USING SHANKS' BABY-STEP GIANT-STEP METHOD TO SOLVE THE GENERALIZED PELL EQUATION $x^2 - Dy^2 = N$

ABSTRACT. For $D > 0$ not a square, and $N \neq 0$, the continued fraction algorithm can be used to solve the generalized Pell equation $x^2 - Dy^2 = N$ in time $O(D^{1/2+\epsilon})$. Shanks' baby-step giant-step algorithm reduces this to $O(D^{1/4+\epsilon})$. We give an explicit algorithm using Shanks' baby-step giant-step algorithm to solve the generalized Pell equation, and we give some detailed examples.

1. INTRODUCTION

Without giving the full technical details, this section outlines the reason the baby-step giant-step method is computationally more efficient than the continued fraction algorithm for large D.

The continued fraction algorithm is at the heart of many methods, the LMM method [3, 4, 5] in particular, for solving general Pell equations $x^2 - Dy^2 = N$. The continued fraction algorithm takes a quadratic irrational $(P_0 + \sqrt{D})/Q_0$ that satisfies $P_0^2 \equiv D \pmod{|Q_0|}$ as input and produces a sequence $(P_i + \sqrt{D})/Q_i$ from the simple formulas

$$a_i = \left\lfloor \frac{P_i + \sqrt{D}}{Q_i} \right\rfloor, \tag{1}$$

$$P_{i+1} = a_i\, Q_i - P_i, \tag{2}$$

$$Q_{i+1} = \frac{D - P_{i+1}^2}{Q_i}. \tag{3}$$

Because

$$Q_0 \prod_{i=1}^{n+1} \frac{P_i + \sqrt{D}}{Q_{i-1}} = G_n + B_n \sqrt{D}$$

and

$$G_n^2 - DB_n^2 = (-1)^{n+1} Q_0 Q_{n+1},$$

the continued fraction algorithm gives what's needed to solve generalized Pell equations—take $Q_0 = |N|$, find a suitable P_0, and iterate until a $Q_{n+1} = 1$ occurs. Here $G_{-2} = -P_0$, $G_{-1} = Q_0$, $G_i = a_i G_{i-1} + G_{i-2}$ for $i \geq 0$, $B_{-2} = 1$, $B_{-1} = 0$, and $B_i = a_i B_{i-1} + B_{i-2}$ for $i \geq 0$.

In Shanks' baby-step giant-step method, a baby step is essentially one iteration of the continued fraction algorithm, i.e., a baby step corresponds to deriving $(P_{i+1} + \sqrt{D})/Q_{i+1}$ from $(P_i + \sqrt{D})/Q_i$.

A giant step lets you derive $(P_{i+k} + \sqrt{D})/Q_{i+k}$ and

$$\prod_{j=i+1}^{i+k} \frac{P_j + \sqrt{D}}{Q_{j-1}}$$

for some $k > 1$ from $(P_i + \sqrt{D})/Q_i$ by more-or-less doing one ideal multiplication instead of doing k iterations of the continued fraction algorithm. Here k generally varies from one giant step to another, but that's OK. As we present the baby-step giant-step method, k will be approximately $D^{1/4}$ for each giant step, so for large D, k will also be large. We said "by more-or-less doing one ideal multiplication" because after doing the ideal multiplication, in some cases a few additional steps are needed.

Generally, we expect the number of iterations needed for the continued fraction algorithm applied to $(P_0 + \sqrt{D})/Q_0$ to be of the order of $D^{1/2+\epsilon}$ (or $D^{1/2} \log \log D$). Under the baby-step giant-step method, we expect the number of baby steps needed to be of the order of $D^{1/4+\epsilon}$ and the number of giant steps to also be of the order of $D^{1/4+\epsilon}$.

This article gives a specific algorithm using Shanks' baby-step giant-step method to solve the generalized Pell equation. Jacobson and Williams [2, pp. 172–181] apply Shanks' baby-step giant-step method to solve the Pell equation when $|N| = 1$ or 4, and give even faster methods for very large D, again when $|N| = 1$ or 4.

An appendix at the very end of this article gives a way to visualize the three major parts of the algorithm.

2. Preliminaries

We will only consider the equation

$$x^2 - Dy^2 = N \tag{4}$$

for squarefree $D > 1$. If D is not a square, you can write $D = e^2 d$ where d is squarefree. You can then solve $x^2 - dy^2 = N$, and use the fact that the y's that solve this equation satisfy some linear recurrence relations to find solutions with $e \mid y$, or show there are no such solutions [6].

We use the notation from [5] and we refer to that article for algorithms for ideal multiplication and other routines not discussed explicitly here.

If $D \not\equiv 1 \pmod 4$ then we will essentially work in the order of conductor $f = 1$ of the quadratic field $\mathbf{Q}(\sqrt{d})$, where $d = D$. The quadratic irrational $(P + \sqrt{D})/Q$ corresponds to the primitive ideal $[Q, P + f\omega]$, where $f = 1$ and $\omega = \sqrt{d}$. For ideals in this order, we have that $[t, v + f\omega] = [t, v + \sqrt{d}]$.

If $D \equiv 1 \pmod 4$ then we will essentially work in the order of conductor $f = 2$ of the quadratic field $\mathbf{Q}(\sqrt{d})$, where $d = D$. The quadratic irrational $(P+\sqrt{D})/Q$ corresponds to the primitive ideal $[Q, P-1+f\omega]$, where $f = 2$ and $\omega = (1 + \sqrt{d})/2$. Note that $P - 1 + f\omega = P + \sqrt{d}$, so $[Q, P - 1 + f\omega] = [Q, P + \sqrt{d}]$. For ideals in this order, we have that $[t, v + f\omega] = [t, v + 1 + \sqrt{d}]$.

