Matthews' Method for Solving $ax^2 + bxy + cy^2 = N$

Introduction

This algorithm finds solutions, or reports there are none, to

$$ax^2 + bxy + cy^2 = N \tag{1}$$

in integers x and y when $\Delta = b^2 - 4ac > 0$ is not square and $N \neq 0$.

This discussion is based on Matthews [9]. The method is an extension of the LMM method presented in [10, 12] for solving the generalized Pell equation $x^2 - Dy^2 = N$ for $D > 0$ not a square and $N \neq 0$. This method is more efficient than the traditional approach of solving binary quadratic form equations by using methods of reduced forms (presented, for instance, in [7, 8, 3, 4, 1]). For a somewhat different spin on the traditional method, see [1]. And, of course, the first complete solution was given in [5]. Many of the references cited in [9] may also be of interest.

Keith Matthews' program CALC, available at

http://www.maths.uq.edu.au/~krm/,

has a routine "binform" that implements the method discussed here. Also of note in CALC is the routine "sqroot," which solves $x^2 \equiv n \pmod{m}$ intelligently.

We assume that $\gcd(a, b, c) = 1$. If not, let $g = \gcd(a, b, c)$ and replace a with a/g, b with b/g, c with c/g, and N with N/g. (If g does not divide N, there are no solutions, and we're done.)

We say N is *represented* or *integrally represented* by the form $f = (a, b, c) = f(x, y) = ax^2 + bxy + cy^2$ if there are integers x, y so that $ax^2 + bxy + cy^2 = N$. This representation is *primitive* if $\gcd(x, y) = 1$ and *imprimitive* if $\gcd(x, y) > 1$.

Equivalent solutions

If (x, y) is a solution to (1) and (t, u) is any solution to $t^2 - \Delta u^2 = 4$, then (x', y') is also a solution to (1) where x' and y' are defined by

$$x' = \left(\frac{t - bu}{2}\right) x - cuy, \quad y' = aux + \left(\frac{t + bu}{2}\right) y \tag{2}$$

which is equivalent to

$$2ax' + by' + y'\sqrt{\Delta} = \left(\frac{t + u\sqrt{\Delta}}{2}\right)(2ax + by + y\sqrt{\Delta}).$$

The two solutions (x, y), (x', y') are said to be *equivalent*. It is not difficult to verify that this defines an equivalence relation.

An equivalent, but often easier, test is that two solutions (x, y), (x', y') are equivalent if and only if

$$2axx' + b(xy' + x'y) + 2cyy' \equiv 0 \pmod{|N|}, \text{ and}$$

$$xy' - x'y \equiv 0 \pmod{|N|}.$$

As all solutions (t, u) to $t^2 - \Delta u^2 = 4$ are generated from the solution (t_1, u_1) with the minimum positive t_1 and u_1 by

$$\frac{t + u\sqrt{\Delta}}{2} = (\pm 1)\left(\frac{t_1 + u_1\sqrt{\Delta}}{2}\right)^n$$

for some integer n (positive, zero, or negative), it is easy, using (2), to generate all solutions to (1) equivalent to a given solution.

There are a finite number of equivalence classes of solutions (possibly zero). See [9] for more on the structure of solutions.

Transform to equation with $\gcd(a, N) = 1$

If $\gcd(a, N) = 1$, skip to the next section. If $\gcd(a, N) \neq 1$, then use a *unimodular transformation* to transform (a, b, c) into a form with $\gcd(a, N) = 1$. A unimodular transformation, often represented by a matrix

$$T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{3}$$

with $\det(T) = \pm 1$, is a transformation of $f = (a,\ b,\ c) = f(x,y) = ax^2 + bxy + cy^2$ to $g = (A,\ B,\ C) = g(X,Y) = AX^2 + BXY + CY^2$ where

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix},$$

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2,$$

$$B = 2a\alpha\beta + b\alpha\delta + b\beta\gamma + 2c\gamma\delta, \text{ and}$$

$$C = a\beta^2 + b\beta\delta + c\delta^2.$$

This transformation is invertible (just use transformation associated with the inverse of the matrix in (3)). Any integral representation of N by f corresponds to an integral representation of N by g, and vice-versa. In particular, the two forms f and g represent the same integers.

