Solving the generalized Pell equation $x^2 - Dy^2 = N$

Copyright 2004 by John P. Robertson

Introduction

This article gives fast, simple algorithms to find integer solutions x, y to generalized Pell equations, $x^2 - Dy^2 = N$, for D a positive integer, not a square, and N a nonzero integer. Pell equations have fascinated for centuries. Consider the smallest positive solution to the equation $x^2 - Dy^2 = 1$ for $980 \le D \le 1005$, as shown in Table 1 below. Sometimes this smallest solution is quite small, and sometimes it is huge. If you don't see a pattern, don't feel bad; neither do I. This lack of an easy relationship between the value of D and the smallest solution is part of the appeal of these equations.

The main method we will present for solving the generalized Pell equation, the LMM algorithm, is only slightly more complex than the standard continued fraction algorithm for solving the Pell equation $x^2 - Dy^2 = 1$. While this method was known to Lagrange, it remained virtually unknown until recently rediscovered independently by Keith Matthews [11] and Richard Mollin [13].

What is presented here is sufficient for cases where D and N are "small." Even to solve these cases, you may want to have efficient algorithms to solve the equation $x^2 \equiv D \pmod{|m|}$, and to factor integers. We give references for algorithms to perform these last two functions, but we do not give the algorithms themselves herein. Also, no proofs are given here, but references to proofs are given. Williams [19] and Lenstra [7] discuss solving Pell equations for large D.

If you just want to solve a particular equation, download Keith Matthews' CALC from

www.numbertheory.org/calc/krm_calc.html

and use the function patz(D, N), or find a link to CALC at Keith Matthews' home page

www.maths.uq.edu.au/~krm.

Or use his online BCMATH solver available at

www.numbertheory.org/php/php.html

Minimum Positive Solutions

D	x	y
980	51841	1656
981	158070671986249	5046808151700
982	8837	282
983	284088	9061
984	88805	2831
985	332929	10608
986	49299	1570
987	377	12
988	14549450527	462879684
989	550271588560695	17497618534396
990	881	28
991	379516400906811930638014896080	12055735790331359447442538767
992	63	2
993	2647	84
994	1135	36
995	8835999	280120
996	8553815	271038
997	14418057673	456624468
998	984076901	31150410
999	102688615	3248924
1000	39480499	1248483
1001	1060905	33532
1002	206869247	6535248
1003	9026	285
1004	27009633024199	852416459730
1005	2950149761	93059568

Table 1: Minimum positive solutions to $x^2 - Dy^2 = 1$.

(or use the link to BCMATH from his home page). Dario Alejandro Alpern also has an online solver, available at

www.alpertron.com.ar/ENGLISH.HTM.

If you want some algorithms for solving these equations, this is the place. If you want the theory behind these algorithms, see the references.

Methods specific to the given equation are presented here for $x^2 - Dy^2 = \pm 1$, for $x^2 - Dy^2 = \pm 4$, and for $x^2 - Dy^2 = N$ when $N^2 < D$. For the general Pell equation (arbitrary $N \neq 0$) there are at least five good methods:

1. Brute-force search (which is good only if the upper search limit, given below, is not too large),

2. The Lagrange-Matthews-Mollin (LMM) algorithm,

3. Lagrange's system of reductions,

4. The cyclic method, and

5. Use of binary quadratic forms.

Of these five, we will present only the first three. For the cyclic method see Edwards [5]. For binary quadratic forms see Hurwitz [6] or Mathews [9].

Section headings are

1. PQa algorithm,

2. Solving $x^2 - Dy^2 = \pm 1$,

3. Solving $x^2 - Dy^2 = \pm 4$,

4. Structure of solutions to $x^2 - Dy^2 = N$,

5. Solving $x^2 - Dy^2 = N$ for $N^2 < D$,

6. Solving $x^2 - Dy^2 = N$ by brute-force search,

7. Solving $x^2 - Dy^2 = N$ by the LMM algorithm.

8. Lagrange's system of reductions.

Annotated references and Tables 2 to 6 are at the end.

Web pages with material on continued fractions generally and Pell equations in particular (or with links to other such pages) are at the Number Theory Web and at Eric Weisstein's World of Mathematics. At the Number Theory Web, look for, "Descriptions of areas/courses in number theory, lecture notes," and look for the topics of interest. The URL is (note that there is no longer a US mirror)

www.numbertheory.org/ntw/web.html

or

www.maths.uq.edu.au/~krm/ntw/

At Eric Weisstein's World of Mathematics, Number Theory section, look for continued fractions and Diophantine equations. The URL is

mathworld.wolfram.com/topics/NumberTheory.html

PQa algorithm

This algorithm is at the heart of many methods to solve Pell equations, including the LMM algorithm. It computes the (simple) continued fraction expansion of the quadratic irrational $(P_0 + \sqrt{D})/Q_0$ for certain P_0, Q_0, D, and it computes some auxiliary variables.

Let P_0, Q_0, D be integers so that $Q_0 \neq 0$, $D > 0$ is not a square, and $P_0^2 \equiv D \pmod{Q_0}$. Set

$$A_{-2} = 0,\ A_{-1} = 1,$$

$$B_{-2} = 1,\ B_{-1} = 0,$$

$$G_{-2} = -P_0, \text{ and } G_{-1} = Q_0.$$

For $i \geq 0$ set

$$a_i = \left\lfloor (P_i + \sqrt{D})/Q_i \right\rfloor,$$

$$A_i = a_i A_{i-1} + A_{i-2},$$

$$B_i = a_i B_{i-1} + B_{i-2},$$

$$G_i = a_i G_{i-1} + G_{i-2},$$

and for $i \geq 1$ set

$$P_i = a_{i-1}Q_{i-1} - P_{i-1} \text{ and}$$

$$Q_i = (D - P_i^2)/Q_{i-1}.$$

Exactly how far to carry these computations is discussed with each use below.

Each of these variables will be an integer for all indices for which they are defined. A key output of this algorithm is the sequence a_0, a_1, a_2, ... which gives the continued fraction expansion of $\xi_0 = (P_0 + \sqrt{D})/Q_0$. That is,

$$(P_0 + \sqrt{D})/Q_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots}}}}$$

We write $\langle a_0, a_1, a_2, \ldots \rangle$ for this continued fraction expansion. The a_i are the *partial quotients* of ξ_0.

Also, for $i \geq 0$, set $\xi_i = (P_i + \sqrt{D})/Q_i$ so the *conjugate* of ξ_i is $\overline{\xi_i} = (P_i - \sqrt{D})/Q_i$. Set $\xi = \xi_0$ and $\overline{\xi} = \overline{\xi_0}$. The ξ_i are the *i-th complete quotients* of ξ. These much-studied variables have many interesting properties, of which we list just a few.

1. For $i > 0$, $a_i > 0$.
2. Each of the sequences $\{a_i\}$, $\{P_i\}$, and $\{Q_i\}$ is eventually periodic. Specifically, there is a least nonnegative integer i_0 and a least positive integer ℓ, the length of the minimal period, so that for any integers $i \geq i_0$ and $k > 0$, $a_{i+k\ell} = a_i$, $P_{i+k\ell} = P_i$, $Q_{i+k\ell} = Q_i$, and $\xi_{i+k\ell} = \xi_i$.
3. For $i \geq i_0$, $0 < P_i < \sqrt{D}$, $0 < \sqrt{D} - P_i < Q_i < \sqrt{D} + P_i < 2\sqrt{D}$.
4. For $i \geq i_0$, if $Q_i \neq 1$ then $a_i < \sqrt{D}$, while if $Q_i = 1$ then $\sqrt{D} < a_i < 2\sqrt{D}$.
5. For $i \geq i_0$, $\xi_i = (P_i + \sqrt{D})/Q_i$ is *reduced*, which means that $\xi_i > 1$ and $-1 < \overline{\xi_i} < 0$.
6. $\xi_i = \langle a_i, a_{i+1}, a_{i+2}, \ldots \rangle$ for $i \geq 0$.
7. The $\xi_i = (P_i + \sqrt{D})/Q_i$ are distinct for $i_0 \leq i \leq i_0 + \ell - 1$.