There are only three major operations involved in this algorithm. Two are ideal multiplication [5, pp. 25–28] and testing whether an ideal is reduced [7, pp. 3, 14]. The third is a combination of a particular ideal reduction $\rho()$ and the computation of a "distance" δ. The details of the computation of $\rho()$ and δ for an ideal in an arbitrary order are given in the appendix "The Reduction Step." For the orders we actually use in this algorithm, $\delta_{i+1} = \delta_i + \ln(|v_{i+1} + \sqrt{d} + \epsilon|) - \ln(|t_i|)$, where $\epsilon = 1$ if $d \equiv 1 \pmod 4$ and $\epsilon = 0$ otherwise. We specify δ_0 for each use of the reduction steps.

We call one application of $\rho()$, and one corresponding distance computation, a *baby step*.

3. The algorithm

First we reduce solving $x^2 - Dy^2 = N$ to a few applications of the baby-step giant-step algorithm.

Matthews [3] shows that a solution in each equivalence class of primitive solutions to $x^2 - Dy^2 = N$ can be found by considering the continued fraction expansions of the quadratic irrationals $(z + \sqrt{D})/|N|$ where $z^2 \equiv D \pmod{|N|}$ and $|N|/2 < z \leq |N|/2$. All solutions are found by finding primitive solutions to each equation $x^2 - Dy^2 = N_1$ where N/N_1 is a square, and making the obvious adjustment.

Given integers $D > 1$ squarefree, $N \neq 0$, and z with $z^2 \equiv D \pmod{|N|}$ and $|N|/2 < z \leq |N|/2$, we show how to apply Shanks' baby-step giant-step method to get a solution to $x^2 - Dy^2 = N$, or determine that no solution corresponds to these inputs. So, assume we are given such integers D, N, and z, and we want to get a solution to $x^2 - Dy^2 = N$, or determine that no solution corresponds to these inputs. Initialize a variable that will be the logarithm of the solution, if there is one, by setting $\delta = 0$.

Our first step is to do some baby steps starting with the ideal $[1, f\omega]$ and $\delta_0 = 0$. We need to retain each iteration. Continue doing iterations until $\delta_i > D^{1/4}$. The first such i for which this holds gives us the ideal we will use in the giant steps, namely the ideal $I_0 = [t_i, v_i + f\omega]$. Also record δ_i as δ_{giant}. Then do two more baby steps, and retain the result with the other baby steps just done. Save t_i, v_i, and δ_i in an array BS1. Denote the maximum i reached as i_{maxbs1}. Set $C_{bs1} = i$.

Our second step is to do some baby steps starting with the ideal $[t_0, v_0 + f\omega] = [|N|, z + \sqrt{d}]$ and $\delta_0 = \ln(|N|)$. Continue until the ideal $[t_i, v_i + f\omega]$ is reduced (which, of course, might be for $i = 0$); denote this i as i_{minbs2}, and denote δ_i as $\delta_{basebs2}$. Now continue doing baby steps until $\delta_i - \delta_{basebs2} > D^{1/4}$, and do two more baby steps. Denote the maximum i reached as i_{maxbs2}, and the corresponding t_i, v_i, and δ_i as t_{maxbs2}, v_{maxbs2}, and δ_{maxbs2}. For $i_{minbs2} \leq i \leq i_{maxbs2}$ record t_i and v_i in an array BS2. Initialize a variable C that will be used to determine whether we have found a solution to the equation $x^2 - Dy^2 = N$ or to the equation $x^2 - Dy^2 = -N$, by setting $C = i$.

Our third, and final step, is to do the giant steps. Start with the ideal $J_0 = [t_{maxbs2}, v_{maxbs2} + f\omega]$, and set $\delta = \delta_{maxbs2}$. For each iteration of a giant step:

(1) Compute an ideal $I = I_0 \times J_i$. Add δ_{giant} to δ and add C_{bs1} to C. If I is primitive and reduced, then the giant step is complete.
(2) If the ideal I is not primitive, then write $I = sI'$ where I' is primitive. Replace I with I' and subtract $\ln(s)$ from δ. (This has no impact on C.)
(3) If $I = [t, v + f\omega]$ is not reduced then iteratively apply the reduction step $\rho()$ to I, starting with $t_0 = t$, $v_0 = v$, and $\delta_0 = 0$. Continue until you get a reduced ideal $[t_i, v_i + f\omega]$ with $t_i > 0$. Replace I with $[t_i, v_i + f\omega]$, add δ_i to δ, and add i to C.

Denote the resulting I as J_{i+1}. Now see whether the ideal J_{i+1} matches any of the ideals saved in $BS1$. If it does, say it is the same as the ideal $[t_i, v_i + f\omega]$ with $0 \le i \le i_{maxbs1}$. Subtract δ_i from δ, subtract i from C, and terminate the algorithm. If J_{i+1} does not match any ideal in $BS1$ but does match an ideal in $BS2$, then there is no solution for this z. If J_{i+1} does not match any ideal in either $BS1$ or $BS2$ then do another giant step.

When this part of the algorithm terminates by matching an ideal in $BS1$, then $\delta = \ln(x + y\sqrt{D})$ where $x^2 - Dy^2 = \pm N$. If C is even we have a solution to $x^2 - Dy^2 = |N|$ and if C is odd we have a solution to $x^2 - Dy^2 = -|N|$.

