A TRANSFORMATION TO SOLVE INDEFINITE QUADRATIC EQUATIONS IN INTEGERS

PAUL C. KETTLER

Abstract. The paper proposes a new method, called the Fast Quadratic Transform (FQT), to solve the general indefinite two-variable quadratic equation in integers. The paper presents the new approach, discusses its properties, and provides a comparative evaluation with the classical technique. The FQT is demonstrated to be markedly superior for all cases in which it applies, including examples for more than sixty percent of the discriminants through two hundred.

Prologue

$\pi\hat{\alpha}\nu\ \mu\acute{\epsilon}\tau\rho o\nu\ \grave{\alpha}\rho\iota\sigma\tau o\nu$ — $\grave{A}\nu\tau\iota\sigma\theta\acute{\epsilon}\nu\eta\sigma$

All mean is best. (There is virtue in moderation.) Antisthenes

1. Introduction

Consider the equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \text{ (note 1)} \tag{1.1}$$

Assume that the coefficients are integers, that $\Delta = b^2 - 4ac$ is positive and not a perfect square, and that $bde - ae^2 - cd^2 - \Delta f \neq 0$, (note 2).

Classical theory implies that the solutions in integers, if any, be determined as follows.

(a) Solve the Pell equation $t^2 - \Delta u^2$ by continued fraction expansion of $\sqrt{\Delta}$. The first or second non-trivial solution provides a rational integer automorph G or G^2 of the solution set for Equation (1.1).

(b) Locate a set of basic solutions by searching the interval on each branch between a chosen point and its transform by G, or by G^2 if G is not integral or has negative eigenvalues. The images of this basic set under powers of G constitute a complete set, (note 3).

This paper proposes an improved method, employing a different automorph T. The new method is superior for many instances of Equation (1.1) because:

(a) The parameters of T are direct functions of the coefficients, and

(b) The basic solution set is never larger than that for G.

Date: 15 June 2007.

2000 *Mathematics Subject Classification.* Primary: 10B05; Secondary: 12A25, 15A42, 68A20.

Key words and phrases. Quadratic diophantine equations; Pell equation; quadratic field units; eigenvalue inequalities; computational efficiency; quadratic integer programming.

This draft is a recomposition by the author in $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-LaTeX of a paper originally drafted in September 1970, with minor edits.

Henceforth the new method shall have the name Fast Quadratic Transform (FQT), in view of the above properties.

2. Review of the Classical Method

The affine transformation

$$G\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}t-bu & -2cu\\ 2au & t+bu\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}(t-1)(be-2cd)/\Delta-eu\\(t-1)(bd-2ae)/\Delta+du\end{pmatrix},$$

with inverse

$$F\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}t+bu & 2cu\\ -2au & t-bu\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}(t-1)(be-2cd)/\Delta+eu\\(t-1)(bd-2ae)/\Delta-du\end{pmatrix},$$

where (t,u) solves the Pell equation, is an element of the automorphism group on solutions to Equation (1.1). G is unimodular, and has eigenvalues $t\pm u\sqrt{\Delta}$, which are units in the field of rational numbers augmented by $\sqrt{\Delta}$.

G may have integer entries for some minimal Pellian solutions, but always has integer entries for next-to-minimal solutions. If Δ divides t_0-1, integrality obtains regardless of d and e. For $(t_1,u_1)=(2u_0^2\Delta+1,2t_0u_0)$, Δ always divides t_1-1.

To complete the solution of Equation (1.1), identify on each branch a point and its transform by G (or by G^2 if G is not integral or has negative eigenvalues.) If desired, select the points equidistant from the intersection of asymptotes to minimize included arc lengths. Then find all solutions on the arcs and transform them under powers of G (or G^2). There is no other solution; if there were, it could be mapped by a power of G (or G^2) into a new element of the basic set, which had been assumed complete.