To find such a transformation, first we find a pair α, γ so that $\gcd(\alpha,\gamma) = 1$, and when $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$, then $\gcd(A,N) = 1$. We will discuss ways to find such α, γ shortly. Given α, γ, find β and δ so that $\alpha\delta - \gamma\beta = 1$. The unimodular transformation $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ transforms $ax^2 + bxy + cy^2$ into $AX^2 + BXY + CY^2$ as above.

Hua [6, pp. 311-312] presents the following method for finding α, γ. Let $\{q_i\}_{i=1\ldots k}$ be the set of primes that divide N. For each q_i we will find x_i and y_i so that $ax_i^2 + bx_iy_i + cy_i^2$ is relatively prime to q_i. If $\gcd(a,q_i) = 1$, then take $x_i = 1$, $y_i = 0$. Otherwise, if $\gcd(c,q_i) = 1$, then take $x_i = 0$, $y_i = 1$. If both $\gcd(a,q_i) \neq 1$ and $\gcd(c,q_i) \neq 1$, then $\gcd(b,q_i) = 1$, so take $x_i = 1$, $y_i = 1$. Now use the Chinese Remainder Theorem to find X so that $X \equiv x_i \pmod{q_i}$ for all i, and again to find Y so that $Y \equiv y_i \pmod{q_i}$ for all i. Then $aX^2 + bXY + cY^2$ is relatively prime to all of the q_i, and hence is relatively prime to N. Set $\alpha = X/\gcd(X,Y)$ and $\gamma = Y/\gcd(X,Y)$, and $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$. Then $\gcd(\alpha,\gamma) = 1$ and $\gcd(A,N) = 1$.

Alternatively, simply search on "small" α, γ with $\gcd(\alpha,\gamma) = 1$, set $A = a\alpha^2 + b\alpha\gamma + c\gamma^2$, and test whether $\gcd(A,N) = 1$. This method frequently finds α, γ very quickly and gives a transformed equation with smaller coefficients than those resulting from the method presented by Hua.

For a third method, see [1, p. 50]. For a method similar to that given by Hua, but more general, see [5, pp. 220-221].

Unimodular transformations preserve equivalence of solutions.

Main algorithm

Henceforth we assume that $\gcd(a, N) = 1$.

First, find all solutions θ to

$$a\theta^2 + b\theta + c \equiv 0 \pmod{|N|} \tag{4}$$

with $0 \le \theta < |N|$. If $|N|$ is small, you can do a brute-force search on θ for $0 \le \theta < |N|$. For large $|N|$ you can take advantage of efficient methods for solving $x^2 \equiv d \pmod{m}$ [2, pp. 31-36] [7] as follows. First solve $t^2 \equiv b^2 - 4ac \pmod{4|N|}$ for $-|N| < t \le |N|$. If there are no solutions t, then there are no primitive solutions to (1). Then solve $a\theta \equiv \frac{t-b}{2} \pmod{|N|}$ for $0 \le \theta < |N|$.

For each θ proceed as follows depending on whether $\Delta = b^2 - 4ac$ is even, odd, or $\Delta = 5$. Let $n = 2a\theta + b$, $R = \lfloor n/2 \rfloor$, $S = a|N|$.

If Δ is even, apply the PQa algorithm (see appendix) to $\omega = (-R + \sqrt{\Delta/4})/S$, i.e., apply the PQa algorithm with $P_0 = -R$, $Q_0 = S$, $D = \Delta/4$. Let ℓ be the length of the period of the continued fraction expansion of ω. If ℓ is even check through the end of the first period, and if ℓ is odd, check through the end of the second period for the smallest $j \ge 1$ with $Q_j = (-1)^j N/|N|$. If there is no such j, there is no solution associated with this θ. If there is such a j, then $y = B_{j-1}$, $x = y\theta + A_{j-1}|N|$ is a solution.

If we found a solution using ω, also apply the PQa algorithm to $\omega^* = (R + \sqrt{\Delta/4})/(-S)$, i.e., apply the PQa algorithm with $P_0 = R$, $Q_0 = -S$, $D = \Delta/4$. Apply the tests in the previous paragraph to this continued fraction expansion, except test for $Q_j = (-1)^{j+1} N/|N|$.

For a given θ, either both ω and ω^* will generate solutions, or neither will. When both generate solutions, the solutions are equivalent. Also, for any solution found, $y > 0$. If one of these solutions has a y that is less than that for the other solution, retain the solution with the smaller y and discard the other. If two solutions have the same y, keep the one with the smaller $|x|$.

