FAST COMPUTATION OF THE REGULATOR OF AN ORDER IN A REAL QUADRATIC FIELD

JOHN P. ROBERTSON

1. Introduction

This article presents an algorithm for computing the regulator $R_\Delta = \ln(\epsilon_\Delta)$ for the quadratic order of conductor f in a real quadratic field $\mathbf{Q}(\sqrt{\Delta_0})$ with fundamental discriminant Δ_0 (so $\Delta = f^2\Delta_0$) and fundamental unit ϵ_Δ. The algorithm uses the continued fraction method to compute the regulator $R_{\Delta_0} = \ln(\epsilon_{\Delta_0})$ for the ring of integers (which is also the maximal order) of the quadratic field with fundamental discriminant Δ_0 and fundamental unit ϵ_{Δ_0}. The algorithm uses theorems on linear recurrence relations to compute the ratio E of the regulator of the order of conductor f to the regulator of the maximal order.

Of course regulators can be computed by applying the continued fraction algorithm to an appropriate quadratic irrational. For $f > 1$, the algorithm presented here is faster.

For large fundamental discriminants there are faster methods than that presented here [14, 4].

We begin by giving mapping out our approach. For additional background see "Computing in Quadratic Orders" and "Linear Recurrences for Pell Equations."

2. The roadmap

Finding fundamental units in orders of real quadratic number fields is equivalent to solving certain Pell equations.

Consider first the case where $d \equiv 1 \pmod 4$, $d > 0$ squarefree. Let $\{x_i, y_i\}$ be the positive solutions to $x^2 - dy^2 = \pm 4$, so $\{x_1, y_1\}$ is the

Date: April 24, 2007.

minimal positive solution. The fundamental unit of the maximal order of $\mathbf{Q}(\sqrt{d})$ is

$$\frac{1}{2}(x_1 + y_1\sqrt{d}).$$

The fundamental unit of the order of conductor f is

$$\frac{1}{2}(x_E + y_E\sqrt{d}) = \frac{1}{2}(x_E + \frac{y_E}{f}f\sqrt{d})$$

where E is the smallest index i so that $f|y_i$. Recall that,

$$\frac{x_E + y_E\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^E.$$

Here the discriminants are $\Delta_0 = d$ and $\Delta = f^2 d$.

Now consider the case where $d \not\equiv 1 \pmod 4$, $d > 0$ squarefree. Let $\{x_i, y_i\}$ be the positive solutions to $x^2 - dy^2 = \pm 1$. The fundamental unit of the maximal order of $\mathbf{Q}(\sqrt{d})$ is

$$x_1 + y_1\sqrt{d}.$$

The fundamental unit of the order of conductor f is

$$x_E + y_E\sqrt{d} = x_E + \frac{y_E}{f}f\sqrt{d}$$

where E is the smallest index i so that $f|y_i$. Here,

$$x_E + y_E\sqrt{d} = (x_1 + y_1\sqrt{d})^E.$$

The discriminants are $\Delta_0 = 4d$ and $\Delta = 4f^2 d$.

The best general method presented here to find the regulator in the order of conductor f of the quadratic field $\mathbf{Q}(\sqrt{d})$ consists of:

(1) Using the continued fraction method to compute the regulator of the maximal order. This gives the minimal positive solution to the Pell equation $x^2 - dy^2 = \pm 4$ or ± 1. From this solution, we can generate all solutions $\{x_i, y_i\}$ to the Pell equation.
(2) Using theorems in the index of apparition of to find the minimal index $\eta(f)$ so that $f|y_{\eta(f)}$. As above, $(x_{\eta(f)} + y_{\eta(f)}\sqrt{d})/2$ or $x_{\eta(f)} + y_{\eta(f)}\sqrt{d}$ is the fundamental unit in the order of conductor f.

The section "PQa algorithm" presents the continued fraction algorithm, and the section "The regulator for quadratic fields" uses the continued fraction algorithm to compute the regulator for a fundamental discriminant. The next section discusses what linear recurrence relations are satisfied by the $\{y_n\}$ that are solutions to Pell equations.

Then two sections give theorems on indexes of apparition for odd prime powers and powers of 2.

The section "Regulator for an arbitrary order" applies the theorems on the indexes of apparition of prime powers to determine the index of apparition of f, and so the fundamental unit of the order of conductor f.

The final section gives an example.

Appendices give methods to speed up particular calculations.