We can recover x and y as follows. With the possible exception of cases where $x + y\sqrt{D} < |N|$,

$$x = \left\lfloor \frac{1}{2}\exp(\delta) + 0.5 \right\rfloor, \qquad y = \left\lfloor \frac{\exp(\delta)}{2\sqrt{D}} + 0.5 \right\rfloor$$

The accuracy with which we know x and y depends on the number of digits used to compute δ. Essentially, to get every last digit of x and y, we need to carry δ to n digits to the right of the decimal point, where n is the number of digits in x. Generally, we will be content with knowing x and y approximately.

First Baby Steps for $x^2 - 2461y^2 = -201$

Index i	t_i	v_i	δ_i
0	1	0	0.000000
1	60	48	4.591157
2	39	10	4.601247
3	43	27	5.289362
4	52	14	5.696507
5	21	36	6.206661
6	12	46	7.732805
7	5	48	9.839056
8	69	45	12.789879

TABLE 1. Iterations of $\rho()$ for $D = 2461$, $t_0 = 1$, $v_0 = 0$, $\delta_0 = 0$

4. Example 1: solve $x^2 - 2461y^2 = -201$

As a first example, we apply Shanks' baby-step giant-step method to solve the equation $x^2 - 2461y^2 = -201$. Solutions to $z^2 \equiv 2461 \pmod{201}$ are $z = \pm 7, \pm 74$. Here $f = 2$ and $\omega = (1 + \sqrt{2461})/2$.

The first baby steps are shown in Table 1. Because $2461^{1/4}$ is approximately 7.043328, we take the ideal $I_0 = [12, 10 + f\omega]$ as the ideal to use for the giant steps, and we have $\delta_{giant} = 7.732805$ (we actually carry 14 decimal places, but we'll only show the first 6 here), and $C_{bs1} = 6$. We do two more steps and store these baby steps in $BS1$. Note that we will use this $BS1$ and the ideal I_0 for each of the four z.

The first z we'll do is $z = 7$. The baby steps for this z are shown in Table 2. We initialize with $t_0 = 201$, $v_0 = 6$, and $\delta_0 = \ln(201) = 5.303305$. Note that with $v_0 = 6$, $v_0 + f\omega = 6 + f\omega = 7 + \sqrt{2461}$. The ideal $[201, 6 + f\omega]$ is not reduced, but the ideal $[12, -8 + f\omega]$ is reduced. For this last ideal, $\delta_1 = 3.752053$, so we want to do baby steps until $\delta_i > \delta_1 + D^{1/4} = 3.752053 + 7.043328 = 10.795381$. This happens first for $\delta_8 = 12.429720$, so we do two more baby steps from there and stop. We store these baby steps in $BS2$ and set $C = 10$.

Second Baby Steps for $x^2 - 2461y^2 = -201$, $z = 7$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	6	5.303305	No
1	12	-8	3.752053	Yes
2	51	42	5.795527	Yes
3	47	7	5.917371	Yes
4	20	38	6.551451	Yes
5	39	40	8.062266	Yes
6	28	36	8.860102	Yes
7	9	46	10.098564	Yes
8	68	42	12.429720	Yes
9	27	24	12.522466	Yes
10	60	28	13.591109	Yes

TABLE 2. Iterations of $\rho()$ for $D = 2461$, $t_0 = 201$, $v_0 = 6$, $\delta_0 = 5.303305$

Table 3 shows the results of the (up to) three parts of each giant step. We start our giant steps from the end of the second set of baby steps, at the ideal $J_0 = [60, 28 + f\omega]$, and $\delta = 13.591109$. First we multiply the ideals J_0 and I_0, obtaining the ideal $J_0 \times I_0 = [180, 112 + 4f\omega]$, which we record on line 2 of Table 3, along with an incremental $\delta = 7.732805$ (that for the ideal for the giant step) and incremental $C = 6$. (In Table 3 we show the incremental δ's and incremental C's; the final values are the sums of what's shown.) The ideal $[180, 112 + 4f\omega]$ is not primitive, so we divide through by 4 and record $[45, 28 + f\omega]$ and an incremental $\delta = -\ln 4 = -1.386294$ on the next line. As $[45, 28 + f\omega]$ is reduced, this becomes J_1.

Now, $J_1 \times I_0 = [540, 298 + f\omega]$, which is primitive but not reduced. We add the ideal $[540, 298 + f\omega]$ to the list of giant steps, with an incremental $\delta = 7.732805$ and incremental $C = 6$. To reduce this ideal, we iteratively apply $\rho()$ starting with $t_0 = 540$, $v_0 = 298$, and $\delta_0 = 0$

Giant Steps for $x^2 - 2461y^2 = -201$, $z = 7$

Index i	t_i	v_i	w_i	δ	C	Comment
1	60	28	1	13.591109	10	Start
2	180	112	4	7.732805	6	Times giant step
3	45	28	1	-1.386294	0	Make primitive
4	540	298	1	7.732805	6	Times giant step
5	12	-36	1	-2.572720	3	Make reduced
6	12	0	12	7.732805	6	Times giant step
7	1	0	1	-2.484907	0	Make primitive
8				0.000000	0	Found a solution
Totals				30.345603	31	

TABLE 3. The Giant Steps for $z = 7$; ideals are $[t_i, v_i + w_i f\omega]$

(see Table 4). The first reduced ideal is $J_2 = [12, -36 + f\omega]$, which we add to the list, along with the incremental $\delta = -2.572720$ and $C = 3$.