Solutions arising from different θ are not equivalent. So once all θ have been tested, and solutions retained as above, you will have exactly one solution from each class, and it will be a solution with the minimal positive y.

If Δ is odd (including the case where $\Delta = 5$), apply the PQa algorithm to $\omega = (-(2R + 1) + \sqrt{\Delta})/(2S)$, i.e., apply the PQa algorithm with $P_0 = -(2R + 1)$, $Q_0 = 2S$, $D = \Delta$. Let ℓ be the length of the period of the continued fraction expansion of ω. If ℓ is even check through the end of the

first period, and if ℓ is odd, check through the end of the second period for the smallest $j \geq 1$ with $Q_j = 2(-1)^j N/|N|$. If there is no such j, there is no solution associated with this θ, P_0, and Q_0. If there is such a j, then $y = B_{j-1}$, $x = y\theta + A_{j-1}|N|$ is a solution.

If $\Delta = 5$ and $aN < 0$ then let r be the minimal nonnegative integer so that $P_{r+1+\ell} = P_{r+1}$ and $Q_{r+1+\ell} = Q_{r+1}$. Let $X = A_r - A_{r-1}$, $y = B_r - B_{r-1}$, $x = y\theta + |N|X$. Then (x, y) is a solution. Call this the "special" test, call the solution found in this paragraph the "special" solution, and call those solutions found in other paragraphs "regular" solutions.

If ω generated a solution, apply the PQa algorithm to $\omega^* = ((2R+1) + \sqrt{\Delta})/(-2S)$, i.e., apply the PQa algorithm with $P_0 = 2R+1$, $Q_0 = -2S$, $D = \Delta$. Apply the test in the second previous paragraph to this continued fraction expansion, except test for $Q_j = 2(-1)^{j+1}N/|N|$. It is not necessary to apply the analogy of the "special" test when $\Delta = 5$ to ω^*, as it would give the same solution as that found above.

As with the case when Δ is even, for a given θ, either both ω and ω^* will generate solutions, or neither will. When both generate solutions, the solutions are equivalent. When the "special" test applies, a third solution will be found, equivalent to the first two. Again, for any solution found, $y > 0$. If one of these solutions has a y that is less than that for the other solution, retain the solution with the smaller (or smallest) y and discard the other(s). If two solutions have the same y, keep the one with the smaller $|x|$ (not all three can have the same y).

As with the case when Δ is even, solutions arising from different θ's are not equivalent. So once all θ's have been tested, and solutions retained as above, you will have exactly one solution from each class, and it will be a solution with the minimal positive y.

All solutions found by this method are primitive, i.e., they have $\gcd(x, y) = 1$. To find imprimitive solutions, apply the above methods to every equation $ax^2+bxy+cy^2 = N/k^2$, where $k > 0$ divides N, and take (kx, ky) as solutions to the original equation.

For some Δ, including $\Delta = 5$, every N and θ satisfying (4) generate a solution to (1). But for some Δ, there are N and θ that satisfy (4) but θ does not generate a solution to (1).

Examples

Example 1, $x^2 + 2xy - 7y^2 = -56$.

Here $\Delta = 32$. The solutions to $\theta^2 + 2\theta - 7 \equiv 0 \pmod{56}$ are $\theta = 7$, 19, 35, 47. For $\theta = 7$ we get $n = 16$, $R = 8$, $S = 56$, $\omega = (-8 + \sqrt{8})/56$, and $\omega^* = (8 + \sqrt{8})/(-56)$. The PQa algorithm with $P_0 = -8$, $Q_0 = 56$, and $D = 8$ is shown in Table 1. As $N = -56$, and so $N/|N| = -1$, we look for Q_i so that $Q_i = (-1)^i(-1) = (-1)^{i+1}$. Clearly there are none, so no solutions arise from this θ (and we do not need to test ω^*).