8. $\gcd(A_i, B_i) = 1$ for $i \geq -2$.
9. The ratios A_i/B_i for $i \geq 0$ are the *convergents* to the continued fraction expansion of $(P_0 + \sqrt{D})/Q_0$.
10. $(P_0 + \sqrt{D})/Q_0 = \lim_{i\to\infty} \dfrac{A_i}{B_i}$.
11. $A_i B_{i-1} - A_{i-1} B_i = (-1)^{i-1}$ for $i \geq -1$.
12. $A_i B_{i-2} - A_{i-2} B_i = (-1)^i a_i$ for $i \geq 0$.
13. $\xi_i = a_i + \dfrac{1}{\xi_{i+1}}$ for $i \geq 0$.
14. $\dfrac{P_0 + \sqrt{D}}{Q_0} = \dfrac{A_i \xi_{i+1} + A_{i-1}}{B_i \xi_{i+1} + B_{i-1}}$ for $i \geq -1$.
15. $P_i^2 \equiv D \pmod{|Q_i|}$ for $i \geq 0$.
16. $Q_i = Q_{i-2} - a_{i-1}(P_i - P_{i-1})$ for $i \geq 2$.
17. $G_i = Q_0 A_i - P_0 B_i$ for $i \geq -2$.
18. $A_i - B_i \xi = \dfrac{G_i - B_i\sqrt{D}}{Q_0}$; $A_i - B_i\overline{\xi} = \dfrac{G_i + B_i\sqrt{D}}{Q_0}$ for $i \geq 0$.
19. $(A_i - B_i\xi)\left(A_i - B_i\overline{\xi}\right) = \dfrac{(-1)^{i+1} Q_{i+1}}{Q_0}$ for $i \geq -1$.
20. $G_{i-1}^2 - DB_{i-1}^2 = (-1)^i Q_0 Q_i$ for $i \geq 0$.
21. $\gcd(G_i, B_i) = \gcd(Q_0, B_i)$ for $i \geq -2$.
22. $\gcd(G_i, B_i)$ divides Q_{i+1} for $i \geq -1$.
23. $\dfrac{1}{B_i + B_{i+1}} \leq \dfrac{a_{i+2}}{B_{i+2}} < |A_i - B_i\xi| < \dfrac{1}{B_{i+1}}$ for $i \geq 0$.
24. $\dfrac{1}{(a_{i+1}+2)\, B_i} \leq \dfrac{1}{B_i + B_{i+1}}$ for $i \geq 0$; $\quad \dfrac{1}{2B_{i+1}} \leq \dfrac{1}{B_i + B_{i+1}}$ for $i \geq 0$.
25. $|A_i - \xi B_i| < \dfrac{1}{2B_i} \iff |Q_{i+1}| < \sqrt{D}$, for sufficiently large i.

26. $\left|\dfrac{G_i - B_i\sqrt{D}}{Q_0}\right| < \dfrac{1}{2B_i} \iff \left|G_i^2 - B_i^2\sqrt{D}\right| < |Q_0|\sqrt{D}$ for sufficiently large i.

27. $\lfloor\sqrt{D}\rfloor + \sqrt{D}$ is reduced.

In 2002 Keith Matthews proved item 22; if you know of earlier references, I would like to hear of them.

The relation $G_i^2 - DB_i^2 = (-1)^{i+1}Q_{i+1}Q_0$ will be important to us because all of the methods of solution we discuss will involve setting $Q_0 = |N|$, and finding those i so that $(-1)^{i+1}Q_{i+1} = N/|N|$. Then G_i, B_i will be a solution to the equation being considered. From a computational viewpoint, also note that, in some sense, G_i and B_i will typically be large, while Q_0 and Q_{i+1} will be small. So this equation sometimes allows accurate computation of the left-hand-side of $G_i^2 - DB_i^2 = (-1)^{i+1}Q_{i+1}Q_0$ when the terms on the left-hand-side exceed the machine accuracy available.

It is useful to determine when one has reached the end of the first period. One method is as follows. As P_i and Q_i are computed, determine whether $(P_i + \sqrt{D})/Q_i$ is reduced, and let i_r be the smallest i for which this occurs. Then find the smallest $j > i_r$ for which $P_{i_r} = P_j$ and $Q_{i_r} = Q_j$. This j will mark the start of the second period, so $j - 1$ is the end of the first period.

For certain P_0 and Q_0 there are ways to determine when one has reached the middle of the first period, without computing the whole period. Whenever either

$P_0 = 0$ and $Q_0 = 1$, or

$D \equiv 1 \pmod 4$, $P_0 = 1$, and $Q_0 = 2$,

the following will hold. Let ℓ be the smallest index so that $\ell > 0$ and $Q_\ell = Q_0$ ($= 1$ or 2). If there is a j so that $P_j = P_{j+1}$, and j is the smallest such, then $\ell = 2j$, and the length of the period is even. Otherwise, there is a j so that $Q_j = Q_{j+1}$, and if j is the smallest such, then $\ell = 2j + 1$, and the length of the period is odd. For either case one can immediately compute the second half of the first period using the following relations that express the palindromic properties of the sequences P_i, Q_i, and a_i: $P_i = P_{\ell+1-i}$ for $i = 1, 2, 3, \ldots, \ell$, $Q_i = Q_{\ell-i}$ for $i = 0, 1, 2, \ldots, \ell$, and $a_i = a_{\ell-i}$ for $i = 1, 2, 3, \ldots, \ell - 1$. Also, $a_\ell = 2a_0$ if $P_0 = 0$ and $Q_0 = 1$, and $a_\ell = 2a_0 - 1$ if $P_0 = 1$ and $Q_0 = 2$. This gives P_i, Q_i, and a_i through $i = \ell$, and periodicity can be used to extend these sequences from here. There are additional palindromic properties of these sequences that are easily seen by considering a few cases, e.g., $(P_0,\ Q_0,\ D) = (0,\ 1,\ 94)$, $(0,\ 1,\ 353)$, $(1,\ 2,\ 217)$, $(1,\ 2,\ 481)$.

Table 2 illustrates the PQa algorithm for $P_0 = 11$, $Q_0 = 108$, and $D = 13$. Computations are carried through a point slightly beyond the end of the second period. Notice that each of the sequences $\{a_i\}$, $\{P_i\}$, and $\{Q_i\}$ is periodic for $i \geq 3$. Within each period there is exactly one $Q_i = 1$. For a given P_0, Q_0, and D, there might not be any $Q_i = 1$. But, if there is at least one $Q_i = \pm 1$, as happens here, then there will be exactly one $Q_i = 1$ in each period of $\{Q_i\}$. Note how the values of A_i, B_i, and G_i grow large as i increases. To compute $G_i^2 - DB_i^2$, it is easiest to compute $(-1)^{i+1}Q_0Q_{i+1}$, as Q_0 is fixed and Q_{i+1} stays relatively small.

Continued fractions in general and the PQa algorithm in particular are discussed in many texts, so we will refer the interested reader to the following references to justify the assertions made above.

References - NZM [14], Mollin [12], Rockett and Szüsz [17], Cohen [3]

Solving $x^2 - Dy^2 = \pm 1$

To solve the equation $x^2 - Dy^2 = \pm 1$, apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$. There will be a smallest ℓ with $a_\ell = 2a_0$, which will also be the smallest $\ell > 0$ so that $Q_\ell = 1$. Here ℓ is the length of the period of the continued fraction expansion of $\sqrt{D}$. There are two cases to consider: ℓ is odd, or ℓ is even.