(As an aside, I'd like to comment on an important nuance in the algorithm being presented, namely the requirement that at the end of these reduction steps $t_i > 0$. If you take an ideal with $t_i < 0$ as the end result of these reduction steps, most of the algorithm will work just fine. But it can throw off the parity of the counter C, so at the end you cannot use C to determine whether you have a solution to the equation $x^2 - Dy^2 = |N|$ or to $x^2 - Dy^2 = -|N|$. This issue does not come up for the case under discussion, reduction of the ideal $[540, 298 + f\omega]$. But, when doing $z = -74$, Table 11, the first reduced ideal derived from $[180, 100 + f\omega]$ is $[-43, -102 + f\omega]$, and using this makes C even, where it should be odd.)

Next $J_2 \times I_0 = [12, 12f\omega]$, which is not primitive. We add $[12, 12f\omega]$ to the list of giant steps, with an incremental $\delta = 7.732805$ and $C = 6$. Dividing by 12, we add the ideal $[1, f\omega]$ to the list and an incremental $\delta = -\ln(12) = -2.484907$. Because $[1, f\omega]$ is reduced, $J_3 = [1, f\omega]$.

And, we are just about done, because J_3 is the ideal with index 0 in $BS1$.

Reduction of the ideal $[540, 298 + f\omega]$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	540	298	0.000000	No
1	-161	-300	-0.772545	No
2	103	137	-0.619592	No
3	12	-36	-2.572720	Yes

TABLE 4. Iterations of $\rho()$ for $D = 2461$, $t_0 = 540$, $v_0 = 298$, $\delta_0 = 0$

Adding the incremental δ's gives

$$30.345603 = 13.591109 + 7.732805 + (-1.386294) + 7.732805 + (-2.572720) + 7.732805 + (-2.484907). \tag{5}$$

Then, for the x and y corresponding to this $z = 7$, $\ln(x + y\sqrt{2461}) = 30.345603$, whence

$$x + y\sqrt{2461} = \exp(30.345603) = 15098302200963.9$$

from which we get that

$$x = 7549151100482, \qquad y = 152174649895.$$

(To get x, y we used more decimal digits than we have displayed.)

Because $C = 31$ is odd, we have a solution to $x^2 - 2461y^2 - = -201$.

Now we look at $z = -7$. The baby steps for the ideal $[201, -8 + f\omega]$ are given in Table 6 and the giant steps are in Table 7. We have $\delta = 77.936768$, giving

$$x = 351947981949070800691602757560647 0,$$

$$y = 709451436611622105316501884603 29.$$

Initial baby steps and the giant steps for $z = 74$ and $z = -74$ are shown in Tables 8 to 11.

First Baby Steps for $x^2 - 2374y^2 = 201$

Index i	t_i	v_i	δ_i
0	1	0	0.000000
1	70	48	4.571859
2	27	22	4.582144
3	50	32	5.677340
4	41	18	5.965877
5	45	23	6.525126
6	42	22	6.977245
7	47	20	7.469669
8	35	27	7.946613
9	15	43	8.910046

TABLE 5. Iterations of $\rho()$ for $D = 2374$, $t_0 = 1$, $v_0 = 0$, $\delta_0 = 0$

5. Example 2: solve $x^2 - 2374y^2 = 201$

This is similar to the previous example, and we'll just present the main calculations, without much discussion. Note that $2374 \equiv 2 \pmod 4$, so $f = 1$ and $\omega = \sqrt{2374}$.

Table 5 gives the baby steps starting at $[1, \sqrt{2374}]$. Because $2374^{1/4}$ is about 6.980237, $I_0 = [47, 20 + \sqrt{2374}]$ and $\delta_{giant} = 7.469669$.

Solutions to $z^2 \equiv 2374 \pmod{201}$ are $z = \pm 37, \pm 97$. Baby steps and giant steps for the ideals $[201, z + \sqrt{2374}]$ are given in Tables 12 to 19.

6. Additional Comments

Sorting the tables $BS1$ and $BS2$ can make determination of whether an ideal is in one of these tables faster.

Terr [9] gives a baby-step giant-step algorithm where the number of baby steps increases by 1 with each iteration and the giant step also grows larger. This lets you find a solution that would take n baby

steps in $O(n^{1/2})$ giant steps, without knowing n in advance. See [5] for a brief description and [1] for more information.

The methods presented here can be used to determine whether an ideal I is principal and to find a generator α so that $I = (\alpha)$. When we reduce $[|N|, z + \sqrt{D}]$ using the baby steps and giant steps, we are more or less testing whether this ideal is principal and finding a generator when it is.

There are many variations on the algorithm presented here. For example, the algorithm can be presented in terms of quadratic irrationals $(P + \sqrt{D})/Q$ instead of ideals $[t, v + f\omega]$. Shanks' original article [8] on the infrastructure of quadratic orders presented everything in terms of binary quadratic forms.

References

[1] Johannes Buchmann and Arthur Schmidt, Computing the Structure of a Finite Abelian Group, *Mathematics of Computation* **74**, No. 252, 2005, pp. 2017-2026.

[2] Michael J. Jacobson Jr. and Hugh C. Williams, *Solving the Pell Equation*, Springer-Verlag, 2008.

[3] Keith Matthews, The diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers, *Expositiones Mathematicae*, **18** (2000), 323-331. Additional material at the "publications" page at http://www.numbertheory.org/keith.html.