For $\theta = 19$ we have $n = 40$, $R = 20$, $S = 56$, $\omega = (-20 + \sqrt{8})/56$, and $\omega^* = (20 + \sqrt{8})/(-56)$. Applying the PQa algorithm to ω, the smallest $i > 0$ with $Q_i = (-1)^{i+1}$ is $i = 3$ (Table 2). As $A_2 = -1$ and $B_2 = 3$, a solution is $y = 3$, $x = 3 \cdot 19 + (-1) \cdot |-56| = 1$. Applying the PQa algorithm to ω^* (Table 3), the smallest $i > 0$ with $Q_i = (-1)^{i+1}(-1) = (-1)^i$ is $i = 4$. As $A_2 = -2$ and $B_2 = 5$, a solution is $y = 5$, $x = 5 \cdot 19 + (-2) \cdot |-56| = -17$. As $3 < 5$, we retain the solution $(1, 3)$ and discard the solution $(-17, 5)$.

For $\theta = 35$, ω gives the solution $(7, 5)$, and ω^* gives the solution $(-7, 3)$. We keep the latter and discard the former. When $\theta = 47$, no solutions result.

So, for $x^2 + 2xy - 7y^2 = -56$, there are two classes for the primitive solutions. The solutions $(1, 3)$, $(-7, 3)$ give the solution from each class of primitive solutions with minimal positive y. Note that one of these solutions was generated from an "ω" and one from an "ω^*". Also, two of the θ's did not yield solutions.

As the only $k > 1$ so that $k^2|N$ is $k = 2$, to look for imprimitive solutions we solve $x^2 + 2xy - 7y^2 = -56/4 = -14$. There are two θ's, $\theta = 5$, 7. Neither yields solutions. So the only solutions to $x^2 + 2xy - 7y^2 = -56$ are the primitive solutions.

Example 2, $29x^2 + xy - y^2 = -27$.

Here $\Delta = 117$. The solutions to $29\theta^2 + \theta - 1 \equiv 0 \pmod{27}$ are $\theta = 5$, 8, 14, 17, 23, 26. For $\theta = 5$, we have $n = 291$, $R = 145$, $S = 783$, $\omega = (-291 + \sqrt{117})/1566$, $\omega^* = (291 + \sqrt{117})/(-1566)$. Application of the PQa algorithm to ω is shown in Table 4. There is no $Q_i = \pm 2$, so this θ does not produce a solution. As ω does not yield a solution, there is no need to test ω^*. Similarly $\theta = 8$, 14, or 26 do not yield solutions.

For $\theta = 17$, $\omega = (-987 + \sqrt{117})/1566$, $\omega^* = (987 + \sqrt{117})/(-1566)$. Applying the PQa algorithm to ω (Table 5), the smallest i with $Q_i = 2(-1)^i(-27)/27 = 2(-1)^{i+1}$ is $i = 5$. Then $A_4 = -5$, $B_4 = 8$, so a solution is $y = 8$, $x = 8 \cdot 17 - 5 \cdot 27 = 1$. Applying the PQa algorithm to ω^* (Table 6), the smallest i with $Q_i = 2(-1)^{i+1}(-27)/27 = 2(-1)^i$ is $i = 4$. Then $A_4 = -7$, $B_4 = 11$, so a solution is $y = 11$, $x = 11 \cdot 17 - 7 \cdot 27 = -2$. We retain the solution $(1, 8)$ and discard the solution $(-2, 11)$.

For $\theta = 23$, $\omega = (-1335 + \sqrt{117})/1566$, $\omega^* = (1335 + \sqrt{117})/(-1566)$. From ω we get the solution $(2, 13)$ and from ω^* we get the solution $(-1, 7)$. We retain the latter and discard the former. This gives us the primitive solutions. As with the first example, one solution has come from an "ω", one solution has come from an "ω^*", and not all θ's led to solutions.

As $3^2|(-27)$, to test for imprimitive solutions we solve $29x^2 + xy - y^2 = -27/9 = -3$. There is one θ, $\theta = 2$, and this yields no solutions. So, the only solutions are the primitive ones.

