^e} \Rightarrow p^e \mid a$.

Theorem 9.19. Let p be an odd prime and $\epsilon_a = ((a^2-4)/p)$. Among $0, 1, \cdots, p-1$ there are $((p-1)/2)-1 = (p-3)/2$ $a's$ such that $\epsilon_a = +1$ and $((p+1)/2)-1 = (p-1)/2$ $a's$ such that $\epsilon_a = -1$.

Proof. Let $A = \{a : 0 \leq a < p$ and $p \perp a^2-4\}$. Then clearly $|A| = p-2$. By Theorem 6.12, $Y_a\left(\frac{p-\epsilon_a}{2}\right) \equiv 0 \pmod{p}$ holds for all $a \in A$. Hence $Y_a((p-1)/2) \equiv 0$ and $Y_a((p+1)/2) \equiv 0$ have in total $p-2$ solutions mod p.

For $\epsilon_a = 1$, $Y_a\left(\frac{p-1}{2}\right) = Y_a\left(\frac{p-\epsilon_a}{2}\right) \equiv 0 \pmod{p}$ has at most $(p-1)/2-1 = (p-3)/2$ solutions since $Y_a((p-1)/2)$ is a polynomial of degree $(p-1)/2-1$ in a.

Similarly in the case $\epsilon_a = -1$, $Y_a\left(\frac{p+1}{2}\right) = Y_a\left(\frac{p-\epsilon_a}{2}\right) \equiv 0 \pmod{p}$ can have at most $(p+1)/2 - 1 = (p-1)/2$ solutions.

Since $(p-3)/2+(p-1)/2 = p-2$, it follows that the number of the solutions for each congruence reaches its maximum. This proves the theorem.

Lemma 9.20. Suppose p is an odd prime and $e \geq 1$. Then for any $\epsilon = \pm 1$, the number of incongruent bases a mod p^e, such that $(n,d)=1$, $\epsilon_a(p) = \epsilon$ and p^e is an *elpsp*(a), is $(p-\epsilon)/2-1$.

Proof. Put $f(x)=Y_x((p-\epsilon)/2)$. Then $f'(a)=Y_a((p-\epsilon)/2)$. Hence if $n=p$, then Lemma 9.14 states that $(p, f'(a)) = 1$. Therefore every solution of $f(a) \equiv 0 \pmod{p^e}$ is nonsingular in the sense of Definition 4.64. By Theorem 9.19, $f(a) \equiv 0 \pmod{p}$ has exactly $(p-\epsilon)/2-1$ solutions a with $\epsilon_a(p) = \epsilon$. Hence by Theorem 4.65 and Corollary 4.68, $f(a) \equiv 0 \pmod{p^e}$ has exactly $(p-\epsilon)/2-1$ solutions a with $\epsilon_a(p) = \epsilon$.

Lemma 9.21. For any $e \geq 0$ and all a such that $(p, 2d)=1$,

$$Y_a\left(\tfrac{p^e-\epsilon_a(p)p^{e-1}}{2}\right) \equiv 0 \pmod{p^e}.$$

Proof. This follows from Corollary 6.8, $r_a(p^e) \mid p^{e-1}(p-\epsilon_a(p))/2$ and Lemma 6.4.

Theorem 9.22. Suppose $n = p^e$, $e \geq 2$, $(p,6)=1$ and $\epsilon = \pm 1$. If $a = p-\epsilon$, then $(n, ad)=1$ and n is not an *elpsp*(a).

Proof. Suppose $\epsilon = \pm 1$, $n = p^e$ where $e \geq 2$ and $(p,6)=1$. Put $a = p - \epsilon$. Then $(n,d) = 1$ since $d \equiv -3 \pmod{p}$. Since $Y_a(3) = a^2 - 1 \equiv 0 \pmod{p}$, we have $r_a(p) = 3$ and therefore $r_a(p^e) = 3p^{e-1}$. Since $e \geq 2$, we have $p \mid r_a(p)$. Suppose n is an *elpsp*(a). Then $Y_a((n-\epsilon_a(n))/2) \equiv 0 \pmod{n}$. Put $k = (n-\epsilon_a(n))/2$. Then $Y_a(k) \equiv 0 \pmod{n}$. Therefore $p \mid Y_a(k)$. Hence $r_a(p) \mid k$. But $p \mid r_a(p)$, so this implies $p \mid k$. Hence $p \mid 2k$. Therefore $p \mid p^e - \epsilon_a(n)$. Hence $p \mid \epsilon_a(n)$, a contradiction. Thus n is not an *elpsp*(a). This proves the theorem.

Theorem 9.23. Suppose $n = p^e$, $e \geq 2$, $(p,6)=1$ and $\epsilon = \pm 1$. If $a = p - \epsilon$, then $(n, ad)=1$ and n is not a $rpsp(a)$.

Proof. Suppose $\epsilon = \pm 1$, $n = p^e$ where $e \geq 2$ and $(p,6)=1$. Let $a = p-\epsilon$. Then $(n,d) = 1$ since $d \equiv -3 \pmod{p}$. Since $Y_a(3) = a^2 - 1 \equiv 0 \pmod{p}$, we have $r_a(p) = 3$ and therefore $r_a(p^e) = 3p^{e-1}$. Since $e \geq 2$, we have $p \mid r_a(p)$. Suppose n is a $rpsp(a)$. Then $Y_a((n+\epsilon_a(n))/2) \equiv \rho_a(n) \pmod{n}$. Hence $Y_a((n+\epsilon_a(n))/2)^2 \equiv 1 \pmod{n}$. Put $k = (n+\epsilon_a(n))/2$. Then $Y_a(k)^2 \equiv 1 \pmod{n}$. Hence by (3.96) $Y_a(k+1)Y_a(k-1) \equiv 0 \pmod{n}$. Therefore $p \mid Y_a(k \pm 1)$. Hence $r_a(p) \mid k \pm 1$. Since $p \mid r_a(p)$, this implies $p \mid k \pm 1$. Hence $p \mid 2k \pm 2$. Therefore $p \mid p^e + \epsilon_a(n) \pm 2$. Hence $p \mid \epsilon_a(n) \pm 2$ and therefore $p \leq 3$, a contradiction. Thus n is not a $rpsp(a)$.

Theorem 9.24. Suppose $n = p^e$, $e \geq 2$, $(p,6)=1$ and $\epsilon = \pm 1$. If $a = p - \epsilon$, then $(n, ad) = 1$ and n is not an $apsp(a)$.

Proof. The proof is similar to the previous one. Suppose $\epsilon = \pm 1$, $n = p^e$ where $e \geq 2$ and $(p,6) = 1$. Let $a = p - \epsilon$. Then again $(n,d) = 1$ and $p \mid r_a(p)$. Suppose n is an $apsp(a)$. Then $X_a((n+\epsilon_a(n))/2) \equiv a\tau_a(n) \pmod{n}$. Hence $X_a((n+\epsilon_a(n))/2)^2 \equiv a^2 \pmod{n}$. Put $k = (n+\epsilon_a(n))/2$. Then $X_a(k)^2 \equiv a^2 \pmod{n}$. Hence by (1.35), $Y_a(k)^2 \equiv 1 \pmod{n}$. Therefore by (3.28′), $Y_a(k+1)Y_a(k-1) \equiv 0 \pmod{n}$. Therefore again $p \mid Y_a(k \pm 1)$. Hence $r_a(p) \mid k \pm 1$. Since $p \mid r_a(p)$, this implies $p \mid k \pm 1$. Hence again $p \mid 2k \pm 2$. Therefore $p \mid \epsilon_a(n) \pm 2$ so that $p \leq 3$. A contradiction. Hence n is not an $apsp(a)$.

Theorem 9.25. For any prime p, if $(p, 2d) = 1$, then

(i) $X_a\left(\frac{p^{2e}-1}{4}\right) \equiv \pm 2 \pmod{p^2}$ and (ii) $Y_a\left(\frac{p^{2e}-1}{4}\right) \equiv 0 \pmod{p}$.

Proof. Put $\epsilon = \epsilon_a(p)$. Then $(p+1)(p-1) = p^2-1 \Rightarrow p-\epsilon \mid p^2-1$ and $p^2-1 \mid p^{2e}-1$. Hence $\left(\frac{p+\epsilon}{2}\right)\left(\frac{p-\epsilon}{2}\right) = \frac{p^2-1}{4}$ and $(p^2-1)/4 \mid (p^{2e}-1)/4$. Therefore $(p-\epsilon)/2 \mid (p^{2e}-1)/4$. By Lemma 6.17, $p \mid Y_a((p-\epsilon)/2)$. Hence $p \mid Y_a((p^{2e}-1)/4)$ by the Division Theorem 4.11. This proves (ii). Now (i) can be derived from (ii). To obtain (i), let $k = (p^{2e}-1)/2$. By identity (1.35) and (ii), $X_a(k)^2 = dY_a(k)^2 + 4 \equiv 4 \pmod{p^2}$. Hence $p^2 \mid (X_a(k)+2)(X_a(k)-2)$. By Lemma 4.8, $(X_a(k)+2, X_a(k)-2) \mid 4$. Consequently $X_a(k) \equiv \pm 2 \pmod{p^2}$.

Lemma 9.26. If p is prime, $(p, 2d) = 1$, $\epsilon = \epsilon_a(p)$, $\tau = \tau_a(p)$ and $\rho = \rho_a(p)$, then

$$X_a\left(\tfrac{p^{e+1}-\epsilon^{e+1}}{2}\right) \equiv X_a\left(\tfrac{p^e-\epsilon^e}{2}\right)\tau \pmod{p}, \quad Y_a\left(\tfrac{p^{e+1}-\epsilon^{e+1}}{2}\right) \equiv 0 \pmod{p},$$

$$2X_a\left(\tfrac{p^{e+1}+\epsilon^{e+1}}{2}\right) \equiv X_a\left(\tfrac{p^e-\epsilon^e}{2}\right)a\tau \pmod{p}, \quad 2Y_a\left(\tfrac{p^{e+1}+\epsilon^{e+1}}{2}\right) \equiv \epsilon^e X_a\left(\tfrac{p^e-\epsilon^e}{2}\right)\rho \pmod{p},$$

Proof. By Lemma 4.36 with $j = e$, Lemma 9.1 and Theorems 7.11, 7.13 and 7.14.

Theorem 9.27. If p is prime and $(p, 2d) = 1$, then for all j

(i) $X_a\left(\tfrac{p^j-\epsilon_a(p)^j}{2}\right) \equiv 2\tau_a(p)^j \pmod{p}$, (ii) $Y_a\left(\tfrac{p^j-\epsilon_a(p)^j}{2}\right) \equiv 0 \pmod{p}$,

(iii) $X_a\left(\tfrac{p^j+\epsilon_a(p)^j}{2}\right) \equiv a\tau_a(p)^j \pmod{p}$, (iv) $Y_a\left(\tfrac{p^j+\epsilon_a(p)^j}{2}\right) \equiv \rho_a(p)^j \pmod{p}$.

Proof. By Lemma 9.26 and induction on j.

Corollary 9.28. Suppose p is an odd prime, $e \geq 0$ and $(p, 2d) = 1$. Then

(i) $X_a(p^e - \epsilon_a(p)^e) \equiv 2 \pmod{p}$, (ii) $Y_a(p^e - \epsilon_a(p)^e) \equiv 0 \pmod{p}$,

(iii) $X_a(p^e + \epsilon_a(p)^e) \equiv a^2 - 2 \pmod{p}$, (iv) $Y_a(p^e + \epsilon_a(p)^e) \equiv a\epsilon_a(p)^e \pmod{p}$.

Proof. A straightforward calculation using Theorem 9.27 and identities (3.88), (3.89), (3.90) and (3.91) with $n = p^e$. Use also $(a\tau^e)^2 - 2 = a^2 - 2$ and $a\tau^e\rho^e = a(\tau\rho)^e = a\epsilon^e$.

Lemma 9.29. If $n>1$ and $(n,2d)=1$, then

n is $ltpsp(a) \Leftrightarrow X_a\left(\frac{n-\epsilon_a(n)}{2}\right) \equiv 2\tau_a(n) \pmod{n^2}$.

Proof. Suppose $n > 1$, n odd. Let $\epsilon_a=\epsilon_a(n)$, $\tau_a=\tau_a(n)$. From (3.96),

$$\left(X_a\left(\frac{n-\epsilon_a}{2}\right)+2\tau_a\right)\left(X_a\left(\frac{n-\epsilon_a}{2}\right)-2\tau_a\right) = d\cdot Y_a\left(\frac{n-\epsilon_a}{2}\right)^2$$

and $(n, X_a((n-\epsilon_a)/2)+2\tau_a)=1$, we have n is $ltpsp(a)$ if and only if $X_a\left(\frac{n-\epsilon_a(n)}{2}\right) \equiv 2\tau_a(n) \pmod{n^2}$ since $(X_a((n-\epsilon_a)/2)+2\tau_a, X_a((n-\epsilon_a)/2)-2\tau_a) = 1$.

Lemma 9.30. If $a \equiv b \pmod{m}$ and m and n have the same set of prime divisors, then $\epsilon_a(n) = \epsilon_b(n)$, $\tau_a(n) = \tau_b(n)$ and $\rho_a(n) = \rho_b(n)$.

Proof. Suppose $n = p_1^{e_1}\cdots p_k^{e_k}$ and $m = p_1^{f_1}\cdots p_k^{f_k}$. Since $a \equiv b \pmod{m}$, we have $a \equiv b \pmod{p_i}$ for each p_i. Hence

$\epsilon_a(n)=\epsilon_a(p_1^{e_1}\cdots p_k^{e_k})=\epsilon_a(p_1)^{e_1}\cdots\epsilon_a(p_k)^{e_k}=\epsilon_b(p_1)^{e_1}\cdots\epsilon_b(p_k)^{e_k}=\epsilon_b(p_1^{e_1}\cdots p_k^{e_k})=\epsilon_b(n)$.

Thus we have $\epsilon_a(n) = \epsilon_b(n)$. Proofs of $\tau_a(n) = \tau_b(n)$ and $\rho_a(n) = \rho_b(n)$ are analogous.

Lemma 9.31. Suppose p is an odd prime, $m=p^hQ$, $n=p^{h+g}Q$, and $g\le h$. Suppose $b \equiv a \pmod{m}$ and n is an $elpsp(a)$. Then n is a $tpsp(b) \Leftrightarrow n$ is a $tpsp(a)$.

Proof. The hypotheses on m and n imply that $n \mid m^2$ and also that m and n have the same set of prime divisors. Since $b \equiv a \pmod{m}$ the second implies that $\epsilon_b(n) = \epsilon_a(n)$ and $\tau_b(n) = \tau_a(n)$, by Lemma 9.30. We have also $(n, a^2-4) = 1$ which implies $(n, b^2-4)=1$. Now $b \equiv a \pmod{m}$ also implies that there exists i such that $b = a \pm im$. By Theorem 4.50 with n replaced by $(n-\epsilon_a(n))/2$ and k replaced by im, we have

$$X_b\left(\frac{n-\epsilon_a(n)}{2}\right) \equiv X_a\left(\frac{n-\epsilon_a(n)}{2}\right) \pm im\left(\frac{n-\epsilon_a(n)}{2}\right)Y_a\left(\frac{n-\epsilon_a(n)}{2}\right) \pmod{(im)^2}.$$

Thus n is an $elpsp(a)$ implies $n \mid Y((n-\epsilon_a(n))/2)$. Hence from $n \mid m^2$ we have

$$X_b\left(\frac{n-\epsilon_a(n)}{2}\right) \equiv X_a\left(\frac{n-\epsilon_a(n)}{2}\right) \pmod{n}.$$

Since $\epsilon_b(n) = \epsilon_a(n)$ and $\tau_b(n) = \tau_a(n)$, we have n is a $tpsp(b)$ iff n is a $tpsp(a)$.

Lemma 9.32. Suppose n is odd and $n > 1$, $n = p^{h+g}Q$, $m = p^hQ$ where $g \leq h$. Then n is a $tpsp(a)$ for all bases b of the form $b = im$ and $b = im \pm 1$, $(i = 0, 1, 2, ...)$.

Proof. By Lemmas 9.31, 7.25 and 7.28. (n is an $elpsp(0)$ and an $elpsp(\pm 1)$.)

REMARK. Examples of n and m to which the corollary applies are: $n=p^2$ and $m=p$, $n=p^3$ and $m=p^2$, $n=p^4$ and $m=p^2$, $n=p^5$ and $m=p^3$, $n=p^6$ and $m=p^3$.

Theorem 9.33. Suppose $n > 1$, n is odd and $(n, 3) = 1$. Then

$$n \text{ is squarefree } \Leftrightarrow (\forall a)[(n, d) = 1 \text{ and } n \text{ is } tpsp(a) \Rightarrow n \text{ is } elpsp(a)].$$

Proof. Suppose $n > 1$ and $(n, 6) = 1$. $\Rightarrow$. Suppose n is squarefree, $(n, d) = 1$ and n is a $tpsp(a)$. Then $X_a((n-\epsilon_a(n))/2) \equiv 2\tau_a(n) \pmod{n}$. Hence $X_a((n-\epsilon_a(n))/2) \equiv \pm 2 \pmod{n}$ so that by (3.96)

$$0 \equiv \left(X_a\left(\frac{n-\epsilon_a(n)}{2}\right)+2\right)\left(X_a\left(\frac{n-\epsilon_a(n)}{2}\right)-2\right) = d \cdot Y_a\left(\frac{n-\epsilon_a(n)}{2}\right)^2 \pmod{n}.$$

Therefore $n \mid Y_a((n-\epsilon_a(n))/2)^2$, since $(n, d) = 1$. So $n \mid Y_a((n-\epsilon_a(n))/2)$, since n is squarefree.

$\Leftarrow$. Suppose $n > 1$ and $(n, 6) = 1$. Suppose n is not squarefree. Write $n = p^{h+1}Q$ where $1 \leq h$ and $(p, Q) = 1$. Let $m = p^hQ$. Then $p^h \| m$ and $n \mid m^2$. We will find b such that n is a $tpsp(b)$ and n is not an $elpsp(b)$. Let $a = \pm 1$ and put $b = m+a$. Then $b \equiv \pm 1 \pmod{m}$ but $b \not\equiv \pm 1 \pmod{n}$ since $p^h \| m$. Also $(n, 3) = 1 \Rightarrow (n, b+2) = 1$ and $(n, b-2) = 1$. Hence $(n, b^2-4) = 1$ (and $(n, b) = 1$). By Lemma 9.32, n is a $tpsp(b)$. But we will show n is not an $elpsp(b)$. Since $b-a = m$, from Theorem 4.50

with $k = m$ we have $X_b(n) \equiv X_a(n) \pm mnY_a(n) \pmod{m^2}$.

Since $n \mid m^2$, $X_b(n) \equiv X_a(n) \pmod{n}$. Since $a = \pm 1$ and $(n,3) = 1$, $X_a(n) = \pm X_1(n) = \pm 1$, by (3.13). Hence $X_b(n) \equiv \pm 1 \pmod{n}$. But $b \not\equiv \pm 1 \pmod{n}$, since $p^h \| m$. Hence $X_b(n) \not\equiv b \pmod{n}$. Therefore n is not an *elpsp*(b) by Theorem 6.24.

Theorem 9.34. Suppose $n > 1$, n odd and $(n,3) = 1$. Then

n is a prime power $\Rightarrow (\forall a)[(n,d) = 1$ and n is an *elpsp*$(a) \Rightarrow n$ is a *tpsp*$(a)]$.

Proof. Suppose $n>1$ and $(n,6)=1$. Suppose n is a prime power, $n=p^e$. By (3.96), $\left(X_a\left(\frac{p^e-\epsilon_a(p)^e}{2}\right) + 2\tau_a(n)\right)\left(X_a\left(\frac{p^e-\epsilon_a(p)^e}{2}\right) - 2\tau_a(n)\right) = d \cdot Y_a\left(\frac{p^e-\epsilon_a(p)^e}{2}\right)^2 \equiv 0 \pmod{p^e}$, which implies $X_a((p^e-\epsilon_a(p)^e)/2) \equiv \pm 2\tau_a(p)^e \pmod{p^e}$. But by Theorem 9.27 with $j=e$ $X_a((p^e-\epsilon_a(p)^e)/2) \equiv 2\tau_a(p^e) \pmod{p}$. Hence $X_a((p^e-\epsilon_a(p)^e)/2) \equiv 2\tau_a(p^e) \pmod{p^e}$.

Theorem 9.35. If $(p,d) = 1$, p^e is *apsp*$(a) \Rightarrow$ p^e is *rpsp*(a). If $(p,ad) = 1$, p^e is *apsp*$(a) \Leftrightarrow p^e$ is *rpsp*(a).

Proof. Let $n = p^e$. By (3.97) $(X_a((n+\epsilon)/2) + a\tau_a(n))(X_a((n+\epsilon)/2) - a\tau_a(n)) = d(Y_a((n+\epsilon)/2)^2 - 1)$. Hence $X_a((n+\epsilon)/2) \equiv \pm a\tau_a(n) \pmod{p^e} \Leftrightarrow Y_a((n+\epsilon)/2) \equiv \pm\rho_a(n) \pmod{p^e}$. Therefore the result follows from 9.27 (iii), $X_a((n+\epsilon)/2) \equiv a\tau_a(n) \pmod{p}$ and $Y_a((n+\epsilon)/2) \equiv \rho_a(n) \pmod{p}$, using Lemma 4.21.

Corollary 9.36. Let p be an odd prime. If $(p,d) = 1$ and p^e is an *elpsp*(a) or *apsp*(a), then p^e is *sltpsp*(a). If $(p,ad) = 1$ and p^e is an *elpsp*(a), *apsp*(a) or *rpsp*(a), then p^e is a *sltpsp*(a).

Proof. By Theorems 9.34, 9.35, 7.5, 7.23 and Corollary 7.17.1, we have

$(n,2d) = 1 \Rightarrow n$ is a *ltpsp*$(a) \Leftrightarrow n$ is a *rapsp*(a).

Lemma 9.37. Suppose p is prime and $p > 3$. If $(p, d) = 1$, then p^e is $rpsp(a) \Rightarrow p^e$ is $tpsp(a)$. Also if $p \mid a$, then p^e is a $rpsp(a) \Leftrightarrow p^e$ is a $tpsp(a) \Leftrightarrow p^{\lceil e/2 \rceil} \mid a$.

Proof. Suppose $p > 3$, $(p, d) = 1$ and p^e is a $rpsp(a)$. By (3.99) with $n = (p^e + \epsilon^e)/2$ we have

$$X_a((p^e+\epsilon^e)/2) - a\tau^e) \cdot X_a((p^e+\epsilon^e)/2) + a\tau^e) = d(Y_a((p^e+\epsilon^e)/2)^2 - 1) \equiv 0 \pmod{p^e}.$$

The GCD of the two terms on the left divides $2a$. So if $(p, a) = 1$, these terms are coprime and hence Theorem 9.27 (iii) $\Rightarrow p^e$ is an $apsp(a)$. Then by Corollary 9.36 p^e is $tpsp(a)$.

Suppose $p \mid a$ and p^e is a $rpsp(a)$. Suppose $p^f \| a$ where $f \geq 1$. Then $r_a(p^f) = 2$ and $r_a(p^{f+1}) = 2p$. Also $Y_a((p^e + \epsilon^e)/2) \equiv \rho_a(p)^e \pmod{p^e}$. Hence by (3.28′) with $n = (p^e + \epsilon^e)/2$, we have $Y_a((p^e + \epsilon^e)/2 - \epsilon^e) \cdot Y_a((p^e + \epsilon^e)/2 + \epsilon^e) \equiv 0 \pmod{p^e}$. In other words $\quad Y_a((p^e - \epsilon^e)/2) \cdot Y_a((p^e + 3\epsilon^e)/2) \equiv 0 \pmod{p^e}$.

Since $p \mid Y_a((p^e - \epsilon^e)/2)$, $2 \mid (p^e - \epsilon^e)/2$. Hence $p^f \| Y_a((p^e - \epsilon^e)/2)$ since $r_a(p^{f+1}) = 2p$. Since $2 \mid (p^e + 3\epsilon^e)/2$ and $(p, (p^e + 3\epsilon^e)/2) = 1$, we also have $p^f \| Y_a((p^e + 3\epsilon^e)/2)$. Hence $e \leq 2f$. Therefore $\lceil e/2 \rceil \leq f$. Now by (3.96)

$$(X_a((p^e - \epsilon^e)/2) - 2\tau(p)^e)(X_a((p^e - \epsilon^e)/2) + 2\tau(p)^e) = dY_a((p^e - \epsilon^e)/2)^2 \equiv 0 \pmod{p^{2f}}.$$

Consequently p^{2f} divides the left side and hence p^e divides the left side. We have $(X_a((p^e - \epsilon^e)/2) - 2\tau_a(p)^e, X_a((p^e - \epsilon^e)/2) + 2\tau_a(p)^e) = 1$. Also by Theorem 9.27 (i) we have $p \mid X_a((p^e - \epsilon^e)/2) - 2\tau_a(p)^e$. Hence $p^e \mid X_a((p^e - \epsilon^e)/2) - 2\tau_a(p)^e)$ so p^e is a $tpsp(a)$. This proves the first statement.

