Algorithmic Number Theory

Lattices, Number Fields, Curves and Cryptography

J. P. Buhler
P. Stevenhagen
Editors

MATHEMATICAL SCIENCES
RESEARCH INSTITUTE
PUBLICATIONS

44

MSRI

For centuries, number theorists have refined their intuition by computing examples. The advent of computers and (especially) sophisticated algorithms has gradually led to the emergence of algorithmic number theory as a distinct field. This young discipline has been shaped by strong connections to computer science, cryptography, and other parts of mathematics. One of its charms is that mathematical ideas often lead to better algorithms. Another striking feature is that the algorithmic worldview has led to fascinating new mathematical ideas and questions.

This volume contains twenty survey articles on topics in algorithmic number theory, written by leading experts in the field. The first two are introductory, aiming to entice the reader into pursuing the subject more deeply. The next eight cover core areas of the field: factoring, primality, smooth numbers, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles survey specific topics, often with a distinctive perspective, including cryptography, Arakelov class groups, computational class field theory, zeta functions over finite fields, arithmetic geometry, and modular forms.

Mathematical Sciences Research Institute
Publications

44

Algorithmic Number Theory

Mathematical Sciences Research Institute Publications

1 Freed/Uhlenbeck: *Instantons and Four-Manifolds*, second edition
2 Chern (ed.): *Seminar on Nonlinear Partial Differential Equations*
3 Lepowsky/Mandelstam/Singer (eds.): *Vertex Operators in Mathematics and Physics*
4 Kac (ed.): *Infinite Dimensional Groups with Applications*
5 Blackadar: *K-Theory for Operator Algebras*, second edition
6 Moore (ed.): *Group Representations, Ergodic Theory, Operator Algebras, and Mathematical Physics*
7 Chorin/Majda (eds.): *Wave Motion: Theory, Modelling, and Computation*
8 Gersten (ed.): *Essays in Group Theory*
9 Moore/Schochet: *Global Analysis on Foliated Spaces*, second edition
10–11 Drasin/Earle/Gehring/Kra/Marden (eds.): *Holomorphic Functions and Moduli*
12–13 Ni/Peletier/Serrin (eds.): *Nonlinear Diffusion Equations and Their Equilibrium States*
14 Goodman/de la Harpe/Jones: *Coxeter Graphs and Towers of Algebras*
15 Hochster/Huneke/Sally (eds.): *Commutative Algebra*
16 Ihara/Ribet/Serre (eds.): *Galois Groups over* $\mathbb{Q}$
17 Concus/Finn/Hoffman (eds.): *Geometric Analysis and Computer Graphics*
18 Bryant/Chern/Gardner/Goldschmidt/Griffiths: *Exterior Differential Systems*
19 Alperin (ed.): *Arboreal Group Theory*
20 Dazord/Weinstein (eds.): *Symplectic Geometry, Groupoids, and Integrable Systems*
21 Moschovakis (ed.): *Logic from Computer Science*
22 Ratiu (ed.): *The Geometry of Hamiltonian Systems*
23 Baumslag/Miller (eds.): *Algorithms and Classification in Combinatorial Group Theory*
24 Montgomery/Small (eds.): *Noncommutative Rings*
25 Akbulut/King: *Topology of Real Algebraic Sets*
26 Judah/Just/Woodin (eds.): *Set Theory of the Continuum*
27 Carlsson/Cohen/Hsiang/Jones (eds.): *Algebraic Topology and Its Applications*
28 Clemens/Kollár (eds.): *Current Topics in Complex Algebraic Geometry*
29 Nowakowski (ed.): *Games of No Chance*
30 Grove/Petersen (eds.): *Comparison Geometry*
31 Levy (ed.): *Flavors of Geometry*
32 Cecil/Chern (eds.): *Tight and Taut Submanifolds*
33 Axler/McCarthy/Sarason (eds.): *Holomorphic Spaces*
34 Ball/Milman (eds.): *Convex Geometric Analysis*
35 Levy (ed.): *The Eightfold Way*
36 Gavosto/Krantz/McCallum (eds.): *Contemporary Issues in Mathematics Education*
37 Schneider/Siu (eds.): *Several Complex Variables*
38 Billera/Björner/Green/Simion/Stanley (eds.): *New Perspectives in Geometric Combinatorics*
39 Haskell/Pillay/Steinhorn (eds.): *Model Theory, Algebra, and Geometry*
40 Bleher/Its (eds.): *Random Matrix Models and Their Applications*
41 Schneps (ed.): *Galois Groups and Fundamental Groups*
42 Nowakowski (ed.): *More Games of No Chance*
43 Montgomery/Schneider (eds.): *New Directions in Hopf Algebras*
44 Buhler/Stevenhagen (eds.): *Algorithmic Number Theory*
45 Jensen/Ledet/Yui: *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*
46 Rockmore/Healy (eds.): *Modern Signal Processing*
47 Uhlmann (ed.): *Inside Out: Inverse Problems and Applications*
48 Gross/Kotiuga: *Electromagnetic Theory and Computation: A Topological Approach*
49 Darmon/Zhang (eds.): *Heegner Points and Rankin L-Series*
50 Bao/Bryant/Chern/Shen (eds.): *A Sampler of Riemann–Finsler Geometry*
51 Avramov/Green/Huneke/Smith/Sturmfels (eds.): *Trends in Commutative Algebra*
52 Goodman/Pach/Welzl (eds.): *Combinatorial and Computational Geometry*
53 Schoenfeld (ed.): *Assessing Mathematical Proficiency*
54 Hasselblatt (ed.): *Dynamics, Ergodic Theory, and Geometry*
55 Pinsky/Birnir (eds.): *Probability, Geometry and Integrable Systems*