Example 3, $5x^2 + 15xy + 11y^2 = -19$

Here $\Delta = 5$. The solutions to $5\theta^2 + 15\theta + 11 \equiv 0 \pmod{19}$ are $\theta = 7$, 9. For $\theta = 7$, $n = 85$, $R = 42$, $S = 95$, $\omega = (-85 + \sqrt{5})/190$, $\omega^* = (85 + \sqrt{5})/(-190)$. The application of the PQa algorithm to ω is shown in Table 7. The smallest i with $Q_i = 2(-1)^i(-19)/19 = 2(-1)^{i+1}$ is $i = 5$. A solution is $y = 16$, $x = 16 \cdot 7 - 7 \cdot 19 = -21$. As $aN = 5 \cdot -19 < 0$, we use the "special" test to get another solution from ω. The smallest r so that $P_{r+1+\ell} = P_{r+1}$ and $Q_{r+1+\ell} = Q_{r+1}$ is $r = 4$. This gives $X = (-7) - (-3) = -4$, $y = 16 - 7 = 9$, $x = 9 \cdot 7 + 19 \cdot (-4) = -13$. From ω^* (PQa algorithm shown in Table 8) the smallest i with $Q_i = 2(-1)^{i+1}(-19)/19 = 2(-1)^i$ is $i = 4$. A solution is $y = 11$, $x = 11 \cdot 7 - 5 \cdot 19 = -18$. Note that for ω^*, in the notation of [9], $s = 5$, $X = (-5) - (-1) = -4$, $y = 11 - 2 = 9$, and, as above, $x = -13$. So, we have three solutions $(x, y) = (-21, 16)$, $(-13, 9)$, $(-18, 11)$. These three solutions are equivalent, and the one with the smallest y is $(x, y) = (-13, 9)$, which came from the "special" test for ω.

For $\theta = 9$, the "regular" test with ω gives the solution $(-15, 11)$, the "special" test with ω gives the solution $(-14, 9)$, and the "regular" test with ω^* gives the solution $(-27, 16)$. These three solutions are equivalent, and that with the smallest y is $(-14, 9)$.

The solution from the "special" calculation always has minimal y.

Example 4, $x^2 + 7xy + 11y^2 = -1$

Here $\Delta = 5$. The only θ is $\theta = 0$. From $\omega = (-7 + \sqrt{5})/2$ we get the solution $(-3, 1)$ by the "regular" method, and the solution $(-4, 1)$ from the "special" test when $\Delta = 5$ and $aN < 0$. From $\omega^* = (7 + \sqrt{5})/(-2)$ we get the solution $(-9, 2)$. While the solution from the "special" test always has y equal to the minimum positive y in the class when $\Delta = 5$ and $aN < 0$, this shows that it is possible for the "regular" test to produce a solution with the minimal y for the class. This can only happen if $aN = -1$, whence the "regular" solution from $\omega = (-b + \sqrt{5})/2$ is $((-b + 1)/2, 1)$, the "special" solution is $((-b - 1)/2, 1)$, and the solution from $\omega^* = (b + \sqrt{5})/(-2)$ is $(-b - 2, 2)$.

Example 5, $55x^2 + 315xy + 451y^2 = -3971$

This example illustrates every technique presented.

As $\gcd(55, -3971) = 11 > 1$, we first need to transform the equation. As $\gcd(451, -3971) = 11 > 1$, we cannot just switch the roles of x and y. So we use the unimodular transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

i.e., $x = X - Y$, $y = X$, to get $A = 55 \cdot 1^2 + 315 \cdot 1 \cdot 1 + 451 \cdot 1^2 = 821$, $B = 2 \cdot 55 \cdot 1 \cdot -1 + 315 \cdot 1 \cdot 0 + 315 \cdot -1 \cdot 1 + 2 \cdot 451 \cdot 1 \cdot 0 = -110 - 315 = -425$, and $C = 55 \cdot 1^2 + 315 \cdot 1 \cdot 0 + 451 \cdot 0^2 = 55$. Our original equation is then transformed to $821X^2 - 425XY + 55Y^2 = -3971$. Now, $\gcd(821, -3971) = 1$, so we can use the main methods to solve this equation. Now note that $3971 = 11 \cdot 19^2$, so, in addition to finding primitive solutions to $821X^2 - 425XY + 55Y^2 = -3971$, we will also need to find the primitive solutions to $821X^2 - 425XY + 55Y^2 = -11$.

There are four θ's so that $821\theta^2 - 425\theta + 55 \equiv 0 \pmod{3971}$, namely $\theta = 287$, 793, 2453, 2959. These are shown, along with the solutions they generate in Table 9.