[4] Richard Mollin, Simple Continued Fraction Solutions for Diophantine Equations, *Expositiones Mathematicae*, **19** (2001), pp. 55–73.

[5] John Robertson, "Computing in Quadratic Orders," at jpr2718.org.

[6] John Robertson, "Linear Recurrences for Pell Equations," at jpr2718.org.

[7] John Robertson, "Ambiguous Forms and Ideals in Quadratic Orders," at jpr2718.org.

[8] Daniel Shanks, The Infrastructure of a Real Quadratic Field and its Applications, *Proceedings of the 1972 Number Theory Conference*, University of Colorado, Boulder, 1972.

[9] David C. Terr, A Modification of Shanks' Baby-Step Giant-Step Algorithm, *Mathematics of Computation* **69**, No. 230, 2000, pp. 767-773.

7. Appendix–The reduction step

We consider ideals in the order of conductor f of the quadratic field $\mathcal{O}(\sqrt{d})$ where $d > 1$ is squarefree and $f \geq 1$. If $d \equiv 1 \pmod 4$ we write $\omega = (1+\sqrt{d})/2$, and otherwise $\omega = \sqrt{d}$. We will need the trace and norm of $f\omega$, $Tr(f\omega) = f(\omega + \overline{\omega})$, and $N(f\omega) = f^2\omega\overline{\omega}$, where $\overline{\omega}$ is the conjugate of ω. If $d \equiv 1 \pmod 4$ then

$$Tr(f\omega) = f, \qquad N(f\omega) = f^2\left(\frac{1-d}{4}\right)$$

while if $d \not\equiv 1 \pmod 4$ then

$$Tr(f\omega) = 0, \qquad N(f\omega) = -f^2 d.$$

We write ideals by specifying the basis of the module; that is, the ideal $I = [t, v + wf\omega]$ is the $\mathbf{Z}$-module $I = \{a \cdot t + b \cdot (v + wf\omega)\}$ where a, $b \in \mathbf{Z}$. Of course, for I to be an ideal we must have $w|t$, $w|v$, and $tw|N(v + wf\omega)$.

The reduction step $\rho()$ is given in [2, p. 99], and we add the computation of a distance δ_i. The input is an ideal $[t_i, v_i + f\omega]$ and a distance δ_i, and the output is an ideal $[t_{i+1}, v_{i+1} + f\omega]$ and a distance δ_{i+1}. We will write $[t_{i+1}, v_{i+1} + f\omega] = \rho([t_i, v_i + f\omega])$.

Write $\alpha = v_i + f\omega$, $q = \lfloor(\alpha/t_i)\rfloor$, $v_{i+1} = qt_i - v_i - Tr(f\omega)$, $t_{i+1} = (-1/t_i)(v_{i+1}^2 + v_{i+1}Tr(f\omega) + N(f\omega))$, and $\delta_{i+1} = \delta_i + \ln(|v_{i+1} + f\omega|) - \ln(|t_i|)$.

For use in Shanks' baby-step giant-step algorithm, it is important to write the ideal $[t_{i+1}, v_{i+1} + f\omega] = \rho([t_i, v_i + f\omega])$ exactly as given by the formulas. In particular, you should not make t_{i+1} positive if it is not otherwise, nor should you make v_{i+1} the minimal positive residue of t_{i+1}. This reduction step is really one iteration of the standard continued fraction algorithm for a quadratic irrational.

8. Appendix–A Visualization

Figures 1 to 3 give a crude visual representation of the different steps in the algorithm. The circle represents reduced principal ideals in the quadratic order. Small dots represent ideals generated by baby steps, and the larger dots represent ideals for the giant steps. A better diagram would vary the distances between the dots, large and small, a little bit, because the "distances" covered by individual steps are not completely uniform.

Figure 1 represents the baby steps starting from the ideal $[1, f\omega]$. Note that the ideal for the giant steps is the third-to-last dot.

Figure 2 represents the baby steps from the ideal $[|N|, z + \sqrt{D}]$. We start this off the circle because, in general, this ideal will not be reduced. Of course, if the ideal $[|N|, z + \sqrt{D}]$ is not principal, the reduction steps will take it to a cycle of reduced ideals different from the cycle of reduced principal ideals.

Figure 3 represents the giant steps. You can see that giant steps are closer together than the distances covered around the circle by either set of baby steps, so a giant step will eventually generate one of the ideals generated by the baby steps.

Second Baby Steps for $x^2 - 2461y^2 = -201$, $z = -7$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	-8	5.303305	No
1	12	6	4.036159	Yes
2	65	40	6.057800	Yes
3	29	23	6.182172	Yes
4	45	33	7.241021	Yes
5	52	10	7.538793	Yes
6	15	40	8.094097	Yes
7	4	48	9.977204	Yes
8	63	46	13.161576	Yes
9	35	15	13.202146	Yes
10	60	18	13.875214	Yes

TABLE 6. Iterations of $\rho()$ for $D = 2461$, $t_0 = 201$, $v_0 = -8$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2461y^2 = -201$, $z = -7$