If ℓ is odd, the equation $x^2 - Dy^2 = -1$ has solutions. The minimal positive solution is given by $x = G_{\ell-1}$, $y = B_{\ell-1}$. For any positive integer k, if k is odd then $x = G_{k\ell-1}$, $y = B_{k\ell-1}$ is a solution to the equation $x^2 - Dy^2 = -1$, and all solutions to this equation with x and y positive are generated this way. If k is an even positive integer, then $x = G_{k\ell-1}$, $y = B_{k\ell-1}$ is a solution to the equation $x^2 - Dy^2 = 1$, and all solutions to this equation with x and y positive are generated this way. The minimal positive solution to $x^2 - Dy^2 = 1$ is $x = G_{2\ell-1}$, $y = B_{2\ell-1}$.

If the smallest ℓ so that $a_\ell = 2a_0$ is even, then the equation $x^2 - Dy^2 = -1$ does not have any solutions. For any positive integer k, $x = G_{k\ell-1}$, $y = B_{k\ell-1}$ is a solution to the equation $x^2 - Dy^2 = 1$, and all solutions to this equation with x and y positive are generated this way. In particular, the minimal positive solution to $x^2 - Dy^2 = 1$ is $x = G_{\ell-1}$, $y = B_{\ell-1}$.

The sequences P_i and a_i are periodic with period ℓ after the zero-th term, i.e., the first period is P_1 to P_ℓ for the sequence P_i, and a_1 to a_ℓ for the sequence a_i. The sequence Q_i is periodic starting at the zero-th term, i.e., the first period is Q_0 to $Q_{\ell-1}$.

The previous section discusses the palindromic properties of the sequences P_i, Q_i, and a_i, and the half-period stopping rule.

There are several methods to generate all solutions to either of the equations $x^2 - Dy^2 = \pm 1$ once the minimal positive solution is known.

Consider first the equation $x^2 - Dy^2 = 1$. If t, u is the minimal positive solution to this equation, then for the n-th positive solution $x_n + y_n\sqrt{D} = (t + u\sqrt{D})^n$ and $x_n - y_n\sqrt{D} = (t - u\sqrt{D})^n$. While each positive solution corresponds to a positive n, these equations also make sense for $n \leq 0$. There is a recursion $x_{n+1} = tx_n + uy_nD$, $y_{n+1} = ty_n + ux_n$. Another pair of recursions is (set $x_0 = 1$, $y_0 = 0$) $x_{n+1} = 2tx_n - x_{n-1}$, $y_{n+1} = 2ty_n - y_{n-1}$. The comments in this paragraph apply whether or not the equation $x^2 - Dy^2 = -1$ has solutions.

Now suppose the equation $x^2 - Dy^2 = -1$ has solutions, let t, u be the minimal positive solution, and define x_n, y_n by the equation $x_n + y_n\sqrt{D} = (t + u\sqrt{D})^n$. Then also $x_n - y_n\sqrt{D} = (t - u\sqrt{D})^n$. If n is odd, x_n, y_n is a solution to the equation $x^2 - Dy^2 = -1$, and if n is even then x_n, y_n is a solution to the equation $x^2 - Dy^2 = 1$. All positive solutions to these two equations are so generated. The recursion $x_{n+1} = tx_n + uy_nD$, $y_{n+1} = ty_n + ux_n$ also alternately generates solutions to the $+1$ and -1 equations. Another recursion is (set $x_0 = 1$, $y_0 = 0$) $x_{n+1} = 2tx_n + x_{n-1}$, $y_{n+1} = 2ty_n + y_{n-1}$.

All solutions are given by taking the four choices of sign, $\pm x_n$, $\pm y_n$.

Perhaps the most succinct way to summarize the set of solutions is as follows. Let x, y be any solution to $x^2 - Dy^2 = \pm 1$. Let t, u be the minimal positive solution of $x^2 - Dy^2 = \pm 1$. Then for some sign, ± 1, and some integer n, $x + y\sqrt{D} = \pm(t + u\sqrt{D})^n$. Note also that $(t + u\sqrt{D})^{-1} = \pm(t - u\sqrt{D})$.

Table 3 applies the PQa algorithm to solve $x^2 - 13y^2 = \pm 1$. The period length ℓ is 5, so the equation $x^2 - 13y^2 = -1$ has solutions. The smallest positive solution is given by $x = 18$, $y = 5$. The smallest positive solution to $x^2 - 13y^2 = 1$ is given by $x = 649$, $y = 180$. Note that $(18 + 5\sqrt{13})^2 = 649 + 180\sqrt{13}$, $(18 + 5\sqrt{13})^3 = 23382 + 6485\sqrt{13}$, and $(18 + 5\sqrt{13})^4 = 842401 + 233640\sqrt{13}$.

References: NZM [14], Mollin [12], Olds [15], Rockett and Szüsz [17], Leveque [8], Rose [18], and many other sources not listed here. Many introductory books on number theory cover the Pell ± 1 equation.

Solving $x^2 - Dy^2 = \pm 4$

In some ways, solutions to the equation $x^2 - Dy^2 = \pm 4$ are more fundamental than solutions to the equation $x^2 - Dy^2 = \pm 1$. The most interesting case is when $D \equiv 1 \pmod 4$, so we cover that first.

When $D \equiv 1 \pmod 4$, apply the PQa algorithm with $D = D$, $P_0 = 1$, and $Q_0 = 2$. There will be a smallest $\ell > 0$ so that $a_\ell = 2a_0 - 1$. This will also be the smallest $\ell > 0$ so that $Q_\ell = 2$. Then ℓ is the length of the period of the continued fraction expansion of $(1 + \sqrt{D})/2$. The minimal positive solution to $x^2 - Dy^2 = \pm 4$ is then $x = G_{\ell-1}$, $y = B_{\ell-1}$. If ℓ is odd, it will be a solution to the -4 equation, while if ℓ is even it will be a solution to the $+4$ equation and the -4 equation will not have solutions.

Periodicity of the sequences P_i, Q_i, and a_i is similar to that for the ± 1 equation. The section "PQa algorithm" discusses the palindromic properties of the sequences P_i, Q_i, and a_i, and the half-period stopping rule.

If $D \equiv 0 \pmod 4$, then for any solution to $x^2 - Dy^2 = \pm 4$, x must be even. Set $X = x/2$, set $Y = y$, and solve $X^2 - (D/4)Y^2 = \pm 1$. If X, Y is the minimal positive solution to this equation, then $x = 2X$, $y = Y$ is the minimal positive solution to $x^2 - Dy^2 = \pm 4$. Alternatively, one can apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 2$. If ℓ is the smallest index so that $a_\ell = 2a_0$, then the minimal positive solution is $G_{\ell-1}$, $B_{\ell-1}$.

If $D \equiv 2$ or $3 \pmod 4$, then by considerations modulo 4 one can see that both x and y must be even. Set $X = x/2$, $Y = y/2$, and solve $X^2 - DY^2 = \pm 1$. If X, Y is the minimal positive solution to this equation, then $x = 2X$, $y = 2Y$ is the minimal positive solution to $x^2 - Dy^2 = \pm 4$. Alternatively, use the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$, but set $G_{-2} = 0$, $G_{-1} = 2$, $B_{-2} = 2$, and $B_{-1} = 0$. If ℓ is the smallest index so that $a_\ell = 2a_0$, then the minimal positive solution is $G_{\ell-1}$, $B_{\ell-1}$.