Volumes 1–4, 6–8 and 10–27 are published by Springer-Verlag

Algorithmic Number Theory:
Lattices, Number Fields, Curves and Cryptography

Edited by

J. P. Buhler
P. Stevenhagen

CAMBRIDGE
UNIVERSITY PRESS

J. P. Buhler
CCR and Reed College
4320 Westerra Ct., San Diego, CA 92121
jpb@reed.edu

P. Stevenhagen
Mathematisch Instituut, Universiteit Leiden
Postbus 9512, 2300 RA Leiden, The Netherlands
psh@math.leidenuniv.nl

Silvio Levy (*Series Editor*)
Mathematical Sciences Research Institute
17 Gauss Way, Berkeley, CA 94720
levy@msri.org

The Mathematical Sciences Research Institute wishes to acknowledge support by the National Science Foundation and the *Pacific Journal of Mathematics* for the publication of this series.

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521808545

© Mathematical Sciences Research Institute 2008

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2008

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data

ISBN 978-0-521-80854-5 hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet Web sites referred to in this publication and does not guarantee that any content on such Web sites is, or will remain, accurate or appropriate.

Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Contents

Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Preface

Our subject arises out of two roots of mathematical thought: fascination with properties of whole numbers and the urge to compute. Number theory and computer science flowered vividly during the last quarter of the twentieth century, and the synergy at their intersection was striking. Algorithmic number theory emerged as an exciting field in its own right, containing deep insights, and having surprising applications.

In the fall of 2000 the Mathematical Sciences Research Institute Berkeley hosted a one-semester program on algorithmic number theory. Its opening workshop, cosponsored by the Clay Mathematics Institute, featured many foundational and survey talks. During the meeting, it was noted that there was a dearth of sources for newcomers to the field. After the conference, some of the speakers agreed to write articles based on their talks, and we were drafted to edit the volume.

A few authors turned in drafts promptly, some retaining the tutorial focus and tone of the original talks, while others were full-blown tutorials or surveys. Many authors (including the editors) dallied. Additional articles were solicited, to provide more coherence and to incorporate newer results that couldn't be ignored (most notably, the polynomial-time primality algorithm due to Manindra Agrawal, Neeraj Kayal, and Nitin Saxena). This led to complications that might have been expected for a volume with 20 substantial articles, 15 authors, and 650 pages. These have finally run their course, and we are delighted that the volume is ready to see the light of day.

We do apologize to the authors who responded promptly, and can only hope that they will be compensated by the greater breadth and interest of the volume in which their contributions appear.

The articles in the volume can be loosely categorized as follows. The first two articles are introductory, and are more elementary than their successors — they attempt to entice the reader into pursuing the ideas more deeply. The next eight articles provide surveys of central topics, including smooth numbers, factoring, primality testing, lattices, elliptic curves, algebraic number theory, and fast arithmetic algorithms. The remaining ten articles study specific topics more deeply,

including cryptography, computational algebraic number theory, modular forms, and arithmetic geometry.