For the second statement suppose $p \mid a$ and p^e is a $tpsp(a)$. Assume $2 \leq e$ and $p^f \| a$. Then $r_a(p^f) = 2$ and $r_a(p^{f+1}) = 2p$. Since p^e is a $tpsp(a)$, by (3.96) with $n = (p^e - \epsilon^e)/2$,

$$dY_a((p^e - \epsilon^e)/2)^2 = (X_a((p^e - \epsilon^e)/2) - 2\tau_a(p)^e)(X_a((p^e - \epsilon^e)/2) + 2\tau_a(p)^e) \equiv 0 \pmod{p^e}.$$

Hence $p^e \mid Y_a((p^e-\epsilon^e)/2)^2$. Therefore $p^{\lceil e/2 \rceil} \mid Y_a((p^e-\epsilon^e)/2)$. But since $(p,(p^e-\epsilon^e)/2)=1$, $Y_a((p^e-\epsilon^e)/2) \not\equiv 0 \pmod{p^{f+1}}$. Hence $\lceil e/2 \rceil \leq f$ and so $e \leq 2f$. Since $r_a(p)=2$ and $2 \mid (p^e-\epsilon^e)/2+2\epsilon^e$, we have $p^f \mid Y_a((p^e-\epsilon^e)/2+2\epsilon^e)$, *i.e.* $p^f \mid Y_a((p^e+3\epsilon^e)/2)$. Therefore $p^e \mid Y_a((p^e+\epsilon^e)/2-\epsilon^e) \cdot Y_a((p^e+\epsilon^e)/2+\epsilon^e)$. Consequently by (3.28′) with $n=(p^e+\epsilon^e)/2$, we have $p^e \mid (Y_a((p^e+\epsilon^e)/2)-\rho_a(p)^e) \cdot (Y_a((p^e+\epsilon^e)/2)+\rho_a(p)^e)$. By Theorem 9.27 (iv) we know that $p \mid Y_a((p^e+\epsilon^e)/2)-\rho_a(p)^e$. Since the two factors are relatively prime it follows that $p^e \mid Y_a((p^e+\epsilon^e)/2)-\rho_a(p)^e$. Therefore p^e is a *rpsp*(a).

Theorem 9.38. Suppose p is an odd prime, $p>3$, $e \geq 1$ and $(p,d)=1$. Then

(i) p^e is a *tpsp*$(a) \Leftrightarrow X_a\left(\frac{p-\epsilon_a(p)}{2}\right) \equiv 2\tau_a(p) \pmod{p^e} \Leftrightarrow p^{\lceil e/2 \rceil}$ is an *elpsp*(a),

(ii) p^e is an *apsp*$(a) \Leftrightarrow X_a\left(\frac{p+\epsilon_a(p)}{2}\right) \equiv a\tau_a(p) \pmod{p^e} \Leftrightarrow p^e$ is an *elpsp*(a),

(iii) p^e is a *rpsp*$(a) \Leftrightarrow Y_a\left(\frac{p+\epsilon_a(p)}{2}\right) \equiv \rho_a(p) \pmod{p^e} \Rightarrow p^{\lceil e/2 \rceil}$ is an *elpsp*(a).

Proof. (i) $\Rightarrow$. Suppose p^e is a *tpsp*(a), *i.e.* that $X_a((p^e-\epsilon^e)/2) \equiv 2\tau_a(p)^e \pmod{p^e}$ where $\epsilon=\epsilon_a(p)$. By (3.96) with $n=(p^e-\epsilon^e)/2$, $\epsilon=\epsilon_a(p)$ and $\tau=\tau_a(p)$, we have

$$(X_a((p^e-\epsilon^e)/2)+2\tau^e)(X_a((p^e-\epsilon^e)/2)-2\tau^e)=dY_a((p^e-\epsilon^e)/2)^2.$$

Hence $p^e \mid Y_a((p^e-\epsilon^e)/2)^2 \Rightarrow p^{\lceil e/2 \rceil} \mid Y_a((p^e-\epsilon^e)/2) \Rightarrow r_a(p^{\lceil e/2 \rceil}) \mid (p^e-\epsilon^e)/2 \Rightarrow (r_a(p^{\lceil e/2 \rceil}),p)=1 \Rightarrow r_a(p^{\lceil e/2 \rceil}) \mid (p-\epsilon)/2 \Rightarrow p^{\lceil e/2 \rceil}$ is *elpsp*$(a) \Rightarrow p^{\lceil e/2 \rceil} \mid Y_a((p-\epsilon)/2) \Rightarrow p^e \mid Y_a((p-\epsilon)/2)^2$. Then by (3.96) with $n=(p-\epsilon)/2$, $\epsilon=\epsilon_a(p)$ and $\tau=\tau_a(p)$,

$$(X_a((p-\epsilon)/2)+2\tau)(X_a((p-\epsilon)/2)-2\tau)=dY_a((p-\epsilon)/2)^2.$$

Now $(X_a((p-\epsilon)/2)+2\tau, X_a((p-\epsilon)/2)-2\tau) \mid 4$. Also by Theorem 9.27 (i), $X_a((p-\epsilon)/2) \equiv 2\tau_a(p) \pmod{p}$. Hence $X_a((p-\epsilon)/2) \equiv 2\tau_a(p) \pmod{p^e}$.

(i) $\Leftarrow$. Suppose $X_a((p-\epsilon)/2) \equiv 2\tau_a(p) \pmod{p^e}$ where $\epsilon=\epsilon_a(p)$. By (3.96) with $n=(p-\epsilon)/2$ where $\epsilon=\epsilon_a(p)$ and with $\tau=\tau_a(p)$, we have

$$(X_a((p-\epsilon)/2)+2\tau)(X_a((p-\epsilon)/2)-2\tau) = dY_a((p-\epsilon)/2)^2.$$

Hence $p^e \mid Y_a((p-\epsilon)/2)^2 \Rightarrow p^{\lceil e/2 \rceil} \mid Y_a((p-\epsilon)/2) \Rightarrow r_a(p^{\lceil e/2 \rceil}) \mid (p-\epsilon)/2 \Rightarrow (r_a(p^{\lceil e/2 \rceil}), p) = 1$ $\Rightarrow$ $r_a(p^{\lceil e/2 \rceil}) \mid (p-\epsilon)/2 \Rightarrow r_a(p^{\lceil e/2 \rceil}) \mid (p^e-\epsilon^e)/2 \Rightarrow p^{\lceil e/2 \rceil} \mid Y_a((p^e-\epsilon^e)/2) \Rightarrow p^e \mid Y_a((p^e-\epsilon^e)/2)^2$. So by (3.96) with $n = (p^e-\epsilon^e)/2$, $\epsilon = \epsilon_a(p)$ and $\tau = \tau_a(p)$,

$$X_a((p^e-\epsilon^e)/2)+2\tau^e)(X_a((p^e-\epsilon^e)/2)-2\tau^e) = dY_a((p^e-\epsilon^e)/2)^2 \equiv 0 (\mathrm{mod}\ p^e).$$

Since the GCD of $X_a((p^e-\epsilon^e)/2)+2\tau$ and $X_a((p^e-\epsilon^e)/2)-2\tau$ divides 4, also by Theorem 9.27 (i) $X_a((p^e-\epsilon^e)/2) \equiv 2\tau_a(p)^e \pmod p$, we then obtain $X_a((p^e-\epsilon^e)/2) \equiv 2\tau_a(p)^e \pmod{p^e}$, i.e. p^e is a $tpsp(a)$.

(ii) $\Rightarrow$. Suppose p^e is an $apsp(a)$. By Corollary 9.36 p^e is an $elpsp(a)$ and a $tpsp(a)$. Lemma 9.4 implies $Y_a((p-\epsilon)/2) \equiv 0 \pmod{p^e}$ where $\epsilon = \epsilon_a(p)$. Since p^e is a $tpsp(a)$, by Theorem 9.27 (i) we have $X_a((p-\epsilon)/2) \equiv 2\tau_a(p) \pmod{p^e}$. Hence by (3.80),

$$2X_a\left(\frac{p+\epsilon_a(p)}{2}\right) = aX_a\left(\frac{p-\epsilon_a(p)}{2}\right) + \epsilon dY_a\left(\frac{p-\epsilon_a(p)}{2}\right) \equiv a2\tau_a(p) = 2a\tau_a(p) \pmod{p^e}.$$

Dividing by 2 we have the result, $X_a((p+\epsilon_a(p))/2) \equiv a\tau_a(p) \pmod{p^e}$.

(ii) $\Leftarrow$. Suppose $X_a((p+\epsilon_a(p))/2) \equiv a\tau_a(p) \pmod{p^e}$. By (3.29′) with $n = (p-\epsilon)/2$,

$$(X_a((p+\epsilon)/2) - a)(X_a((p+\epsilon)/2) + a) = d(Y_a((p+\epsilon)/2) - \epsilon)(Y_a((p+\epsilon)/2) + \epsilon).$$

where $\epsilon = \epsilon_a(p)$. Hence $Y_a((p+\epsilon)/2) \equiv \pm\epsilon \pmod{p^e}$. By (3.28′) we have

$$Y_a((p+\epsilon)/2-\epsilon)\cdot Y_a((p+\epsilon)/2+\epsilon) = (Y_a((p+\epsilon)/2)+\epsilon)(Y_a((p+\epsilon)/2)-\epsilon).$$

Hence $p^e \mid Y_a((p+\epsilon)/2+\epsilon)\cdot Y_a((p+\epsilon)/2-\epsilon)$. We consider two cases:

Case 1. $(p,a) = 1$. Corollary 4.19 states that $(Y_a((p+\epsilon)/2-\epsilon), Y_a((p+\epsilon)/2+\epsilon)) \mid a$. Since $(p,a) = 1$ we have $p^e \mid Y_a((p+\epsilon)/2-\epsilon)$ or $p^e \mid Y_a((p+\epsilon)/2+\epsilon)$. In the first case $p^e \mid Y_a((p-\epsilon)/2)$ so that p^e is an $elpsp(a)$ and hence by Corollary 9.36 p^e is an $apsp(a)$. In the second case $p^e \mid Y_a((p+\epsilon)/2+\epsilon)$. Hence $p^e \mid Y_a((p+3\epsilon)/2)$ and then $p^e \mid Y_a(p+3\epsilon)$. Since $(p,3) = 1$, this implies $(r_a(p^e), p) = 1$. By Lemma 6.13 (v), $r_a(p^e) = r_a(p)$ and

hence $r_a(p^e) \mid (p-\epsilon)/2$. Therefore by Lemma 9.4, p^e is an $elpsp(a)$. Hence by Lemma 9.27, p^e is an $apsp(a)$.

Case 2. $p \mid a$. We will show that $p \mid a$ and $X_a((p+\epsilon_a(p))/2) \equiv \pm a \pmod{p^e} \Rightarrow p^e \mid a$. Suppose $p^f \| a$ where $1 \leq f$ and $f \leq e$. Let $\epsilon = \epsilon_a(p)$. Since $p^f \| a$ and $f \leq e$, $p^f \mid X_a((p+\epsilon)/2)$. Also $p^f \| a$ and $Y_a(2) = a \Rightarrow p^f \mid Y_a(2)$ so that $r_a(p^f) = 2$ and $r_a(p^{f+1}) = 2p$. By Lemma 6.12, $p \mid Y_a((p-\epsilon)/2)$. Hence $p^f \mid Y_a((p-\epsilon)/2)$. By (3.99),

$$(X_a((p+\epsilon)/2)+a)(X_a((p+\epsilon)/2)-a) = d(Y_a((p+\epsilon)/2)+\rho_a(p))(Y_a((p+\epsilon)/2)-\rho_a(p)).$$

Now p^{e+f} divides the left side. Also $p \mid Y_a((p+\epsilon)/2)-\rho_a(p)$, by Theorem 9.27 (iv). And $(Y_a((p+\epsilon)/2)+\rho_a(p), Y_a((p+\epsilon)/2)-\rho_a(p)) = 1$. Hence $p^{e+f} \mid Y_a((p+\epsilon)/2)-\rho_a(p)$. By (3.28′) we obtain

$$Y_a((p-\epsilon)/2)(Y_a((p+3\epsilon)/2) = (Y_a((p+\epsilon)/2)+\rho_a(p))(Y_a((p+\epsilon)/2)-\rho_a(p)) \equiv 0 \pmod{p^{e+f}}.$$

Thus $p^{e+f} \mid Y_a((p-\epsilon)/2)(Y_a((p+3\epsilon)/2)$. Since $p^f \| Y_a((p-\epsilon)/2)$, it follows that $p^e \mid Y_a((p+3\epsilon)/2)$ and hence that $p^e \mid Y_a(p+3\epsilon)$. Therefore $r_a(p^e) \mid p+3\epsilon$. Since $(p,3) = 1$, we have $(p, p+3\epsilon) = 1$. But $p \mid r_a(p^{f+1})$. Hence $r_a(p^e) \mid p+3\epsilon \Rightarrow e \leq f$. This proves $p^e \mid a$. Hence $a \equiv 0 \pmod{p^e}$. By Theorem 7.25, p^e is an $apsp(0)$. Hence p^e is an $apsp(a)$.

(iii) $\Rightarrow$. Suppose p^e is a $rpsp(a)$. Then $(p,d) = 1$. We consider two cases:

Case 1. $(p,a) = 1$. Let $\epsilon = \epsilon_a(p)$. By Theorem 9.35, p^e is an $apsp(a)$ and hence p^e is an $elpsp(a)$ and a $tpsp(a)$. By Lemma 9.4, p^e is an $elpsp(a) \Rightarrow Y_a((p-\epsilon)/2) \equiv 0 \pmod{p^e}$. Since p^e is a $tpsp(a)$, by Theorem 9.27 (i) we have $X_a((p-\epsilon_a(p))/2) \equiv 2\tau_a(p) \pmod{p^e}$. Hence by (3.81) with n replaced by p we have

$$2Y_a\left(\tfrac{p+\epsilon_a(p)}{2}\right) = aY_a\left(\tfrac{p-\epsilon_a(p)}{2}\right) + \epsilon X_a\left(\tfrac{p-\epsilon_a(p)}{2}\right) \equiv 0 + \epsilon_a 2\tau_a(p) = 2\rho_a(p) \pmod{p^e}.$$

Dividing by 2 we have the result, $Y_a((p+\epsilon_a(p))/2) \equiv \rho_a(p) \pmod{p^e}$.

Case 2. $p \mid a$. Let $\epsilon = \epsilon_a(p)$. In this case by Lemma 9.37, since p^e is a $rpsp(a)$, p^e is a $tpsp(a)$ and $p^{\lceil e/2 \rceil} \mid a$. By (3.96), with $n = (p-\epsilon)/2$, and by Theorem 9.38 (i), we have $p^e \mid Y_a((p-\epsilon)/2)^2$. Hence $p^{\lceil e/2 \rceil} \mid Y_a((p-\epsilon)/2)$. Therefore $p^e \mid aY_a((p-\epsilon)/2)$ since $p^{\lceil e/2 \rceil} \mid a$. By Theorem 9.38 (i), since p^e is $tpsp(a)$, $X_a((p-\epsilon)/2) \equiv 2\tau_a(p) \pmod{p^e}$. Therefore by (3.81) with n replaced by p, again we have

$$2Y_a\left(\tfrac{p+\epsilon_a(p)}{2}\right) = aY_a\left(\tfrac{p-\epsilon_a(p)}{2}\right) + \epsilon X_a\left(\tfrac{p-\epsilon_a(p)}{2}\right) \equiv 0 + \epsilon_a 2\tau_a(p) = 2\rho_a(p) \pmod{p^e}.$$

Dividing by 2 we obtain the result, $Y_a((p+\epsilon_a(p))/2) \equiv \rho_a(p) \pmod{p^e}$.

(iii) $\Leftarrow$. Suppose $Y_a((p+\epsilon_a(p))/2) \equiv \rho_a(p) \pmod{p^e}$. We will consider two cases:

Case 1. $(p,a) = 1$. Let $\epsilon = \epsilon_a(p)$. By (3.99) with n replaced by $(p+\epsilon)/2$, we have

$$(X_a((p+\epsilon)/2)+a)(X_a((p+\epsilon)/2)-a) = d(Y_a((p+\epsilon)/2)+1)(Y_a((p+\epsilon)/2)-1) \pmod{p^e}.$$

Since $(p,a) = 1$, by Theorem 9.27 (i) this implies $X_a((p+\epsilon)/2) \equiv a\tau_a(p) \pmod{p^e}$. Hence by Theorem 9.38 (ii), p^e is an $apsp(a)$. Hence by Theorem 9.35 p^e is an $rpsp(a)$.

Case 2. $p \mid a$. We will show $Y_a((p+\epsilon_a(p))/2) \equiv \pm 1 \pmod{p^e} \Rightarrow p^e$ is $tpsp(a)$. (Also that $p^{\lceil e/2 \rceil} \mid a$.) Since $p \mid a$, it will follow by Lemma 9.37 that p^e is a $rpsp(a)$. Suppose $p \mid a$ and $Y_a((p+\epsilon)/2) \equiv \pm 1 \pmod{p^e}$ where $\epsilon = \epsilon_a(p)$. Suppose $p^f \| a$ where $1 \le f$. Again we have $r_a(p^f) = 2$ and $r_a(p^{f+1}) = 2p$. By (3.28′) with $n = (p+\epsilon)/2$, we have

$$Y_a((p-\epsilon)/2) \cdot Y_a((p+3\epsilon)/2) = (Y_a((p+\epsilon)/2)+1)(Y_a((p+\epsilon)/2)-1) \equiv 0 \pmod{p^e}.$$

Since $p^f \| Y_a((p-\epsilon)/2)$ and $p^f \| Y_a((p+3\epsilon)/2)$, we have $e \le 2f$ and hence that $e/2 \le f$. Now $p^f \mid Y_a((p^e-\epsilon^e)/2) \Rightarrow p^{2f} \mid Y_a((p^e-\epsilon^e)/2)^2$. Also by (3.96) with $n = (p^e-\epsilon^e)/2$,

$$(X_a((p^e-\epsilon^e)/2)-2\tau_a(p)^e)(X_a((p^e-\epsilon^e)/2)+2\tau_a(p)^e) = dY_a((p^e-\epsilon^e)/2)^2 \equiv 0 \pmod{p^e}.$$

Thus the product of the two factors on the left side is divisible by p^e. Their GCD divides 4 and p divides the first, by Theorem 9.27 (i). Hence

$p^e \mid X_a((p^e-\epsilon^e)/2)-2\tau_a(p)^e$. Thus p^e is a $tpsp(a)$. By Lemma 9.37, since $p \mid a$, we have p^e is a $rpsp(a)$.

Remark. In Theorem 9.38 the hypothesis $p > 3$ is necessary since *e.g.* if $p = 3$, $e = 4$ and $a = 3$, then (iii) fails to hold in the direction $\Leftarrow$ because 3^4 is not a $rpsp(3)$. However $Y_3((3+\epsilon_3(3))/2) \equiv Y_3((3+(-1))/2) \equiv Y_3(1) = 1 = \rho_3(3) \pmod{3^4}$.

Theorem 9.39. If p is prime, $(p, 2d) = 1$ and p^e is an $elpsp(a)$, then

(i) p^e is a $tpsp(a) \Leftrightarrow (\forall i \geq 0)\left[X_a\left(\frac{p^i-\epsilon_a(p)^i}{2}\right) \equiv 2\tau_a(p)^i \pmod{p^e}\right]$

(ii) p^e is an $apsp(a) \Leftrightarrow (\forall i \geq 0)\left[X_a\left(\frac{p^i+\epsilon_a(p)^i}{2}\right) \equiv a\tau_a(p)^i \pmod{p^e}\right]$

(iii) p^e is a $rpsp(a) \Leftrightarrow (\forall i \geq 0)\left[Y_a\left(\frac{p^i+\epsilon_a(p)^i}{2}\right) \equiv \rho_a(p)^i \pmod{p^e}\right]$.

Proof. $\Leftarrow$ is trivial.

$\Rightarrow$. By Theorem 9.38, Corollary 9.5 and induction on i using Lemma 4.36.

Corollary 9.40. If $c \leq e$ and p^e is a $tpsp(a)$, then p^c is a $tpsp(a)$.

Lemma 9.41. Suppose k is odd and $\epsilon = \pm 1$. Then

(i) $2X_a(p^e k) \equiv X_a(p^e - \epsilon^e)X_a(k) \pmod{Y_a(p^e - \epsilon^e)}$,

(ii) $2Y_a(p^e k) \equiv \epsilon^e X_a(p^e - \epsilon^e)Y_a(k) \pmod{Y_a(p^e - \epsilon^e)}$.

Proof. By (4.32) and (4.35) with $n = p^e - \epsilon^e$ and $r = \epsilon^e k$. Also for any odd k, $X_a(\epsilon^e k) = X_a(k)$ and $Y_a(\epsilon^e k) = \epsilon^e Y_a(k)$ by (1.46).

Theorem 9.43. If p is an odd prime, k is odd and $(p, d) = 1$, then

(i) $X_a(p^e k) \equiv X_a(k) \pmod{p}$, (ii) $Y_a(p^e k) \equiv \epsilon_a(p)^e Y_a(k) \pmod{p}$.

Proof. By Corollary 9.28 and Lemma 9.41 with $\epsilon = \epsilon_a(p)$.

Corollary 9.44. If p and q are distinct odd primes, $(p, a^2-4) = 1$ and $(q, a^2-4) = 1$,

then (i) $aX_a(p^eq^f) \equiv X_a(p^e)X_a(q^f) \pmod{pq}$,

(ii) $Y_a(p^eq^f) \equiv Y_a(p^e)Y_a(q^f) \pmod{pq}$.

Proof. By Lemma 9.2 we have $X_a(p^e) = a \pmod{p}$, $X_a(q^f) = a \pmod{q}$, $Y_a(p^e) = \epsilon_a(p)^e \pmod{p}$ and $Y_a(q^f) = \epsilon_a(q)^f \pmod{q}$. Hence by Theorem 9.42,

$aX_a(p^eq^f) \equiv X_a(p^e)X_a(q^f) \pmod{p}$, $Y_a(p^eq^f) \equiv Y_a(p^e)Y_a(q^f) \pmod{p}$,

$aX_a(p^eq^f) \equiv X_a(p^e)X_a(q^f) \pmod{q}$, $Y_a(p^eq^f) \equiv Y_a(p^e)Y_a(q^f) \pmod{q}$.

§10. Quadratic residues and Lucas primitive roots

In this section, we will discuss some results about quadratic residues. These will be used in next section. Also we will define a new concept, Lucas primitive roots mod n, prove that each prime has a Lucas primitive root and that each odd integer n has a Lucas primitive root. Recall the definition of the totient function which we defined in §6. $T_a(n)$ is analogous to Euler's ϕ function in that it has the properties:
(i) $n \mid Y_a(T_a(n))$, (ii) if $r_a(n)$ denotes the rank of n, then $r_a(n) \mid T_a(n)$.

Theorem 10.1. Let p be an odd prime and $\epsilon_a = ((a^2-4)/p)$. Among $0, 1, \cdots, p-1$ there are $((p-1)/2)-1=(p-3)/2$ $a's$ such that $\epsilon_a=+1$ and $((p+1)/2)-1=(p-1)/2$ $a's$ such that $\epsilon_a=-1$.

Proof. This is proved in §9. (Theorem 9.19.)

Lemma 10.2. Suppose p is an odd prime. For any $\epsilon = \pm 1$, if $r \mid (p-\epsilon)/2$, then

$$Y_a(r) \equiv 0 \pmod{p} \tag{10.2}$$

has exactly $r-1$ solutions in a, each satisfying $(p, a^2-4)=1$ and $\epsilon_a(p) = \epsilon$.

Proof. Suppose $\epsilon=\pm 1$. If $r=1$, then $Y_a(r)=1$. Hence it is clear that (10.2) has no solution. Suppose $r>1$ and $r \mid (p-\epsilon)/2$. Let the congruence (10.2) have k incongruent solutions. Since the degree of $Y_a(r)$ is $r-1$ and since the leading coefficient is 1 which is prime to p, by Lagrange's theorem $k \leq r-1$. Also we know by Theorem 10.1 that

$$Y_a\left(\frac{p-\epsilon}{2}\right) \equiv 0 \pmod{p} \tag{1}$$

has exactly $\frac{p-\epsilon}{2}-1$ solutions mod p. Since $r \mid \frac{p-\epsilon}{2}$, by the Division Theorem 4.11, we have

(2) $$Y_a\left(\frac{p-\epsilon}{2}\right) = Y_a(r)\cdot H(a).$$

where $H(a)$ is a polynomial in a of degree $((p-\epsilon)/2)-r$. Since congruence (10.2) has k solutions, (1) and (2) imply $H(a)\equiv 0 \pmod p$ has exactly $((p-\epsilon)/2)-1-k$ solutions. Hence $((p-\epsilon)/2)-1-k \le ((p-\epsilon)/2)-r$. This implies $k \ge r-1$. Then $k \le r-1$ and $k \ge r-1$ imply $k = r-1$. That each solution a satisfies $(p, a^2-4)=1$ and $\epsilon_a(p)=\epsilon$ follows from the GCD Theorem. This proves the lemma.

Definition 10.3. $\psi_n(r) = |\{a:\ 0\le a<n, (n,a^2-4)=1 \text{ and } r_a(n)=r\}|$.

In particular, if n is a prime power, $n=p^e$, then for $\epsilon=\pm 1$ we define

$$\psi_n^\epsilon(r) = |\{a:\ 0\le a<n, (n,a^2-4)=1, \epsilon_a(p)=\epsilon \text{ and } r_a(n)=r\}|.$$

Lemma 10.4. Suppose p is an odd prime, $\epsilon=\pm 1$ and k is a positive integer. Then

$$\text{if } \ k \mid \frac{p-\epsilon}{2}, \ \text{ then } \ \sum_{r\mid k}\psi_p^\epsilon(r) = k-1.$$

If $k \nmid (p-\epsilon)/2$, then the sum is 0.

Proof. By Lemma 6.4, $r_a(p) \mid k \Leftrightarrow Y_a(k)\equiv 0 \pmod p$. Hence by the Division Theorem 4.11 the above sum $\sum_r \psi_p^\epsilon(r)$ counts the elements in the union of the sets in the definition 10.3. Thus by Lemma 10.2

$$\sum_{r\mid k}\psi_p^\epsilon(r) = |\{a: 0\le a<p, (p,a^2-4)=1, \epsilon_a(p)=\epsilon \text{ and } Y_a(k)\equiv 0 \pmod p\}| = k-1$$

We shall use next the Möbius function μ. Recall that $\mu(1)=1$, $p^2\mid n \Rightarrow \mu(n)=0$ and if n is squarefree, $n=p_1p_2\cdots p_k$, then $\mu(n)=(-1)^k$. Recall also that μ satisfies

Lemma 10.5. If $1<k$, then $\sum_{j\mid k}\mu(j)=0$. For any k, $\sum_{j\mid k}\mu(j)\frac{k}{j}=\phi(k)$.