Index i	t_i	v_i	w_i	δ	C	Comment
1	60	18	1	13.875214	10	Start
2	120	48	6	7.732805	6	Times giant step
3	20	8	1	-1.791759	0	Make primitive
4	60	52	4	7.732805	6	Times giant step
5	15	13	1	-1.386294	0	Make primitive
6	180	118	1	7.732805	6	Times giant step
7	7	53	1	-0.486960	2	Make reduced
8	84	46	1	7.732805	6	Times giant step
9	504	344	2	7.732805	6	Times giant step
10	252	172	1	-0.693147	0	Make primitive
11	15	63	1	-0.672656	2	Make reduced
12	60	54	3	7.732805	6	Times giant step
13	20	18	1	-1.098612	0	Make primitive
14	120	56	2	7.732805	6	Times giant step
15	60	28	1	-0.693147	0	Make primitive
16	180	112	4	7.732805	6	Times giant step
17	45	28	1	-1.386294	0	Make primitive
18	540	298	1	7.732805	6	Times giant step
19	12	-36	1	-2.572720	3	Make reduced
20	12	0	12	7.732805	6	Times giant step
21	1	0	1	-2.484907	0	Make primitive
22				0.000000	0	Found a solution
Totals				77.936768	77	

TABLE 7. The Giant Steps for $z = -7$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2461y^2 = -201$, $z = 74$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	73	5.303305	No
1	15	-75	3.194236	Yes
2	35	43	5.025307	Yes
3	51	25	5.795527	Yes
4	36	24	6.175955	Yes
5	7	46	7.163103	Yes
6	75	43	9.756313	Yes
7	20	30	9.828429	Yes
8	3	48	11.423854	Yes
9	84	46	14.895908	Yes
10	13	36	14.926489	Yes

TABLE 8. Iterations of $\rho()$ for $D = 2461$, $t_0 = 201$, $v_0 = 73$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2461y^2 = -201$, $z = 74$

Index i	t_i	v_i	w_i	δ	C	Comment
1	13	36	1	14.926489	11	Start
2	156	10	1	7.732805	6	Times giant step
3	15	-12	1	-1.396384	1	Make reduced
4	60	54	3	7.732805	6	Times giant step
5	20	18	1	-1.098612	0	Make primitive
6	120	56	2	7.732805	6	Times giant step
7	60	28	1	-0.693147	0	Make primitive
8	180	112	4	7.732805	6	Times giant step
9	45	28	1	-1.386294	0	Make primitive
10	540	298	1	7.732805	6	Times giant step
11	12	-36	1	-2.572720	3	Make reduced
12	12	0	12	7.732805	6	Times giant step
13	1	0	1	-2.484907	0	Make primitive
14				0.000000	0	Found a solution
Totals				51.691255	51	

TABLE 9. The Giant Steps for $z = 74$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2461y^2 = -201$, $z = -74$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	-75	5.303305	No
1	-68	-128	4.348877	No
2	15	58	4.817119	Yes
3	23	45	6.669330	Yes
4	15	45	8.094097	Yes
5	35	43	9.925168	Yes
6	51	25	10.695388	Yes
7	36	24	11.075817	Yes
8	7	46	12.062964	Yes
9	75	43	14.656175	Yes
10	20	30	14.728290	Yes

TABLE 10. Iterations of $\rho()$ for $D = 2461$, $t_0 = 201$, $v_0 = -75$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2461y^2 = -201$, $z = -74$

Index i	t_i	v_i	w_i	δ	C	Comment
1	20	30	1	14.728290	10	Start
2	120	80	2	7.732805	6	Times giant step
3	60	40	1	-0.693147	0	Make primitive
4	180	40	4	7.732805	6	Times giant step
5	45	10	1	-1.386294	0	Make primitive
6	540	190	1	7.732805	6	Times giant step
7	28	64	1	-0.741649	2	Make reduced
8	84	4	4	7.732805	6	Times giant step
9	21	1	1	-1.386294	0	Make primitive
10	252	190	1	7.732805	6	Times giant step
11	5	55	1	-0.823432	2	Make reduced
12	60	10	1	7.732805	6	Times giant step
13	360	200	2	7.732805	6	Times giant step
14	180	100	1	-0.693147	0	Make primitive
15	21	57	1	-0.336184	2	Make reduced
16				-6.206661	-5	Found a solution
Totals				56.591117	53	

TABLE 11. The Giant Steps for $z = -74$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2374y^2 = 201$, $z = 37$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	37	5.303305	No
1	5	-37	2.461613	Yes
2	33	47	5.413641	Yes
3	61	19	6.132570	Yes
4	10	42	6.529515	Yes
5	7	48	8.798789	Yes
6	75	43	11.371659	Yes
7	18	32	11.445204	Yes
8	43	40	13.040359	Yes

TABLE 12. Iterations of $\rho()$ for $D = 2374$, $t_0 = 201$, $v_0 = 37$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2374y^2 = 201$, $z = 37$

Index i	t_i	v_i	w_i	δ	C	Comment
1	43	40	1	13.040359	8	Start
2	2021	255	1	7.469669	7	Times giant step
3	30	8	1	-1.253391	3	Make reduced
4	1410	1148	1	7.469669	7	Times giant step
5	47	27	1	-1.512441	2	Make reduced
6	47	0	47	7.469669	7	Times giant step
7	1	0	1	-3.850148	0	Make primitive
8	0	0	0	0.000000	0	Found a solution
Totals				28.833388	34	

TABLE 13. The Giant Steps for $z = 37$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2374y^2 = 201$, $z = -37$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	-37	5.303305	No
1	5	37	4.451129	Yes
2	14	48	7.413550	Yes
3	77	36	9.213888	Yes
4	9	41	9.366818	Yes
5	86	40	11.655121	Yes
6	3	46	11.751738	Yes
7	55	47	15.214591	Yes

TABLE 14. Iterations of $\rho()$ for $D = 2374$, $t_0 = 201$, $v_0 = -37$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2374y^2 = 201$, $z = -37$