As with the ± 1 equation, all solutions can be generated from the minimal positive solution. Consider first the equation $x^2 - Dy^2 = 4$. If t, u is the minimal positive solution to this equation, then for the n-th solution $x_n + y_n\sqrt{D} = [(t + u\sqrt{D})^n]/(2^{n-1})$ and $x_n - y_n\sqrt{D} = [(t - u\sqrt{D})^n]/(2^{n-1})$. We also have the recursion $x_{n+1} = (1/2)(tx_n + uy_nD)$, $y_{n+1} = (1/2)(ty_n + ux_n)$. Another recursion is (set $x_0 = 2$, $y_0 = 0$) $x_{n+1} = tx_n - x_{n-1}$, $y_{n+1} = ty_n - y_{n-1}$.

Now suppose the equation $x^2 - Dy^2 = -4$ has solutions, let t, u be the minimal positive solution, and define x_n, y_n by the equation $x_n + y_n\sqrt{D} = [(t + u\sqrt{D})^n]/(2^{n-1})$. Then if n is odd, x_n, y_n is a solution to the equation $x^2 - Dy^2 = -4$, and if n is even then x_n, y_n is a solution to the equation $x^2 - Dy^2 = 4$. All positive solutions to these two equations are so generated. The recursion $x_{n+1} = (1/2)(tx_n + uy_nD)$, $y_{n+1} = (1/2)(ty_n + ux_n)$ also alternately generates solutions to the $+4$ and -4 equations. Another recursion is (set $x_0 = 2$, $y_0 = 0$) $x_{n+1} = tx_n + x_{n-1}$, $y_{n+1} = ty_n + y_{n-1}$.

The set of solutions can be summarized as follows. Let t, u be the minimal positive solution of $x^2 - Dy^2 = \pm 4$. Then for any solution to $x^2 - Dy^2 = \pm 4$, there is a sign, ± 1, and an integer n so that $(x + y\sqrt{D})/2 = (\pm 1)[(t + u\sqrt{D})/2]^n$.

In some ways, the equation $x^2 - Dy^2 = \pm 4$ is more fundamental than the equation $x^2 - Dy^2 = \pm 1$. The numbers 1 and 4 are the only N's so that, for any D, if you know the minimal positive solution to the equation $x^2 - Dy^2 = \pm N$, you can generate all solutions, and you can do this without solving any other Pell equation. Also, if you know the minimal positive solution to $x^2 - Dy^2 = \pm 4$, you can generate all the solutions to $x^2 - Dy^2 = \pm 1$. But the converse does not hold. The best that can be said as a converse is that for D not 5 or 12, the solutions to the equation $x^2 - Dy^2 = \pm 4$ can be derived from the intermediate steps when the PQa algorithm is used to solve the equation $x^2 - Dy^2 = \pm 1$.

When $D \equiv 1 \pmod 4$, considerations modulo 4 show that for any solution to $x^2 - Dy^2 = \pm 4$, x and y are both odd or both even. If the minimal positive solution has both x and y even, then all solutions have both x and y even. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. If the minimal positive solution to $x^2 - Dy^2 = \pm 4$ has both x and y odd, then $D \equiv 5 \pmod 8$, every third solution has x and y even, and all other solutions have x and y odd. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of one of the solutions to $x^2 - Dy^2 = \pm 4$ that has both x and y even. When $D \equiv 1 \pmod 4$, the equation $x^2 - Dy^2 = -4$ has solutions if and only if the equation $x^2 - Dy^2 = -1$ has solutions.

When $D \equiv 0 \pmod 4$, considerations modulo 4 show that for any solution to $x^2 - Dy^2 = \pm 4$, x is even. If the minimal positive solution has y even, then all solutions have y even (and x is always even). In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. If the minimal positive solution to $x^2 - Dy^2 = \pm 4$ has y odd, then every other solution has y even, and every other solution has y odd. In this case, every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of one of the solutions to $x^2 - Dy^2 = \pm 4$ that has x and y both even. When $D \equiv 0 \pmod 4$, it is possible for there to be solutions to $x^2 - Dy^2 = -4$, but not solutions to $x^2 - Dy^2 = -1$. This happens for $D = 8$, 20, 40, 52 and many more values. Of course, $x^2 - Dy^2 = -1$ never has solutions when $D \equiv 0 \pmod 4$.

When $D \equiv 2$ or $3 \pmod 4$, all solutions to $x^2 - Dy^2 = \pm 4$ have both x and y even. Every solution to $x^2 - Dy^2 = \pm 1$ is just one-half of a solution to $x^2 - Dy^2 = \pm 4$. The equation $x^2 - Dy^2 = -4$ has solutions if and only if the equation $x^2 - Dy^2 = -1$ has solutions.

Table 4 uses the PQa algorithm to solve $x^2 - 13y^2 = \pm 4$. The smallest $\ell > 0$ so that $a_\ell = 2a_0 - 1$, and hence $Q_\ell = 2$, is $\ell = 1$. As ℓ is odd, the equation $x^2 - 13y^2 = -4$ has solutions, and the smallest positive solution is $x = 3$, $y = 1$. Then $(3+\sqrt{13})^2/2 = 11 + 3\sqrt{13}$, $(3+\sqrt{13})^3/4 = 36 + 10\sqrt{13}$, $(3+\sqrt{13})^4/8 = 119 + 33\sqrt{13}$, $(3+\sqrt{13})^5/16 = 393 + 109\sqrt{13}$, and so on. These alternately give solutions to the $+4$ and -4 equations. Every third solution has both x and y even. Taking half of these solutions generates every solution to $x^2 - 13y^2 = \pm 1$.

References - Cohen [3], NZM [14], Mollin [12], Leveque [8]. Cohen treats the cases $D \equiv 1 \pmod 4$ for D squarefree, and $D = 4r$ for $r \equiv 2$ or $3 \pmod 4$, r squarefree. The above material is not really addressed directly in either of NZM or Mollin. But the only matter above that is not trivially derived from material in one or both of these sources is the proof that the method for solving the equation works in the case $D \equiv 1 \pmod 4$. Here, one can imitate the proof in NZM for the equation $x^2 - Dy^2 = \pm 1$, and make use of Mollin's Theorem 5.3.4, p. 246. This will result in a proof for all $D \equiv 1 \pmod 4$, D not a square; not just for the D treated in Cohen. Leveque only treats the generation of all solutions from the base solution.

Structure of solutions to $x^2 - Dy^2 = N$

If r, s is a solution to $x^2 - Dy^2 = N$, and t, u is any solution to $x^2 - Dy^2 = 1$, then $x = rt + suD$, $y = ru + st$, is also a solution to $x^2 - Dy^2 = N$. This follows from the relation $(rt + suD)^2 - D(ru + st)^2 = (r^2 - Ds^2)(t^2 - Du^2)$. This fact can be used to separate solutions to $x^2 - Dy^2 = N$ into equivalence classes. Two solutions x, y and r, s are equivalent if there is a solution t, u to $t^2 - Du^2 = 1$ so that $x = rt + suD$ and $y = ru + st$. An equivalent test, which is easier to apply, is that two solutions x, y and r, s are equivalent if and only if both $(xr - Dys)/N$ and $(xs - yr)/N$ are integers. As $r = -1$, $s = 0$ satisfies $r^2 - Ds^2 = 1$ for any D, $(-x,\ -y)$ is always equivalent to $(x,\ y)$.

It may help to view the set of solutions geometrically. If $N > 0$, then, as an equation in real numbers, $x^2 - Dy^2 = N$ is a hyperbola with the x-axis as its axis, and the y-axis as an axis of symmetry. The asymptotes are the lines $x \pm y\sqrt{D} = 0$. Let t, u be the minimal positive solution to $x^2 - Dy^2 = 1$. Draw the graph of $x^2 - Dy^2 = N$ over the reals. Mark the point $(\sqrt{N}, 0)$, which is on this graph. Now mark the point $(t\sqrt{N}, u\sqrt{N})$, which is also on the graph. Continue marking points so that if (x, y) is the most recently marked point, then the next point marked is $(xt + yuD, xu + yt)$. All of the points marked so far, apart from the first, have $x > 0$ and $y > 0$. Now, for each point (x, y) that has been marked, mark all of the points $(\pm x, \pm y)$ not yet marked.