Theorem 10.6. (Williams [51]). If $\epsilon=\pm 1$, $1<k$ and $k\,|\,\frac{p-\epsilon}{2}$, then $\psi_p^\epsilon(k)=\phi(k)$.

Proof. We use 10.4, 10.5 and Möbius Inversion. Since $i\,|\,k$ and $j\,|\,(k/i)$ if and only if $j\,|\,k$ and $i\,|\,(k/j)$,

$$\psi_p^\epsilon(k)=\sum_{i=k}\psi_p^\epsilon(i)1=\sum_{i|k}\psi_p^\epsilon(i)\left(\sum_{j|k/i}\mu(j)\right)=\sum_{i|k}\sum_{j|k/i}\psi_p^\epsilon(i)\mu(j)=\sum_{j|k}\sum_{i|k/j}\mu(j)\psi_p^\epsilon(i)$$

$$=\sum_{j|k}\mu(j)\left(\sum_{i|k}\psi_p^\epsilon(i)\right)=\sum_{j|k}\mu(j)\left(\frac{k}{j}-1\right)=\sum_{j|k}\mu(j)\frac{k}{j}-\sum_{j|k}\mu(j)=\phi(k)-0=\phi(k),$$

by Lemmas 10.4 and 10.5, since $(k/j)\,|\,(p-\epsilon)/2$. This proves the theorem.

Lemma 10.7. Suppose $\epsilon=((a^2-4)/p)$ and $r\,|\,(p-\epsilon)/2$. If $Y_a(r)\equiv 0 \pmod p$, then $Y_a'(r)\not\equiv 0 \pmod p$.

Proof. This is Lemma 9.14.

Lemma 10.8. (i) If $p>3$ is a prime, then there exists a such that $(p,a(a^2-4))=1$ and $r_a(p)=(p+1)/2$. If $p>5$, there exists a such that $(p,a(a^2-4))=1$ and $r_a(p)=(p-1)/2$.

(ii) If p is an odd prime, then there exists a such that $(p,a^2-4)=1$ and $r_a(p)=(p+1)/2$. If $p>3$, there exists a such that $(p,a^2-4)=1$ and $r_a(p)=(p-1)/2$.

Proof. Let $k=(p-\epsilon)/2$. $5\le p \Rightarrow 1<k$. Hence by Theorem 10.6, $\psi_p^\epsilon(k)=\phi(k)>0$. Here $p=3$ and $\epsilon=+1$ is an exception since then $\phi((p-\epsilon)/2)=\phi((3-1)/2)=\phi(2/2)=\phi(1)=0$, but the number of Lucas primitive roots a with $\epsilon_a(p)=\epsilon$ is 0.

Lemma 10.9. Suppose $p \mid n$ and p is an odd prime. (i) If $p \geq 5$, then there exists a such that $(n, a(a^2-4))=1$ and $r_a(p) = (p+1)/2$. If $p \geq 5$, there exists a such that $(n, a(a^2-4))=1$ and $r_a(p) = (p-1)/2$.

(ii) If $p \geq 3$, then there exists a such that $(n, a^2-4)=1$ and $r_a(p) = (p+1)/2$. If $p \geq 5$, then there exists a such that $(n, a^2-4)=1$ and $r_a(p) = (p-1)/2$.

Proof. Let $n = mp^e$ with $(m,p)=1$. For (i). By Lemma 10.8 (i), we can find a such that $r_a(p) = (p \pm 1)/2$ and $(p, a(a^2-4)) = 1$. By the CRT, there exists b, $b \equiv a \pmod{p}$ and $b \equiv 1 \pmod{m}$. Hence $r_b(p) = r_a(p) = (p \pm 1)/2$. To show that $(n, b(b^2-4)) = 1$, it is enough to show that if a prime $q \mid n$, then $(q, b(b^2-4)) = 1$. If $q = p$, since $b \equiv a \pmod{p}$ and $(p, a(a^2-4)) = 1$, it implies $(q, b(b^2-4)) = 1$. If $q \neq p$, then $q \mid m$. Hence from $b \equiv 1 \pmod{m}$, we have $b \equiv 1 \pmod{q}$. Thus $b \not\equiv \pm 2 \pmod{q}$ and $b \not\equiv 0 \pmod{q}$ so that $(q, b(b^2-4)) = 1$. The proof of (ii) is same as the proof of (i).

Theorem 10.10. Suppose p is an odd prime. Let $\epsilon = \pm 1$. If $r \mid (p-\epsilon)/2$, then the congruence $Y_a(r) \equiv 0 \pmod{p^e}$ has $r-1$ incongruent solutions in $a \bmod p^e$, each satisfying $(p, a^2-4)=1$ and $\epsilon_a(p) = \epsilon$.

Proof. Suppose $\epsilon = \pm 1$ and $r \mid (p-\epsilon)/2$. Suppose $Y_a(r) \equiv 0 \pmod{p}$. Then by Lemma 10.7 we have $p \not| Y_a'(r)$. Since $Y_a(r) \equiv 0 \pmod{p}$ has $r-1$ incongruent solutions, by Theorem 4.65 and Corollary 4.68, it follows that $Y_a(r) \equiv 0 \pmod{p^e}$ also has $r-1$ incongruent solutions.

Lemma 10.11. Suppose $n > 1$ and $(n, 6)=1$, then

(i) there exists a such that $(n, a^2-4)=1$ and $\epsilon_a(n) = 1$.

(ii) $n \neq \square$ implies that there exists a such that $(n, a^2-4)=1$ and $\epsilon_a(n) = -1$.

Proof. For the proof (i). Suppose $p_1, \ldots, p_k$ are all prime divisors of n. Since $(n,6)=1$, $p_i > 3$ for all $1 \le i \le k$. Hence by Theorem 10.1, we can find a_i for each i such that $\epsilon_{a_i}(p_i) = 1$. Applying the CRT, we can find a such that $(n, a^2-4)=1$ and $\epsilon_a(p_i) = \epsilon_{a_i}(p_i)$ for each i. Therefore $\epsilon_a(n) = 1$.

For the proof (ii). Suppose $p_1, \ldots, p_k$ are all prime divisors of n. Since $n \neq \square$, there is a i such that $p_i^{e_i} \| n$ and e_i is odd. By Theorem 10.1, we can find a_i such that $\epsilon_{a_i}(p_i) = -1$ and for all $j \neq i$ find a_j such that $\epsilon_{a_j}(p_j) = 1$. Using the CRT we can find a such that $(n, a^2-4)=1$ and $\epsilon_a(p_i) = \epsilon_{a_i}(p_i)$ for all i. Hence we have $\epsilon_a(n) = -1$.

Lemma 10.12. If $n>3$ and $n \neq \square$, then there exist a, b such that

$$1 \le a, b \le n, (n, ab(a^2-4)(b^2-4))=1 \text{ and } \rho_a = -\rho_b.$$

If $n > 3$ and $n \neq \square$, then exist a, b such that

$$1 \le a, b \le n, (n, ab(a^2-4)(b^2-4))=1 \text{ and } \tau_a = -\tau_b.$$

Proof. This is directly from the theory of quadratic residues.

Lemma 10.13. If $n > 1$, $(n,6) = 1$ and $n \neq \square$, then there exist a, b such that $1 \le a, b \le n$, $(n, a(a^2-4))=1$, $(n, b(b^2-4))=1$, $\epsilon_a = \epsilon_b$ and $\rho_a = -\rho_b$.

Proof. Since $n \neq \square$, by Lemma 10.12, there exist $1 \le a, b \le n$ such that $(n, a(a^2-4))=1$, $(n, b(b^2-4))=1$ and $\rho_a=1$, $\rho_b=-1$. Put

$$A=\{a : 1 \le a \le n, (n, a(a^2-4)) = 1 \text{ and } \rho_a=1\}$$

$$B=\{b : 1 \le b \le n, (n, b(b^2-4)) = 1 \text{ and } \rho_b=-1\}.$$

If for all $a \in A$, all $b \in B$, $\epsilon_a \neq \epsilon_b$, then either

(i) $\forall a \in A \forall b \in B(\epsilon_a = 1 \ \& \ \epsilon_b = -1)$ or (ii) $\forall a \in A \forall b \in B(\epsilon_a = -1 \ \& \ \epsilon_b = 1)$.

Let $C = A \cup B = \{1 \le c \le n : (n, c(c^2-4)) = 1\}$. Since $\epsilon = \rho \cdot \tau$, case (i) implies $\rho_c = \epsilon_c$ for all $c \in C$, and case (ii) implies $\rho_c = -\epsilon_c$ for all $c \in C$. Since $n \neq \square$, τ_c is not

constantly 1 and also τ_c is not constantly -1. It shows neither (i) nor (ii) holds. So the lemma follows.

Lemma 10.14. Suppose $n = uv$, $u \neq \square$, $(u,v)=1$, then there exist $1 \leq a,b \leq n$ such that $(n, ab(a^2-4)(b^2-4))=1$, $\rho_a(n) = -\rho_b(n)$, $\epsilon_a(n) = \epsilon_b(n)$ and $a \equiv b \pmod{v}$.

Proof. Applying Lemma 10.13 with $n = u$, we can find $1 \leq a, a_1 \leq u$, such that $(u, aa_1(a^2-4)(a_1^2-4))=1$, $\rho_a(u) = -\rho_{a_1}(u)$ and $\epsilon_a(u) = \epsilon_{a_1}(u)$. By the CRT we can make $(n, aa_1(a^2-4)(a_1^2-4))=1$. Then using the CRT we can find $1 \leq b \leq n$ such that $b \equiv a_1 \pmod{u}$ and $b \equiv a \pmod{v}$. Hence $(n, b(b^2-4))=1$ and

$$\rho_a(n) = \rho_a(u)\rho_a(v) = (-\rho_{a_1}(u))\rho_a(v) = -\rho_b(u)\rho_b(v) = -\rho_b(n),$$

$$\epsilon_a(n) = \epsilon_a(u)\epsilon_a(v) = \epsilon_{a_1}(u)\epsilon_a(v) = \epsilon_b(u)\epsilon_b(v) = \epsilon_b(n).$$

This completes the proof.

Now we give the definition of Lucas primitive root mod n and then prove the existence of Lucas primitive roots for each odd integer $n > 1$.

Definition 10.15. a is a *Lucas primitive root* mod n if $r_a(n) = T_a(n)$. In the case that n is a prime power, $n = p^e$, a is a *Lucas primitive root+* for p^e if $(p, a^2-4)=1$, $\epsilon_a(p) = 1$, $r_a(p^e) = p^{e-1}(p - \epsilon_a(p))/2 = p^{e-1}(p-1)/2$, and a is a *Lucas primitive root−* for p^e if $(p, a^2-4)=1$, $\epsilon_a(p) = -1$ and $r_a(p^e) = p^{e-1}(p-\epsilon_a(p))/2 = p^{e-1}(p+1)/2$.

Examples: 0 is a Lucas primitive root− for 3. 3 is a Lucas primitive root− for 3^e.
0 is a Lucas primitive root+ for 5. ± 1 are Lucas primitive roots− for 5.
5 is a Lucas primitive root+ for 5^e. ± 1 are Lucas primitive roots+ for 7.

Lemma 10.16. Suppose p is an odd prime and $e \geq 1$. Then for all a such that $(p, a^2-4)=1$,

(i) $-a$ is a Lucas primitive root for $p^e \Leftrightarrow a$ is a Lucas primitive root for p^e.

(ii) a is a Lucas primitive root for $p^e \Rightarrow a$ is a Lucas primitive root for p.

(iii) If $5 < p$, then 0 is not a Lucas primitive root for p.

(iv) If $5 < p$, then p is not a Lucas primitive root for p^2.

(v) If $7 < p$, then 1 and -1 are not Lucas primitive roots for p.

Proof. (i) holds since $\epsilon_{-a}(p) = \epsilon_a(p)$, $(\forall k)[Y_{-a}(k) = \pm Y_a(k)]$ and $r_{-a}(p^e) = r_a(p^e)$. For others use Lemma 6.7.

Theorem 10.17. Every odd prime has a Lucas primitive root. If $p > 3$, then p has Lucas primitive roots of both $+$ and $-$ type. If $\epsilon = \pm 1$, then there exists an integer a such that $(p, a^2-4) = 1$, $\epsilon_a(p) = \epsilon$ and $r_a(p) = \frac{p-\epsilon}{2}$. Further, for each $\epsilon = \pm 1$, the number of a which satisfy $\epsilon_a(p) = \epsilon$ and are Lucas primitive roots mod p, is $\phi((p-\epsilon)/2)$.

Proof. This follows from Theorem 10.6.

Lemma 10.18. Suppose p is an odd prime, $p > 3$, $(p, a^2-4) = 1$, $1 \leq c$ and $(p, s)=1$. Then $r_a(p^c) = s \Leftrightarrow r_a(p^{c+1}) = ps$ or $r_{a\pm p^c}(p^{c+1}) = ps$.

Proof. $\Rightarrow$. Suppose $r_a(p^c) = s$. Note that by Lemma 6.3, $a \pm p^c \equiv a \pmod{p^c}$ implies $r_{a\pm p^c}(p^c) = r_a(p^c) = s$. Since $r_a(p^c) = s$ implies $p^c \mid Y_a(s)$, we consider 2 cases: Case 1: $p^c \| Y_a(s)$. In this case, since $r_a(p^c) = s$, we have $p^c \| Y_a(r_a(p^c))$. Hence by Lemma 6.6 with $e = c$ and $f = 1$ we have $r_a(p^{c+1}) = p \cdot r_a(p^c)$. Hence $r_a(p^{c+1}) = ps$.

Case 2: $p^{c+1} | Y_a(s)$. By Theorem 4.50 with $k = p^c$ and $n = s$, we have

$$dY_{a\pm p^c}(s) \equiv \pm p^c s X_a(s) + (d \mp ap^c) Y_a(s) \pmod{p^{2c}}.$$

Since $p^{c+1} | Y_a(s)$ and $c+1 \leq 2c$, this implies

$$dY_{a\pm p^c}(s) \equiv \pm p^c s X_a(s) \pmod{p^{c+1}}.$$

Since p is odd, Lemma 4.8 implies $p \mid Y_a(s) \Rightarrow (p, X_a(s)) = 1$. By assumption $(p, s) = 1$. Thus $(p, sX_a(s)) = 1$. Hence $p^c \| Y_{a\pm p^c}(s)$. Therefore $p^c \| Y_{a\pm p^c}(r_a(p^c))$ and $p^c \| Y_{a\pm p^c}(r_{a\pm p^c}(p^c))$. Consequently by Lemma 6.6 with a replaced by $a \pm p^c$, $e = c$ and $f = 1$, we have

$$r_{a\pm p^c}(p^{c+1}) = p \cdot r_{a\pm p^c}(p^c) = p \cdot r_a(p^c) = ps,$$

which completes the proof in the $\Rightarrow$ direction. Next we consider the converse.

$\Leftarrow$. Suppose $r_a(p^{c+1}) = ps$ or $r_{a\pm p^c}(p^{c+1}) = ps$. Since $(p, d) = 1$, Lemma 6.7.1 (with $e = 0$) applies to both cases and tells us that $r_a(p^c) = s$ or $r_{a\pm p^c}(p^c) = s$. By Lemma 6.3 the second equality implies $r_a(p^c) = s$. Hence we have $r_a(p^c) = s$.

Corollary 10.19. Suppose p is an odd prime, $p > 3$ and $(p, a^2-4) = 1$. Then a is a Lucas primitive root for $p \Leftrightarrow a$ or $a \pm p$ is a Lucas primitive root for p^2.

Proof. Put $c = 1$ and $s = (p-\epsilon)/2$ in Lemma 10.18.

REMARK. a and $a \pm p$ can both be Lucas primitive roots for p^2. For example if $p = 23$ and $a = 4$, then both a and $a \pm p$ are Lucas primitive roots for p^2. $\epsilon_a(p) = +1$. Also if $p = 23$ and $a = 3$, then a and $a \pm p$ are both Lucas primitive roots for p^2. $\epsilon_a(p) = -1$.

$p = 23$ and $a = 12$ is an example of p and a where a is a Lucas primitive root for p but not a Lucas primitive root for p^2. (In this example $\epsilon_a(p) = +1$.) Another such example is $p = 23$ and $a = 15$. (In this example $\epsilon_a(p) = -1$.)

Theorem 10.20. Suppose p is an odd prime and $p > 3$. Then the following are equivalent:

(i) a is a Lucas primitive root for p^2,

(ii) a is a Lucas primitive root for p^e for some $e \geq 2$,

(iii) a is a Lucas primitive root for p^e for all $e \geq 2$.

Proof. Obviously (i) $\Rightarrow$ (ii) and (iii) $\Rightarrow$ (i). Hence we need to show (ii) $\Rightarrow$ (iii). This will be done by showing (ii) $\Rightarrow$ (i) and (i) $\Rightarrow$ (iii). First we show (i) $\Rightarrow$ (iii).

To see that (i) $\Rightarrow$ (iii) we use Lemma 6.7 with $s = (p - \epsilon)/2$. (i) implies $r_a(p^2) = ps = p(p - \epsilon)/2$. Hence by Lemma 10.18 and the Law of Repetition 6.5, $r_a(p^{e+1}) = p^e s = p^e(p - \epsilon)/2$ for all $e \geq 0$.

To see that (ii) $\Rightarrow$ (i), suppose a is a Lucas primitive root for p^c and $c \geq 2$. Then $r_a(p^c) = p^{c-1}(p - \epsilon)/2$. Hence $p^2 \nmid Y_a((p - \epsilon)/2)$ for if $p^2 \mid Y_a((p - \epsilon)/2)$, then by the Law of Repetition, 6.5, $p^c \mid Y_a(p^{c-2}(p - \epsilon)/2$, contradicting $r_a(p^c) = p^{c-1}(p - \epsilon)/2$. Hence $p^2 \nmid Y_a((p - \epsilon)/2)$. Therefore we must have $r_a(p^2) = ps$ for some s such that $s \mid (p-\epsilon)/2$. By Lemma 6.7 $r_a(p^c) = p^{c-1}s$ and $s = r_a(p)$. But $r_a(p^c) = p^{c-1}(p-\epsilon)/2$. Consequently $s = (p - \epsilon)/2$ and therefore we have $r_a(p^2) = p(p - \epsilon)/2$ which proves a is a Lucas primitive root for p^2.

Theorem 10.21. Suppose p is an odd prime and e and f are integers such that $2 \leq e \leq f$. Then a is a Lucas primitive root for p^e if and only if a is a Lucas primitive root for p^f.

Proof. $\Rightarrow$. By Theorem 10.20. $\Leftarrow$. Suppose a is a Lucas primitive root for p^f and $2 \leq e \leq f$. Then $r_a(p^f) = p^{f-1}(p-\epsilon)/2$. Again it is easy to see that $p^2 \nmid Y_a((p-\epsilon)/2$. Hence $r_a(p^2) = ps$ for some s such that $s \mid (p - \epsilon)/2$. Then by Lemma 6.7, $s = r_a(p)$

and $r_a(p^f) = p^{f-1}s$. Thus $s = (p-\epsilon)/2$ so that $r_a(p^2) = p(p-\epsilon)/2$. Hence a is a Lucas primitive root for p^2. By Theorem 10.20, a is a Lucas primitive root for p^e.

Theorem 10.22. Suppose p^e is a power of an odd prime and $p \geq 5$. Then there exist Lucas primitive roots a for p^e of both positive and negative type and $0 < a < p$.

Proof. By Theorem 10.17, since $p > 3$, p has a Lucas primitive root a. Hence by Corollary 10.19, a or $a \pm p$ is a Lucas primitive root for p^2. If a is not a Lucas primitive root for p^2, then by Lemma 10.16, $-a$ is also not one, so $-a+p$ is a Lucas primitive root for p^2 and $0 < -a + p < p$.

Theorem 10.23. For each odd integer n, $(n,3)=1$, $\exists a\,[1 \leq a \leq n,\ r_a(n) = T_a(n)]$.

Proof. Put $n = p_1^{e_1} \cdots p_k^{e_k}$. By Theorem 10.22, for each i $(1 \leq i \leq k)$, we can choose a_i, $1 \leq a_i \leq p_i$ such that $(p_i, a_i^2-4)=1$, and $r_{a_i}(p_i^{e_i}) = p_i^{e_i-1} \cdot (p_i-\epsilon_i)/2$.

By the CRT we can find b such that $1 \leq b \leq n$ and for each i, $a_i \equiv b \pmod{p_i^{e_i}}$. Then for each i, $r_b(p_i^{e_i}) = r_{a_i}(p_i^{e_i}) = p_i^{e_i-1} \cdot (p_i - \epsilon_i)/2$. Therefore

$$r_b(n) = [r_b(p_1^{e_1}), \cdots, r_b(p_k^{e_k})] = \left[\frac{p_1 - \epsilon_b(p_1)}{2} p_1^{e_1-1}, \cdots, \frac{p_k - \epsilon_b(p_k)}{2} p_k^{e_k-1}\right] = T_b(n).$$

This establishes the theorem.

If n is a prime power, $n = p^e$, we have following new results. We will generalize Lemma 10.4 and Theorem 10.6. (see Theorems 10.30 and 10.34 below.)

Lemma 10.24. If p is an odd prime, $\epsilon = \pm 1$ and $k \,|\, (p-\epsilon)/2$, then

$$\sum_{r|k} \psi_{p^e}^{\epsilon}(r) = k - 1.$$

If $k \not| \, p^{e-1}(p-\epsilon)/2$, then the sum is 0.

Proof. By Lemma 6.4 $r_a(p^e) \mid k \Leftrightarrow Y_a(k) \equiv 0 \pmod{p^e}$. By the Division Theorem 4.11, the sum $\sum_r \psi^\epsilon_{p^e}(r)$ counts the number of elements in a union of the sets in Definition 10.3. Thus by Lemma 10.4

$$\sum_{r|k} \psi^\epsilon_{p^e}(r) = |\{a : 0 \le a < p^e, (p, a^2-4)=1, \epsilon_a(p)=\epsilon \text{ and } Y_a(k) \equiv 0 \pmod{p^e}\}| = k-1$$

as $k \mid (p-\epsilon)/2$. If $k \nmid p^{e-1}(p-\epsilon)/2$, then the sum is 0 by Corollary 6.15.1.

Lemma 10.25. Suppose p is an odd prime, $\epsilon = \pm 1$, $1 \le i$, $1 \le c$ and $s \mid (p-\epsilon)/2$. Then

$$\psi^\epsilon_{p^{c+i}}(p^i s) = p^{i-1}\psi^\epsilon_{p^{c+1}}(ps).$$

Proof. Suppose p is an odd prime, $\epsilon = \pm 1$, $1 \le i$, $1 \le c$ and $s \mid (p-\epsilon)/2$. Using Lemma 6.7.1 with e replaced by i, we see that if $(p,d) = 1$ and $\epsilon_a(p) = \epsilon$, then $r_a(p^{c+i}) = p^i s$ iff $r_a(p^{c+1}) = ps$. Also there are p^{i-1} times as many such a in the interval $0 \le a < p^{c+i}$ as a in the interval $0 \le a < p^{c+1}$.

Lemma 10.26. If p is an odd prime, $\epsilon = \pm 1$, $1 < s$ and $s \mid (p-\epsilon)/2$, then $\psi^\epsilon_{p^e}(s) = \phi(s)$.

Proof. We will use Lemma 10.24 and the method of proof of Theorem 10.6,

$$\psi^\epsilon_{p^e}(s) = \sum_{i=s} \psi^\epsilon_{p^e}(i)1 = \sum_{i|s} \psi^\epsilon_{p^e}(i)\Big(\sum_{j|s/i} \mu(j)\Big) = \sum_{i|s}\sum_{j|s/i} \psi^\epsilon_{p^e}(i)\mu(j) = \sum_{j|s}\sum_{i|s/j} \mu(j)\psi^\epsilon_{p^e}(i)$$

$$= \sum_{j|s} \mu(j)\Big(\sum_{i|s/j} \psi^\epsilon_{p^e}(i)\Big) = \sum_{j|s} \mu(j)\Big(\frac{s}{j} - 1\Big) = \sum_{j|s} \mu(j)\frac{s}{j} - \sum_{j|s} \mu(j) = \phi(s) - 0 = \phi(s).$$

Lemma 10.27. Suppose p is an odd prime, $2 \le e$, $1 \le i < e$, $1 < s$ and $(p,s) = 1$. Then for any b there exist a and j such that $b = a + jp^{e-i}$, $(j,p) = 1$ and $r_a(p^e) = s$ iff $r_b(p^e) = p^i s$. Furthermore for each b, the values of a mod p^e and j mod p^i are unique. j ranges over $p^i - p^{i-1}$ values.

Proof. Suppose p is an odd prime, $2 \leq e$, $1 \leq i < e$, $1 < s$ and $(p,s)=1$.

$\Rightarrow$. Suppose $b = a+jp^{e-i}$, $(j,p) = 1$ and $r_a(p^e) = s$. Then $r_a(p) = s$ by Lemma 6.13 (ii). Also $p^e \mid Y_a(s)$. By Corollary 6.14.1, $r_a(p^e) = s$, $1 < s$ and $(p,s) = 1$ imply $(p, a^2-4)=1$. Since $a \equiv b \pmod{p}$, we have $r_a(p) = r_b(p)$. Hence $r_b(p) = s$. Applying Theorem 4.50 with $k = jp^{e-i}$ and $n = s$, we get

$$(a^2-4)Y_b(s) \equiv jp^{e-i}sX_a(s) + (a^2-4-ajp^{e-i})Y_a(s) \pmod{p^{2(e-i)}}.$$

Since $i<e$, $e-i+1 \leq 2(e-i)$. Also since $1 \leq i$, $e-i+1 \leq e$. Hence $p^{e-i+1} \mid Y_a(s)$. This implies $(a^2-4)Y_b(s) \equiv jp^{e-i}sX_a(s) \pmod{p^{e-i+1}}$.