Although the articles in this volume are surveys in the broadest sense, the word should not be taken to mean an encyclopedic treatment that captures current conventional wisdom. We prefer the term overviews, and the articles have a distinctive and in some cases even nonstandard perspective.

It remains our pleasant duty to thank a number of institutions and people. Most obviously, the authors have produced many fascinating pages, sure to inspire others to pursue the subject. We thank the Clay Institute and MSRI for their generous funding for the workshop that provided the initial spark for this volume. We thank Cambridge University Press and MSRI for their support and patience during the production of this volume, and we especially thank Silvio Levy for his extensive efforts on this volume. John Voight took notes (by typing nearly real-time TEX into his laptop) at most of the talks at workshop, and these were valuable to some of the authors.

Finally, Hendrik Lenstra has long been a source of pervasive and brilliant inspiration to the entire field of algorithmic number theory, and this volume is no exception: in addition to two distinctive articles, he has provided much-appreciated advice over the years to the editors and to virtually all of the other authors.

Joe Buhler
Peter Stevenhagen
San Diego, May 2008

Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Solving the Pell equation

HENDRIK W. LENSTRA, JR.

ABSTRACT. We illustrate recent developments in computational number theory by studying their implications for solving the Pell equation. We shall see that, if the solutions to the Pell equation are properly represented, the traditional continued fraction method for solving the equation can be significantly accelerated. The most promising method depends on the use of smooth numbers. As with many algorithms depending on smooth numbers, its run time can presently only conjecturally be established; giving a rigorous analysis is one of the many open problems surrounding the Pell equation.

1. Pell's equation

The *Pell equation* is the equation

$$x^2 = dy^2 + 1,$$

to be solved in positive integers x, y for a given nonzero integer d. For example, for $d = 5$ one can take $x = 9$, $y = 4$. We shall always assume that d is positive but not a square, since otherwise there are clearly no solutions.

The English mathematician John Pell (1611–1685) has nothing to do with the equation. Euler (1707–1783) mistakenly attributed to Pell a solution method that had in fact been found by another English mathematician, William Brouncker (1620–1684), in response to a challenge by Fermat (1601–1665); but attempts to change the terminology introduced by Euler have always proved futile.

Pell's equation has an extraordinarily rich history, to which Weil [1984] is the best guide; see also [Dickson 1920, Chapter XII; Konen 1901; Whitford 1912]. Brouncker's method is in substance identical to a method that was known to Indian mathematicians at least six centuries earlier. As we shall see, the equation

This paper appeared in slightly different form in *Notices Amer. Math. Soc.* **49** (2002), 182–192, with the permission of MSRI and the editors of the present volume.

also occurred in Greek mathematics, but no convincing evidence that the Greeks could solve the equation has ever emerged.

A particularly lucid exposition of the "Indian" or "English" method of solving the Pell equation is found in Euler's *Algebra* [Euler 1770, Abschnitt 2, Capitel 7]. Modern textbooks usually give a formulation in terms of continued fractions, which is also due to Euler (see for example [Niven et al. 1991, Chapter 7]). Euler, as well as his Indian and English predecessors, appears to take it for granted that the method always produces a solution. That is true, but it is not obvious — all that is obvious is that *if* there is a solution, the method will find one. Fermat was probably in possession of a proof that there is a solution for every d (see [Weil 1984, Chapter II, § XIII]), and the first to publish such a proof was Lagrange (1736–1813) [1773].

One may rewrite Pell's equation as

$$(x + y\sqrt{d}) \cdot (x - y\sqrt{d}) = 1,$$

so that finding a solution comes down to finding a nontrivial unit of the ring $\mathbb{Z}[\sqrt{d}]$ of norm 1; here the norm $\mathbb{Z}[\sqrt{d}]^* \to \mathbb{Z}^* = \{\pm 1\}$ between unit groups multiplies each unit by its conjugate, and the units ± 1 of $\mathbb{Z}[\sqrt{d}]$ are considered trivial. This reformulation implies that once one knows a solution to Pell's equation, one can find infinitely many. More precisely, if the solutions are ordered by magnitude, then the n-th solution x_n, y_n can be expressed in terms of the first one, x_1, y_1, by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Accordingly, the first solution x_1, y_1 is called the *fundamental solution* to the Pell equation, and *solving* the Pell equation means finding x_1, y_1 for given d. By abuse of language, we shall also refer to $x + y\sqrt{d}$ instead of the pair x, y as a solution to Pell's equation and call $x_1 + y_1\sqrt{d}$ the fundamental solution.