The marked points divide the graph into intervals. Make the interval $((\sqrt{N},\ 0),\ (t\sqrt{N},\ u\sqrt{N})]$ a half-open interval, and then make the other intervals on this branch half-open by assigning endpoints to one interval. Make the intervals on the other branch half-open by mapping (x, y) in the right branch to $(-x, -y)$ on the left branch. If there are integer solutions to $x^2 - Dy^2 = N$, then

1) No two solutions within the same (half-open) interval are equivalent,

2) Every interval has exactly one solution in each class, and

3) The order of solutions by class is the same in every interval.

Instead of starting with the point $(\sqrt{N}, 0)$, we could have started with any point (r, s) on the graph, and marked off the points corresponding to $(r + s\sqrt{D}) \cdot (\pm 1) \cdot (t + u\sqrt{D})^n$. The above three comments would still apply.

The situation is similar when $N < 0$, except that the graph has the y-axis as its axis, and the x-axis is an axis of symmetry.

If $x^2 - Dy^2 = -1$ has solutions, then any of these solutions can be used to form a correspondence between solutions to $x^2 - Dy^2 = N$ and $-N$.

Within a class there is a unique solution with x and y nonnegative, but smaller than any other nonnegative solution. This is the *minimal nonnegative* solution for the class. There is also either one or two solutions so that y is nonnegative, and is less than or equal to any other nonnegative y in any solution x, y within the class. If there is one such solution, it is called the *fundamental solution*. If there are two such solutions, then they will be equivalent and their x-values will be negatives of each other. In this case, the solution with the positive x-value is called the fundamental solution for the class. For $N > 0$, the fundamental solutions are on the hyperbola in the intervals

$$\left(\sqrt{N}, 0\right) \text{ to } \left(\sqrt{N(r+1)/2}, \sqrt{N(r-1)/(2D)}\right), \text{ and}$$

$$\left(-\sqrt{N}, 0\right) \text{ to } \left(-\sqrt{N(r+1)/2}, \sqrt{N(r-1)/(2D)}\right).$$

For the first interval, the endpoints should be included, while for the second interval they should be excluded.

For $N < 0$, the fundamental solutions are in the interval

$$\left(-\sqrt{|N|(r-1)/2}, \sqrt{|N|(r+1)/(2D)}\right) \text{ to}$$

$$\left(\sqrt{|N|(r-1)/2}, \sqrt{|N|(r+1)/(2D)}\right),$$

with midpoint $\left(0, \sqrt{-N/D}\right)$. In this interval, the first point should be excluded, and the last point included.

When tabulating solutions, it is usually convenient to make a list consisting of one solution from each class. Often, this list will be either the minimal nonnegative solutions, or the fundamental solutions. Given any solution in a class, it is easy to find the fundamental solution or the minimal nonnegative solution for that class.

To summarize, given any solution in a class, all solutions in that class are found by applying solutions to the equation $x^2 - Dy^2 = 1$. If r, s is any particular solution to $x^2 - Dy^2 = N$, x, y is any other solution to the same equation in the same class as r, s, and if t, u is the minimal positive solution to the equation $x^2 - Dy^2 = 1$, then for some choice of sign, ± 1, and for some integer n, $x + y\sqrt{D} = \pm(r + s\sqrt{D})(t + u\sqrt{D})^n$.

There are recursion relations among solutions similar to those presented for the ± 1 and ± 4 equations. For instance, if (x_1, y_1), (x_2, y_2), and (x_3, y_3) are three solutions in the same class, in consecutive intervals, and t, u is the minimal positive solution to $x^2 - Dy^2 = 1$, then $x_3 = 2tx_2 - x_1$ and $y_3 = 2ty_2 - y_1$.

As an example, consider solutions to $x^2 - 13y^2 = 27$. The minimal positive solution to $t^2 - 13u^2 = 1$ is $t = 649$, $u = 180$ (Table 3). On the hyperbola $x^2 - 13y^2 = 27$ mark off the intervals bounded by the points ($\pm\sqrt{27}$, 0), ($\pm 649\sqrt{27}$, $\pm 180\sqrt{27}$), ($\pm 842401\sqrt{27}$, $\pm 233640\sqrt{27}$),($\pm 1093435849\sqrt{27}$, $\pm 303264540\sqrt{27}$), and so on. The points bounding these intervals are approximately ($\pm$5.196, 0), ($\pm$3372.303, $\pm$935.307), ($\pm$4377243.997, $\pm$1214029.052), ($\pm$5681659335.856, $\pm$1575808774.242).

The minimal positive solutions to $x^2 - 13y^2 = 27$ for each equivalence class are (12, 3), (40, 11), (220, 61), and (768, 213) (methods for finding these are given below). Note that they all lie in the interval (5.196, 0) to (3372.303, 935.307). The next larger solutions, equivalent respectively to the first four listed, are (14808, 4107), (51700, 14339), (285520, 79189), (996852, 276477). These lie in the interval (3372.303, 935.307) to (4377243.997, 1214029.052). The next larger solutions, again equivalent respectively to the first four are (19220772, 5330883), (67106560, 18612011), (370604740, 102787261), and (1293913128, 358866933). These all lie in the interval (4377243.997, 1214029.052) to (5681659335.856, 1575808774.242). Other equivalent points, and the intervals they fall into are readily computed.

References - NZM [14], Mollin [12], Chrystal [2], Leveque [8], Rose [18]

Solving $x^2 - Dy^2 = N$ for $N^2 < D$

When $1 < N^2 < D$, apply the PQa algorithm with $D = D$, $P_0 = 0$, $Q_0 = 1$. Continue the computations until you reach the first $\ell_e > 0$ with $G_{\ell_e-1}^2 - DB_{\ell_e-1}^2 = 1$ (i.e., $Q_{\ell_e} = 1$ and ℓ_e is even. Note that $\ell_e = \ell$ or 2ℓ, above). For $0 \leq i \leq \ell_e - 1$, if $G_i^2 - dB_i^2 = N/f^2$ for some $f > 0$, add fG_i, fB_i to the list of solutions. When done, the list of solutions will have the minimal positive member of each class.

The list of all solutions can be generated using the methods of the previous section. Alternatively, all positive solutions can be generated by extending the PQa algorithm indefinitely.

As an example, consider $x^2 - 157y^2 = 12$. Here $12^2 < 157$. Apply the PQa algorithm with $D = 157$, $P_0 = 0$, and $Q_0 = 1$. The first ℓ_e with $Q_{\ell_e} = 1$ and ℓ_e even is $\ell_e = 34$. For i from 0 to 33, those i for which $G_i^2 - 157B_i^2 = 12$ or 3 $(= 12/2^2)$ are $i = 1$, 9, 13, 19, 23, and 31. For these i, $(i, G_i, B_i, G_i^2 - 157B_i^2)$ are (1, 13, 1, 12), (9, 10663, 851, 12), (13, 289580, 23111, 3), (19, 241895480, 19305361, 3), (23, 26277068347, 2097138361, 12), (31, 21950079635497, 1751807067011, 12). The corresponding solutions to $x^2 - 157y^2 = 12$ are (13, 1), (10663, 851), (579160, 46222), (483790960, 38610722), (26277068347, 2097138361), and (21950079635497, 1751807067011). These are the minimal positive solutions for each equivalence class.