Since p is odd, $p \mid Y_a(s)$ implies $(p, X_a(s))=1$. Hence $(p, X_a(s))=1$, $(p, (a^2-4))js)=1$ and $e-i < e-i+1$. Therefore $p^{e-i} \| Y_b(s)$. By the Law of Repetition 6.5, applied i times, we obtain $p^e \| Y_b(p^is)$. Hence by Lemma 6.13 (iv) $r_b(p) = s$ and $p^e \| Y_b(p^is)$ imply $r_b(p^e) = p^is$.

$\Leftarrow$. Suppose $r_b(p^e) = p^is$. By Corollary 6.14.1, $1 < s$ and $(p,s)=1$ imply $(p, b^2-4)=1$. Since $r_b(p^e) = p^is$ and $1 \leq i < e$. Lemma 6.7.1 implies that $r_b(p^{e-i+1}) = ps$ and $r_b(p^{e-i}) = s$. Thus $p^{e-i} \mid Y_b(s)$. Also $r_b(p^{e-i}) = s$ implies $r_b(p) = s$ by Lemma 6.13 (ii). Hence $s \mid (p-\epsilon_b(p))/2$, by Corollary 6.12.1. Therefore by Lemma 9.4, p^{e-i} is an *elpsp*(b). Since $(p, b^2-4) = 1$, by Theorem 9.14 there exists a unique a mod p^e such that $a \equiv b \pmod{p}$ and p^e is *elpsp*(a). Then $a \equiv b \pmod{p}$ implies $r_a(p) = r_b(p) = s$ and $\epsilon_a(p) = \epsilon_b(p)$. By Corollary 9.10 since $e - i \leq e$, p^{e-i} is *elpsp*(a). Since p^{e-i} is *elpsp*(a), p^{e-i} is *elpsp*(b) and $a \equiv b \pmod{p}$, Theorem 9.13 implies $a \equiv b \pmod{p^{e-i}}$. Consequently there exists j such that $b = a + jp^{e-i}$. Since p^e is an *elpsp*(a), we have $p^e \mid Y_a((p^e-\epsilon^e)/2)$. Hence $(r_a(p^e), p)=1$. Therefore since $r_a(p) = s$, we have $r_a(p^{e-i+1}) = s$ by Lemma 6.13 (v). But $r_b(p^{e-i+1}) = ps$.

Hence $a \not\equiv b \pmod{p^{e-i+1}}$. Therefore $(j,p) = 1$. To see that j is unique mod p^i, suppose $b = a + kp^{e-i}$. Then we have $a+kp^{e-i} \equiv a+jp^{e-i} (\mathrm{mod} p^e) \Rightarrow kp^{e-i} \equiv jp^{e-i} (\mathrm{mod} p^e) \Rightarrow k \equiv j (\mathrm{mod} p^i)$. This proves the lemma.

Corollary 10.28. Suppose p is an odd prime, $(p, b^2-4) = 1$, $2 \leq e$, $\epsilon = \pm 1$ and $s \mid (p-\epsilon)/2$. Then there exist a and j such that $(j,p)=1$, $b = a+jp^{e-1}$ and $r_a(p^e) = s$ iff $r_b(p^e) = ps$. Further, for each b, a is unique mod p^e and j is unique mod p. j ranges over $p-1$ values mod p.

Proof. Put $i = 1$ in Lemma 10.27.

Lemma 10.29. If p is an odd prime, $\epsilon = \pm 1$, $1 < s$ and $s \mid (p-\epsilon)/2$, then for any $c \geq 2$, $\qquad \psi^{\epsilon}_{p^c}(ps) = \phi(ps) = (p-1)\phi(s)$.

Proof. $s \mid (p-\epsilon)/2$ implies $(p,s) = 1$. Hence by Corollary 10.28, every b, for which $r_b(p^c) = ps$, has a unique representation in the form $b = a+jp^{c-1}$, where $1 \leq j < p$ and $r_a(p^c) = s$. Thus $\psi^{\epsilon}_{p^c}(ps) = \phi(ps) = (p-1)\psi^{\epsilon}_{p^c}(s)$. Therefore by Lemma 10.26, $\psi^{\epsilon}_{p^c}(s) = \phi(s)$, we have $\psi^{\epsilon}_{p^c}(ps) = \phi(ps) = (p-1)\phi(s)$.

Theorem 10.30. Suppose p is an odd prime. If $\epsilon = \pm 1$, $e \geq 2$, $0 \leq i < e$, $1 < s$ and $s \mid (p-\epsilon)/2$, then $\qquad \psi^{\epsilon}_{p^e}(p^i s) = \phi(p^i s)$.

Proof. Suppose p is an odd prime, $\epsilon = \pm 1$, $e \geq 2$, $0 \leq i < e$, $1 < s$ and $s \mid (p-\epsilon)/2$. We will consider 3 cases for i. The case $i = 0$ is Lemma 10.26. The case $i = 1$ is Lemma 10.29. Suppose $i \geq 2$. In this case we may calculate $\psi^{\epsilon}_{p^e}(p^i s)$ by Lemma 10.25 with $c = e - i$ and Lemma 10.29 with $c = e - i + 1$,

$$\psi^{\epsilon}_{p^e}(p^i s) = \psi^{\epsilon}_{p^{e-i+i}}(p^i s) = p^{i-1}\psi^{\epsilon}_{p^{e-i+1}}(ps) = p^{i-1}(p-1)\phi(s) = \phi(p^i s).$$

Corollary 10.31. Suppose p is an odd prime, $p > 3$ and $\epsilon = \pm 1$. Then the number of Lucas primitive roots a mod p^e of type ϵ is $\phi(p^{e-1}(p-\epsilon)/2)$.

Proof. Put $i = e-1$ in Theorem 10.30.

Lemma 10.32. If p is an odd prime, $(p,s)=1$ and $1 \le n$, then $\sum_{j=0}^{n} \phi(p^j s) = p^n \phi(s)$.

Proof. Induction on n.

$$p^n\phi(s) + p^n(p-1)\phi(s) = [p^n + p^n(p-1)]\,\phi(s) = p^{n+1}\phi(s).$$

Lemma 10.33. For any positive integer s, $\sum_{r|s} \phi(r) = s$. Hence $\sum_{r|s, r>1} \phi(r) = s-1$.

Proof. Well known.

Theorem 10.34. Suppose p is an odd prime, $\epsilon = \pm 1$, $k = p^i s$ where $0 \le i < e$ and $s \,|\, (p-\epsilon)/2$. Then

$$\sum_{r|k} \psi^{\epsilon}_{p^e}(r) = p^i s - p^i.$$

Proof. Write each $r = p^j t$ where $0 \le j < i$, $1 < t$ and $t \,|\, s$. Then by Lemmas 10.30, 10.32 and 10.33 we have

$$\sum_{r|k,} \psi^{\epsilon}_{p^e}(r) = \sum_{t|s, t>1} \sum_{j=0}^{i} \psi^{\epsilon}_{p^e}(p^j t) = \sum_{t|s, t>1} \sum_{j=0}^{i} \phi(p^j t) = \sum_{t|s, t>1} p^i \phi(t) = p^i \sum_{t|s, t>1} \phi(t) = p^i(s-1).$$

The theorem is proved.

Corollary 10.35. Suppose p is an odd prime, $\epsilon = \pm 1$, $k = p^i s$ where $0 \le i < e$ and $s \,|\, (p-\epsilon)/2$. Then the congruence $Y_a(k) \equiv 0 \pmod{p^e}$ has exactly $p^i s - p^i$ incongruent solutions a mod p^e. Each solution a satisfies $(p, a^2-4)=1$ and $\epsilon_a(p) = \epsilon$.

Proof. If $i = 0$, this is by Lemma 10.24. If $i \ge 1$, then this is by Theorem 10.34.

The following two theorems may be used to give a constructive proof of Lemma 10.26 and Corollary 10.35.

Theorem 10.36. Suppose p is an odd prime, $1 \leq c \leq e$ and $(p,s)=1$. Then for any a $\quad r_a(p^c)=s \Leftrightarrow \exists b\,[r_b(p^e)=s$ and $b \equiv a \pmod{p^c}]$.
Here b is unique mod p^e.

Proof. By Lemma 6.13, Theorems 9.13, 9.14 and Corollary 9.10.

Theorem 10.37. Suppose p is an odd prime, $1 \leq e$, $0 \leq k < e$ and $(p,s)=1$. Then for all b, $\exists a,j\ (b = a+jp^{e-k}$ and $Y_a(p^{k-1}s) \equiv 0 \pmod{p^e}) \Leftrightarrow Y_b(p^k r) \equiv 0 \pmod{p^e}$.

Proof. $\Rightarrow$. Suppose $Y_a(p^{k-1}s) \equiv 0 \pmod{p^e})$ and $b = a+jp^{e-k}$. Since $k-1 < e$, we have $(p, a^2-4)=1$. Hence $(r_a(p),p)=1$. Let $w = r_a(p)$. Then $(w,p)=1$ and $w \mid s$. Since $a \equiv b \pmod{p}$, we also have $(p,b^2-4)=1$. Hence $r_a(p) = r_b(p)$. Let $j = j'p^t$ where $0 \leq t$ and $(p,j')=1$. Put $i = k-t$. Then $b = a+j'p^{e-i}$ and $p^e \mid Y_a(p^{k-1}w)$. Suppose $t<k$. Then $1 \leq i < e$ since $k < e$. Therefore by Corollary 10.28 $r_b(p^e) = p^i w$. Then $p^e \mid Y_b(p^i w)$. Hence $p^e \mid Y_b(p^i s)$. Suppose $k \leq t$. Then $b = a+j'p^t pe - k = a+j'p^{e+t-k} \Rightarrow a \equiv b \pmod{p^e}$. So by (4.1) $Y_b(p^{k-1}s) \equiv Y_a(p^{k-1}s) \pmod{p^e}$. Hence $p^e \mid Y_b(p^{k-1}s)$, which implies $p^e \mid Y_b(p^k s)$.

$\Leftarrow$. Suppose $Y_b(p^k s) \equiv 0 \pmod{p^e}$. Since $k < e$, $(p, b^2-4)=1$. Hence $(r_b(p),p)=1$. Thus $r_b(p) \mid s$. Let $w = r_b(p)$. Then $w \mid s$. Since $k \leq e-1$, $r_b(p^e) \mid p^k s$ and $r_b(p^e) \mid p^{e-1}w$ imply $r_b(p^e) \mid p^k w$. Let i be such that $r_b(p^e) = p^i w$. Then we have $1 \leq i \leq k < e$. Hence $1 \leq i < e$. So by Corollary 10.28, $\exists a, j'$ such that $(j',p)=1$, $a = b+j'p^{e-i}$, $r_a(p) = w$ and $r_a(p^e) \mid p^{i-1}w$. Let $j = j'p^{k-i}$. Then $a = b+jp^{e-k}$. Also $i-1 \leq k-1$, $w \mid s$ and $p^e \mid Y_a(p^{i-1}w) \Rightarrow p^e \mid Y_a(p^{k-1}s)$. Hence we have $Y_a(p^{k-1}s) \equiv 0 \pmod{p^e}$ and $b = a+jp^{e-k}$.

§11. Lucas Carmichael numbers

In this section we will show that properties of Lucas sequences are very closely connected with factorization. Recall that an odd composite integer n is called an (ordinary) *Carmichael number* if for all a, $(a,n)=1$, $a^{n-1} \equiv 1 \pmod{n}$. Carmichael numbers sometimes are also called *absolute pseudoprimes*. In this section, we will define various types of Lucas Carmichael number, analogous to ordinary Carmichael numbers. We will show some kind Lucas Carmichael numbers n satisfy classical Lucas pseudoprime tests like $X_a(n) \equiv a \pmod{n}$, for all possible bases a, even if n is composite. We will also show that if n is an odd composite integer, then n is not an absolute *Lucas pseudoprime*, not an absolute *a-pseudoprime*, not an absolute *r-pseudoprime* and that if $n \neq \square$, then n is not an absolute *t-pseudoprime*. Hence if n is composite, then n is not an absolute *Euler Lucas pseudoprime*, is not an absolute *strong Lucas pseudoprime* and is not an absolute *extra strong Lucas pseudoprime.* First we give some definitions.

Definition 11.1. An odd integer n is a two sided *Lucas Carmichael* if n is squarefree and for all $p \mid n$, $(p-1)/2 \mid n \pm 1$ and $(p+1)/2 \mid n \pm 1$ hold for some choice of signs $\pm$.

Definition 11.2. An odd integer n is a *strong two sided Lucas Carmichael* if n is squarefree and for all $p \mid n$, $p-1 \mid n \pm 1$ and $p+1 \mid n \pm 1$ for some choice of signs $\pm$.

Definition 11.3. An odd integer n is a *one sided Lucas Carmichael* $+$ if n is squarefree and $(p-1)/2 \mid n-1$ and $(p+1)/2 \mid n-1$ for all $p \mid n$.

Definition 11.4. An odd integer n is a *one sided Lucas Carmichael* $-$ if n is squarefree and $(p-1)/2 \mid n+1$ and $(p+1)/2 \mid n+1$ for all $p \mid n$. Equivalently if $(p^2-1)/4 \mid n+1$ for all $p \mid n$.

Definition 11.5. An odd integer n is a *strong one sided Lucas Carmichael* $+$ if n is squarefree and $(p^2-1)/2 \mid n-1$ for all $p \mid n$.

Definition 11.6. An odd integer n is a *strong one sided Lucas Carmichael* $-$ if n is squarefree and $(p^2-1)/2 \mid n+1$ for all $p \mid n$.

Definition 11.7. An odd integer n is a *super one sided Lucas Carmichael* $+$ if n is squarefree and $(p^2-1) \mid n-1$ for all $p|n$.

Definition 11.8. An odd integer n is a *super one sided Lucas Carmichael* $-$ if n is squarefree and $(p^2-1)|n+1$ for all $p|n$.

It can be seen that for a fixed sign, $+$ or $-$, super one sided $\Rightarrow$ strong one sided $\Rightarrow$ one sided; strong two sided $\Rightarrow$ two sided. But one sided and strong two sided are independent. It is clear that every prime is a strong two sided Lucas Carmicheal, and hence is a two sided Lucas Carmicheal. However we are more interested in composite ones. One sided Lucas Carmichael numbers are rare, as can be seen from the following list (with types of one sided indicated $+$ or $-$ and if without sign $+$ and $-$, then two sided). The numbers in the following list which are $\geq 63,278,892,599$ were found by R.G.E. Pinch [41].

3, (*a strong* + *and a strong* −), $1,930,499 = 89 \cdot 109 \cdot 199 -$,

$5 -$, $7,056,721 = 7 \cdot 47 \cdot 89 \cdot 241$, (*strong*)

$35 -$, $7,110,179 = 37 \cdot 41 \cdot 43 \cdot 109 -$,

$3,059 = 7 \cdot 19 \cdot 23$, $15,857,855 = 5 \cdot 13 \cdot 17 \cdot 113 \cdot 127 -$,

$6479 = 11 \cdot 19 \cdot 31 -$, $17,966,519 = 23 \cdot 67 \cdot 89 \cdot 131$,

$84,419 = 29 \cdot 41 \cdot 71 -$, $35,626,501 = 19 \cdot 59 \cdot 61 \cdot 521$,

$63,278,892,599 = 13 \cdot 47 \cdot 137 \cdot 239 \cdot 3163 -$,

$79,397,009,999 = 23 \cdot 29 \cdot 41 \cdot 43 \cdot 251 \cdot 269 -$, (*super* −),

$28,295,303,263,921 = 29 \cdot 31 \cdot 67 \cdot 271 \cdot 331 \cdot 5237 +$,

$443,372,888,629,441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331 +$, (*super* +),

$582,920,080,863,121 = 41 \cdot 53 \cdot 79 \cdot 103 \cdot 239 \cdot 271 \cdot 509 +$ (*strong* +),

$894,221,105,778,001 = 17 \cdot 23 \cdot 29 \cdot 31 \cdot 79 \cdot 89 \cdot 181 \cdot 1999 +$

$2,013,745,337,604,001 = 17 \cdot 37 \cdot 41 \cdot 131 \cdot 251 \cdot 571 \cdot 4159 +$,

$39,671,149,333,495,681 = 17 \cdot 37 \cdot 41 \cdot 71 \cdot 79 \cdot 97 \cdot 113 \cdot 131 \cdot 191 +$, (*super* +).

If n is a strong one sided Lucas Carmichael +, then n is an ordinary Carmichael number. The converse holds only very rarely.

Lemma 11.9. Every odd prime is a strong two sided Lucas Carmichael. However 3 and 5 are the only primes which are one sided Lucas Carmichaels.

Proof. Any prime p is a strong Lucas Carmichael since $(p+1) \mid p+1$ and $(p-1) \mid p-1$. However it is easy to see that only 3 or 5 can meet the condition $(p^2-1)/4 \mid p-1$ or the condition $(p^2-1)/4 \mid p+1$.

Since we normally suppose $(n, 2ad) = 1$ which implies $(n, 3) = 1$, 3 should probably be excluded from the set of Lucas Carmichaels. Another reason to exclude 3 is the following.

Lemma 11.10. If n is a Lucas Carmichael and $n > 3$, then $(n, 3) = 1$.

Proof. Suppose $n > 3$. If $3 \mid n$, then $3p \mid n$ for some $p > 3$. If $p \equiv 1 \pmod 3$, then $3 \mid (p-1)/2$. Hence $(p-1)/2 \nmid n \pm 1$. If $p \equiv -1 \pmod 3$, then $3 \mid (p+1)/2$. Hence $(p+1)/2 \nmid n \pm 1$. Thus n is not a Lucas Carmichael.

Lemma 11.11. Suppose $1 < n$ and $(n, 6) = 1$. Then n is a Lucas Carmichael if and only if n is squarefree and for all a, such that $(n, a^2-4) = 1$, if $p \mid n$, then

$$\frac{p - \epsilon_a(p)}{2} \mid n \pm 1. \tag{11.11}$$

Proof. Certainly every Lucas Carmichael satisfies (11.11). To show the converse, suppose $p \mid n$. Then $p > 3$. By Theorem 10.1, there exists a such that $\epsilon_a(p) = -1$ and also there exists b such that $\epsilon_b(p) = 1$. These two together show that n is a Lucas Carmichael.

Condition (11.11) is similar to the divisibility conditions that for all a such that $(n, a^2-4) = 1$,

$$\text{(i)} \quad \frac{p - \epsilon_a(p)}{2} \mid n - \epsilon_a(n), \qquad \text{(ii)} \quad p - \epsilon_a(p) \mid n - \epsilon_a(n).$$

Condition (ii) was considered by Williams [50]. (His results about it are difficult to compare to ours because he considered a fixed discriminant D, $D = A^2 - 4B$.) Conditions (i) and (ii) are very strong. Either one will imply that n is prime provided n is squarefree. Clearly (ii) implies (i). Later we will prove (Theorem 11.24) that if $n \mid V_a(n - \epsilon_a(n))$ for all a such that $(n, a^2-4) = 1$, then n is prime. From this we can show that if n is squarefree and (i) holds for all a such that $(n, d) = 1$, then n is

prime. Here is the proof: Assume Theorem 11.24 and suppose n is squarefree. Let $p|n$. Then $p|Y_a(\frac{p-\epsilon_a(p)}{2})$ for all a, $(n, a^2-4)=1$. Hence (i) and the Division Theorem together imply $p|Y_a(n-\epsilon_a(n))$ for all such a. Since p is arbitrary and n is squarefree, it follows that $n|Y_a(n-\epsilon_a(n))$ for all a, $(n, a^2-4)=1$. Thus by Theorem 11.24, n is prime.

Theorem 11.12. The only Lucas Carmichael with exactly two prime factors is $n = 35$. If $n \neq 35$, n is composite and n is Lucas Carmichael, then n has at least three prime factors.

Proof. Suppose $n = pq$, where p and q are odd primes. By Lemma 11.10 we can suppose $3 < p < q$. Then $5 \leq p$ and $7 \leq q$. We will show $p = 5$ and $q = 7$, and hence $n = 35$.

Case 1. $q = p + 2$. In this case $n = pq = p(p+2) \equiv 1(1+2) = 3 \pmod{p-1}$. Hence $n - 1 \equiv 2 \pmod{p-1}$ and $n + 1 \equiv 4 \pmod{p-1}$. Hence $(p-1)/2$ cannot divide $n - 1$ unless $(p-1)/2 = 2$ in which case $p = 5$ and $q = 7$. If $(p-1)/2 \mid n+1$, then $(p-1)/2 \mid 4 \Rightarrow (p-1)/2 = 1,\ 2 \text{ or } 4 \Rightarrow p = 3,\ p = 5 \text{ or } p = 9 \Rightarrow q = 7$.

Case 2. $q > p + 2$. In this case we can suppose $p + 4 \leq q$. We claim that

(i) $(\frac{q-1}{2} \nmid n-1 \text{ and } \frac{q-1}{2} \nmid n+1)$ or $(\frac{q+1}{2} \nmid n-1 \text{ and } \frac{q+1}{2} \nmid n+1)$.

First we shall show that

(ii) $q - 1 \nmid n \pm 1$ and (*iii*) $q + 1 \nmid n \pm 1$.

The proof of (ii) is that $n = pq \equiv p \cdot 1 = p \pmod{q-1}$, which implies $n \pm 1 \equiv p \pm 1 \pmod{q-1}$, and we have $p \pm 1 \leq p + 1 < p + 3 \leq q - 1$. The proof of (ii) is that $n = pq \equiv p \cdot (-1) = -p \pmod{q+1}$, which implies $n \pm 1 \equiv -p \pm 1 = -(p \mp 1) \pmod{q+1}$, and we have $p \pm 1 \leq p + 1 < p + 3 < q + 1$.

Now we can prove (i). Suppose (i) does not hold, i.e. suppose $\frac{q-1}{2} \mid n \pm 1$ and $\frac{q+1}{2} \mid n \pm 1$. Then there are 4 possible cases:

Case 1. $\frac{q-1}{2} \mid n-1$ *and* $\frac{q+1}{2} \mid n-1$. Case 2. $\frac{q-1}{2} \mid n+1$ *and* $\frac{q+1}{2} \mid n+1$.

Case 3. $\frac{q-1}{2} \mid n-1$ *and* $\frac{q+1}{2} \mid n+1$. Case 4. $\frac{q-1}{2} \mid n+1$ *and* $\frac{q+1}{2} \mid n-1$.

Since $((q+1)/2, (q-1)/2) = 1$ and $4 \mid q+1$ or $4 \mid q-1$, cases 1 and 2 are impossible by (ii) and (iii). Case 3 is also impossible since $(q+1)/2 - (q-1)/2 = 1$ implies one of $(q+1)/2$ or $(q-1)/2$ is odd. Suppose $(q-1)/2$ is odd. Then since $n-1$ is even, if $(q-1)/2 \mid n-1$, then $q-1 \mid n-1$, contradicting (ii). Similarly if $(q+1)/2$ is odd, then since $n-1$ is even, if $(q+1)/2 \mid n-1$, then $q+1 \mid n-1$, contradicting (iii). A similar argument shows case 4 is also impossible.

Theorem 11.13. Suppose $1 < n$ and $(n, 6) = 1$. Then n is a Lucas Carmichael if and only if n satisfies any one of

(i) $\quad (\forall a)[(n, a^2-4)=1 \Rightarrow Y_a(n+1)Y_a(n-1) \equiv 0 \pmod{n}]$,

(ii) $\quad (\forall a)[(n, a^2-4)=1 \Rightarrow Y_a(n)^2 \equiv 1 \pmod{n}]$,

(iii) $\quad (\forall a)[(n, a^2-4)=1 \Rightarrow X_a(n)^2 \equiv a^2 \pmod{n}]$.

(iv) $\quad (\forall a)[X_a(n)^2 \equiv a^2 \pmod{n}]$.

Proof. Let $d = a^2 - 4$. From (1.35) $X_a(n)^2 - a^2 = d(Y_a(n)^2 - 1)$ and (3.28) $Y_a(n-1)Y_a(n+1) = Y_a(n)^2 - 1$, we have (i), (ii) and (iii) are equivalent. Obviously (iv) $\Rightarrow$ (iii). To prove the theorem we show that n is a Lucas Carmichael $\Rightarrow$ (iv) and (i) $\Rightarrow$ n is a Lucas Carmichael.

Suppose n is a Lucas Carmichael. Then n is squarefree, put $n = p_1 \cdots p_k$. Let an arbitrary integer a be given and consider an arbitrary prime p dividing n. If $(n, d) = 1$, then by (11.11) $p - \epsilon_a(p)/2 \mid n \pm 1$. Thus from the Division Theorem 4.11,

$Y_a\left(\frac{p-\epsilon_i}{2}\right) | Y_a(n \pm 1)$. Hence Theorem 6.12 implies that $p \mid Y_a(n \pm 1)$. Therefore $p \mid Y_a(n-1)Y_a(n+1)$. Using (1.35) and (3.28) we obtain $p \mid X_a(n)^2 - a^2$. If $p \mid d$, then by (3.28) we also have that $p \mid X_a(n)^2 - a^2$. Since n is squarefree and a, p are arbitrary, it follows that (iv) holds.

Suppose (i) holds. Then n is squarefree by the Squarefree Lemma 6.23. Suppose $p \mid n$. Since $3 < p$, by Lemma 10.8, we can find a such that $(n, a^2-4) = 1$ and $r_a(p) = (p-1)/2$. Also we can find b such that $(n, b^2-4) = 1$ and $r_b(p) = (p+1)/2$. Hence by (i), $p \mid Y_a(n-1)Y_a(n+1)$ and $p \mid Y_b(n-1)Y_b(n+1)$. Thus $p \mid Y_a(n \pm 1)$. Then $(p-1)/2 = r_a(p) \mid n \pm 1$ and $(p+1)/2 = r_b(p) \mid n \pm 1$. Hence n is a Lucas Carmichael.