As $19^2 | (-3971)$, to find imprimitive solutions we also solve the equation $821X^2 - 425XY + 55Y^2 = -3971/19^2 = -11$. There are two θ's, $\theta = 0$, 1, and these generate the solutions $(X, Y) = (22, 85)$, $(23, 89)$. Multiplying by 19, we get imprimitive solutions to $821X^2 - 425XY + 55Y^2 = -3971$ of $(418, 1615)$, $(437, 1691)$.

We apply our unimodular transformation to obtain solutions to the original equation, as shown in Table 10.

Send comments to John Robertson at jpr2718@aol.com.

References

[1] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer–Verlag, New York, 1989. As the title says, including solution of binary quadratic form equations. The standard method is summarized in Theorem 4.4 on page 53. The forms listed on the last line of this page are not necessarily distinct. A somewhat different approach is summarized in Theorems 4.26 and 4.27 on page 75.

[2] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer–Verlag, New York, 1992. Section 1.5, pp. 31-36, covers fast methods to solve $x^2 \equiv D \pmod{p}$, for p prime.

[3] Alain Faisant, *L'equation diophantienne du second degré*, Hermann, Paris, 1991.

[4] Alain Faisant, Résolution de l'équation du second degré en nombres entiers, *Séminaire d'analyse (Clermont-Ferrand, France) 1987-88 (Clermont-Ferrand II)*, 1990, exposé no. 23, L'Université Clermont-Ferrand.

[5] Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, English edition, translated by Arthur A. Clarke, revised by William C. Waterhouse, Springer–Verlag, New York, 1986. A classic.

[6] Hua, Loo Keng, *Introduction to Number Theory*, translated by Peter Shiu, Springer–Verlag, New York, 1982. Pages 311–312 give the method to find A with $\gcd(A, N) = 1$. Chapters 12 and 13 develop the theory of binary quadratic forms.

[7] Adolf Hurwitz, *Lectures on Number Theory*, Springer–Verlag, New York, 1986. Chapter 5, especially §32 to §36 is a discussion of the solutions of $x^2 \equiv a \pmod{m}$. Chapter 6 is a good exposition of of standard reduction methods to solve binary quadratic form equations, $Ax^2+Bxy+Cy^2 = N$. Much theory of simple continued fractions is also developed.

[8] G. B. Mathews, *Theory of Numbers*, Chelsea, New York, not dated. Chapters III to VI discuss the theory of binary quadratic forms.

[9] Keith Matthews, The diophantine equation $ax^2 + bxy + cy^2 = N$, $D = b^2 - 4ac > 0$, *J. Théor. Nombres Bordeaux*, **14** (2002) 257-270. Develops the method presented here. For additions see http://www.numbertheory.org/papers.html#jntb.

[10] 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.

[11] 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 the PQa algorithm for computing the continued fraction expansion of a quadratic irrational is discussed in exercise 5.3.6, p. 251.

[12] Richard E. 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.

[13] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *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. 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.

[14] Andrew M. Rockett and Peter Szüsz, *Continued Fractions*, World Scientific, 1992. Good introduction to continued fractions generally, including the PQa algorithm.

Appendix: The PQa algorithm

This algorithm 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 $Q_0 \neq 0$, $D > 0$, D is not a square, and $P_0^2 \equiv D \pmod{|Q_0|}$. Set $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, and $B_{-1} = 0$. For $i \geq 0$ set

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

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

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

and for $i \geq 1$ set

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

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

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 $(P_0 + \sqrt{D})/Q_0$. 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. 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 $k > 0$, $a_{i+k\ell} = a_i$, $P_{i+k\ell} = P_i$, and $Q_{i+k\ell} = Q_i$.

3. $\gcd(A_i, B_i) = 1$ for $i \geq -2$.

4. The ratios A_i/B_i are the convergents to the continued fraction expansion of $(P_0 + \sqrt{D})/Q_0$.

5. $A_i B_{i-1} - A_{i-1} B_i = (-1)^{i-1}$ for $i \geq -1$.

6. $P_i^2 \equiv D \pmod{|Q_i|}$.

7. $Q_i = Q_{i-2} - a_{i-1}(P_i - P_{i-1})$ for $i \geq 2$.

8. $\gcd(Q_0, B_i)$ divides Q_{i+1} for $i \geq -1$.

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*, which means that $(P_i + \sqrt{D})/Q_i > 1$ and $-1 < (P_i - \sqrt{D})/Q_i < 0$. 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.