References - NZM [14], Mollin [12], Chrystal [2]

Solving $x^2 - Dy^2 = N$ by brute-force search

Let t, u be the minimal positive solution to $x^2 - Dy^2 = 1$. If $N > 0$, set $L_1 = 0$, and $L_2 = \sqrt{N(t-1)/(2D)}$. If $N < 0$, set $L_1 = \sqrt{(-N)/D}$, and $L_2 = \sqrt{(-N)(t+1)/(2D)}$. For $L_1 \leq y \leq L_2$, if $N + Dy^2$ is a square, set $x = \sqrt{N + Dy^2}$. If (x, y) is not equivalent to $(-x, y)$, add both to the list of solutions, otherwise just add (x, y) to the list. When finished, this list gives the fundamental solutions.

This method works well if L_2 is not too large, which means that

$$\sqrt{|N|(t \pm 1)/(2D)}$$

is not too large. You must be able to perform the search between the limits L_1 and L_2.

To generate all solutions from these, see the section "Structure of solutions to $x^2 - Dy^2 = N$".

As an example, let's solve $x^2 - 13y^2 = 108$ by the method of brute-force search. The minimal positive solution of $t^2 - 13u^2 = 1$ is $t = 649$, $u = 180$ (Table 3), so $L1 = 0$ and $L2 = \sqrt{108(649 - 1)/(2 \cdot 13)} \approx 51.882$. The y so that $0 \leq y \leq 51.882$ and $108 + 13y^2$ is square are $y = 1, 3, 6, 11, 22, 39$. This gives solutions $(x,\ y)$ of (±11, 1), (±15, 3), (±24, 6), (±41, 11), (±80, 22), and (±141, 39). These are the fundamental solutions for each of the 12 classes. The minimal positive solution equivalent to (−11, 1) is (4799, 1331) (because $108 > 0$ we take (−11, 1) times −1 to get (11, −1), and then "apply" (649, 180) to this to get $4799 = 11 \cdot 649 + (-1) \cdot 180 \cdot 13$, $1331 = 11 \cdot 180 + (-1) \cdot 649$). Similarly the minimal positive solution equivalent to (−15, 3) is (2715, 753). Continuing this way, and the sorting the final results into increasing order, gives minimal positive solutions for each class of (11, 1), (15, 3), (24, 6), (41, 11), (80, 22), (141, 39), (249, 69), (440, 122), (869, 241), (1536, 426), (2715, 753), and (4799, 1331).

References - Mollin [12], Leveque [8], Rose [18]

Solving $x^2 - Dy^2 = N$ by the LMM algorithm

This algorithm finds exactly one member from each family of solutions to the captioned equation for $N \neq 0$, $D > 0$, D not a square.

Make a list of $f > 0$ so that f^2 divides N. For each f in this list, set $m = N/f^2$. Find all z so that $-|m|/2 < z \leq |m|/2$ and $z^2 \equiv D \pmod{|m|}$. For each such z, apply the PQa algorithm with $P_0 = z$, $Q_0 = |m|$, $D = D$. Continue until either there is an $i \geq 1$ with $Q_i = \pm 1$, or, without having reached an i with $Q_i = \pm 1$, you reach the end of the first period for the sequence a_i. In the latter case, there will not be any i with $Q_i = \pm 1$. If you reached an i with $Q_i = \pm 1$, then look at $r = G_{i-1}$, $s = B_{i-1}$. If $r^2 - Ds^2 = m$, then add $x = fr$, $y = fs$ to the list of solutions. Otherwise, $r^2 - Ds^2 = -m$. If the equation $t^2 - Du^2 = -1$ does not have solutions, test the next z. If the equation $t^2 - Du^2 = -1$ has solutions, let the minimal positive solution be t, u, and add $x = f(rt + sud)$, $y = f(ru + st)$ to the list of solutions. Alternatively, continue the PQa algorithm for one more period, to the next $Q_i = \pm 1$, take $r = G_{i-1}$, $s = B_{i-1}$, and add $x = fr$, $y = fs$ to the list of solutions. Note that $\gcd(r, s) = 1$, so the solution generated to the equation $x^2 - Dy^2 = m$ is primitive (the solution being either r, s, or $(rt + sud)$, $(ru + st)$).

When you have done every f, and every z for each f, the list of solutions will have one member from each class. These solutions will be either fundamental or the minimal positive solution for the class.

To generate all solutions from these, see the section "Structure of solutions to $x^2-Dy^2=N$". Alternatively, for each z that gives rise to solutions, you can extend the PQa algorithm indefinitely.

When $N=\pm 1$ this is the method given in the section "Solving $x^2-Dy^2=\pm 1$," above. When $N=\pm 4$ and $D \equiv 1 \pmod 4$ this method is an alternative to the method presented in the section "Solving $x^2-Dy^2=\pm 4$."

If $|N|$ is large, it may be necessary to have an efficient method to factor N to make the list of f's so that f^2 divides N. The literature on factoring is vast. Many mathematical software packages, such as Maple or PARI, have efficient factoring systems built in. Methods for factoring integers n include trial division up to $\sqrt{n}$, Fermat's method, Pollard's rho method. Pollard's $p-1$ method, using binary quadratic forms, the Brillhart-Morrison continued fraction factoring algorithm, D. Shanks' square-free factorization, Pomerance's quadratic sieve, Pollard's number field sieve, and Lenstra's elliptic curve method. See NZM [14], Crandall and Pomerance [4], Pomerance [16], Bressoud [1], Mollin [12], and many other sources.

Also, if $|N|$ is large, it may be necessary to have an efficient method to solve the equation $x^2 \equiv D \pmod{|m|}$. Cohen [3] gives some methods for solving $x^2 \equiv D \pmod p$ where p is an odd prime. From such solutions, one can readily solve the more general equation $x^2 \equiv D \pmod{|m|}$.

When N is large, the other methods (Lagrange's system of reductions, cyclic method, binary quadratic forms) also require efficient methods to factor integers and to solve $x^2 \equiv D \pmod{|m|}$.

Keith Matthews has a program CALC, available at

www.maths.uq.edu.au/˜krm

that applies this algorithm. Use the function patz(D, N).
He also has an online BCMATH solver available at

www.numbertheory.org/php/php.html.

I call this the LMM algorithm because it has been independently discovered by Lagrange, Matthews, and Mollin. Matthews [10] has extended this algorithm to an efficient algorithm for solving the more general binary quadratic form equations $ax^2+bxy+cy^2=N$, where $D=b^2-4ac>0$ and $N \neq 0$.

As an example, let's solve $x^2-13y^2=108$ using the LMM algorithm. The $f>0$ so that f^2 divides 108 are $f=1, 2, 3, 6$. Start with $f=1$, so

$m = 108$. The solutions to $P_0^2 \equiv 13 \pmod{108}$ are $P_0^2 \equiv \pm 11 \pmod{108}$ and $P_0^2 \equiv \pm 43 \pmod{108}$. The PQa algorithm with $P_0 = 11$, $Q_0 = 108$ and $D = 13$ is shown in Table 2. As $Q_1 = -1$ we look at $G_0^2 - 13B_0^2 = (-11)^2 - 13 \cdot 1^2 = 108$. So start the list of solutions with $(G_0, B_0) = (-11, 1)$. Applying the PQa algorithm with $P_0 = -11$, $Q_0 = 108$ and $D = 13$ gives $Q_2 = 1$, and we add (11, 1) to the list of solutions.