Theorem 11.14. Suppose $1 < n$ and $(n, 6) = 1$. Each of the following conditions is equivalent to n being a strong two sided Lucas Carmichael:

(i) $\quad (\forall a)[(n, a(a^2-4) = 1 \Rightarrow X_a(n) \equiv a \pmod{n})]$,

(ii) $\quad (\forall a)[(n, a^2-4) = 1 \Rightarrow X_a(n) \equiv a \pmod{n})]$,

(iii) $\quad (\forall a)[X_a(n) \equiv a \pmod{n})]$.

Proof. Obviously we have (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). First we show that n is a strong two sided Lucas Carmichael $\Rightarrow$ (iii). Then we show (i) $\Rightarrow$ n is a strong two sided Lucas Carmichael.

Suppose $n > 1$, $(n, 6) = 1$ and n is a strong two sided Lucas Carmichael. By definition then n is squarefree, $n = p_1 p_2 \cdots p_k$. Also $p-1 \mid n \pm 1$ and $p+1 \mid n \pm 1$ for all $p \mid n$. Let an arbitrary integer a be given and consider an arbitrary prime p dividing n. Since $p-1 \mid n \pm 1$ and $p+1 \mid n \pm 1$, $p-\epsilon_a(p) \mid n \pm 1$. Hence $(p-\epsilon_a(p))/2 \mid (n \pm 1)/2$. Therefore by the Division Theorem 4.11, we have $Y_a((p-\epsilon_a(p))/2) \mid Y_a((n \pm 1)/2)$. If

$(p,d)=1$, then by Theorem 6.12 $p|Y_a((n-\epsilon_a(p))/2)$, and hence that $p|Y_a((n\pm1)/2)$. Therefore if $(p,d)=1$, $p|d\cdot Y_a((n-1)/2)Y_a((n+1)/2)$. Identity (3.20') states that

(iv) $$X_a(n)-a=dY_a\left(\frac{n+1}{2}\right)Y_a\left(\frac{n-1}{2}\right)\equiv 0 \pmod p.$$

Hence if $(p,d)=1$, then $p \mid X_a(n)-a$ holds. But this same identity (iv) implies $p|X_a(n)-a$ holds also when $p|d$. Thus $p|X_a(n)-a$ holds whether $(p,d)=1$ or not. Thus for all a, $X_a(n)\equiv a \pmod p$. Since p was arbitrary and n is squarefree, the congruence $X_a(n)\equiv a \pmod n$ holds for all a. Hence (iii) holds.

To prove that (i) implies n is a strong two sided Lucas Carmichael, suppose (i) holds. Then n is squarefree by the Squarefree Lemma. Let $p|n$. Then $p>3$. If $p=5$, then $p-1=4|n\pm1$ holds. Next we show that if $p=5$, then $p+1|n\pm1$ and that if $p>5$, then $p-1|n\pm1$ and $p+1|n\pm1$. By Lemma 10.8, we can find a and b such that $(n,a(a^2-4))=1$, $(n,b(b^2-4)=1$ and $r_a(p)=\frac{p-1}{2}$, $r_b(p)=\frac{p+1}{2}$. Then by (3.20') and (iv) we have

$$(a^2-4)Y_a\left(\frac{n-1}{2}\right)Y_a\left(\frac{n+1}{2}\right)\equiv 0 \pmod p \quad \text{and}$$

$$(b^2-4)Y_b\left(\frac{n-1}{2}\right)Y_b\left(\frac{n+1}{2}\right)\equiv 0 \pmod p.$$

Since $(p,a^2-4)=1$ and $(p,b^2-4)=1$, we have $p \mid Y_a\left(\frac{n-1}{2}\right)Y_a\left(\frac{n+1}{2}\right)$, and hence $r_a(p)\,|\,\frac{n\pm1}{2}$. Also $p|Y_b\left(\frac{n-1}{2}\right)Y_b\left(\frac{n+1}{2}\right)$, and hence $r_b(p)\,|\,\frac{n\pm1}{2}$. Therefore $\frac{p-1}{2}=r_a(p)\,|\,\frac{n\pm1}{2}$ and $\frac{p+1}{2}=r_b(p)\,|\,\frac{n\pm1}{2}$. Since p is arbitrary, it shows that n is a strong two sided Lucas Carmichael. Hence (i) holds.

Theorem 11.15. If $1<n$ and $(n,6)=1$, then the following conditions are equivalent.

(i) n is a one sided Lucas Carmichael +, i.e. $p|n \Rightarrow (p\pm1)/2|n-1$,

(ii) $(\forall a)[(n,d)=1 \Rightarrow Y_a(n-1)\equiv 0 \pmod n]$,

(iii) $(\forall a)[(n,ad)=1 \Rightarrow Y_a(n-1)\equiv 0 \pmod n]$.

Proof. (i) $\Rightarrow$ (ii). Suppose (i). Then n is squarefree by definition. Suppose $(n,d)=1$. Let $p \mid n$. Then $(p,d)=1$. Hence $p \mid Y_a((p-\epsilon_a(p))/2)$. By (i), $(p \pm 1)/2 \mid n-1$, then $(p-\epsilon_a(p))/2 \mid n-1$. Thus the Division Theorem and $p \mid Y_a((p-\epsilon_a(p))/2)$ together imply $p \mid Y_a(n-1)$. Since p is arbitrary and n is squarefree, $n \mid Y_a(n-1)$. Therefore (ii) holds. (ii) $\Rightarrow$ (iii) is trivial.

(iii) $\Rightarrow$ (i). Suppose (iii) holds. Then n is squarefree by the Squarefree Lemma 6.23. Let $p \mid n$. Then $3 < p$. By Lemma 10.8, we can find b such that $r_b(p) = (p+1)/2$ and $(n, b(b^2-4)) = 1$. Hence $n \mid Y_b(n-1)$. Then $p \mid Y_b(n-1)$. So by Lemma 6.3 $(p+1)/2 = r_b(p) \mid n-1$. Again let $p \mid n$. We will show $(p-1)/2 \mid n-1$. If $p = 5$, this is true since $(5-1)/2 = 2 \mid n-1$. If $5 < p$, then the condition of Lemma 10.8 is satisfied. Hence by same argument we can show $(p-1)/2 \mid n-1$.

Thus for any prime $p \mid n$ we have shown that $(p \pm 1)/2 \mid n-1$. So n is a one sided Lucas Carmichael $+$. (i) holds.

Theorem 11.16. If $1 < n$ and $(n,6)=1$, then the following conditions are equivalent.

(i) n is a one sided Lucas Carmichael $-$, i.e. $p \mid n \implies (p \pm 1)/2 \mid n+1$,

(ii) $(\forall a)[(n,d)=1 \Rightarrow Y_a(n+1) \equiv 0 \pmod{n}]$,

(iii) $(\forall a)[(n,ad)=1 \Rightarrow Y_a(n+1) \equiv 0 \pmod{n}]$.

Proof. Similar to the proof of Theorem 11.15, replacing $n-1$ by $n+1$.

Theorem 11.17. Suppose $1 < n$ and $(n,6)=1$. Then the following conditions are equivalent.

(i) n is a strong one sided Lucas Carmichael $+$, i.e. $p \mid n \Rightarrow (p^2-1)/2 \mid n-1$,

(ii) $(\forall a)[(n,d)=1 \Rightarrow Y_a((n-1)/2) \equiv 0 \pmod{n}]$,

(iii) $(\forall a)[(n,d)=1 \Rightarrow X_a(n-1) \equiv 2 \pmod{n}$ and $Y_a(n-1) \equiv 0 \pmod{n}]$,

(iv) $(\forall a)[(n,d)=1 \Rightarrow X_a(n+1)\equiv a^2-2 \pmod n$ and $Y_a(n+1)\equiv a \pmod n)]$,

(v) $(\forall a)[(n,d)=1 \Rightarrow X_a(n) \equiv a \pmod n$ and $Y_a(n) \equiv 1 \pmod n)]$.

Proof. Similar to the proof of Theorem 6.24 with $\epsilon = 1$ we can show that (ii) - (v) are equivalent. Hence we need only show (i) $\Leftrightarrow$ (ii).

(i) $\Rightarrow$ (ii). Suppose (i) holds. Let $p|n$. For all a, we have $p|Y_a((p-\epsilon)/2)$ and $(p-\epsilon)/2|(p-1)(p+1)/4 = (p^2-1)/4$ imply $p|Y_a((p^2-1)/4)$. Then by (i) $(p^2-1)/4|(n-1)/2$ and hence $Y_a((p^2-1)/4)\,|\,Y_a((n-1)/2)$. Thus $p\,|\,Y_a((n-1)/2)$. Since p is arbitrary and n is squarefree, $n|Y_a((n-1)/2)$ for all a.

(ii) $\Rightarrow$ (i). Suppose (ii) holds. By Squarefree Lemma 6.23, n is squarefree. Let $p|n$, then $p > 3$. By Lemma 10.8, we can find a_1 and a_2 such that $r_{a_1}(p) = (p+1)/2$, $r_{a_2}(p) = (p-1)/2$ and $(n,(a_1^2-4)(a_2^2-4))=1$. Then (ii) implies $p|Y_{a_1}((n-1)/2)$ and $p|Y_{a_2}((n-1)/2)$. Hence $(p+1)/2=r_{a_1}(p)\,|\,(n-1)/2$ and $(p-1)/2=r_{a_2}(p)\,|\,(n-1)/2$. It follows $(p^2-1)/4|(n-1)/2$. Note that p is arbitrary and so (i) holds.

Theorem 11.18. Let $1<n$ and $(n,6)=1$. The following conditions are equivalent.

(i) n is a strong one sided Lucas Carmichael $-$, i.e. $p|n \Rightarrow (p^2-1)/2|n+1$,

(ii) $(\forall a)[(n,d)=1 \Rightarrow Y_a((n+1)/2) \equiv 0 \pmod n)]$,

(iii) $(\forall a)[(n,d)=1 \Rightarrow X_a(n+1) \equiv 2 \pmod n$ and $Y_a(n+1) \equiv 0 \pmod n)]$,

(iv) $(\forall a)[(n,d)=1 \Rightarrow X_a(n-1)\equiv a^2-2 \pmod n$ and $Y_a(n-1)\equiv -a \pmod n)]$,

(v) $(\forall a)[(n,d)=1 \Rightarrow X_a(n) \equiv a \pmod n$ and $Y_a(n) \equiv -1 \pmod n)]$.

Proof. Similar to the above with 1 replaced by -1.

Theorem 11.19. Suppose $1 < n$ and $(n,6)=1$. Then n is a super one sided Lucas Carmichael $+$ if and only if $4|n-1$ and

(11.19) $(\forall a)[(n,d)=1 \Rightarrow Y_a((n-1)/4) \equiv 0 \pmod n)]$.

Proof. $\Rightarrow$. Suppose n is a super one sided Lucas Carmichael $+$. Let $p \mid n$. Then by definition $p^2-1 \mid n-1$. Since p^2-1 is divisible by 4, we have $4 \mid n-1$. Also by the Division Theorem, $p \mid Y_a((p-\epsilon)/2)$ implies $p \mid Y_a((p^2-1)/4)$. Then $p \mid Y_a((n-1)/4)$. Since p is arbitrary and n is squarefree, $n \mid Y_a((n-1)/4)$.

$\Leftarrow$. Suppose (11.19) holds. Then it follows that $Y_a((n-1)/2) \equiv 0 \pmod{n}$ for all a; thus n is squarefree. Let $p \mid n$. As above, by Lemma 10.8, we can find a_1 and a_2 such that $(n,(a_1^2-4)(a_2^2-4))=1$ and $r_{a_1}(p)=(p-1)/2$, $r_{a_2}(p)=(p+1)/2$. Hence (11.19) implies $p \mid Y_{a_1}((n-1)/4)$ and $p \mid Y_{a_2}((n-1)/4)$. It is equivalent to $(p-1)/2=r_{a_1}(p) \mid (n-1)/4$ and $(p+1)/2=r_{a_2}(p) \mid (n-1)/4$. Hence $(p^2-1)/4 \mid (n-1)/4$. This is true for all $p \mid n$. Thus n is a super one sided Lucas Carmichael $+$.

Theorem 11.20. Suppose $1 < n$ and $(n,6)=1$. Then n is a super one sided Lucas Carmichael $-$ if and only if $4 \mid n+1$ and

(11.20) $$(\forall a)[(n,d)=1 \;\Rightarrow\; Y_a((n+1)/4) \equiv 0 \pmod{n}].$$

Proof. Similar to the proof of Theorem 11.19. Replace $n-1$ by $n+1$.

Theorem 11.21. Suppose $1 < n$ and $(n,6)=1$. Then n is prime if and only if following three conditions hold simultaneously

(i) $$(\exists a)[(n,a(a^2-4))=1 \text{ and } Y_a(n) \equiv +1 \pmod{n}],$$

(ii) $$(\exists b)[(n,b(b^2-4))=1 \text{ and } Y_b(n) \equiv -1 \pmod{n}],$$

(iii) $$(\forall c)[(n,c(c^2-4))=1 \;\Rightarrow\; Y_c(n) \equiv \pm 1 \pmod{n}].$$

Proof. $\Rightarrow$. Suppose n is prime. Then $n > 3$. By Theorem 10.1, there are $(n-3)/2$ $a's$ such that $\epsilon_a(n)=1$, and there are $(n-1)/2$ $b's$ such that $\epsilon_b(n)=-1$. Then by Theorem 6.11, (i) (ii) and (iii) are all hold.

$\Leftarrow$. Suppose (i) (ii) and (iii) hold. By the Squarefree Lemma 6.23, (iii) implies n is

squarefree. If n is composite, put $n = u \cdot v$, $(u,v)=1$, $u>3$ and $v>3$. Let a and b satisfy (i) and (ii) respectively. By the CRT we can find c such that $c \equiv a \pmod{u}$ and $c \equiv b \pmod{v}$. From $(n, a^2-4)=1$ and $(n, b^2-4)=1$, we have $(u, c^2-4)=1$ and $(v, c^2-4)=1$ and so $(n, c^2-4)=1$. The Congruence Rule (4.1) implies that $Y_c(n) \equiv Y_a(n) \pmod{u}$ and $Y_c(n) \equiv Y_b(n) \pmod{v}$. Hence $Y_c(n) \equiv 1 \not\equiv -1 \pmod{u}$ and $Y_c(n) \equiv -1 \not\equiv 1 \pmod{v}$. Then $Y_c(n) \not\equiv 1 \pmod{n}$ and $Y_c(n) \not\equiv -1 \pmod{n}$ which contradicts (iii). Thus n is prime.

Theorem 11.22. Suppose $1 < n$ and $(n,6)=1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4))=1 \Rightarrow Y_a(n) \equiv \epsilon_a(n) \pmod{n}]. \tag{11.22}$$

Proof. $\Rightarrow$. This is Theorem 6.11.

$\Leftarrow$. n is squarefree by Lemma 6.23. From Lemma 10.8, we can find a and b such that $(n, a^2-4)=1$, $(n, a^2-4)=1$, $\epsilon_a(n)=1$ and $\epsilon_b(n)=-1$. Then (11.22) will imply that all conditions (i), (ii) and (iii) in Theorem 11.21 hold. Hence n is prime by 11.21.

Theorem 11.23. Suppose $n > 1$ and $(n,6)=1$. Then n is prime if and only if following conditions hold simultaneously

(i) $\exists a[(n, a(a^2-4))=1 \text{ and } Y_a(n-1) \equiv 0 \pmod{n}]$,

(ii) $\exists b[(n, b(b^2-4))=1 \text{ and } Y_b(n+1) \equiv 0 \pmod{n}]$,

(iii) $\forall c[(n, c(c^2-4))=1 \Rightarrow Y_c(n \pm 1) \equiv 0 \pmod{n}]$.

Proof. $\Rightarrow$. Suppose n is prime. Then $n > 3$. By Theorem 10.1, there are $(n-3)/2$ $a's$ such that $\epsilon_a(n) = 1$, and there are $(n-1)/2$ $b's$ such that $\epsilon_b(n) = -1$. Then by Theorem 6.12, (i) (ii) and (iii) are all hold.

$\Leftarrow$. Suppose (i) (ii) and (iii) hold. By Lemma 6.23, (iii) implies n is squarefree. If n is composite, put $n = u \cdot v$, $(u,v)=1$, $u > 3$ and $v > 3$. Let a and b satisfy (i) and (ii)

respectively. By the CRT we can find c such that $c \equiv a \pmod{u}$ and $c \equiv b \pmod{v}$. Then from $(n, a(a^2-4)) = 1$ and $(n, b(b^2-4)) = 1$, we have $(u, c(c^2-4)) = 1$ and $(v, c(c^2-4)) = 1$ and hence $(n, c(c^2-4)) = 1$. The Congruence Rule (4.1) implies that $Y_c(n-1) \equiv Y_a(n-1) \pmod{u}$ and $Y_c(n+1) \equiv Y_b(n+1) \pmod{v}$. And the GCD Theorem implies $(Y_c(n-1), Y_c(n+1)) = Y_c(2) = c$. Hence $(n, c) = 1$ implies $Y_c(n+1) \not\equiv 0 \pmod{u}$ and $Y_c(n-1) \not\equiv 0 \pmod{v}$. Then $Y_c(n+1) \not\equiv 0 \pmod{n}$ and $Y_c(n-1) \not\equiv 0 \pmod{n}$ which contradicts (iii). Consequently n is prime.

Theorem 11.24. Suppose $1 < n$ and $(n, 6) = 1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4)) = 1 \implies Y_a(n - \epsilon_a(n)) \equiv 0 \pmod{n}]. \tag{11.24}$$

Proof. $\Rightarrow$. This is Theorem 6.12.

$\Leftarrow$. By Lemma 6.23, n is squarefree. From Lemma 10.11, we can find a and b such that $(n, a^2-4) = 1$, $(n, a^2-4) = 1$, $\epsilon_a(n) = 1$ and $\epsilon_b(n) = -1$. Then (11.24) will imply all conditions (i), (ii) and (iii) in Theorem 11.23 hold. Hence n is prime by 11.23.

Theorem 11.25. Suppose $1 < n$ and $(n, 6) = 1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4)) = 1 \Rightarrow n \text{ is an } elpsp(a)]. \tag{11.25}$$

Theorem 11.26. Suppose $1 < n$ and $(n, 6) = 1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4)) = 1 \Rightarrow n \text{ is a } slpsp(a)]. \tag{11.26}$$

Theorem 11.27. Suppose $1 < n$ and $(n, 6) = 1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4)) = 1 \Rightarrow n \text{ is a } slxpsp(a)]. \tag{11.27}$$

Theorem 11.28. Suppose $1 < n$ and $(n, 6) = 1$. Then n is prime if and only if

$$(\forall a)[(n, a(a^2-4)) = 1 \implies n \text{ is a } rpsp(a)]. \tag{11.27}$$

Proof. $\Rightarrow$. This follows from Theorem 7.13.

$\Longleftarrow$. Suppose (11.28) holds. Let $p \mid n$. By Lemma 6.23, n is squarefree. Hence $(p, n/p)=1$. By Lemma 10.14 we can find $1 \le a, b \le n$, $(n, ab(a^2-4)(b^2-4))=1$ such that $a \equiv b \pmod{n/p}$ and $\rho_a(n) = -\rho_b(n)$, $\epsilon_a(n) = \epsilon_b(n)$. Denote them ϵ. From the hypothesis on n,

$$Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a(n) \pmod{n}, \quad \text{hence } Y_a\left(\frac{n+\epsilon}{2}\right) \equiv \rho_a(n) \pmod{n/p},$$
$$Y_b\left(\frac{n+\epsilon}{2}\right) \equiv \rho_b(n) \pmod{n}, \quad \text{hence } Y_b\left(\frac{n+\epsilon}{2}\right) \equiv \rho_b(n) \pmod{n/p}.$$

Then $$-\rho_b(n) = \rho_a(n) \equiv Y_a\left(\tfrac{n+\epsilon}{2}\right) \equiv Y_b\left(\tfrac{n+\epsilon}{2}\right) \equiv \rho_b(n) \pmod{n/p}.$$

It follows $2\rho_b(n) \equiv 0 \pmod{n/p}$. Then we must have $n/p = 1$ and so n is prime.

Theorem 11.29. Suppose $1 < n$ and $(n, 6)=1$. Then n is prime if and only if

(11.29) $$(\forall a)[(n, a(a^2-4))=1 \implies n \text{ is an } apsp(a)].$$

Proof. $\Rightarrow$. This follows from Theorem 7.14.

$\Leftarrow$. Suppose (11.29) holds. Let $p \mid n$. By Lemma 6.23, n is squarefree. Hence $(p, n/p) = 1$. By Lemma 10.14 we can choose $1 \le a, b \le n$ such that $(n, ab(a^2-4)(b^2-4)) = 1$, $a \equiv b \pmod{n/p}$, $\rho_a(n) = -\rho_b(n)$ and $\epsilon_a(n) = \epsilon_b(n) = \epsilon$. Hence $\tau_a(n) = -\tau_b(n)$. The hypothesis on n implies

$$X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a(n) \pmod{n}, \quad \text{so } X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a(n) \pmod{n/p},$$
$$X_b\left(\frac{n+\epsilon}{2}\right) \equiv b\tau_b(n) \pmod{n}, \quad \text{so } X_b\left(\frac{n+\epsilon}{2}\right) \equiv b\tau_b(n) \pmod{n/p}.$$

Since $a \equiv b \pmod{n/p}$,

$$-a\tau_a(n) \equiv -b\tau_a(n) = b\tau_b(n) \equiv X_b\left(\frac{n+\epsilon}{2}\right) \equiv X_a\left(\frac{n+\epsilon}{2}\right) \equiv a\tau_a(n) \pmod{n/p}.$$

It follows that $-a\tau_a(n) \equiv a\tau_a(n) \pmod{n/p}$ and hence $2a\tau_a(n) \equiv 0 \pmod{n/p}$. Since $(n, a)=1$, we must have $n/p = 1$ so that $n = p$ and n is prime.

The condition (11.28) or (11.29) with $rpsp(a)$ or $apsp(a)$ replaced by $tpsp(a)$ is not sufficient for primality of n. We have a slightly weaker version. To prove it we first need a lemma.

Lemma 11.30. Suppose $1<n$, $(n,6)=1$ and $(\forall a)[(n,a(a^2-4))=1 \Rightarrow n$ is a $tpsp(a)]$. Then n is cube-free.

Proof. Suppose there exists an odd prime p such that $p^3 \mid n$. By Lemma 6.22, we can choose a such that $(n,a(a^2-4))=1$ and $p \mid r_a(p^2)$. Hence $p^2 \nmid Y_a((n\pm1)/2)$. However by the assumption, for this a, we have

$X_a((n-\epsilon_a)/2)\equiv 2\tau_a \pmod{n} \Rightarrow X_a((n-\epsilon_a)/2)\equiv 2\tau_a \pmod{p^3} \Rightarrow X_a((n-\epsilon_a)/2)^2\equiv 4 \pmod{p^3} \Rightarrow dY_a((n-\epsilon_a)/2)^2\equiv 0 \pmod{p^3} \Rightarrow Y_a((n-\epsilon_a)/2)\equiv 0 \pmod{p^2}$.

This is a contradiction. Hence $p^3 \nmid n$. The lemma follows.

Theorem 11.31. Let $1<n$, $(n,6)=1$ and $n\neq\square$. Then n is prime if and only if

(11.31) $\qquad (\forall a)[(n,a(a^2-4))=1 \Rightarrow n$ is a $tpsp(a)]$.

Proof. $\Rightarrow$. This follows from Theorem 7.11.

$\Leftarrow$. Suppose (11.31) holds. If n is composite, from Lemma 11.30 and $n \neq \square$, n is not a prime power. Let $n = m\cdot p^e$ with e odd and $(m,p)=1$. By Lemma 10.14 we can choose $1 \leq a,b \leq n$ such that $(n, ab(a^2-4)(b^2-4))=1$, $a \equiv b \pmod{p^e}$, and $\rho_a(n)=-\rho_b(n)$, $\epsilon_a(n)=\epsilon_b(n)=\epsilon$. Hence $\tau_a(n)=-\tau_b(n)$. The hypothesis on n implies

$$X_a\left(\frac{n-\epsilon}{2}\right)\equiv 2\tau_a \pmod{n}, \quad \text{so } X_a\left(\frac{n-\epsilon}{2}\right)\equiv 2\tau_a \pmod{p^e},$$

$$X_b\left(\frac{n-\epsilon}{2}\right)\equiv 2\tau_b \pmod{n}, \quad \text{so } X_b\left(\frac{n-\epsilon}{2}\right)\equiv 2\tau_b \pmod{p^e}.$$

Hence $\quad -2\tau_a = 2\tau_b \equiv X_b((n-\epsilon)/2) \equiv X_a((n-\epsilon)/2) \equiv 2\tau_a \pmod{p^e}$.

It follows $2\tau_a \equiv 0 \pmod{p^e}$. So $p^e \mid 2$. This contradiction shows that n is a prime.

The assumption of $n \neq \square$ in Theorem 11.31 cannot be removed. This can be seen from the following lemma.

Lemma 11.32. Suppose $n = p^2$ with $p > 3$. Then

(11.32) $\qquad (\forall a)[(n, a^2-4)=1 \Rightarrow n \text{ is a } tpsp(a)].$

Proof. For any given a with $(n, a^2-4)=1$, since $n = p^2 = \square$, $\epsilon_a(n) = \tau_a(n) = 1$. From Theorem 6.12, $p \mid Y_a((p-\epsilon_a(p))/2)$, then $p \mid Y_a((p^2-1)/4)$ by the Division Theorem. Hence $p^2 \mid Y_a((p^2-1)/4)^2$. By the Double Angle Formula (3.4), we have

$$(*) \quad X_a\left(\frac{p^2-\epsilon_a(p^2)}{2}\right) = X_a\left(\frac{p^2-1}{2}\right) = dY_a\left(\frac{p^2-1}{4}\right)^2 + 2 \equiv 0+2 = 2\tau_a(p^2) \pmod{p^2}.$$

Since $n = p^2$, congruence $(*)$ shows that n is a $tpsp(a)$. Since a is arbitrary, the lemma follows.