One may view the solvability of Pell's equation as a special case of *Dirichlet's unit theorem* from algebraic number theory, which describes the structure of the group of units of a general ring of algebraic integers [Stevenhagen 2008a]; for the ring $\mathbb{Z}[\sqrt{d}]$, it is the product of $\{\pm 1\}$ and an infinite cyclic group.

As an example, consider $d = 14$. One has

$$\sqrt{14} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \sqrt{14}}}}},$$

so the continued fraction expansion of $3+\sqrt{14}$ is purely periodic with period length 4. Truncating the expansion at the end of the first period, one finds that the fraction

$$3+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\cfrac{1}{1}}}}=\frac{15}{4}$$

is a fair approximation to $\sqrt{14}$. The numerator and denominator of this fraction yield the fundamental solution $x_1=15$, $y_1=4$; indeed one has $15^2=14\cdot4^2+1$. Furthermore, one computes $(15+4\sqrt{14})^2=449+120\sqrt{14}$, so $x_2=449$, $y_2=120$; and so on. One finds:

n	x_n	y_n
1	15	4
2	449	120
3	13455	3596
4	403201	107760
5	12082575	3229204
6	362074049	96768360

The shape of the table reflects the exponential growth of x_n and y_n with n.

For general d, the continued fraction expansion of $[\sqrt{d}]+\sqrt{d}$ is again purely periodic, and the period displays a symmetry similar to the one visible for $d=14$. If the period length is even, one proceeds as above; if the period length is odd, one truncates at the end of the *second* period [Buhler and Wagon 2008].

2. The cattle problem

An interesting example of the Pell equation, both from a computational and from a historical perspective, is furnished by the *cattle problem* of Archimedes (287–212 B.C.). A manuscript containing this problem was discovered by Lessing (1729–1781) in the Wolffenbüttel library, and published by him in 1773 (see [Lessing 1773; Heiberg 1913, pp. 528–534]). It is now generally credited to Archimedes [Fraser 1972; Weil 1984]. In twenty-two Greek elegiac distichs, the problem asks for the number of white, black, dappled, and brown bulls and cows belonging to the Sun god, subject to several arithmetical restrictions. A version in English heroic couplets, published in [Archimedes 1999], is shown on page 4. In modern mathematical notation the problem is no less elegant. Writing x, y, z, t for the numbers of white, black, dappled, and brown bulls,

PROBLEM

that Archimedes conceived in verse
and posed to the specialists at Alexandria
in a letter to Eratosthenes of Cyrene.

The Sun god's cattle, friend, apply thy care
to count their number, hast thou wisdom's share.
They grazed of old on the Thrinacian floor
of Sic'ly's island, herded into four,
colour by colour: one herd white as cream,
the next in coats glowing with ebon gleam,
brown-skinned the third, and stained with spots the last.
Each herd saw bulls in power unsurpassed,
in ratios these: count half the ebon-hued,
add one third more, then all the brown include;
thus, friend, canst thou the white bulls' number tell.
The ebon did the brown exceed as well,
now by a fourth and fifth part of the stained.
To know the spotted — all bulls that remained —
reckon again the brown bulls, and unite
these with a sixth and seventh of the white.
Among the cows, the tale of silver-haired
was, when with bulls and cows of black compared,
exactly one in three plus one in four.
The black cows counted one in four once more,
plus now a fifth, of the bespeckled breed
when, bulls withal, they wandered out to feed.
The speckled cows tallied a fifth and sixth
of all the brown-haired, males and females mixed.
Lastly, the brown cows numbered half a third
and one in seven of the silver herd.
Tell'st thou unfailingly how many head
the Sun possessed, o friend, both bulls well-fed
and cows of ev'ry colour — no-one will
deny that thou hast numbers' art and skill,
though not yet dost thou rank among the wise.
But come! also the foll'wing recognise.
Whene'er the Sun god's white bulls joined the black,
their multitude would gather in a pack
of equal length and breadth, and squarely throng
Thrinacia's territory broad and long.
But when the brown bulls mingled with the flecked,
in rows growing from one would they collect,
forming a perfect triangle, with ne'er
a diff'rent-coloured bull, and none to spare.
Friend, canst thou analyse this in thy mind,
and of these masses all the measures find,
go forth in glory! be assured all deem
thy wisdom in this discipline supreme!