3. PQa algorithm

The PQa 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 $Q_0 \neq 0$, $D > 0$ is not a square, and $P_0^2 \equiv D \pmod{Q_0}$. Set

$$\begin{aligned} &A_{-2} = 0,\ A_{-1} = 1,\\ &B_{-2} = 1,\ B_{-1} = 0,\\ &G_{-2} = -P_0, \text{ and } G_{-1} = Q_0. \end{aligned}$$

For $i \geq 0$ set

$$\begin{aligned} a_i &= \left\lfloor (P_i + \sqrt{D})/Q_i \right\rfloor,\\ A_i &= a_i A_{i-1} + A_{i-2},\\ B_i &= a_i B_{i-1} + B_{i-2},\\ G_i &= a_i G_{i-1} + G_{i-2}, \end{aligned}$$

and for $i \geq 1$ set

$$\begin{aligned} P_i &= a_{i-1} Q_{i-1} - P_{i-1} \text{ and}\\ Q_i &= (D - P_i^2)/Q_{i-1}. \end{aligned}$$

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,

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

The sequences $\{P_i\}$, $\{Q_i\}$, and $\{a_i\}$ are periodic. We write ℓ for the smallest period, and note that if either $P_0 = 0$ and $Q_0 = 1$ or $P_0 = 1$ and $Q_0 = 2$ then $P_{\ell+i} = P_i$ for $i \geq 1$, $Q_{\ell+i} = Q_i$ for $i \geq 0$, and $a_{\ell+i} = a_i$ for $i \geq 1$. A key to computing units is the fact that $P_{\ell-1}^2 - DQ_{\ell-1}^2 = (-1)^\ell Q_0^2 = \pm 4$ or ± 1.

See "Solving the Pell Equation", Perron [13], or Mollin [12] for more information on the continued fraction algorithm.

4. The regulator for quadratic fields

This section will give an algorithm for computing the regulator for the ring of integers of the quadratic field $\mathbf{Q}(\sqrt{d})$ where $d > 1$ is square-free.

We will exploit the equation

$$\epsilon_{\Delta_0} = \left(G_{\ell-1} + B_{\ell-1}\sqrt{d}\right)/Q_0 = \prod_{i=1}^{\ell} \frac{P_i + \sqrt{d}}{Q_{i-1}} \tag{1}$$

and the fact that for the starting values of P_0 and Q_0 that we will use

$$P_i = P_{\ell+1-i} \text{ for } i \geq 1 \text{ and } Q_i = Q_{\ell-i} \text{ for } i \geq 0.$$

If $d \equiv 1 \pmod 4$, apply the PQa algorithm with $P_0 = 1$ and $Q_0 = 2$; otherwise apply the PQa algorithm with $P_0 = 0$ and $Q_0 = 1$. Stop when either

$P_{j+1} = P_j$ and $j \geq 1$, or
$Q_{j+1} = Q_j$.

Note that it is not necessary to keep all of the intermediate calculations; it suffices to keep the last two rows at any step.

Let

$$S = \sum_{i=1}^{j} \log\left(\left(P_i + \sqrt{d}\right)/Q_i\right).$$

If $P_{j+1} = P_j$ and $j \geq 1$ then $\ell = 2j$ and

$$R_{\Delta_0} = \log(Q_j/Q_0) + 2S.$$

If $Q_{j+1} = Q_j$ then $\ell = 2j+1$ and

$$R_{\Delta_0} = \log\left(\left(P_{j+1} + \sqrt{d}\right)/Q_0\right) + 2S.$$

While $G_{\ell-1}$ and $B_{\ell-1}$ might be too big to compute, for a given p^α it can be useful (see below) to have $G_{\ell-1}$ and $B_{\ell-1}$ modulo p^α. While running the PQa algorithm, you can compute the minimal nonnegative residues of G_i and B_i modulo p^α at each step, and use the half-period formulas below to finish the calculation.

If ℓ is even,

$$\begin{aligned} G_{\ell-1} &= B_{j-1}(G_j + G_{j-2}) + (-1)^j Q_0 \\ &= B_{j-1}(2G_j - a_j G_{j-1}) + (-1)^j Q_0 \text{ and} \end{aligned}$$

$$B_{\ell-1} = B_{j-1}(B_j + B_{j-2}) = B_{j-1}(2B_j - a_j B_{j-1}).$$

If ℓ is odd,

$$G_{\ell-1} = G_j B_j + G_{j-1} B_{j-1} \text{ and}$$

$$B_{\ell-1} = B_j^2 + B_{j-1}^2.$$

In particular, these formulas can be used modulo 2 to determine whether $G_{\ell-1}$ and $B_{\ell-1}$ are odd or even. When $d \equiv 5 \pmod 8$, this tells whether ϵ_{Δ_0} is integers or half-integers.