The Corollary 7.23 shows that

n is a $lpsp(a) \Leftrightarrow n$ is a $lpsp(n-a)$, $\quad n$ is an $elpsp(a) \Leftrightarrow n$ is an $elpsp(n-a)$,

n is a $tpsp(a) \Leftrightarrow n$ is a $tpsp(n-a)$, $\quad n$ is a $rpsp(a) \Leftrightarrow n$ is a $rpsp(n-a)$,

n is an $apsp(a) \Leftrightarrow n$ is an $apsp(n-a)$, n is a $slpsp(a) \Leftrightarrow n$ is a $slpsp(n-a)$,

n is a $slxpsp(a) \Leftrightarrow n$ is a $slxpsp(n-a)$.

Also for any odd integer n, 0, 1, $n-1$ are trivial bases of all types of pseudoprimes we discussed so far. Hence applying Theorems 11.22, 11.24, 11.25, 11.26, 11.27, 11.28, 11.29 and 11.31, we have following theorem

Theorem 11.33. Suppose $n > 1$ and $(n,6)=1$. Each of the following statements is equivalent to primality of n:

(i) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow Y_a(n) \equiv \epsilon \pmod{n}]$,

(ii) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is a } lpsp(a)]$,

(iii) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is an } elpsp(a)]$,

(iv) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is a } slpsp(a)]$,

(v) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is a } slxpsp(a)]$,

(vi) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is a } rpsp(a)]$,

(vii) $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is an } apsp(a)]$,

(viii) $n \neq \square$ and $\forall a[3 \le a \le (n-1)/2 \text{ and } (n, a(a^2-4))=1 \Rightarrow n \text{ is a } tpsp(a)]$.

Some variants of statements in this theorem are known for general Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$, e.g. variants of (iii) and (iv). See Lieuwens [30], Rotkiewicz [46] and Williams [51].

§12. Formulas for the number of ordinary pseudoprime bases

In this section we will discuss properties of ordinary pseudoprimes and give formulas for the number of bases to which an odd integer n is a pseudoprime, Euler pseudoprime and strong pseudoprime. Three of these formulas are known, ((12.9), (12.10) and (12.11)), and three are new, ((12.12), (12.13) and (12.14)).

Recall the concept of order of a mod n, which is the least positive integer t such that $a^t \equiv 1 \pmod{n}$. We shall denote it here by $O_a(n)$. Lots of properties are shared by the rank, denoted here by $r_a(n)$ and the order $O_a(n)$. E.g. $a^k \equiv 1 \pmod{n}$ if and only if $O_a(n) \mid k$, corresponds to the divisibility property of the rank, Lemma 6.4. Another one is $k \mid p-1$ implies there are $\phi(k)$ a's such that $O_a(p) = k$. This is easy to prove from the theorem of the primitive element and we can generalize this theorem mod p to mod p^e. This is analogous to the property of the rank $r_a(p)$: there are $\phi(k)$ a's such that $r_a(p) = k$, provided $k \mid (p - \epsilon_a(p))/2$ and $k > 1$, which we proved in Section 10. Note that there is a small difference here. For order, this property still holds even for $k = 1$.. If $k \mid p-1$, then there are exactly k solutions mod p of $a^k \equiv 1 \pmod{p}$.

We shall need some definitions.

Definition 12.1. An odd integer $n > 1$ is a *pseudoprime* to the base a, $psp(a)$, if $a^{n-1} \equiv 1 \pmod{n}$. (Here we can add $(n, a) = 1$, but it is implied.)

Definition 12.2. An odd integer $n > 1$ is a *Euler pseudoprime* to base a, $epsp(a)$, if $(a, n) = 1$ and $a^{(n-1)/2} \equiv (a/n) \pmod{n}$, where (a/n) is a Jacobi symbol.

Definition 12.3. A odd number n, $n = u2^t + 1$ and u odd, is a *strong pseudoprime* to base a, *spsp*(a), if

(i) $a^s \equiv 1 \pmod{n}$ or (ii) $a^{s2^r} \equiv -1 \pmod{n}$ for some r $(0 \leq r < t)$.

Obviously *epsp*(a) $\Rightarrow$ *psp*(a). Also it is known that *spsp*(a) $\Rightarrow$ *epsp*(a) (Williams [52]). We mention some other needed lemmas.

Lemma 12.4. If m has a primitive root and $(a, m) = 1$, then the congruence

(12.4) $$x^k \equiv a \pmod{m}$$

has $(k, \phi(m))$ solutions x or no solutions, mod m.

Proof. Let g be a primitive root mod m. By the index argument, we can write $x = g^i$ and $a = g^j$. Hence $x^k \equiv a \pmod{m} \Leftrightarrow g^{ik} \equiv g^j \pmod{m} \Leftrightarrow ik \equiv j \pmod{\phi(m)}$. The number of solutions of the last congruence is $(k, \phi(m))$, or 0 if $(k, \phi(m))$ does not divide j. In particular, if $a = 1$, then $j = 0$. Hence $(k, \phi(m)) \mid j$. In this case the congruence (12.4) has exactly $(k, \phi(m))$ incongruent solutions.

Lemma 12.5. If p^e divides n, then the number of solutions mod p^e of

(12.5) $$x^{n-1} \equiv 1 \pmod{p^e} \quad \text{is } (n-1, p-1).$$

Proof. p^e has a primitive root so Lemma 12.4 can be applied. Put $k = n - 1$ and $m = p^e$ in Lemma 12.4. Then it says there are $(n-1, \phi(p^e))$ solutions to (12.5). Since $p^e \mid n$, we have $(n-1, p) = 1$ so that $(n-1, \phi(p^e)) = (n-1, p^e(p-1)) = (n-1, p-1)$.

Lemma 12.6. Suppose $(k, p) = 1$. If $a^k \equiv 1 \pmod{p^e}$, then $O_a(p^e) \mid (k, p-1)$. Further, $O_a(p^e) \mid (k, (p-1)/2)$ if and only if $(a/p) = 1$.

Proof. From $a^k \equiv 1 \pmod{p^e}$ and $a^{p^{e-1}(p-1)} = a^{\phi(p^e)} \equiv 1 \pmod{p^e}$, we have $O_a(p^e) \mid (k, p^{e-1}(p-1)) = (k, p-1)$. Here we can drop p^{e-1} since $(k, p) = 1$. If $(a/p) = +1$, then $a^{(p-1)/2} \equiv 1 \pmod{p}$. This implies $a^{(p-1)/2} \equiv 1 \pmod{p^e}$ by the identity

$a^{p-1}-1=(a^{(p-1)/2}+1)(a^{(p-1)/2}-1)$ and the fact $p \mid a^{(p-1)/2}-1$. Hence $O_a(p^e) \mid (k, \frac{p-1}{2})$. If $(a/p) = -1$, then a similar argument shows $a^{(p-1)/2} \equiv -1 \pmod{p^e}$. Then $O_a(p^e) \nmid (p-1)/2$.

Theorem 12.7. Suppose $(k,p)=1$. Then the following two congruences have the same set of solutions mod p^e,

(1) $\quad a^k \equiv 1 \pmod{p^e}$ and

(2) $\quad a^{(k,p-1)} \equiv 1 \pmod{p^e}$.

Proof. Let T be the set of solutions of (1) and S be the set of solutions of (2). Since $(k,p-1) \mid k$, we know each solution of (2) is a solution of (1). Hence $S \subseteq T$. Next we show $T \subseteq S$. If not, then there exists a such that

$$a^k \equiv 1 \pmod{p^e} \text{ and } a^{(k,p-1)} \not\equiv 1 \pmod{p^e}.$$

This is equivalent to saying there exists a such that

(*) $\quad O_a(p^e) \mid k$ and (**) $\quad O_a(p^e) \nmid p-1$.

By Euler's Theorem we have $O_a(p^e) \mid \phi(p^e)$ where $\phi(p^e)=p^{e-1}(p-1)$. This together with (**) implies $p \mid O_a(p^e)$. Hence by (*) we have $p \mid k$, which contradicts the assumption $(p,k)=1$. Therefore $S=T$. The theorem is proved.

Theorem 12.8. For any $(k,p)=1$, there are $(2k,p-1)-(k,p-1)$ solutions mod p^e for $a^k \equiv -1 \pmod{p^e}$.

Proof. We use Theorem 12.7 and the identity $a^{2k}-1=(a^k-1)(a^k+1)$.

Let $B(n) = |\{a : 0 \le a < n \text{ and } n \text{ is an } psp(a)\}|,$

$E(n) = |\{a : 0 \le a < n \text{ and } n \text{ is an } epsp(a)\}|,$

$S(n) = |\{a : 0 \le a < n \text{ and } n \text{ is a } spsp(a)\}|.$

Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$. Baillie and Wagstaff [2] give the following formula for $B(n)$:

$$B(n) = \prod_{i=1}^{k} (n-1, p_i - 1). \tag{12.9}$$

About the same time, Monier [38] gave the following formula for $E(n)$:

Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$, and $n = r2^t + 1$, r odd, $p_i = r_i 2^{s_i} + 1$, r_i odd $(i = 1, \cdots, k)$.

Suppose further the p_i have been ordered so that $s_1 \le s_2 \le \cdots \le s_k$. Then

$$E(n) = \delta_n \prod_{i=1}^{k} \left(\frac{n-1}{2}, p_i - 1 \right), \tag{12.10}$$

where δ_n has one of the values 2, 1/2 or 1 according to the rule

$$\delta_n = \begin{cases} 2 & \text{if } s_1 = t, \\ 1/2 & \text{if } s_i < t \text{ holds for some prime } p_i \text{ with } e_i \text{ odd}, \\ 1 & \text{otherwise.} \end{cases}$$

Monier [38] also gave the following formula for $S(n)$:

Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$, and $n = r2^t + 1$, r odd, $p_i = r_i 2^{s_i} + 1$, r_i odd $(i = 1, \cdots, k)$.

Suppose further the p_i have been ordered so that $s_1 \le s_2 \le \cdots \le s_k$. Then

$$S(n) = \left(1 + \frac{2^{ks_1} - 1}{2^k - 1} \right) \prod_{i=1}^{k} (r, r_i). \tag{12.11}$$

We give some different formulas for $B(n)$, $E(n)$ and $S(n)$.

Theorem 12.12. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$. Then

$$B(n) = \sum_{\epsilon_i = \pm 1} \prod_{i=1}^{k} \left(\frac{n-1}{2}, \frac{p_i - 1}{2} \right). \tag{12.12}$$

Proof. We have $((n-1)/2, (p_i-1)/2) = (n-1, p_i-1)/2$ and the $\epsilon_i = \pm 1$ range over exactly 2^k values. Hence $\sum_{\epsilon_i=\pm1} \prod_{i=1}^k [(n-1, p_i-1)/2] = \sum_{\epsilon_i=\pm1} (1/2^k) \prod_{i=1}^k (n-1, p_i-1) = (2^k) \cdot (1/2^k) \prod_{i=1}^k (n-1, p_i-1) = \prod_{i=1}^k (n-1, p_i-1)$. The formula is equivalent to that of 12.9.

In the next formula the ϵ_i will range over same set, $\epsilon_1 = \pm 1, \cdots, \epsilon_k = \pm 1$.

Theorem 12.13. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$. Then

$$
\begin{aligned}
E(n) = \sum_{\epsilon_i=\pm1} \prod_{i=1}^k \Big[&\Big(\frac{n-1}{2^\mu}, \frac{p_i-1}{2^{\mu_i}}\Big) - \Big(\frac{1-\epsilon_i}{2}\Big)\Big(\frac{n-1}{2^\mu}, \frac{p_i-1}{2}\Big) \\
&- \Big(\frac{1-\epsilon}{2}\Big)\Big(\frac{n-1}{2}, \frac{p_i-1}{2^{\mu_i}}\Big) + \Big(\frac{1-\epsilon_i}{2}\Big)\Big(\frac{1-\epsilon}{2}\Big)\Big(\frac{n-1}{2}, \frac{p_i-1}{2}\Big)\Big].
\end{aligned} \tag{12.13}
$$

where $\epsilon = \epsilon_1^{e_1} \cdots \epsilon_i^{e_i}$, $\mu = \frac{1+\epsilon}{2}$ and $\mu_i = \frac{1+\epsilon_i}{2}$.

Proof. Let $O_a(p^e)$ denote the order of a mod p^e. Also for $1 \le i \le k$, $\epsilon = \pm 1$ and $\epsilon_i = \pm 1$, define

$$
\begin{aligned}
A_i(\epsilon, \epsilon_i) \;=\; &\Big(\frac{n-1}{2^\mu}, \frac{p_i-1}{2^{\mu_i}}\Big) - \Big(\frac{1-\epsilon_i}{2}\Big)\Big(\frac{n-1}{2^\mu}, \frac{p_i-1}{2}\Big) - \Big(\frac{1-\epsilon}{2}\Big)\Big(\frac{n-1}{2}, \frac{p_i-1}{2^{\mu_i}}\Big) \\
&+ \Big(\frac{(1-\epsilon_i)(1-\epsilon)}{4}\Big)\Big(\frac{n-1}{2}, \frac{p_i-1}{2}\Big).
\end{aligned}
$$

The sum over the k-tuples $\langle \epsilon_1, \cdots, \epsilon_k \rangle$ represents a consideration of all possible cases $(a/n) = \epsilon$ and $(a/p_i) = \epsilon_i$. We divide these cases into 4 groups and consider them separately for each fixed $p_i^{e_i}$.

Case (i). $(a/n) = 1$ and $(a/p_i) = 1$. Let $\epsilon = (a/n)$ and $\epsilon_i = (a/p_i)$. Then $\mu = 1$ and $\mu_i = 1$. Thus

(1) $\qquad A_i(\epsilon, \epsilon_i) = A_i(1,1) = \Big(\frac{n-1}{2}, \frac{p_i-1}{2}\Big)$.

Suppose $a^{(n-1)/2} \equiv (a/n) = 1 \pmod{n}$. Since $((n-1)/2, p_i) = 1$ and $(a/p_i) = 1$, by Lemma 12.6, for all these bases a, we have $O_a(p_i^{e_i}) \,|\, \Big(\frac{n-1}{2}, \frac{p_i-1}{2}\Big) = A_i(\epsilon, \epsilon_i)$.

Thus $A_i(\epsilon, \epsilon_i)$ counts the number of bases mod $p_i^{e_i}$ such that n is an $epsp(a)$, $(a/n)=1$ and $(a/p_i) = 1$.

Case (ii). $(a/n) = 1$ and $(a/p_i) = -1$. Let $\epsilon = (a/n)$ and $\epsilon_i = (a/p_i)$. Then $\mu = 1$ and $\mu_i = 0$. Thus

(2) $\quad A_i(\epsilon, \epsilon_i) = A_i(1, -1) = \left(\frac{n-1}{2}, p_i - 1\right) - \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$.

Suppose $a^{(n-1)/2} \equiv (a/n) = 1 \pmod{n}$. Then $a^{(n-1)/2} \equiv (a/n) = 1 \pmod{p_i^{e_i}}$. By Lemma 12.6, we have $O_a(p_i^{e_i}) \mid \left(\frac{n-1}{2}, p_i - 1\right)$ and $O_a(p_i^{e_i}) \nmid \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$. Now $\left(\frac{n-1}{2}, p_i - 1\right) - \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$ is the number of bases mod $p_i^{e_i}$ such that $O_a(p_i^{e_i}) \mid \left(\frac{n-1}{2}, p_i - 1\right)$ and $O_a(p_i^{e_i}) \nmid \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$. Hence $A_i(\epsilon, \epsilon_i) = \left(\frac{n-1}{2}, p_i - 1\right) - \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$ counts the number of bases mod $p_i^{e_i}$ such that n is an $epsp(a)$, $(a/n) = 1$ and $(a/p_i) = -1$.

Case (iii) $(a/n) = -1$ and $(a/p_i) = 1$. Let $\epsilon = (a/n)$ and $\epsilon_i = (a/p_i)$. Then $\mu = 0$ and $\mu_i = 1$. Thus

(3) $\quad A_i(\epsilon, \epsilon_i) = A_i(-1, 1) = \left(n - 1, \frac{p_i-1}{2}\right) - \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$.

If $a^{(n-1)/2} \equiv (a/n) = -1 \pmod{n}$, then $a^{(n-1)/2} \equiv -1 \pmod{p_i^{e_i}}$. Hence $O_a(p_i^{e_i}) \mid n-1$ and $O_a(p_i^{e_i}) \nmid (n-1)/2$. Then using Lemma 12.6, $O_a(p_i^{e_i}) \mid (n-1, (p_i-1)/2)$ and $O_a(p_i^{e_i}) \nmid ((n-1)/2, (p_i-1)/2)$. Hence $A_i(\epsilon, \epsilon_i) = \left(n - 1, \frac{p_i-1}{2}\right) - \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$ counts the number of bases mod $p_i^{e_i}$ such that n is an $epsp(a)$, $(a/n) = -1$ and $(a/p_i) = 1$.

Case (iv) $(a/n) = -1$ and $(a/p_i) = -1$. Let $\epsilon = (a/n)$ and $\epsilon_i = (a/p_i)$. Then $\mu = 0$ and $\mu_i = 0$. Thus

(4) $A_i(\epsilon, \epsilon_i) = A_i(-1, -1) = (n-1, p_i-1) - \left(n - 1, \frac{p_i-1}{2}\right) - \left(\frac{n-1}{2}, p_i - 1\right) + \left(\frac{n-1}{2}, \frac{p_i-1}{2}\right)$.

If $a^{(n-1)/2} \equiv (a/n) = -1 \pmod{n}$, then $a^{(n-1)/2} \equiv -1 \pmod{p_i^{e_i}}$. Hence $O_a(p_i^{e_i}) \mid n-1$ and $O_a(p_i^{e_i}) \nmid \frac{n-1}{2}$. Since $(a/p_i^{e_i}) = -1$, from Lemma 12.6, $O_a(p_i^{e_i}) \mid (n-1, p_i-1)$, $O_a(p_i^{e_i}) \nmid ((n-1), (p_i-1)/2)$ and $O_a(p_i^{e_i}) \nmid ((n-1)/2, (p_i-1))$. As we know

$(n-1, p_i-1)-((n-1), (p_i-1)/2)$ is the number of incongruent bases mod $p_i^{e_i}$ such that $O_a(p_i^{e_i}) \mid (n-1, p_i-1)$ and $O_a(p_i^{e_i}) \nmid (n-1, (p_i-1)/2)$. Also $(n-1, p_i-1)-((n-1)/2, p_i-1)$ is the number of incongruent bases mod $p_i^{e_i}$ such that $O_a(p_i^{e_i}) \mid (n-1, p_i-1)$ and $O_a(p_i^{e_i}) \nmid ((n-1)/2, p_i-1)$. Thus it would appear that $(n-1, p_i-1) - ((n-1)/2, p_i-1) - (n-1, (p_i-1)/2)$ would count the number of bases mod $p_i^{e_i}$ such that $O_a(p_i^{e_i}) \mid (n-1, p_i-1)$, $O_a(p_i^{e_i}) \nmid ((n-1), (p_i-1)/2)$ and $O_a(p_i^{e_i}) \nmid ((n-1)/2, (p_i-1))$. However, since

$$((n-1, (p_i-1)/2), ((n-1)/2, p_i-1)) = ((n-1)/2, (p_i-1)/2),$$

when we subtract $(\frac{n-1}{2}, p_i-1)$ and $(n-1, \frac{p_i-1}{2})$, we subtract $(\frac{n-1}{2}, \frac{p_i-1}{2})$ twice. Thus this must be added in again. Therefore by (4) $A_i(\epsilon, \epsilon_i)$ counts the number of bases mod $p_i^{e_i}$ such that n is an $epsp(a)$, $(a/n) = -1$ and $(a/p_i) = -1$.

Since for each $p_i^{e_i}$ $A_i(\epsilon, \epsilon_i)$ always counts the number of bases a mod $p_i^{e_i}$ such that n is an $epsp(a)$, by the CRT, the product $\prod_i A_i(\epsilon, \epsilon_i)$ counts the number of bases a corresponding to a fixed k-tuple $\langle \epsilon_1, \cdots, \epsilon_k \rangle$ such that n is an $epsp(a)$. Hence the sum over all k-tuples, $\sum_{\epsilon_i=\pm 1} \prod_i A_i(\epsilon, \epsilon_i)$, gives the number of bases a mod n such that n is an $epsp(a)$. This completes the proof.

Our formula $E(n)$ looks like much more complicated than that of Monier's. However, when one uses Monier's formula (12.10) to count $E(n)$ he has to express n in the form $n = r2^t + 1$ and each prime factor p_i of n in the form $p_i = r_i 2^{t_i} + 1$, and then decide the complicated coefficient δ_n; while in using our formula (12.13), these are all omitted. Hence we think our formula is easier to use.

Theorem 12.14. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is odd, and $n = u2^t + 1$ where u odd. Then the number of incongruent bases a such that n is a $spsp(a)$ is given by

$$S(n) = \prod_{i=1}^{k} \left(\frac{n-1}{2^t}, p_i - 1\right) + \sum_{s=1}^{t} \prod_{i=1}^{k} \left[\left(\frac{n-1}{2^{s-1}}, p_i - 1\right) - \left(\frac{n-1}{2^s}, p_i - 1\right)\right]. \tag{12.14}$$

Proof. By Lemma 12.7, the first term in $S(n)$ counts the bases a such that $a^{\frac{n-1}{2^t}} \equiv 1 \pmod{n}$. By Lemma 12.8, the second term in $S(n)$ counts the bases a such that for some s, $1 \leq s \leq t$ and $a^{\frac{n-1}{2^s}} \equiv -1 \pmod{n}$. Thus the sum of these two terms, $S(n)$, is the number of incongruent bases such that n is a strong pseudoprime. This completes the proof.

Again, by the same reason as the above, we think that our formula (12.14) has its advantage to use.

§13. Formulas for the number of Lucas pseudoprime bases

In this section we will give formulas which count the number of incongruent bases a mod n to which n is $lpsp(a)$, or $elpsp(a)$, or $slpsp(a)$. These three formulas (13.7), (13.8) and (13.9) appear to be new.

Lemma 13.1. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is odd and $(n,d) = 1$. Let $\epsilon = (d/n)$ and $\epsilon_i = (d/p_i)$. Then n is $elpsp(a)$ if and only if for all i $(1 \le i \le k)$,

$$r_a(p_i^{e_i}) \,|\, ((n-\epsilon)/2, (p_i - \epsilon_i)/2).$$

Proof. $\Leftarrow$. Suppose that for all $p_i^{e_i} \,|\, n$, we have $r_a(p_i^{e_i}) \,|\, ((n-\epsilon)/2, (p_i - \epsilon_i)/2)$. Then $r_a(p_i^{e_i}) \,|\, (n-\epsilon)/2$. Hence $Y_a((n-\epsilon)/2) \equiv 0 \pmod{p_i^{e_i}}$. Since for $i \neq j$, $(p_i^{e_i}, p_j^{e_j}) = 1$, this implies $Y_a((n-\epsilon)/2) \equiv 0 \pmod{n}$, we have that n is an $elpsp(a)$.
$\Rightarrow$. Suppose $p_i^{e_i} | n$ and $Y_a((n-\epsilon)/2) \equiv 0 \pmod{n}$. Then $Y_a((n-\epsilon)/2) \equiv 0 \pmod{p_i^{e_i}}$. Hence $r_a(p_i^{e_i}) \,|\, (n-\epsilon)/2$. From Theorem 6.15 we have $r_a(p_i^{e_i}) \,|\, T_a(p_i^{e_i})$ where $T_a(p_i^{e_i}) = p_i^{e_i-1}(p_i - \epsilon_i)/2$. Hence $r_a(p_i^{e_i}) \,|\, ((n-\epsilon)/2, p_i^{e_i-1}(p_i-\epsilon_i)/2) = ((n-\epsilon)/2, (p_i-\epsilon_i)/2)$. The last equality holds since $(p_i, n-\epsilon) = 1$. This proves the lemma.

Lemma 13.2. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is odd and $(n,d) = 1$. Let $\epsilon = (d/n)$ and $\epsilon_i = (d/p_i)$. Then n is $lpsp(a)$ if and only if for all i $(1 \le i \le k)$,

$$r_a(p_i^{e_i}) \,|\, (n - \epsilon, (p_i - \epsilon_i)/2).$$

Proof. Recall that $lpsp(a)$ means $Y_a(n-\epsilon) \equiv 0 \pmod{n}$. Then use an argument similar to that of the proof for 13.1.

Theorem 13.3. Suppose $\epsilon = \pm 1$ and $k \mid (p-\epsilon)/2$. Then there are exactly $k-1$ incongruent solutions $a \bmod p^e$ of $Y_a(k) \equiv 0 \pmod{p^e}$ with $\epsilon_a = \epsilon$.

Proof. This is Theorem 10.10.

Lemma 13.4. Suppose $\epsilon = \pm 1$, $p \equiv \epsilon \pmod 4$ and $k \mid (p-\epsilon)/4$. Then

$X_a(k) \equiv 0 \pmod{p^e}$ has k incongruent solutions with $(n,d)=1$ and $\epsilon_a(p) = \epsilon$.

Proof. Suppose $k \mid (p-\epsilon)/4$. Then $2k \mid (p-\epsilon)/2$ and $k \mid (p-\epsilon)/2$. By Theorem 13.3,

$$(*) \qquad Y_a(2k) \equiv 0 \pmod{p^e}$$

has $2k-1$ incongruent solutions and

$$(**) \qquad Y_a(k) \equiv 0 \pmod{p^e}$$

has $k-1$ incongruent solutions. It remains to count the number of solutions of

$$(***) \qquad X_a(k) \equiv 0 \pmod{p^e}.$$

By (3.5), we know that the set of solutions to $(*)$ is the union of the sets of solutions to $(**)$ and $(***)$. By Lemma 4.8, $(X_a(k), Y_a(k)) \mid 2$. Thus the sets of solutions for $Y_a(k) \equiv 0 \pmod{p^e}$ and $X_a(k) \equiv 0 \pmod{p^e}$ are disjoint. Hence the number of solutions mod p^e for the congruence $(***)$ is $2k-1-(k-1) = k$. It is easy to see that for all these solutions a, $\epsilon_a = \epsilon$. This proves the lemma.