respectively, one reads in lines 8–16 the restrictions

$$x = (\tfrac{1}{2} + \tfrac{1}{3})y + t,$$
$$y = (\tfrac{1}{4} + \tfrac{1}{5})z + t,$$
$$z = (\tfrac{1}{6} + \tfrac{1}{7})x + t.$$

Next, for the numbers x', y', z', t' of cows of the same respective colors, the poet requires in lines 17–26

$$x' = (\tfrac{1}{3} + \tfrac{1}{4})(y + y'), \qquad z' = (\tfrac{1}{5} + \tfrac{1}{6})(t + t'),$$
$$y' = (\tfrac{1}{4} + \tfrac{1}{5})(z + z'), \qquad t' = (\tfrac{1}{6} + \tfrac{1}{7})(x + x').$$

Whoever can solve the problem thus far is called merely competent by Archimedes; to win the prize for supreme wisdom, one should also meet the conditions formulated in lines 33–40 that $x + y$ be a *square* and that $z + t$ be a *triangular number*.

The first part of the problem is just linear algebra, and there is indeed a solution in *positive* integers. The general solution to the first three equations is given by $(x, y, z, t) = m \cdot (2226,\ 1602,\ 1580,\ 891)$, where m is a positive integer. The next four equations turn out to be solvable if and only if m is divisible by 4657; with $m = 4657 \cdot k$ one has

$$(x', y', z', t') = k \cdot (7206360,\ 4893246,\ 3515820,\ 5439213).$$

The true challenge is now to choose k such that $x + y = 4657 \cdot 3828 \cdot k$ is a square and $z + t = 4657 \cdot 2471 \cdot k$ is a triangular number. From the prime factorization $4657 \cdot 3828 = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657$ one sees that the first condition is equivalent to $k = al^2$, where $a = 3 \cdot 11 \cdot 29 \cdot 4657$ and l is an integer. Since $z + t$ is a triangular number if and only if $8(z + t) + 1$ is a square, we are led to the equation $h^2 = 8(z + t) + 1 = 8 \cdot 4657 \cdot 2471 \cdot al^2 + 1$, which is the Pell equation $h^2 = dl^2 + 1$ for

$$d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657)^2 = 410\,286423\,278424.$$

Thus, by Lagrange's theorem, the cattle problem admits infinitely many solutions.

In 1867 the otherwise unknown German mathematician C. F. Meyer set out to solve the equation by the continued fraction method [Dickson 1920, p. 344]. After 240 steps in the continued fraction expansion for $\sqrt{d}$ he had still not detected the period, and he gave up. He may have been a little impatient; it was later discovered that the period length equals 203254; see [Grosjean and De Meyer 1991]. The first to solve the cattle problem in a satisfactory way was A. Amthor in 1880 (see [Krumbiegel and Amthor 1880]). Amthor did *not* directly apply the continued fraction method; what he did do we shall discuss

below. Nor did he spell out the decimal digits of the fundamental solution to the Pell equation or the corresponding solution of the cattle problem. He did show that, in the smallest solution to the cattle problem, the total number of cattle is given by a number of 206545 digits; of the four leading digits 7766 that he gave, the fourth was wrong, due to the use of insufficiently precise logarithms. The full number occupies forty-seven pages of computer printout, reproduced in reduced size on twelve pages of the *Journal of Recreational Mathematics* [Nelson 1980/81]. In abbreviated form, it reads

$$77602714\ldots237983357\ldots55081800,$$

each of the six dots representing 34420 omitted digits.

Several nineteenth century German scholars were worried that so many bulls and cows might not fit on the island of Sicily, contradicting lines 3 and 4 of the poem; but, as Lessing remarked, the Sun god, to whom the cattle belonged, will have coped with it.

The story of the cattle problem shows that the continued fraction method is not the last word on the Pell equation.