In fact, for many purposes, it suffices to have $B_{\ell-1}$ modulo p^α, and it is not necessary to keep track of the G_i to do this.

Note that the methods in this section actually work for any $d > 0$ not a square.

The method of computing the regulator follows that in Williams [14, Section 4]. Faster methods are discussed in [14], [4], and [2, Sections 5.7 to 5.10]. The half-period formulas are from [11].

Linear Recurrences for Pell Equations

Equation	$x_1^2 - dy_1^2$	a	c	Minimum a
$x^2 - dy^2 = 1$	$+1$	$2x_1$	-1	4
$x^2 - dy^2 = \pm 1$	-1	$2x_1$	$+1$	2
$x^2 - dy^2 = 4$	$+4$	x_1	-1	3
$x^2 - dy^2 = \pm 4$	-4	x_1	$+1$	1

TABLE 1. For the given equation, $y_{n+1} = ay_n + cy_{n-1}$

5. Linear recurrences for solutions to Pell equations

The problem of finding the minimal positive y so that $x^2 - f^2dy^2 = \pm 4$ or ± 1 is equivalent to finding the minimal positive Y that satisfies $X^2 - dY^2 = \pm 4$ or ± 1 and $f|Y$.

The problem of finding E so that $\epsilon_\Delta = \epsilon_{\Delta_0}^E$ reduces to finding the minimal index i so that $f|Y_i$ in the sequence of solutions $\{X_i, Y_i\}$ to the equation $X^2 - dY^2 = \pm 4$ or ± 1.

Because the solutions $\{Y_i\}$ satisfy certain linear recurrence relations, the theory of linear recurrence relations can be brought to bear, and we do that in the following sections.

The table "Linear Recurrences for Pell Equation" gives the linear recurrence relations satisfied by solutions to Pell equations. In each case, the sequence $\{y_i\}$ begins with $y_0 = 0$.

6. Indexes of apparition powers of odd primes in the sequence $\{y_n\}$

The issue is what is the smallest j so that $p^t|y_j$ for p an odd prime, $t \geq 1$, and $\{x_n, y_n\}$ the sequence of positive solutions to $x^2 - dy^2 = \pm 1$ or ± 4, with $d > 1$ squarefree. We denote the smallest such j by $\eta(p^t)$, also called the *index of apparition of* p^t *in the sequence* $\{y_j\}$.

There are three cases to consider: (A) $p|y_1$, (B) $p \nmid y_1$ and $p|d$, and (C) $p \nmid dy_1$.

For (A), if $p^r \| y_1$, then for $s = \max(0, t - r)$, $\eta(p^t) = p^s$.

For (B) we need to consider $p \neq 3$ and $p = 3$. If $p \neq 3$, $p|d$, and $p \nmid y_1$, then $\eta(p^t) = p^t$.

If $p = 3$, $3|d$, and $3 \nmid y_1$, and $3^r \| y_3$ (which will happen for some $r \geq 1$), for $s = \max(0, t - r)$, $\eta(3^t) = 3^{s+1}$.

For (C), $p \nmid dy_1$,

$$\eta(p) \left| \frac{1}{s} \left(p - \left(\frac{d}{p} \right) \right) \right.$$

where $s = 2$ if $p \equiv 1 \pmod 4$ or $c = -1$ and $s = 1$ if $p \equiv 3 \pmod 4$ and $c = 1$. In the latter case, $\left(p - \left(\frac{d}{p} \right) \right) / \eta(p)$ is odd. If $p^r \| y_{\eta(p)}$ for some $r \geq 1$, then $\eta(p^t)$ is $\eta(p)p^s$ where $s = \max(0, t - r)$. That r need not be 1 can be seen by taking $d = 2285$ and $p = 13$. Then $\eta(13) = 3$ and $13^4 \| y_3 = 285610$. See Appendix 2 for a reasonably efficient way to find $\eta(p)$.

For more on the theory behind linear recurrence relations and proofs of the results used above, see "Linear Recurrences for Pell Equations" at this website, or [8]. Additional references include [7, 1, 9, 3, 6].