Theorem 13.5. Suppose $(k,p) = 1$. Then the following two congruences have the same set of solutions mod p^e:

$$(1) \quad Y_a(k) \equiv 0 \pmod{p^e} \quad \text{and} \quad (2) \quad Y_a\left(\left(k, \tfrac{p-\epsilon_a(p)}{2}\right)\right) \equiv 0 \pmod{p^e}.$$

Proof. Let T be the set of solutions to (1) and S be the set of solutions to (2). Since $(k, (p-\epsilon_a(p))/2) \mid k$, the Division Theorem tells us that each solution of (2) is a solution of (1). Hence $S \subseteq T$. Next we show $T \subseteq S$. If $T \not\subseteq S$, then there exists

an a such that $Y_a(k) \equiv 0 \pmod{p^e}$ and $Y_a\left(\left(k, \frac{p-\epsilon_a(p)}{2}\right)\right) \not\equiv 0 \pmod{p^e}$. This is equivalent to saying that there exists an a such that

$$(*) \qquad r_a(p^e) \mid k \qquad \text{and} \qquad (**) \qquad r_a(p^e) \nmid \frac{p-\epsilon_a(p)}{2}.$$

By Theorem 6.15, we have $r_a(p^e) \mid T_a(p^e)$ where $T_a(p^e) = p^{e-1} \cdot (p - \epsilon_a(p))/2$. This together with $(**)$ implies $p \mid r_a(p^e)$. Hence $p \mid k$ which contradicts the assumption $(p,k)=1$. Therefore $S = T$. The theorem is proved.

Theorem 13.6. Suppose $\epsilon = \pm 1$ and $(k,p)=1$. Then there are exactly $(2k, \frac{p-\epsilon}{2}) - (k, \frac{p-\epsilon}{2})$ solutions $a \bmod p^e$ for $X_a(k) \equiv 0 \pmod{p^e}$ with $\epsilon_a(p) = \epsilon$.

Proof. Consider those a with $\epsilon_a(p) = \epsilon$ and $X_a(k) \equiv 0 \pmod{p^e}$. From (3.5) we have $Y_a(2k) = Y_a(k)X_a(k) \equiv 0 \pmod{p^e}$. By Theorem 13.5 and Theorem 13.3, $Y_a(2k) \equiv 0 \pmod{p^e}$ has $((2k,(p-\epsilon)/2) - 1$ incongruent solutions mod p^e and $Y_a(k) \equiv 0 \pmod{p^e}$ has $((k,(p-\epsilon)/2) - 1$ incongruent solutions mod p^e. Since $(Y_a(k), X_a(k)) \mid 2$, it follows that the sets of solutions for $Y_a(k) \equiv 0 \pmod{p^e}$ and $X_a(k) \equiv 0 \pmod{p^e}$ are disjoint. Hence the number of solutions mod p^e for the latter congruence equals $((2k,(p-\epsilon)/2) - ((k,(p-\epsilon)/2)$. This proves the theorem.

REMARK. Theorem 13.6 is the generalization of Lemma 13.4.

Let
$$\begin{aligned} L(n) &= |\{a : 0 \le a < n, (n, a^2-4)=1 \text{ and } n \text{ is a } lpsp(a)\}|, \\ EL(n) &= |\{a : 0 \le a < n, (n, a^2-4)=1 \text{ and } n \text{ is an } elpsp(a)\}|, \\ SL(n) &= |\{a : 0 \le a < n, (n, a^2-4)=1 \text{ and } n \text{ is a } slpsp(a)\}|. \end{aligned}$$

Theorem 13.7. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is odd. Then

$$EL(n) = \sum_{\epsilon_i = \pm 1} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right]. \tag{13.7}$$

where $\epsilon = \epsilon_1^{e_i} \cdots \epsilon_k^{e_k}$.

Proof. For a given k-tuple $\langle \epsilon_1 \cdots \epsilon_k \rangle$, where $\epsilon_i \in \{-1, 1\}$, consider those a such that n is $elpsp(a)$, for each prime power $p_i^{e_i}$ where the Jacobi symbol $(d/p_i) = \epsilon_i$ and therefore $(d/n) = \epsilon$. Let s be the number of those bases a, i.e. the number of solutions of $Y_a\left((n-\epsilon)/2\right) \equiv 0 \pmod{n}$. By the CRT, then $s = s_1 \cdot s_2 \cdots s_k$, where s_i is the number of solutions of $Y_a\left((n-\epsilon)/2\right) \equiv 0 \pmod{p_i^{e_i}}$, $(i = 1, \cdots, k)$. Since $((n-\epsilon)/2, p_i) = 1$, we may apply Theorem 13.5 to obtain $s_i = (\frac{n-\epsilon}{2}, \frac{p_i - \epsilon_i}{2}) - 1$. Hence by the CRT $s = \prod_{i=1}^{k} [((n-\epsilon)/2, (p_i - \epsilon_i)/2) - 1]$. The sum over all possible k-tuples, that is $\sum_{\epsilon_i = \pm 1} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right]$, then gives the total number of bases a such that n is an $elpsp(a)$.

Using a similar idea one can give a formula for the number of bases a to which n is a Lucas pseudoprime in the sense of Rotkiewicz [46], $lpsp(a)$.

Theorem 13.8. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ and n is odd. Then the number of incongruent bases a mod n to which n is a Lucas pseudoprime is given by

$$L(n) = \sum_{\epsilon_i = \pm 1} \prod_{i=1}^{k} \left[\left(n - \epsilon, \frac{p_i - \epsilon_i}{2} \right) - 1 \right]. \tag{13.8}$$

where $\epsilon = \epsilon_1^{e_i} \cdots \epsilon_k^{e_k}$.

Next we give a formula for the number of bases a to which n is a strong Lucas pseudoprime, $slpsp(a)$.

Theorem 13.9. Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ and $n = u2^t + w$ where u is odd, $w = \pm 1$ and $2 \leq t$. Then the number of bases to which n is a strong Lucas pseudoprime, *slpsp*(a), is given by $SL(n) =$

$$\sum_{\epsilon_i = \pm 1, \epsilon = -w} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right] +$$

$$\sum_{\epsilon_i = \pm 1, \epsilon = w} \left\{ \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2^t}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right] + \sum_{s=2}^{t} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2^{s-1}}, \frac{p_i - \epsilon_i}{2} \right) - \left(\frac{n-\epsilon}{2^s}, \frac{p_i - \epsilon_i}{2} \right) \right] \right\}$$

where $\epsilon = \epsilon_1^{e_i} \cdots \epsilon_k^{e_k}$.

Proof. We consider 3 possible types of bases:

Type (i). The bases a such that $(d/p_i) = \epsilon_i$ and $(d/n) = \epsilon = -w$. Then $(n-\epsilon)/2$ is odd. It follows from Theorem 7.5 that n is a *slpsp*(a) if and only if n is an *elpsp*(a). Hence by Theorem 13.7, for case $\epsilon = -w$, the number of bases is

$$(1) \qquad \sum_{\epsilon_i = \pm 1, \epsilon = -w} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right].$$

Type (ii). The bases a such that $(d/p_i) = \epsilon_i$, $(d/n) = \epsilon = w$ and $n \mid Y_a(\frac{n-\epsilon}{2^t})$. Since $((n-\epsilon)/2^t, p_i) = 1$ for each i, we may apply Theorem 13.5. The sum over all possible k-tuples which satisfy $\epsilon = w$ gives the number of all such bases,

$$(2) \qquad \sum_{\epsilon_i = \pm 1, \epsilon = w} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2^t}, \frac{p_i - \epsilon_i}{2} \right) - 1 \right].$$

Type (iii). The bases a such that $(d/p_i) = \epsilon_i$, $(d/n) = \epsilon = w$ and for some $2 \leq s \leq t$,

$$(*) \qquad X_a \left(\frac{n-\epsilon}{2^s} \right) \equiv 0 \pmod{n}.$$

Since $((n-\epsilon)/2^s, p_i) = 1$ for each $2 \leq s \leq t$ and each $1 \leq i \leq k$, we may apply Theorem 13.6 to see that the number of solutions of congruence $(*)$ for each s is $\prod_{i=1}^{k} [(\frac{n-\epsilon}{2^{s-1}}, \frac{p_i - \epsilon_i}{2}) - (\frac{n-\epsilon}{2^s}, \frac{p_i - \epsilon_i}{2})]$. Then summing from $s = 2$ to $s = t$ and taking the

sum over all possible k-tuples such that $\epsilon = w$, we find that the number of bases in this case is

$$(3) \qquad \sum_{\epsilon_i=\pm 1, \epsilon=w} \sum_{s=2}^{t} \prod_{i=1}^{k} \left[\left(\frac{n-\epsilon}{2^{s-1}}, \frac{p_i - \epsilon_i}{2} \right) - \left(\frac{n-\epsilon}{2^s}, \frac{p_i - \epsilon_i}{2} \right) \right].$$

Hence the total number of bases such that n is a strong Lucas pseudoprime is the sum of these 3 sums: (1), (2) and (3), i.e. the formula given in the statement of the theorem. This completes the proof.

§14. Estimates of the number of bases for Euler Lucas pseudoprimes

Recall that $EL(n)$ is the number of bases a, $0 \leq a < n$, such that $(n, a^2-4) = 1$ and n is an *elpsp*(a). Suppose $n > 1$ and n is odd. If n is prime, then $EL(n) = n-2$ and so $EL(n)/(n-2) = 1$. In this section we will give upper bounds for $EL(n)/(n-2)$. We will show that if n is an odd composite integer, then $EL(n)/(n-2) < 1/2$ and if n is not a Lucas Carmichael, then $EL(n)/(n-2) < 1/3$. Also we will show that if n satisfies some further conditions, such as

(i) n is not squarefree and $(n, 6) = 1$,

or (ii) n is squarefree and n has a special prime divisor p such that $p-1 \nmid n+1$, $p-1 \nmid n-1$, $p+1 \nmid n+1$ and $p+1 \nmid n-1$,

or (iii) n is a product of two primes,

then $EL(n)/(n-2) < 1/4$.

Theorem 14.1. Suppose p is an odd prime and $e \geq 1$. Then $EL(p^e) = p-2$.

Proof. This was proved in Section 9 (Theorem 9.16).

Lemma 14.2. Suppose $m_i \geq 2$ and $k \geq 2$. Then $\prod_{i=1}^{k}(m_i - 1) < \left(\prod_{i=1}^{k} m_i\right) - 2$.

Proof. Induction on k. Consider the first case $k = 2$.

$$\prod_{i=1}^{2}(m_i - 1) = (m_1 - 1)(m_2 - 1) = m_1 m_2 - m_1 - m_2 + 1$$

$$\leq m_1 m_2 - 2 - 2 + 1 < m_1 m_2 - 2 = \left(\prod_{i=1}^{2} m_i\right) - 2.$$

Suppose the lemma holds for $k \geq 2$. Consider the case $k+1$.

$$\prod_{i=1}^{k+1}(m_i-1) = (m_{k+1}-1)\prod_{i=1}^{k}(m_i-1) < (m_{k+1}-1)\left(\left(\prod_{i=1}^{k} m_i\right)-2\right)$$

$$= m_{k+1}\prod_{i=1}^{k} m_i - 2m_{k+1} - \prod_{i=1}^{k} m_i + 2 < \prod_{i=1}^{k+1} m_i - 2(m_{k+1}-1) \le \left(\prod_{i=1}^{k+1} m_i\right) - 2.$$

Hence the inequality holds for $k+1$. The lemma is proved.

Lemma 14.3. Suppose $n > 1$, n is odd and $n = \prod_{i=1}^{k} p_i^{e_i}$. Then

$$EL(n) \le (n-2)/(p_1^{e_1-1}\cdots p_k^{e_k-1}).$$

Hence if n is not squarefree, then $EL(n) \le (n-2)/p_i$ for some i.

Proof. Case $k = 1$. By Theorem 14.1, we have

$$EL(n) = EL(p^e) = p-2 = (p^e - 2p^{e-1})/p^{e-1} \le (p^e-2)/p^{e-1}.$$

Case $k \ge 2$. For each i, $(1 \le i \le k)$, we have, for the GCD,

$$\left(\frac{n-\epsilon}{2}, \frac{p_i-\epsilon_i}{2}\right) - 1 \le \frac{p_i-\epsilon_i}{2} - 1 \le \frac{p_i+1}{2} - 1 = \frac{p_i-1}{2} = \frac{p_i^{e_i} - p_i^{e_i-1}}{2p_i^{e_i-1}} \le \frac{p_i^{e_i}-1}{2p_i^{e_i-1}}$$

Since $k \ge 2$ and $p_i \ge 2$, we can apply Lemma 14.2, with $m_i = p_i^{e_i}$, to get

$$\prod_{i=1}^{k}\left[\left(\frac{n-\epsilon}{2}, \frac{p_i-\epsilon_i}{2}\right) - 1\right] \le \prod_{i=1}^{k} \frac{p_i^{e_i}-1}{2p_i^{e_i-1}} = \frac{\prod_{i=1}^{k}(p_i^{e_i}-1)}{\prod_{i=1}^{k} 2p_i^{e_i-1}}$$

$$= \frac{\prod_{i=1}^{k}(p_i^{e_i}-1)}{2^k p_1^{e_1-1}\cdots p_k^{e_k-1}} < \frac{(\prod_{i=1}^{k} p_i^{e_i}) - 2}{2^k p_1^{e_1-1}\cdots p_k^{e_k-1}} = \frac{n-2}{2^k p_1^{e_1-1}\cdots p_k^{e_k-1}}.$$

Therefore using the formula for $EL(n)$ that we derived in Theorem 13.7 and observing that it is a sum over 2^k terms, we get

$$EL(n) = \sum_{\epsilon_1=\pm1,\cdots,\epsilon_k=\pm1} \prod_{i=1}^{k}\left[\left(\frac{n-\epsilon}{2}, \frac{p_i-\epsilon_i}{2}\right) - 1\right] < 2^k \frac{n-2}{2^k p_1^{e_1-1}\cdots p_k^{e_k-1}} = \frac{n-2}{p_1^{e_1-1}\cdots p_k^{e_k-1}}.$$

This proves the lemma.

Lemma 14.4. Let a, b and c be positive integers. Then the following hold.

(i) $(a,b)=1 \Rightarrow (a,c)+(b,c) \le c+1.$

(ii) $(a,b)=1,\ c \nmid a,\ c \nmid b \Rightarrow (a,c)+(b,c) \le c/2+2.$

(iii) $(a,b)=1,\ c \nmid a,\ (a,c)>1 \Rightarrow (a,b)=1,\ c \nmid a,\ c \nmid b.$

Proof. Since $(a,c)\,|\,c$, $\exists A\ [c=(a,c)A$ and $1\le A\le c]$. Since $(b,c)\,|\,c$, $\exists B\ [c=(b,c)B$ and $1\le B\le c]$. Also $(a,b)=1$ implies $((a,c),(b,c))=1$. Hence $(b,c)\,|\,c$ and $c=(a,c)A \Rightarrow (b,c)\,|\,A$. Then $(b,c)\le A$. Now for the proof of (i), $1\le A\le c \Rightarrow (A-1)A\le(A-1)c \Rightarrow A^2-A\le Ac-c \Rightarrow c+A^2\le Ac+A \Rightarrow c/A+A\le c+1$. This proves (i) since $(a,c)+(b,c)=c/A+(b,c)\le c/A+A$.

For the proof of (ii), suppose further $c\nmid a$ and $c\nmid b$. Then $c\nmid a \Rightarrow (a,c)<c$, so $c=(a,c)A<cA \Rightarrow 1<A \Rightarrow 2\le A$. Hence $(a,c)=c/A\le c/2$. Similarly we can show $(b,c)\le c/2$. If $(a,c)\le 2$, then $(a,c)+(b,c)\le 2+c/2$. Suppose $(a,c)>2$. Then $2A<(a,c)A=c \Rightarrow 2A<c$. Since $c\nmid a$, $2\le A$. Hence $2\le A$ and $2A<c \Rightarrow (A-2)2A\le(A-2)c \Rightarrow 2A^2-4A\le Ac-2c$ $\Rightarrow 2c+2A^2\le cA+4A \Rightarrow c+A^2\le cA/2+2A \Rightarrow c/A+A\le c/2+2$. Since $(b,c)\le A$, $(a,c)+(b,c)=c/A+(b,c)\le c/A+A\le c/2+2$. This proves (ii). For the proof of (iii), if $c\mid b$, then $(a,b)=1 \Rightarrow (a,c)=1$. But $(a,c)>1$. So $c\nmid b$. This shows (iii).

Throughout the remainder of this section we will use the following definitions to simplify the notation.

Definition 14.5. Suppose $n=p_1p_2\cdots p_k$ is odd, $\mu=\pm1$, $\delta=\pm1$ and $1\le i\le k$.

$$H(\delta,\mu,p_i,n)=\left(\frac{n-\mu}{2},\frac{p_i-\delta}{2}\right)-1.$$

Definition 14.6. Suppose $n=p_1p_2\cdots p_k$, n is odd, $\gamma=\pm1$ and $1\le l\le k$. Then

$$M(\gamma,l,n)=\sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1}\prod_{i=1}^{l}\left[\left(\frac{n-\gamma\epsilon_1\cdots\epsilon_l}{2},\frac{p_i-\epsilon_i}{2}\right)-1\right],$$

Definition 14.7. Suppose $n=p_1p_2\cdots p_k$, n is odd and $1\le l\le k$. Then

$$S(l,n) = M(+1,l,n) + M(-1,l,n).$$

Let $A(p)=(p-1)/2$ and $B(p)=(p+1)/2$. Then for all n, $A(p)$ and $B(p)$ satisfy

(14.8) $$\left(\frac{n\pm 1}{2}, \frac{p-1}{2}\right) - 1 \le A(p)-1 \quad \text{and} \quad \left(\frac{n\pm 1}{2}, \frac{p+1}{2}\right) - 1 \le B(p)-1.$$

Suppose $n = p_1 p_2 \cdots p_k$ is odd and $k \ge 1$. Then the following propositions hold.

(1) $EL(n) = M(1,k,n)$, (2) $M(1,1,p) = p-2$,

(3) $M(-1,1,p) = 0$, (4) $S(1,p) = p-2$,

(5) $M(\gamma,l,n) = \sum_{\epsilon_1=\pm 1,\cdots,\epsilon_l=\pm 1} \prod_{i=1}^{l} H(\epsilon_i, \gamma\epsilon_1\cdots\epsilon_l, p_i, n)$,

(6) $A(p)-1 < (p-1)/2$ and $B(p)-1 \le (p-1)/2$, (7) $A(p)+B(p)-2 \le p-2$.

(8) If $p-1 \nmid n+1$, $p-1 \nmid n-1$, $p-1 \nmid n+1$ and $p+1 \nmid n-1$, then we can define $A(p) = (p-1)/4$ and $B(p) = (p+1)/4$ and (14.8) will still hold.

(9) If $(p-1)/2 \nmid n-1$ and $(p-1)/2 \nmid n+1$, or if $(p+1)/2 \nmid n-1$ and $(p+1)/2 \nmid n+1$, then we can define $A(p)$ and $B(p)$ in such a way that (14.8) holds and also $A(p)+B(p)-2 < 2(p-2)/3$ holds.

Proof. Proposition (1) is Theorem 13.7. Proposition (2) is Theorem 14.1 with $e=1$. Proposition (3) holds since $((p-\epsilon)/2, (p+\epsilon)/2) = 1$. Proposition (4) follows from Definition 14.7 and (2) and (3). Proposition (5) follows from Definitions 14.5 and 14.6. Propositions (6), (7) and (8) are trivial. For the proof of (9), we consider two cases. First we suppose that $(p-1)/2 \nmid n-1$ and $(p-1)/2 \nmid n+1$. Then $((n-1)/2, (p-1)/2) \le (p-1)/6$ and $((n+1)/2, (p-1)/2) \le (p-1)/6$. Hence we have $((n\pm 1)/2, (p-1)/2) - 1 \le (p-7)/6$. In this case we can define $A(p) = (p-1)/6$ and $B(p) = (p+1)/2$. Then clearly (14.8) holds. Secondly suppose $(p+1)/2 \nmid n-1$ and $(p+1)/2 \nmid n+1$. Then $((n-1)/2, (p+1)/2) \le (p+1)/6$ and $((n+1)/2, (p+1)/2) \le (p+1)/6$.

Hence $((n\pm1)/2,(p+1)/2)-1 \le (p-5)/6$. In this case we can define $A(p) = (p-1)/2$ and $B(p) = (p+1)/6$. Again (14.8) holds. But in either case, we always have $A(p)+B(p)-2 < 2(p-2)/3$. This completes the proof of (9).

Lemma 14.9. $M(\gamma,1,n) = H(1,\gamma,p_1,n) + H(-1,-\gamma,p_1,n)$.

Proof. $M(\gamma,1,n) = \sum_{\epsilon_1=\pm1}\left[\left(\frac{n-\gamma\epsilon_1}{2},\frac{p_1-\epsilon_1}{2}\right)-1\right]$

$$= \left[\left(\frac{n-\gamma}{2},\frac{p_1-1}{2}\right)-1\right]+\left[\left(\frac{n+\gamma}{2},\frac{p_1+1}{2}\right)-1\right] = H(1,\gamma,p_1,n)+H(-1,-\gamma,p_1,n).$$

If $A(p)$ and $B(p)$ satisfy (14.8), then for $\mu = \pm1$ the following inequalities hold.

(14.10) $\quad H(1,\mu,p_i,n) \le A(p_i)-1, \qquad H(-1,\mu,p_i,n) \le B(p_i)-1.$

(14.11) $\quad H(1,\mu,p_i,n) + H(1,-\mu,p_i,n) \le (p_i-3)/2,$

(14.11′) $\quad H(-1,\mu,p_i,n) + H(-1,-\mu,p_i,n) \le (p_i-1)/2,$

Proof. The first two inequalities are equivalent to (14.8). For the proof of (14.11), since $((n-\mu)/2,(n+\mu)/2)=1$, we can apply Lemma 14.4 (i) to get

$$H(1,\mu,p_i,n) + H(1,-\mu,p_i,n) = \left(\frac{n-\mu}{2},\frac{p_i-1}{2}\right)-1+\left(\frac{n+\mu}{2},\frac{p_i-1}{2}\right)-1$$
$$= \left(\frac{n-\mu}{2},\frac{p_i-1}{2}\right)+\left(\frac{n+\mu}{2},\frac{p_i-1}{2}\right)-2 \le \frac{p_i-1}{2}+1-2 = \frac{p_i-3}{2}.$$

The proof of (14.11′) is similar to the proof of (14.11).

Lemma 14.13. Suppose $n = p_1\cdots p_k$ is odd, squarefree and $A(p)$, $B(p)$ are arbitrary functions satisfying (14.8). Then for $\gamma = \pm1$, $0 \le l < k$ and $2 \le k$, we have

$$M(\gamma,l+1,n) \le (A(p_{l+1})-1)M(\gamma,l,n) + (B(p_{l+1})-1)M(-\gamma,l,n).$$

Proof. Using (5) and inequalities (14.10) we have

$$M(\gamma, l+1, n) = \sum_{\epsilon_1=\pm1,\cdots,\epsilon_{l+1}=\pm1} \prod_{i=1}^{l+1} H(\epsilon_i, \gamma\epsilon_1\cdots\epsilon_l\epsilon_{l+1}, p_i, n)$$

$$= \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} H(1, \gamma\epsilon_1\cdots\epsilon_l, p_{l+1}, n) \prod_{i=1}^{l} H(\epsilon_i, \gamma\epsilon_1\cdots\epsilon_l, p_i, n) \qquad (\epsilon_{l+1}=1)$$

$$+ \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} H(-1, -\gamma\epsilon_1\cdots\epsilon_l, p_{l+1}, n) \prod_{i=1}^{l} H(\epsilon_i, -\gamma\epsilon_1\cdots\epsilon_l, p_i, n) \qquad (\epsilon_{l+1}=-1)$$

$$\leq \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} (A(p_{l+1})-1) \prod_{i=1}^{l} H(\epsilon_i, \gamma\epsilon_1\cdots\epsilon_l, p_i, n)$$

$$+ \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} (B(p_{l+1})-1) \prod_{i=1}^{l} H(\epsilon_i, -\gamma\epsilon_1\cdots\epsilon_l, p_i, n)$$

$$= (A(p_{l+1})-1) \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} \prod_{i=1}^{l} H(\epsilon_i, \gamma\epsilon_1\cdots\epsilon_l, p_i, n)$$

$$+ (B(p_{l+1})-1) \sum_{\epsilon_1=\pm1,\cdots,\epsilon_l=\pm1} \prod_{i=1}^{l} H(\epsilon_i, -\gamma\epsilon_1\cdots\epsilon_l, p_i, n)$$

$$= (A(p_{l+1})-1)M(\gamma, l, n) + (B(p_{l+1})-1)M(-\gamma, l, n).$$

This proves the lemma.

Lemma 14.14. Suppose $n = p_1\cdots p_k$ is odd. Then $S(1,n) \leq p_1 - 2$.