The PQa algorithm with $P_0 = 43$, $Q_0 = 108$ and $D = 13$ is shown in Table 5. Here $Q_3 = 1$, but $G_2^2 - 13B_2^2 = 23^2 - 13 \cdot 7^2 = -108$. As the equation $t^2 - 13u^2 = -1$ has solutions, with the minimal positive solution being $t = 18$, $u = 5$ (Table 3), we add $x = 23 \cdot 18 + 7 \cdot 5 \cdot 13 = 869$, $y = 7 \cdot 18 + 23 \cdot 5 = 241$ to the list of solutions. Note that we also could have read this solution off the line for $i = 7$ in Table 5. Applying the PQa algorithm with $P_0 = -43$, $Q_0 = 108$ and $D = 13$ gives $Q_6 = 1$, and we add (41, 11) to the list of solutions.

For $f = 2$, we have $m = 27$. The solutions to $P_0^2 \equiv 13 \pmod{27}$ are $P_0^2 \equiv \pm 11 \pmod{27}$. Applying the PQa algorithm with $P_0 = 11$, $Q_0 = 27$ and $D = 13$ gives $Q_3 = 1$, and gives (5, 2) as a solution to $x^2 - 13y^2 = -27$. From this we derive the solution (220, 61) to the equation $x^2 - 13y^2 = 27$, and multiply by $f = 2$ to get the solution (440, 122) to the equation $x^2 - 13y^2 = 108$. Continuing in this manner, we get the list of solutions shown in Table 6. Each is either the fundamental solution or the minimal positive solution for its class. Note also that each solution found to an equation $x^2 - 13y^2 = 108/f^2$ has x and y relatively prime.

References - Matthews [11, 10], Mollin [13]

Lagrange's system of reductions

This method can be applied to the equation $x^2 - Dy^2 = N$ when $N^2 > D$. If $N^2 < D$, see the appropriate section above.

The basic observation is that if $x \geq 0$, $y \geq 0$ is a solution to $x^2 - Dy^2 = N$ with $N^2 > D$, then there are $0 \leq k \leq |N|/2$, X, Y so that $h = (k^2 - D)/N$ is an integer, X, Y is a solution to $X^2 - DY^2 = h$, and either $x = |(kX + DY)/h|$, $y = |(kY + X)/h|$ or $x = |(kX - DY)/h|$, $y = |(kY - X)/h|$.

Often, it is necessary to apply this reduction recursively. That is, one starts with an equation $x^2 - Dy^2 = N$, and for each $0 \leq k \leq |N|/2$ with $h = (k^2 - D)/N$ an integer, one gets an equation $X^2 - DY^2 = h$. If $h^2 > D$ then one applies the reduction to this last equation. Continue each branch that may result until you get an equation with $h^2 < D$, which will happen eventually. This is then solved by methods in previous sections. Take one solution from each class. Then track back through the several reductions to get solutions to the original equation. To find a solution to the original equation in each class, solve each equation $x^2 - Dy^2 = N/f^2$ for every $f > 0$ so that N/f^2 is an integer, and take fx, fy as solutions to the original equation.

References - Chrystal [2, pp. 482–485] or Mollin [12, p. 305]

Please send comments to JPR2718@AOL.COM.

References

[1] David M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, NY, 1989. Covers the Pomerance quadratic sieve factoring method, the elliptic curve factoring method, and more. Also gives the PQa algorithm for solving Pell equations $x^2 - Dy^2 = \pm 1$.

[2] G. Chrystal, *Algebra, An Elementary Text-Book* (a.k.a. *Textbook of Algebra*), Part II, Dover, NY, 1961. Other editions include Adam and Charles Black, 1900, and Chelsea, perhaps published in the 1950's, and AMS currently. Chapter XXXII, pages 423 to 452, begins a discussion of continued fractions. Chapter XXXIII, pp. 453 to 490, discusses recurring continued fractions. In Chapter XXXIII, Sections 15 to 17, pages 478 to 481, recurring continued fractions are studied and applied to solve the equations $x^2 - Dy^2 = \pm 1$, and $x^2 - Dy^2 = m$ for $m^2 < D$. Chapter XXXIII, Section 18, pages 482 to 485, discusses Lagrange's method of reduction for the case $m^2 > D$, but apart from the fact that the heading on page 482 is "Lagrange's Chain of Reductions," the section does not reference Lagrange. Section 19, on page 486, discusses the cases $D < 0$ and $D > 0$, D a square. Section 20, pages 486 to 488, reduces the general equation $ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0$ to a Pell equation covered previously. Data for the current AMS edition is: *Algebra, an Elementary Text-Book for the Higher Classes of Secondary Schools and for Colleges*: Seventh Edition - G. Chrystal - AMS — CHEL, 1964, 1212 pp., Hardcover, ISBN 0-8218-1931-3, List: $40, All AMS Members: $36, CHEL/84.H

[3] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993. Section 1.5, pp. 31-36, covers methods to solve $x^2 \equiv D \pmod{p}$, for p prime. Algorithm 5.7.2 in Section 5.7, pages 264

to 274, solves the equation $x^2 - Dy^2 = \pm 4$ when $D \equiv 1 \pmod 4$ for D squarefree, or $D = 4r$ for $r \equiv 2$ or $3 \pmod 4$, r squarefree.

[4] Richard Crandall and Carl Pomerance, *Primes - A Computational Perspective*, Springer-Verlag, New York, 2002. Discusses several methods of factoring, and many other topics related to primes.

[5] Harold M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, NY, 1977. Chapters 7 (pp. 245 to 304) and 8 (pp. 305 to 341), especially sections 8.2 (pp. 313-318) and 8.7 (pp. 339-341) apply the cyclic method to solve equations of the form $ax^2 + bxy + cy^2 + dx + ey + f = 0$.

[6] Adolf Hurwitz, *Lectures on Number Theory*, Springer-Verlag, New York, 1986. Chapter 6 is a wonderful exposition of methods to solve binary quadratic form equations, $Ax^2 + Bxy + Cy^2 = N$. Much theory of simple continued fractions is also developed.

[7] H. W. Lenstra Jr., Solving the Pell equation, *Notices of the American Mathematical Society*, **49** No. 2 (February 2002), pp. 182–192. The equation $x^2 - Dy^2 = \pm 1$ for large D.

[8] William Judson Leveque, *Topics in Number Theory*, Volume 1, Addison-Wesley, New York , 1956. Also, Dover 2002. Chapter 8, sections 1 to 3, pages 137 to 148, discuss the equations $x^2 - Dy^2 = \pm 1$, $x^2 - Dy^2 = \pm 4$, and $x^2 - Dy^2 = N$ for general N. Limits on the size of $|x|$ for fundamental solutions are given in Theorem 8-9, page 147, and in exercise 3, page 148 (the first inequality in this exercise should be $0 \leq u$, not $0 < u$; limits sharper than those given in Theorem 8-9 or exercise 3 are possible).

[9] G. B. Mathews, *Number Theory*, Chelsea, New York. A classic treatment of binary quadratic forms.

[10] Keith Matthews, The diophantine equation $ax^2 + bxy + cy^2 = N$, $D = b^2 - 4ac > 0$, *J. Théor. Nombres Bordeaux*, **14** (2002) 257-270. For additions see http://www.numbertheory.org/papers.html#jntb (which is in "publications" at http://www.maths.uq.edu.au/˜krm/).

[11] Keith Matthews, The diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers, *Expositiones Mathematicae*, **18** (2000), 323-331. Gives the LMM algorithm for solving $x^2 - Dy^2 = N$ for any nonzero N. Available with some additional material at

http://www.numbertheory.org/papers.html#patz, or at the "publications" page at http://www.maths.uq.edu.au/˜krm/.