7. Indexes of apparition for powers of 2

There are several cases to consider when $p = 2$. If $d \equiv 1 \pmod 4$, we consider only solutions to $x^2 - dy^2 = \pm 4$, while if $d \not\equiv 1 \pmod 4$ we consider only solutions to $x^2 - dy^2 = \pm 1$. We let $\{x_1, y_1\}$ denote the minimal positive solution to $x^2 - dy^2 = \pm 4$ or ± 1, as the case might be.

The cases for $p = 2$ are as follows.

(1) If $d \equiv 5 \pmod 8$, and $x_1^2 - dy_1^2 = -4$, then
   (a) If y_1 is odd, then x_1 is odd, $\eta(2) = 3$, $\eta(4) = \eta(8) = 6$, and $\eta(2^t) = 3 \cdot 2^{t-2}$ for $t \geq 3$.
   (b) If y_1 is even, then $y_1 \equiv 2 \pmod 4$, $x_1 \equiv 4 \pmod 8$, $\eta(2) = 1$, $\eta(4) = \eta(8) = 2$, and $\eta(2^t) = 2^{t-2}$ for $t \geq 3$.

(2) If $d \equiv 5 \pmod 8$, and $x_1^2 - dy_1^2 = +4$, then
   (a) If y_1 is odd, then x_1 is odd, as are y_2 and x_2. Let $2^r \| y_3$, where $r \geq 3$. For $t \leq r$, $\eta(2^t) = 3$, and $\eta(2^t) = 3 \cdot 2^{t-r}$ for $t \geq r$.

(b) If y_1 is even, then $y_1 \equiv 0 \pmod 8$ and $x_1 \equiv 2 \pmod 4$. Let $2^r \| y_1$, where $r \geq 3$. For $t \leq r$, $\eta(2^t) = 1$, and $\eta(2^t) = 2^{t-r}$ for $t \geq r$.

(3) If $d \equiv 1 \pmod 8$ and $x_1^2 - dy_1^2 = -4$, then $2 \| y_1$ and $8 | x_1$. We have $\eta(2) = 1$. Also, $2^r \| y_2$ for some $r \geq 4$. If $1 < t \leq r$ then $\eta(2^t) = 2$. If $t \geq r$ then $\eta(2^t) = 2^{t-r+1}$.

(4) If $d \equiv 1 \pmod 8$ and $x_1^2 - dy_1^2 = +4$ then $2^r \| y_1$ for some $r \geq 3$ and $2 \| x_1$. If $t \leq r$ then $\eta(2^t) = 1$. If $t \geq r$, then $\eta(2^t) = 2^{t-r}$.

(5) If $d \not\equiv 1 \pmod 4$, then

(a) If y_1 is odd then $2^r \| y_2$ for some $r \geq 1$. For $t \geq 1$, if $t \leq r$ then $\eta(2^t) = 2$, while if $t \geq r$ then $\eta(2^t) = 2^{1+t-r}$.

(b) If y_1 is even, and $2^r \| y_1$, then for $1 \leq t \leq r$, $\eta(2^t) = 1$, while for $t \geq r$, $\eta(2^t) = 2^{t-r}$.

For theory behind these results, see the articles cited at the end of the previous section.

8. Regulator for an arbitrary order

If $f = \prod_{i=1}^n p_i^{\alpha_i}$ is the canonical factorization of f and $k(p_i^{\alpha_i})$ is the index of apparition of $p_i^{\alpha_i}$, then the index of apparition of f, $E = E(f)$, is the least common multiple of $k(p_1^{\alpha_1})$, $k(p_2^{\alpha_2})$, $\ldots$, $k(p_n^{\alpha_n})$. It is a theorem that $E \leq 2f$.

The regulator of the order of conductor f in the quadratic field $\mathbf{Q}(\sqrt{d})$ is E times the regulator of the maximal order. Of course, $N(\epsilon_\Delta) = N(\epsilon_{\Delta_0})^E$.

9. An example

As an example of the above algorithms, we compute the regulator of the order of conductor $f = 3{,}691{,}878{,}903{,}900{,}000 = 2^5 \cdot 3^5 \cdot 5^5 \cdot 11^2 \cdot 29^2 \cdot 1493$ in the quadratic field $\mathbf{Q}(\sqrt{d})$ for $d = 97045 = 5 \cdot 13 \cdot 1493$. Observe that $d \equiv 5 \pmod 8$.

Applying the PQa algorithm with $D = 97045$, $P_0 = 1$, and $Q_0 = 2$, we find that $Q_{20} = Q_{21} = 18$, so $\ell = 41$. This tells us that $x_1^2 - dy_1^2 = -4$.