Proof. By Lemma 14.9 and inequalities (14.11) and (14.11′), we have

$$S(1,n) = M(1,1,n) + M(-1,1,n)$$

$$= [\, H(1,1,p_1,n) + H(-1,-1,p_1,n) \,] + [\, H(1,-1,p_1,n) + H(-1,1,p_1,n) \,]$$

$$= [\, H(1,1,p_1,n) + H(1,-1,p_1,n) \,] + [\, H(-1,1,p_1,n) + H(-1,-1,p_1,n) \,]$$

$$\leq (p_1-3)/2 + (p_1-1)/2 = p_1 - 2.$$

Lemma 14.15. Suppose n is odd, $n = p_1\cdots p_k$ and $1 \leq l < k$. Suppose also $A(p)$ and $B(p)$ satisfy (14.8). Then

$$S(l+1,n) \leq S(l,n)\,(A(p_{l+1}) + B(p_{l+1}) - 2).$$

Proof. By Definition 14.7 and Lemma 14.13,

$$S(l+1,n) = M(1,l+1,n) + M(-1,l+1,n)$$
$$\leq (A(p_{l+1})-1)M(1,l,n)+(B(p_{l+1})-1)M(-1,l,n)$$
$$+(A(p_{l+1})-1)M(-1,l,n)+(B(p_{l+1})-1)M(1,l,n)$$
$$=(A(p_{l+1})-1)\,[\,M(1,l,n)+M(-1,l,n)\,]+(B(p_{l+1})-1)\,[\,M(1,l,n)+M(-1,l,n)\,]$$
$$=(A(p_{l+1})-1)S(l,n) + (B(p_{l+1})-1)S(l,n) = S(l,n)(A(p_{l+1}) + B(p_{l+1}) - 2).$$

This proves the lemma.

Lemma 14.16. Suppose n odd, $n = p_1 \cdots p_k$ (primes in any order) and $1 \leq l \leq k$.

Then $$S(l,n) < p_1 p_2 \cdots p_l.$$

Proof. By induction on l. If $l = 1$, then the lemma holds by Lemma 14.14,

$S(1,n) \leq p_1 - 2 < p_1$. The induction step follows from Lemma 14.15 and (7),

$$S(l+1,n) \leq S(l,n)(p_{l+1}-2) < S(l,n)p_{l+1} \leq p_1 \cdots p_{l+1}.$$

This proves the lemma.

Lemma 14.17. Suppose n is odd and $n = p_1 \cdots p_k$ (primes in any order) and $2 \leq k$.

Then
$$EL(n) < \left(\frac{p_k - 1}{2}\right) S(k-1,n).$$

Proof. By (1), (6) and Lemma 14.13,

$$EL(n) = M(1,k,n) \leq (A(p_k)-1)M(1,k-1,n) + (B(p_k)-1)M(-1,k-1,n)$$
$$< \left(\frac{p_k-1}{2}\right) M(1,k-1,n) + \left(\frac{p_k-1}{2}\right) M(-1,k-1,n)$$
$$= \left(\frac{p_k-1}{2}\right) [M(1,k-1,n) + M(-1,k-1,n)] = \left(\frac{p_k-1}{2}\right) S(k-1,n).$$

This completes the proof of the lemma.

Lemma 14.18. Suppose $n = p_1 \cdots p_k$, $2 \leq k$, n is odd and n has a special prime divisor $p_i | n$ such that $p_i - 1 \nmid n+1$, $p_i - 1 \nmid n-1$, $p_i + 1 \nmid n+1$ and $p_i + 1 \nmid n-1$. Then

$$EL(n) < \left(\frac{p_i - 3}{4}\right) S(k-1, n).$$

Proof. Without loss of generality we can assume that p_k is a such special prime divisor. Then by (8), (14.8) still holds for $A(p_k) = (p_k - 1)/4$ and $B(p_k) = (p_k + 1)/4$. Hence by (1) and Lemma 14.13

$$\begin{aligned} EL(n) = M(1,k,n) &\leq (A(p_k)-1)M(1,k-1,n) + (B(p_k)-1)M(-1,k-1,n) \\ &\leq \left(\frac{p_k-5}{4}\right) M(1,k-1,n) + \left(\frac{p_k-3}{4}\right) M(-1,k-1,n) \\ &< \left(\frac{p_k-3}{4}\right)(M(1,k-1,n) + M(-1,k-1,n)) = \left(\frac{p_k-3}{4}\right) S(k-1,n). \end{aligned}$$

The lemma is proved.

Recall the definition that n is a Lucas Carmichael means that for all primes p, if $p|n$, then $(p-1)/2 | n \pm 1$ and $(p+1)/2 | n \pm 1$. Hence that n is not a Lucas Carmichael means there exists p such that $p|n$ and either $(p-1)/2 \nmid n-1$ and $(p-1)/2 \nmid n+1$, or $(p+1)/2 \nmid n-1$ and $(p+1)/2 \nmid n+1$. We now prove the following lemma.

Lemma 14.19. Suppose $n = p_1 p_2 \cdots p_k$ is odd, squarefree, $3 \leq k$ and n is not Lucas Carmichael. Then

$$EL(n) < \frac{n - 2p_1 \cdots p_{k-2}}{3}.$$

Proof. Suppose $n = p_1 p_2 \cdots p_k$ where $3 \leq k$. Without loss of generality we can suppose $p_{k-1} = p$ is the prime divisor such that

either $(p-1)/2 \nmid n-1$ and $(p-1)/2 \nmid n+1$

or $(p+1)/2 \nmid n-1$ and $(p+1)/2 \nmid n+1$.

Since $3 \leq k$ and so $1 \leq k-2$, we can apply Lemma 14.15, with $l = k-2$, to get

$$S(k-1,n) \leq [A(p_{k-1}) + B(p_{k-1}) - 2]S(k-2,n).$$

Hence by (9) we can suppose $A(p_{k-1}) + B(p_{k-1}) - 2 < 2(p_{k-1}-2)/3$. Therefore

$$S(k-1,n) \leq \frac{2(p_{k-1}-2)}{3} S(k-2,n).$$

Using Lemma 14.17, since $3 \leq k$ we have

$$EL(n) < \left(\frac{p_k - 1}{2}\right) S(k-1,n) \leq \left(\frac{p_k - 1}{2}\right) \frac{2(p_{k-1}-2)}{3} S(k-2,n).$$

Then by Lemma 14.16, it follows that

$$EL(n) < \left(\frac{p_k - 1}{2}\right) \frac{2(p_{k-1}-2)}{3} p_1 \cdots p_{k-2} < \left(\frac{p_k p_{k-1} - 2}{3}\right) p_1 \cdots p_{k-2} = \frac{n - 2p_1 \cdots p_{k-2}}{3}.$$

This proves the lemma.

Lemma 14.20. Suppose $n = p_1 \cdots p_k$, $2 \leq k$, n is odd and squarefree. Then

$$EL(n) < \frac{n - p_1 \cdots p_{k-1}}{2}.$$

Proof. By Lemmas 14.16 and 14.17 with $l = k-1$, we have

$$EL(n) \leq \left(\frac{p_k - 1}{2}\right) S(k-1,n) < \left(\frac{p_k - 1}{2}\right) p_1 p_2 \cdots p_{k-1} = \frac{n - p_1 \cdots p_{k-1}}{2}.$$

This proves the lemma.

Lemma 14.21. Suppose $n = p_1 p_2 \cdots p_k$, $2 \leq k$ and n has a special prime divisor p_i, $1 \leq i \leq k$, such that $p_i - 1 \nmid n+1$, $p_i - 1 \nmid n-1$, $p_i + 1 \nmid n+1$ and $p_i - 1 \nmid n-1$. Then

$$EL(n) < \frac{n - 3p_1 p_2 \cdots p_{k-1}}{4}.$$

Proof. Without loss of generality we can assume that p_k is the special prime divisor of n. Since $2 \leq k$ we can use Lemma 14.16 with $l = k-1$ and Lemma 14.18 to get

$$EL(n) \leq \left(\frac{p_k - 3}{4}\right) S(k-1,n) < \left(\frac{p_k - 3}{4}\right) p_1 p_2 \cdots p_{k-1} = \frac{n - 3p_1 p_2 \cdots p_{k-1}}{4}.$$

This proves the lemma.

Lemma 14.22. Suppose p and q are odd primes and $p < q$. Then

(i) $q-1 \nmid pq-1$; (ii) $q+1 \nmid pq-1$;

(iii) $q+1 \nmid pq+1$; (iv) $q-1 \mid pq+1 \iff p+2=q$.

Proof. (i). $pq-1 = p(q-1)+p-1 \equiv p-1 \not\equiv 0 \pmod{q-1}$.

(ii). $pq-1 = p(q+1)-p-1 \equiv -p-1 = -(p+1) \not\equiv 0 \pmod{q+1}$.

(iii). $pq+1 = p(q+1)-p+1 \equiv -p+1 = -(p-1) \not\equiv 0 \pmod{q+1}$.

(iv). $pq+1 = p(q-1)+p+1 \equiv p+1 \pmod{q-1}$. Hence

$$pq+1 \equiv 0 \pmod{q-1} \iff p+1 = q-1 \iff p+2 = q.$$

Lemma 14.23. Suppose p, q are odd primes and $p+2=q$. Then

$$EL(pq)/(pq-2) < 1/4.$$

Proof. Suppose $q = p+2$. Hence $p+1 = q-1$ and $p+3 = q+1$.

Since $$\frac{pq-1}{2} = \frac{p(p+2)-1}{2} = \frac{p^2+2p-1}{2} = \frac{(p+1)^2}{2} - 1,$$

we have $$\left(\frac{pq-1}{2}, \frac{p+1}{2}\right) = \left(\frac{pq-1}{2}, \frac{q-1}{2}\right) = 1.$$

Since $$\frac{pq-1}{2} = \frac{p(p+2)-1}{2} = \frac{p^2+2p-3+2}{2} = \frac{(p-1)(p+3)}{2} + 1,$$

we have $$\left(\frac{pq-1}{2}, \frac{p-1}{2}\right) = 1 \text{ and } \left(\frac{pq-1}{2}, \frac{p+3}{2}\right) = \left(\frac{pq-1}{2}, \frac{q+1}{2}\right) = 1.$$

Since $$\frac{pq+1}{2} = \frac{p(p+2)+1}{2} = \frac{p^2+2p-3+4}{2} = \frac{(p-1)(p+3)}{2} + 2,$$

we have $$\left(\frac{pq+1}{2}, \frac{p-1}{2}\right) \le 2 \text{ and } \left(\frac{pq+1}{2}, \frac{p+3}{2}\right) = \left(\frac{pq+1}{2}, \frac{q+1}{2}\right) \le 2.$$

Therefore

$$\begin{aligned} EL(n) &= \left[\left(\frac{pq-1}{2}, \frac{p-1}{2}\right) - 1\right]\left[\left(\frac{pq-1}{2}, \frac{q-1}{2}\right) - 1\right] \\ &+ \left[\left(\frac{pq-1}{2}, \frac{p+1}{2}\right) - 1\right]\left[\left(\frac{pq-1}{2}, \frac{q+1}{2}\right) - 1\right] \\ &+ \left[\left(\frac{pq+1}{2}, \frac{p-1}{2}\right) - 1\right]\left[\left(\frac{pq+1}{2}, \frac{q+1}{2}\right) - 1\right] \end{aligned}$$

$$
\begin{aligned}
&+ \left[\left(\frac{pq+1}{2}, \frac{p+1}{2}\right) - 1\right]\left[\left(\frac{pq+1}{2}, \frac{q-1}{2}\right) - 1\right] \\
&\leq (1-1)(1-1)+(1-1)(1-1)+(2-1)(2-1)+\left(\frac{p+1}{2}-1\right)\left(\frac{q-1}{2}-1\right) \\
&= 0+0+1+\frac{p-1}{2}\cdot\frac{q-3}{2} = \frac{pq-q-3p+7}{4} < \frac{pq-2}{4}
\end{aligned}
$$

The last inequality holds since $9 < q + 3p$. This completes the proof.

Theorem 14.24. Suppose $n = p_1 p_2 \cdots p_k$, $2 \leq k$ and n has a special prime divisor $p|n$ such that $p-1 \nmid n+1$, $p-1 \nmid n-1$, $p+1 \nmid n+1$ and $p+1 \nmid n-1$. Then

$$\frac{EL(n)}{n-2} < \frac{1}{4}.$$

Proof. This is by Lemma 14.21, $EL(n) < (n - 3p_1 \cdots p_{k-1})/4 < (n-2)/4$.

Theorem 14.25. Suppose $n = pq$ and p, q are distinct odd primes. Then

$$\frac{EL(n)}{n-2} < \frac{1}{4}.$$

Proof. Suppose $n = pq$ and $p < q$. Consider two cases. Case 1. $q = p+2$. The theorem then follows from Lemma 14.23. Case 2. $q \neq p+2$. Then $q > p+2$. Then by Lemma 14.22 q is a special prime divisor of n, i.e. $q-1 \nmid n+1$, $q-1 \nmid n-1$, $q+1 \nmid n+1$ and $q+1 \nmid n-1$. Hence by Theorem 14.24, $EL(n)/(n-2) < 1/4$. This completes the proof.

Theorem 14.26. If $n > 1$, n is odd and n is not squarefree, then

$$\frac{EL(n)}{n-2} \leq \frac{1}{3}.$$

Proof. Suppose n is odd and not squarefree. Then there exists an odd prime p such that $p^2 \mid n$. Hence by Lemma 14.3, we have $EL(n) \leq (n-2)/p \leq (n-2)/3$ so that $EL(n)/(n-2) \leq 1/3$. This proves the theorem.

Theorem 14.27. If $n > 1$, $(n, 6) = 1$ and n is not squarefree, then

$$\frac{EL(n)}{n-2} \leq \frac{1}{5}.$$

Proof. Suppose $(n, 6) = 1$ and n is not squarefree. Then there exists an odd prime p, $p \geq 5$ such that $p^2 | n$. Hence by Lemma 14.3, we have $EL(n) \leq (n-2)/p \leq (n-2)/5$ so that $EL(n)/(n-2) \leq 1/5$. This proves the theorem.

Theorem 14.28. If $n > 1$, n is odd, composite and n is not Lucas Carmichael, then

$$\frac{EL(n)}{n-2} < \frac{1}{3}. \tag{14.28}$$

Proof. By Theorem 14.26, (14.28) holds for the case n is not squarefree. Hence we can suppose n is squarefree. If n is a product of two primes, then (14.28) holds by Theorem 14.25. And (14.28) also holds for the case that n has at least 3 prime divisors. This is from Lemma 14.19. This proves the theorem for all cases.

Theorem 14.29. Suppose $n > 1$, n is odd and composite. Then

$$\frac{EL(n)}{n-2} < \frac{1}{2}.$$

Proof. If n is not squarefree, then by Theorem 14.26 $EL(n)/(n-2) \leq 1/3$. Hence $EL(n)/(n-2) < 1/2$. If n is squarefree, say $n = p_1 \cdots p_k$, then $2 \leq k$ so by Lemma 14.20 $EL(n) < (n - p_1 \cdots p_{k-1})/2 < (n-2)/2$. Hence $EL(n)/(n-2) < 1/2$. The theorem is proved.

The number $n = 1,930,499$ with $EL(n)/(n-2) \approx 0.2645$ shows that the hypotheses in Theorems 14.24 and 14.25 are necessary. The example $n = 582,920,080,863,121$ (strong Lucas Carmichael $+$) with $EL(n)/(n-2) \approx 0.4289$ shows that $1/4$ or even $1/3$ is not an upper bound of $EL(n)/(n-2)$ for all composite

integers n. Also the number $n = 39203 = 197{\cdot}199$ with $EL(n)/(n-2) \approx 0.245$ shows that only a small improvement is possible in Theorem 14.25.

From Corollary 7.23, we know that for any odd integer $n > 1$, n is $elpsp(a)$ if and only if n is $elpsp(n-a)$. Hence a consequence of Theorem 14.29 is

Theorem 14.30. Suppose $n > 1$, $(n, 6) = 1$ and $i = \pm 1$ and is such that $4 \mid n - i$. Then n is prime if and only if

$$\forall a \, [\, 3 \leq a \leq (n-i)/4 \text{ and } (n, a^2-4) = 1 \;\Rightarrow\; n \text{ is } elpsp(a) \,].$$

Conclusion

In this thesis we have studied properties of Diophantine equations and Lucas sequences, especially the sequences of solutions of the Pell equation

$$x^2 - (a^2 - 4)y^2 = 4.$$

By studying these sequences, we believe we have obtained some interesting results. Some of these results may have applications to the study of prime numbers, to primality testing and to Diophantine representation of r.e. sets such as the set of primes, also to exponential Diophantine representation of r.e. sets.

This whole subject is a very rich one. Below we list some unsolved problems and some conjectures which we think are worth further study.

(1) In §11 we defined some types of Lucas Carmichaels. (Definitions 11.1 - 11.8.) A natural problem is: for each type of Lucas Carmichael, are there infinitely many of them?

Since all odd primes are two sided strong Lucas Carmichaels, the question, for example for the two sided strong Lucas Carmichael, should be: are there infinitely many composite ones? Methods of Alford, Granville and Pomerance [1] probably extended to include these kinds of numbers.

(2) Is the following statement true?

$$\forall a\,[n \text{ is an } elpsp(a) \Rightarrow n \text{ is a } tpsp(a)] \Rightarrow n \text{ is a prime power.}$$

we don't know but we believe it to be true. In Theorem 9.34 we proved the converse. See also Theorem 9.33 where squarefree has been characterized in this way.

(3) Is the following statement equivalent to the primality of n?

$$\forall a\,[n \text{ is a } tpsp(a) \Leftrightarrow n \text{ is an } elpsp(a)]\,.$$

(4) Does it hold that n is an *slxpsp*(a) implies n is a *tpsp*(a) and hence implies n is a *sltpsp*(a)? We don't know it now but we believe it to be true.

(5) Let $SLT(n)$ denote the number of incongruent bases a mod n to which n is a *sltpsp*(a). We conjecture the following inequality holds if $n > 25$ and n is an odd composite number:

$$SLT(n) < \frac{n-2}{8}.$$

(6) Let $SLX(n)$ denote the number of incongruent bases a mod n to which n is a *slxpsp*(a). We conjecture the following inequality holds if $n > 25$ and n is an odd composite number:

$$SLX(n) < \frac{n-2}{8}.$$

Bibliography

[1] W.R. Alford, Andrew Granville and Carl Pomerance, *There are infinitly many Carmichael numbers*, Annals of Math, (to appear).

[2] R. Baillie and S.S. Wagstaff Jr., *Lucas pseudoprimes*, Math. Comp. vol.35 (1980), 1391 - 1417.

[3] C. Baxa, *A note on Diophantine representations*, Amer. Math. Monthly, 100 (1993), 138 - 143

[4] B.D. Beach and H.C. Williams, *A numerical investigation of the Diophantine equations* $x^2 - dy^2 = -1$, Proc. of the Third Southeastern Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Florida, (1972), 37 - 68.

[5] J. Brillhart, D.H. Lehmer and J.L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Mathematics of Computation, 29 (1975), 620 - 647.

[6] P. Bundschuh and F.J. Shiue, *A generalization of a paper by D.D. Wall*, Atti. Accad. Naz. Lincei, Rend. Cl. Sci., Fis. Mat. Nat., Ser. II, 56 (1974), 135 - 144.

[7] R.D. Carmichael, *On the composite numbers p which satisfy the Fermat congruence,* $a^{p-1} \equiv 1 \pmod{p}$, Amer. Math. Monthly, 19 (1912), 22 - 27.

[8] R.D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Math (2) 15 (1913 - 14), 30 - 70.

[9] G.V. Chudnovskii, *Diophantine predicates* (Russian), Uspehi Matematicheskikh Nauk, vol. 25 (1970), 185 - 186.

[10] M. Davis, *An explicit diophantine definition of the exponential function*, Comm. Pure and Applied Math., vol. 24 (1971), 137 - 145.

[11] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly, vol. 80 (1973), 233 - 269. MR 47, #6465.

[12] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Annals of Math. Series 2, vol. 74 (1961), 425 - 436. MR 24, #A3061.

[13] M.J. Delon, *Pell's equation and Pell number triples*, Fibonacci Quarterly, 14 (1976), 456 - 460. RNT 54, #7365.

[14] D. Flath and S. Wagon, *How to pick out the integers in the rationals: an application of number theory to logic*, Amer. Math. Monthly, 98 (1991), 812 - 823.

[15] K. Hensel, Zahlentheorie, Göshen, Berlin - Leipzig, 1913.

[16] Hua, Liu - Keng, *On the least solution to Pell's equation*, Bull. Amer. Math. Soc., vol. 48 (1942), 731 - 735.

[17] J.P. Jones, *Diophantine representation of Mersenne and Fermat primes*, Acta Arithmetica vol. 35 (1979), 209 - 221.

[18] J.P. Jones, *Universal diophantine equation*, Jour. Symbolic Logic, vol. 47 (1982), 549 - 571.

[19] J.P. Jones and Y.V. Matijasevič, *Exponential diophantine representation of recursively enumerable sets*, Proceedings of the Herbrand Symposium, Logic Colloquium '81, Studies in Logic and the Foundations of Mathematics, vol. 107, North - Holland, Amsterdam, (1982), 159 - 177. MR 85i, #03138.

[20] J.P. Jones and Y.V. Matijasevič, *Register Machine proof of the theorem on exponential Diophantine representation of enumerable sets*, Jour. of Symbolic Logic 49 (1984), 818 - 819.

[21] J.P. Jones and Y.V. Matijasevič, *Proof of recursive unsolvability of Hilbert's tenth problem*, Amer. Math. Monthly, 98 (1991), 689 - 709.

[22] P. Kiss, *A Diophantine approximative property of the second order linear recurrences*, Period. Math. 11 (1980), 281 - 287.

[23] D.E. Knuth, *The Art of Computer Programming* Vol. II, Seminumerical Algorithms, 2nd ed. Addison - Wesley, (1981), 688pp.

[24] Moshe Koppel, *Some decidable Diophantine problems: positive solution to a problem of Davis, Matijasevič and Robinson*, Proc. Amer. Math. Sco., 77 (1979), 319 - 323. MR 81a: 10069.

[25] J.C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $x^2 - dy^2 = -1$, Trans. Amer. Math. Soc. vol. 260 (1980), 485 - 508.

[26] D.H. Lehmer, *On the multiple solutions of the Pell equation*, Annals of Math 30 (1928), 66 - 72.

[27] D.H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math 31 (1930), 419 - 448.

[28] D.H. Lehmer, *On Lucas' test for the primality of Mersenne's numbers*, Jour. London Math. Sco. vol. 10 (1935), 162 - 165.

[29] D.H. Lehmer, *Computer technology applied to the theory of numbers*, Studies in Number Theory (W.J. LeVeque, editor), MAA Studies in Mathematics, Mathematical Association of America, Buffalo, New York (Prentice - Hall, Englewood Cliffs, New Jersey), vol. 6, (1969), 117 - 151.

[30] E. Lieuwens, Fermat Pseudo-Primes, Ph.D. Thesis, Delft, Netherlands, (1971).

[31] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier*, Bulletin de la Société Mathématique de France, vol. 6 (1877 - 78), 49 - 54.

[32] E. Lucas, *Theorie des fonctions numeriques simplement periodiques*, American Journal of Mathematics, vol. 1 (1878), 184 - 240, 289 - 321. English translation: The Fibonacci Association, Santa Clara University, CA. 95053, (1969).

[33] Y.V. Matijasevič and J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arithmetica, vol. 27 (1975), 521 - 553.

[34] Y.V. Matijasevič, *A class of primality criteria formulated in terms of binomial coefficients*, Zapiski Naučhnhh Seminarov Leningradskogo Otdelennija Matematičeskogo Instituta im. V.A. Steklov Akademii Nauk SSSR vol. 67 (1977), pp. 167 - 183. Engl. transl. Jour. of Sov. Math. 16 (1981), 874 - 884.

[35] Y.V. Matijasevič, *Algorithmic unsolvability of exponential Diophantine equations in three unknowns*, Studies in the Theory of Algorithms and Mathematical Logic, (A.A. Markov nd V.I. Homič, eds) "Nauka" Moscow, 1979, pp. 69 - 78. English transl., Selecta Math. Sovietica 3 (1983/84), 223 - 232.

[36] W.L. McDaniel, *The G.C.D. in Lucas sequences and Lehmer number sequences*, Fibonacci Quarterly 29 (1991), 24 -29.

[37] G.L. Miller, *Riemann's hypothesis and tests for primality*, Jour. Computer & System Sicences 13 (1976), 300 - 317.

[38] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science 11 (1980), 97 - 108.

[39] T. Pepin, *Sur la formule* $2^{2^n}+1$, C.R. Acad. Sci. Paris vol. 85 (1877), pp.329–331.

[40] A. Pethö, *Perfect powers in second order linear recurrences*, Jour. of Number Theory, 15 (1982), 5 - 13.

[41] R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, (to appear).

[42] M.O. Rabin, *Probabilistic algorithm for primality testing*, Jour. of Number Theory 12 (1980), 128 - 138.

[43] J. Robinson, *Existential definability in Arithmetic*, Trans. Amer. Mathematical Society, vol. 72 (1952), 437 - 449. MR 14, #4.

[44] J. Robinson, *Diophantine decision problems*, Studies in Number Theory (W.J. LeVeque, editor), MAA Studies in Mathematics vol. 6, (1969), 76 - 116.

[45] J.B. Rosser, *The n^{th} prime is greater than nlogn*, Proc. of the London Math. Soc. (Series 2), 45 (1939), 21 - 44.

[46] A. Rotkiewicz, *On the pseudoprimes with respect to Lucas sequences*, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys., 21 (1973), 793 - 797.

[47] A. Rotkiewicz, *Euler Lehmer pseudoprimes in arithmetic progressions*, Math. Comp. 39 (1982), 239 - 247.

[48] S. Smorynski, *Notes on Hilbert's Tenth Problem*, Vol. 1, An Introduction to Unsolvability, Dept. Mathematics, Univ. of Illinois at Chicago Circle, parts I and II (1972), x+133 pp.

[49] R. Solovay and V. Strassen, *A fast Monte Carlo test for primality*, S.I.A.M. Jour. Computing, 6 (1977), 84 - 85. Erratum 7 (1978), p. 118.

[50] A.E. Western, *On Lucas's and Pepin's tests for the primeness of Mersenne numbers*, Jour. London Math. Sco. vol. 7 (1932), 130 - 137.

[51] H.C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bulletin, 20 (1977), 133 -143.

[52] H.C. Williams, *Primality testing on a computer*, ARS Combinatoria, vol. 5 (1978), 127 - 185.

[53] H.C. Williams, *A $p+1$ method of factoring*, Math. Comp. 39 (1982), 225 - 234.