Index i	t_i	v_i	w_i	δ	C	Comment
1	55	47	1	15.214591	7	Start
2	2585	1477	1	7.469669	7	Times giant step
3	30	62	1	-1.438107	4	Make reduced
4	1410	302	1	7.469669	7	Times giant step
5	2	50	1	-1.267674	2	Make reduced
6	94	20	1	7.469669	7	Times giant step
7	21	-20	1	-1.185572	1	Make reduced
8	987	631	1	7.469669	7	Times giant step
9	15	22	1	-1.468966	3	Make reduced
10	705	67	1	7.469669	7	Times giant step
11	9	49	1	-0.169061	2	Make reduced
12	423	67	1	7.469669	7	Times giant step
13	33	14	1	-0.189740	3	Make reduced
14	1551	443	1	7.469669	7	Times giant step
15	18	68	1	-1.438107	2	Make reduced
16	846	302	1	7.469669	7	Times giant step
17	58	92	1	-0.913200	2	Make reduced
18	2726	208	1	7.469669	7	Times giant step
19	35	8	1	-1.029220	3	Make reduced
20	1645	1618	1	7.469669	7	Times giant step
21	1	27	1	-3.078404	1	Make reduced
22	0	0	0	0.000000	0	Found a solution
Totals				77.733234	100	

TABLE 15. The Giant Steps for $z = -37$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2374y^2 = 201$, $z = 97$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	97	5.303305	No
1	-35	-97	3.876941	Yes
2	42	62	5.028630	Yes
3	45	22	5.549742	Yes
4	41	23	6.015901	Yes
5	50	18	6.502889	Yes
6	27	32	6.981898	Yes
7	70	22	7.944842	Yes
8	1	48	8.268206	Yes
9	70	48	12.840064	Yes
10	27	22	12.850350	Yes
11	50	32	13.945545	Yes

TABLE 16. Iterations of $\rho()$ for $D = 2374$, $t_0 = 201$, $v_0 = 97$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2374y^2 = 201$, $z = 97$

Index i	t_i	v_i	w_i	δ	C	Comment
1	50	32	1	13.945545	11	Start
2	2350	2182	1	7.469669	7	Times giant step
3	11	157	1	-2.383547	2	Make reduced
4	517	443	1	7.469669	7	Times giant step
5	6	68	1	-1.438107	2	Make reduced
6	282	20	1	7.469669	7	Times giant step
7	7	-20	1	-2.284184	1	Make reduced
8	329	302	1	7.469669	7	Times giant step
9	5	27	1	-1.468966	1	Make reduced
10	235	67	1	7.469669	7	Times giant step
11	3	49	1	-0.169061	2	Make reduced
12	141	67	1	7.469669	7	Times giant step
13	22	52	1	-0.138824	2	Make reduced
14	1034	866	1	7.469669	7	Times giant step
15	25	143	1	-1.562567	2	Make reduced
16	1175	443	1	7.469669	7	Times giant step
17	35	13	1	-1.132494	3	Make reduced
18	1645	678	1	7.469669	7	Times giant step
19	45	122	1	-1.448500	2	Make reduced
20	2115	302	1	7.469669	7	Times giant step
21	3	50	1	-1.267674	2	Make reduced
22	141	20	1	7.469669	7	Times giant step
23	14	-20	1	-1.591037	1	Make reduced
24	658	302	1	7.469669	7	Times giant step
25	10	22	1	-1.468966	3	Make reduced
Totals				109.531523	154	

TABLE 17. The Giant Steps for $z = 97$; ideals are $[t_i, v_i + w_i f\omega]$

Second Baby Steps for $x^2 - 2374y^2 = 201$, $z = -97$

Index i	t_i	v_i	δ_i	Is Ideal Reduced?
0	201	-97	5.303305	No
1	-42	-104	4.012344	Yes
2	35	62	4.981712	Yes
3	15	43	5.945145	Yes
4	11	47	7.798561	Yes
5	63	41	9.897401	Yes
6	30	22	10.013047	Yes
7	31	38	11.074577	Yes
8	58	24	11.927257	Yes
9	21	34	12.282321	Yes

TABLE 18. Iterations of $\rho()$ for $D = 2374$, $t_0 = 201$, $v_0 = -97$, $\delta_0 = 5.303305$

Giant Steps for $x^2 - 2374y^2 = 201$, $z = -97$

Index i	t_i	v_i	w_i	δ	C	Comment
1	21	34	1	12.282321	9	Start
2	987	349	1	7.469669	7	Times giant step
3	75	107	1	-0.937674	2	Make reduced
4	3525	1007	1	7.469669	7	Times giant step
5	33	-14	1	-2.332632	3	Make reduced
6	1551	349	1	7.469669	7	Times giant step
7	9	32	1	-1.489023	3	Make reduced
8	423	302	1	7.469669	7	Times giant step
9	29	92	1	-0.913200	2	Make reduced
10	1363	208	1	7.469669	7	Times giant step
11	33	58	1	-0.877757	2	Make reduced
12	1551	1477	1	7.469669	7	Times giant step
13	2	72	1	-2.536720	2	Make reduced
14	94	20	1	7.469669	7	Times giant step
15	21	-20	1	-1.185572	1	Make reduced
16	987	631	1	7.469669	7	Times giant step
17	15	22	1	-1.468966	3	Make reduced
18	705	67	1	7.469669	7	Times giant step
19	9	49	1	-0.169061	2	Make reduced
20	423	67	1	7.469669	7	Times giant step
21	33	14	1	-0.189740	3	Make reduced
22	1551	443	1	7.469669	7	Times giant step
23	18	68	1	-1.438107	2	Make reduced
24	846	302	1	7.469669	7	Times giant step
25	58	92	1	-0.913200	2	Make reduced
Totals				98.298417	138	