Then

$$S = \sum_{i=1}^{20} \log((P_i + \sqrt{D})/Q_i) = 21.90145\ldots \text{ , so}$$

$$\begin{aligned} R_{\Delta_0} &= \log\left(\left(P_{21} + \sqrt{d}\right)/Q_0\right) + 2S \\ &= \log\left(\left(311 + \sqrt{97045}\right)/2\right) + 2 \cdot 21.90145 = 49.54353\ldots \end{aligned}$$

Applying the PQa algorithm modulo $32 = 2^5$, we find that

$$B_{19} \equiv B_{20} \equiv 5 \pmod{32}$$

and so

$$B_{40} \equiv 5^2 + 5^2 \equiv 18 \pmod{32}.$$

As such, $2 \| y_1$. Because $2 \nmid 97045$, by (1)(b) above, $\eta(2^5) = 8 = 2^3$.

Applying the PQa algorithm modulo 3^5 gives $x_1 \equiv 192 \pmod{3^5}$ and $y_1 \equiv 167 \pmod{3^5}$, so $3 \nmid y_1$. We have $97045 \equiv 1 \pmod 3$ so $\left(\frac{d}{3}\right) = 1$ and $\eta(3) | (3-1)$, hence $\eta(3) = 2$. Then $y_2 = x_1 y_1 \equiv 192 \cdot 167 \pmod{3^5}$ and $3 \| y_2$. From this we have that $\eta(3^5) = 162 = 2 \cdot 3^4$.

Applying the PQa method modulo 5^5 gives $y_1 \equiv 1375 \pmod{5^5}$ so $5^3 \| y_1$. That $\eta(5^5) = 25 = 5^2$ follows.

Applying the PQa method modulo 11^2 gives $x_1 \equiv 117 \pmod{11^2}$ and $y_1 \equiv 104 \pmod{11^2}$ so $11 \nmid dy_1$. Because $\left(\frac{d}{11}\right) = 1$, possibilities for $\eta(11)$ are 2 and 10. By direct computation, $11 \nmid y_2$ and $y_{10} \equiv 99 \pmod{121}$ so $\eta(11^2) = 110 = 10 \cdot 11$.

Applying the PQa method modulo 29^2 gives $x_1 \equiv 222 \pmod{29^2}$ and $y_1 \equiv 472 \pmod{29^2}$ so $29 \nmid dy_1$. Because $\left(\frac{d}{29}\right) = -1$, the only possibilities for $\eta(29)$ are 3, 5 and 15. By direct computation, $29 \nmid y_3$, $29 \nmid y_5$ and $y_{15} \equiv 348 = 12 \cdot 29 \pmod{841}$ so $\eta(29^2) = 110 = 15 \cdot 29$.

Applying the PQa method modulo 1493 gives $y_1 \equiv 42 \pmod{1493}$ so $1493 \nmid y_1$. Because $1493 | d$, $\eta(1493) = 1493$.

Taking the least common multiple of the several η gives

$$E = 2^3 \cdot 3^4 \cdot 5^2 \cdot 11 \cdot 29 \cdot 1493 = 7,715,525,400.$$

Finally,

$$R_\Delta = ER_{\Delta_0} = 382,254,359,264.06\ldots$$

Please direct comments or questions to jpr2718@aol.com.

10. Appendix 1: Fast computation of y_k

If k is "small" it is straightforward and reasonably fast to just directly compute y_k. If k is large, we can use a routine analogous to right-to-left binary exponentiation to compute y_k with a number of steps proportional to $\ln(k)$. If p is odd, the calculations below can be done modulo p to compute y_k modulo p (where division by 2 is called for below, instead multiply by $(p+1)/2$).

Let $\{y_i\}$ satisfy the recurrence relation $y_{r+1} = ay_r + cy_{r-1}$ (so $a = x_1$ or $2x_1$ and $c = \pm 1$). We need two auxiliary sequences, $u_0 = 0$, $u_1 = 1$, $u_{r+1} = au_r + cu_{r-1}$, and $v_0 = 2$, $v_1 = a$, $v_{r+1} = av_r + cv_{r-1}$. Then $y_r = y_1 u_r$. For $D = a^2 + 4c$ we have that $v_r^2 - Du_r^2 = 4(-c)^r$. This gives us the relations

$$u_{r+1} = (u_r v_1 + u_1 v_r)/2,\ v_{r+1} = (v_1 v_r + u_r u_1 D)/2,$$

$$u_{2r} = v_r u_r, \text{ and } v_{2r} = (v_r^2 + du_r^2)/2.$$

With that background, here's the algorithm to compute u_k. Set $z_1 = 2$, $z_2 = 0$, $w_1 = a$, $w_2 = 1$, and $n = k$. Repeat the following until $n = 0$.