[12] Richard E. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998. Chapter 5, pp. 221 to 272, discusses the continued fractions generally. In particular, Section 5.3, pages 238 to 250 studies periodic continued fractions, and applies this study to find all solutions to the Pell equation $x^2 - Dy^2 = \pm 1$ for $D > 0$, D not a square. The PQa algorithm for computing the continued fraction expansion of a quadratic irrational is discussed in exercise 5.3.6, p. 251. While the method above for the ± 4 equation is not discussed explicitly, Mollin's Theorem 5.3.4 on page 246 gives the main machinery needed to prove that that method is correct. Mollin also discusses the continued fraction expansion of $(1 + \sqrt{D})/2$ for $D \equiv 1 \pmod 4$ in exercise 5.3.14 on page 252. For the general equation $x^2 - Dy^2 = m$, for any positive nonsquare D and any m, limits to search on x or y are given in Chapter 6 on pages 299 and 300. Theorem 5.2.5 on page 232 gives the main criterion for solving $x^2 - Dy^2 = m$ when $m^2 < D$. Corollary 6.2.1 (page 305) to Theorem 6.2.7 (page 302) gives the essence of Lagrange's system of reduction, which can be used to solve $x^2 - Dy^2 = m$ for $D > 0$, D not a square, $m^2 > D$. Chrystal gives a more complete exposition of Lagrange's system of reduction.

[13] Richard Mollin, Simple Continued Fraction Solutions for Diophantine Equations, *Expositiones Mathematicae*, **19** (2001), pp. 55–73. Gives the LMM algorithm for solving $x^2 - Dy^2 = N$ for any nonzero N.

[14] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery (NZM), *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, Inc., New York, 1991. Sections 7.1 to 7.7, pages 325 to 351 cover continued fractions generally. Section 7.8, pages 351 to 356 covers the Pell ± 1 equation, and the case $x^2 - Dy^2 = n$ where $n^2 < D$. The PQa algorithm for computing the solution to the ± 1 Pell equation is given in Section 7.9, page 358. This is also covered in Section 7.7, pages 346-348. Page 295 has notes on factoring integers.

[15] C. D. Olds, *Continued Fractions*, MAA, 1963. An easy introduction to simple continued fractions, and the Pell equation $x^2 - Dy^2 = \pm 1$. Does not develop the PQa algorithm.

[16] Carl Pomerance, A Tale of Two Sieves, *Notices of the American Mathematical Society*, **43** No. 12, December 1996, pages 1473 to 1485. Dis-

cusses the Pomerance quadratic sieve factoring algorithm and the Pollard number field sieve factoring algorithm. Available as a pdf file at the AMS journals page, www.ams.org/notices/199612/pomerance.pdf.

[17] Andrew M. Rockett and Peter Szüsz, *Continued Fractions*, World Scientific, 1992. Good introduction to continued fractions generally, with treatment of $x^2 - Dy^2 = \pm 1$.

[18] H. E. Rose, *A Course in Number Theory*, Clarendon Press, 1988. Chapter 7, section 3, pages 125 to 128 treats the equation $x^2 - Dy^2 = \pm 1$. Theorem 3.3, page 128, gives limits on $|x|$ for a fundamental solution to the general case $x^2 - Dy^2 = m$ (although the first inequality has to be changed from $0 < u$ to $0 \leq u$).

[19] H. C. Williams, Solving the Pell equation, in Bruce Berndt et al., *Surveys in Number Theory: Papers from the Millennial Conference on Number Theory*, A. K. Peters, 2002. Also included in *Number Theory for the Millennium*, Volumes 1, 2, 3, M. A. Bennett et al. editors, A. K. Peters, 2002. Williams' web page gives this last reference as H. C. Williams, Solving the Pell equation, *Proc. Millennial Conference on Number Theory*, A. K. Peters, Natick MA, 2002, pp. 397-435. Discusses the equation $x^2 - Dy^2 = \pm 1$. Terrific overview, including discussion when D is large.

The PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	-11	
-1				1	0	108	
0	11	108	0	0	1	-11	108
1	-11	-1	7	1	7	31	324
2	4	3	2	2	15	51	-324
3	2	3	1	3	22	82	432
4	1	4	1	5	37	133	-108
5	3	1	6	33	244	880	432
6	3	4	1	38	281	1013	-324
7	1	3	1	71	525	1893	324
8	2	3	1	109	806	2906	-432
9	1	4	1	180	1331	4799	108
10	3	1	6	1189	8792	31700	-432
11	3	4	1	1369	10123	36499	324
12	1	3	1	2558	18915	68199	-324
13	2	3	1	3927	29038	104698	432
14	1	4	1	6485	47953	172897	-108
15	3	1	6	42837	316756	1142080	432
16	3	4	1	49322	364709	1314977	-324

Table 2: PQa algorithm for $P_0 = 11$, $Q_0 = 108$, and $D = 13$.

Solving $x^2 - 13y^2 = \pm 1$

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	0	0
-1				1	0	1	1
0	0	1	3	3	1	3	-4
1	3	4	1	4	1	4	3
2	1	3	1	7	2	7	-3
3	2	3	1	11	3	11	4
4	1	4	1	18	5	18	-1
5	3	1	6	119	33	119	4
6	3	4	1	137	38	137	-3
7	1	3	1	256	71	256	3
8	2	3	1	393	109	393	-4
9	1	4	1	649	180	649	1
10	3	1	6	4287	1189	4287	-4
11	3	4	1	4936	1369	4936	3
12	1	3	1	9223	2558	9223	-3
13	2	3	1	14159	3927	14159	4
14	1	4	1	23382	6485	23382	-1
15	3	1	6	154451	42837	154451	4
16	3	4	1	177833	49322	177833	-3
17	1	3	1	332284	92159	332284	3
18	2	3	1	510117	141481	510117	-4
19	1	4	1	842401	233640	842401	1
20	3	1	6	5564523	1543321	5564523	-4

Table 3: PQa algorithm for $P_0 = 0$, $Q_0 = 1$, and $D = 13$.

Solving $x^2 - 13y^2 = \pm 4$

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	-1	0
-1				1	0	2	4
0	1	2	2	2	1	3	-4
1	3	2	3	7	3	11	4
2	3	2	3	23	10	36	-4
3	3	2	3	76	33	119	4
4	3	2	3	251	109	393	-4
5	3	2	3	829	360	1298	4
6	3	2	3	2738	1189	4287	-4
7	3	2	3	9043	3927	14159	4
8	3	2	3	29867	12970	46764	-4
9	3	2	3	98644	42837	154451	4
10	3	2	3	325799	141481	510117	-4
11	3	2	3	1076041	467280	1684802	4
12	3	2	3	3553922	1543321	5564523	-4
13	3	2	3	11737807	5097243	18378371	4
14	3	2	3	38767343	16835050	60699636	-4

Table 4: PQa algorithm for $P_0 = 1$, $Q_0 = 2$, and $D = 13$.

One Step in the LMM Solution of $x^2 - 13y^2 = 108$

i	P_i	Q_i	a_i	A_i	B_i	G_i	$G_i^2 - DB_i^2$
-2				0	1	-43	
-1				1	0	108	
0	43	108	0	0	1	-43	1836
1	-43	-17	2	1	2	22	432
2	9	4	3	3	7	23	-108
3	3	1	6	19	44	160	432
4	3	4	1	22	51	183	-324
5	1	3	1	41	95	343	324
6	2	3	1	63	146	526	-432
7	1	4	1	104	241	869	108
8	3	1	6	687	1592	5740	-432

Table 5: PQa algorithm for $P_0 = 43$, $Q_0 = 108$, and $D = 13$.

The LMM Algorithm

f	P_0	Q_0	x	y
1	11	108	-11	1
1	-11	108	11	1
1	43	108	869	241
1	-43	108	41	11
2	11	27	440	122
2	-11	27	80	22
3	1	12	141	39
3	-1	12	249	69
3	5	12	-15	3
3	-5	12	15	3
6	1	3	1536	426
6	-1	3	24	6

Table 6: Results of LMM algorithm for $x^2 - 13y^2 = 108$.