TABLE 19. The Giant Steps for $z = -97$; ideals are $[t_i, v_i + w_i f\omega]$

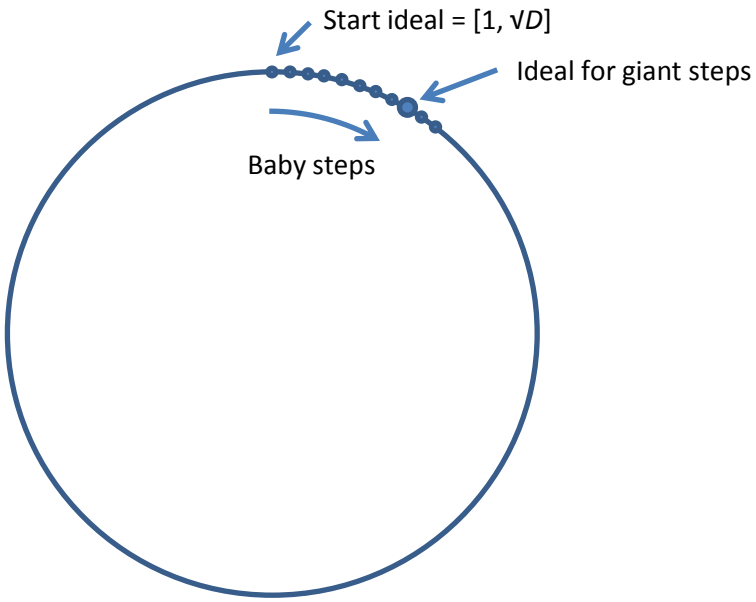

FIGURE 1. First Baby Steps and the Giant Step

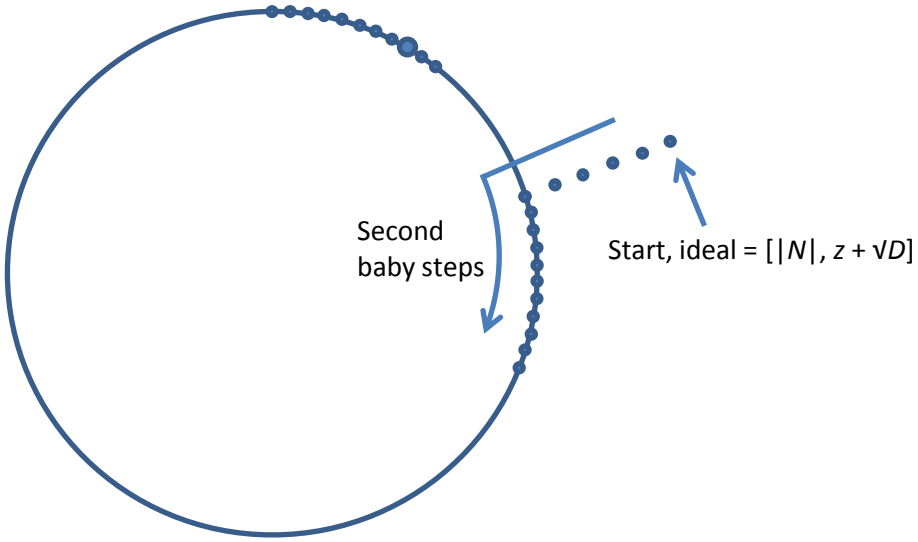

FIGURE 2. Second Set of Baby Steps

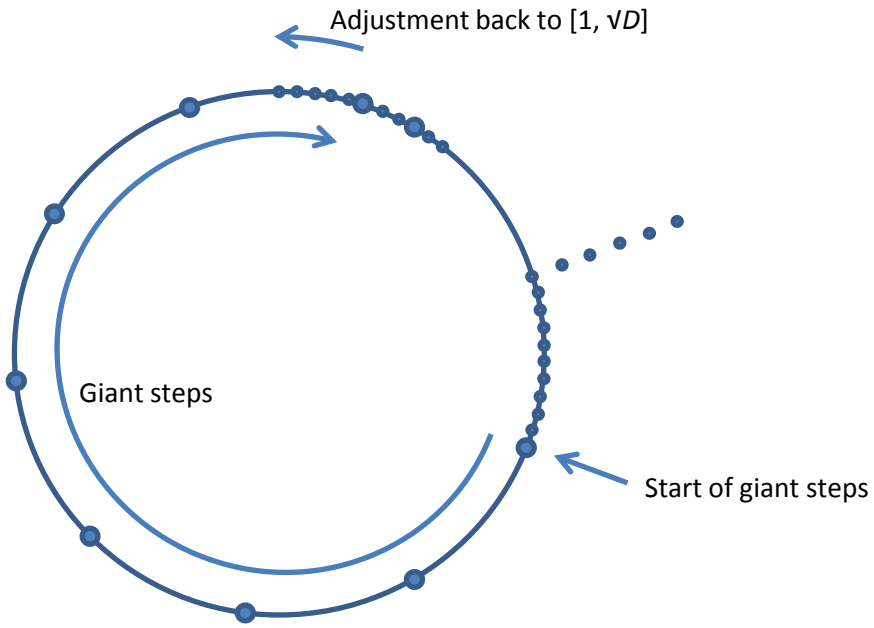

FIGURE 3. Giant Steps