3. Efficiency

We are interested in the *efficiency* of solution methods for the Pell equation. Thus, how much time does a given algorithm for solving the Pell equation take? Here *time* is to be measured in a realistic way, which reflects, for example, that large positive integers are more time-consuming to operate with than small ones; technically, one counts *bit operations*. The input to the algorithm is d, and the running time estimates are accordingly expressed as functions of d. If one supposes that d is specified in binary or in decimal, then the *length of the input* is approximately proportional to $\log d$. An algorithm is said to run in *polynomial time* if there is a positive real number c_0 such that for all d the running time is at most $(1+\log d)^{c_0}$, in other words, if the time that it takes the algorithm to *solve* the Pell equation is not much greater than the time required to *write down* the equation.

How fast is the continued fraction method? Can the Pell equation be solved in polynomial time? The central quantity that one needs to consider in order to answer such questions is the *regulator* R_d, which is defined by

$$R_d = \log(x_1 + y_1\sqrt{d}),$$

where $x_1 + y_1\sqrt{d}$ denotes, as before, the fundamental solution to Pell's equation. The regulator coincides with what in algebraic number theory would be called the regulator of the kernel of the norm map $\mathbb{Z}[\sqrt{d}]^* \to \mathbb{Z}^*$. From

$x_1 - y_1\sqrt{d} = 1/(x_1 + y_1\sqrt{d})$ one deduces that $0 < x_1 - y_1\sqrt{d} < 1/(2\sqrt{d})$, and combining this with $x_1 + y_1\sqrt{d} = \mathrm{e}^{R_d}$, one finds that

$$\frac{\mathrm{e}^{R_d}}{2} < x_1 < \frac{\mathrm{e}^{R_d}}{2} + \frac{1}{4\sqrt{d}}, \qquad \frac{\mathrm{e}^{R_d}}{2\sqrt{d}} - \frac{1}{4d} < y_1 < \frac{\mathrm{e}^{R_d}}{2\sqrt{d}}.$$

This shows that R_d is very close to $\log(2x_1)$ and to $\log(2y_1\sqrt{d})$. That is, if x_1 and y_1 are to be represented in binary or in decimal, then R_d is approximately proportional to the *length of the output* of any algorithm solving the Pell equation. Since the time required for spelling out the output is a lower bound for the total running time, we may conclude: *there exists c_1 such that any algorithm for solving the Pell equation takes time at least $c_1 R_d$.* Here c_1 denotes, just as do $c_2, c_3, \ldots$ below, a positive real number that does not depend on d.

The continued fraction method almost meets this lower bound. Let l be the period length of the continued fraction expansion of $[\sqrt{d}] + \sqrt{d}$ if that length is even and twice that length if it is odd. Then one has

$$\frac{\log 2}{2} \cdot l < R_d < \frac{\log(4d)}{2} \cdot l;$$

see [Lenstra 1982, (11.4)]. Thus R_d and l are approximately proportional. Using this, one estimates easily that the time taken by a straightforward implementation of the continued fraction method is at most $R_d^2 \cdot (1 + \log d)^{c_2}$ for suitable c_2; and a more refined implementation, which depends on the fast Fourier transform, reduces this to $R_d \cdot (1 + \log d)^{c_3}$ for suitable c_3; see [Schönhage 1971]. We conclude that the latter version of the continued fraction method is optimal, apart from a logarithmic factor.

In view of these results it is natural to ask how the regulator grows as a function of d. It turns out that it fluctuates wildly. One has

$$\log(2\sqrt{d}) < R_d < \sqrt{d} \cdot (\log(4d) + 2),$$

the lower bound because of the inequality $y_1 < \mathrm{e}^{R_d}/(2\sqrt{d})$ above and the upper bound by [Hua 1942]. The gap between the two bounds is very large, but it cannot be helped: if d ranges over numbers of the form $k^2 - 1$, for which one has $x_1 = k$ and $y_1 = 1$, then $R_d - \log(2\sqrt{d})$ tends to 0; and one can show that there exist an infinite set D of d's and a constant c_4 such that all $d \in D$ have $R_d = c_4\sqrt{d}$. In fact, if d_0, d_1 are integers greater than 1 and d_0 is not a square, then there exists a positive integer $m = m(d_0, d_1)$ such that $D = \{d_0 d_1^{2n} : n \in \mathbb{Z}, n \geq m\}$ has this property for some $c_4 = c_4(d_0, d_1)$.

It is believed that for most d the upper bound is closer to the truth. More precisely, a folklore conjecture asserts that there is a set D of nonsquare positive