Examples are given in many of the tables below. A more complete discussion of the PQa algorithm is at the web page

http://hometown.aol.com/jpr2718/

Look for the file, "Solving the generalized Pell equation - PDF File." Also, continued fractions in general and the PQa algorithm in particular are discussed in many texts, so we will refer the interested reader to [13, 11, 14] for justification of most of the assertions made above.

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	-8	56	-1	-1	1
1	-48	-41	1	0	1
2	7	1	9	-1	10
3	2	4	1	-1	11
4	2	1	4	-5	54
5	2	4	1	-6	65
6	2	1	4	-29	314

Table 1: PQa Algorithm with $P_0 = -8$, $Q_0 = 56$, $D = 8$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	-20	56	-1	-1	1
1	-36	-23	1	0	1
2	13	7	2	-1	3
3	1	1	3	-3	10
4	2	4	1	-4	13
5	2	1	4	-19	62
6	2	4	1	-23	75
7	2	1	4	-111	362

Table 2: PQa Algorithm with $P_0 = -20$, $Q_0 = 56$, $D = 8$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	20	-56	-1	-1	1
1	36	23	1	0	1
2	-13	-7	1	-1	2
3	6	4	2	-2	5
4	2	1	4	-9	22
5	2	4	1	-11	27
6	2	1	4	-53	130
7	2	4	1	-64	157

Table 3: PQa Algorithm with $P_0 = 20$, $Q_0 = -56$, $D = 8$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	-291	1566	-1	-1	1
1	-1275	-1038	1	0	1
2	237	54	4	-1	5
3	-21	-6	1	-1	6
4	15	18	1	-2	11
5	3	6	2	-5	28
6	9	6	3	-17	95
7	9	6	3	-56	313

Table 4: PQa Algorithm with $P_0 = -291$, $Q_0 = 1566$, $D = 117$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	-987	1566	-1	-1	1
1	-579	-214	2	-1	2
2	151	106	1	-2	3
3	-45	-18	1	-3	5
4	27	34	1	-5	8
5	7	2	8	-43	69
6	9	18	1	-48	77
7	9	2	9	-475	762
8	9	18	1	-523	839
9	9	2	9	-5182	8313

Table 5: PQa Algorithm with $P_0 = -987$, $Q_0 = 1566$, $D = 117$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	987	-1566	-1	-1	1
1	579	214	2	-1	2
2	-151	-106	1	-2	3
3	45	18	3	-7	11
4	9	2	9	-65	102
5	9	18	1	-72	113
6	9	2	9	-713	1119
7	9	18	1	-785	1232

Table 6: PQa Algorithm with $P_0 = 987$, $Q_0 = -1566$, $D = 117$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	-85	190	-1	-1	1
1	-105	-58	1	0	1
2	47	38	1	-1	2
3	-9	-2	3	-3	7
4	3	2	2	-7	16
5	1	2	1	-10	23
6	1	2	1	-17	39

Table 7: PQa Algorithm with $P_0 = -85$, $Q_0 = 190$, $D = 5$

PQa Algorithm

i	P_i	Q_i	a_i	A_i	B_i
-2				0	1
-1				1	0
0	85	-190	-1	-1	1
1	105	58	1	0	1
2	-47	-38	1	-1	2
3	9	2	5	-5	11
4	1	2	1	-6	13
5	1	2	1	-11	24

Table 8: PQa Algorithm with $P_0 = 85$, $Q_0 = -190$, $D = 5$

Solutions

θ	ω	X	y	x
287	$(-470829+\sqrt{5})/6520382$	-119	1648	427
793	$(-1301681+\sqrt{5})/6520382$	-326	1633	423
2453	$(-4027401+\sqrt{5})/6520382$	-1105	1789	462
2959	$(-4858253+\sqrt{5})/6520382$	-1327	1781	462

Table 9: Solutions to $821x^2 - 425xy + 55y^2 = -3971$

Solutions to equations
$g(X,Y) = -3971, \qquad f(x,y) = -3971$

X	Y	x	y
427	1648	-1221	427
423	1633	-1210	423
462	1789	-1327	462
462	1781	-1319	462
418	1615	-1197	418
437	1691	-1254	437

Table 10: Solutions to
$g(X,Y) = 821X^2 - 425XY + 55Yy^2 = -3971,$
$f(x,y) = 55x^2 + 315xy + 451y^2 = -3971.$