> If n is odd, set $z_1' = (z_1 w_1 + z_2 w_2 D)/2$, $z_2 = (z_1 w_2 + z_2 w_1)/2$, $z_1 = z_1'$. Whether or not n is odd, set $w_1' = (w_1^2 + Dw_2^2)/2$, $w_2 = w_1 w_2$, $w_1 = w_1'$. Set $n = \lfloor n/2 \rfloor$.

When $n = 0$, z_2 is u_k.

11. Appendix 2: Index of apparition for prime $p > 2$, $p \nmid dy_1$

In this appendix we discuss a method for finding the index of apparition k_0 of an odd prime p that does not divide dy_1. Then

$$k_0 | k = \frac{1}{s}\left(p - \left(\frac{d}{p}\right)\right)$$

Let $k = \prod_{i=1}^n q_i^{\alpha_i}$ be the canonical factorization of k. Then $k_0 = \prod_{i=1}^n q_i^{\beta_i}$ where $0 \le \beta_i \le \alpha_i$ for $1 \le i \le n$. If $j = \prod_{i=1}^n q_i^{\gamma_i}$ where each γ_i equals either β_i or α_i (we really just need $\gamma_i \ge \beta_i$) then $p | y_j$.

Here's a way to determine the β_i one by one. Start with setting $k' = k$. For each q_i in turn, do the following.
Step 1: If $q_i \nmid k'$ go to Step 4 (of course, q_i will divide k' the first time you come to this step for a given q_i).
Step 2: Set $k'' = k'/q_i$.
Step 3: If $q_i | y_{k''}$, set $k' = k''$ and return to Step 1.
Step 4: Go on to the next q_i, if there is one.

When all q_i have been done, $k_0 = k'$.

The method of Appendix 1 can be used to calculate $y_{k''}$ modulo q_i quickly.

This method essentially starts with α_i and keeps subtracting 1 until β_i is found. For large α_i, it would be faster to use a binary search to find β_i.

References

[1] R. D. Carmichael, *On the Numerical Factors of the Arithmetic Forms $a^n \pm \beta^n$*, The Annals of Mathematics, 2nd Ser., Vol. 15, No. 1/4 (1913-1914), 30-48, 49-70.

[2] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, AMS Chelsea Publishing, Providence, Rhode Island, 1999.

[4] R. de Haan, M. J. Jacobson Jr., and H. C. Williams, *A fast, rigorous technique for computing the regulator of a real quadratic field*, Math. Comp., posted April 19, 2007, PII: S 0025-5718(07)01935-7, to appear in print.

[5] Donald E. Knuth, *The Art of Computer Programming*, Volume 2, *Seminumerical Algorithms*, Second Edition, Addison-Wesley, Reading, Massachusetts, 1981.

[6] Derrick Henry Lehmer, *On the Indeterminate Equation $t^2 - p^2Du^2 = 1$*, The Annals of Mathematics, 2nd Ser., Vol. 27, No. 4. (Jun., 1926), pp. 471-476.

[7] D. H. Lehmer, *On the Multiple Solutions of the Pell Equation*, The Annals of Mathematics, 2nd Ser., Vol. 30, No. 1/4. (1928 - 1929), pp. 66-72.

[8] D. H. Lehmer, *An Extended Theory of Lucas' Functions*, The Annals of Mathematics, 2nd Ser., Vol. 31, No. 3 (July 1930), 419–448

[9] Edouard Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, American Journal of Mathematics, Vol. 1, No. 2 (1878), 184-196; Vol. 1, No. 3 (1878), 197-240; Vol. 1, No. 4 (1878), 289-321.

[10] G. B. Mathews, *Number Theory*, Chelsea, New York, undated (also as *Number Theory, Part I*, G. E. Stechert & Co, New York, 1927).

[11] K. R. Matthews, *Some Continued Fraction Identities*, at www.numbertheory.org/pdfs/pell.pdf. Is an unpublished paper available at www.numbertheory.org/keith.html.

[12] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, 1998.

[13] O. Perron, *Die Lehre von den Kettenbrüchen*, Vol. 1, third edition, Teubner, Stuttgart, 1954.

[14] 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.