3. The Fast Quadratic Transform

The transform

$$T\begin{pmatrix}x\\y\end{pmatrix}=\frac{1}{ac}\left[\begin{pmatrix}-ac & -bc\\ ab & b^2-ac\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}-cd\\bd-ae\end{pmatrix}\right],$$

with inverse

$$S\begin{pmatrix}x\\y\end{pmatrix}=\frac{1}{ac}\left[\begin{pmatrix}b^2-ac & bc\\ -ab & -ac\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}be-cd\\-ae\end{pmatrix}\right],$$

is also invariant on the solutions to Equation (1.1). The determinant is 1, and iff $ac|b^2$ the eigenvectors $b^2/2ac-1\pm(b/2ac)\sqrt{\Delta}$ are units in the field of rational numbers augmented by $\sqrt{\Delta}$. The entries of T are integral iff $a|b$, $a|d$, $c|b$, and $c|e$, in which case $ac|b^2$.

T has the property of conjugate propagation, meaning that if (x_1,y_1) and (x_2,y_2) are distinct solutions to Equation (1.1) for which $x_1=x_2$ or $y_1=y_2$, then respectively: $(\hat{x}_1,\hat{y}_1)=S(x_1,y_1)$ is such that $\hat{y}_1=y_2$; or $(\tilde{x}_1,\tilde{y}_1)=T(x_1,y_1)$ is such that $\tilde{x}_1=x_2$.

Observe that unimodular change of coordinates need not preserve the property. For example, let $f(x,y)=x^2-3xy+y^2-x+y=0$, and let

$$\begin{pmatrix}x\\y\end{pmatrix}=U\begin{pmatrix}\hat{x}\\\hat{y}\end{pmatrix}=\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}\hat{x}\\\hat{y}\end{pmatrix}$$

Then $\hat{f}(\hat{x},\hat{y})=f(x,y)=\hat{x}^2-\hat{x}\hat{y}-\hat{y}^2-\hat{x}=0$. The coefficients of f and $\hat{f}$ determine transformations T and $\widehat{T}$, but $U^{-1}TU\neq\widehat{T}$.

Solution of Equation (1.1) using T follows the same steps as solution using G.

4. A Comparison of the Methods

To compare G and T, note first that both have positive eigenvalues iff

$$\operatorname{sgn}(t) = \operatorname{sgn}\left(\frac{b^2}{2ac} - 1\right) = 1,$$

and have their larger eigenvalues corresponding to the same eigenvectors iff

$$\operatorname{sgn}(u) = \operatorname{sgn}\left(\frac{b}{2ac}\right) = \operatorname{sgn}\left(\frac{b}{ac}\right)$$

Assume therefore that these choices prevail. Then, let Λ_G and Λ_T be the eigenvalue norms of G and T. If Λ_T is a quadratic unit, then $p = \log \Lambda_G / \log \Lambda_T$, the power to which T must be raised to equal $\pm G$, is rational by Dirichlet. If p is irrational, then it is transcendental, by Gel'fond, (note 4).

The proof of the following result is sufficiently involved to require formal statement as a theorem.

Theorem 4.1. $\Lambda_T \leq \Lambda_G$

Proof. Demonstration proceeds in two phases.

(a) Parametric generation of all triples (t, u, Δ) solving $t^2 - \Delta u^2 = 1$, where $\Delta = b^2 - 4ac$ for some pair (b, ac).
(b) Selection of a pair (B, AC) such that
  (i) $\operatorname{sgn}(AC) = \operatorname{sgn}(t)$
  (ii) $\operatorname{sgn}(B/AC) = \operatorname{sgn}(u)$
  (iii) $\Lambda_T(B, AC) \leq \Lambda_G(\Delta)$
  (iv) $\Lambda_T(b, ac) < \Lambda_T(B, AC)$ for any other pair satisfying (i) and (ii)

Part (a). Since $t^2 - \Delta u^2 = 1$, $u^2 | t^2 - 1$. If u is odd, $u^2 | t - 1$ or $u^2 | t + 1$, hence $t = u^2 j \pm 1$, and $\Delta = (uj)^2 \pm 2j$. If u is even, $u^2 | 2(t - 1)$ or $u^2 | 2(t + 1)$, hence $t = (u^2/2)j \pm 1$, and $\Delta = (uj/2)^2 \pm j$. Identify the cases as P (for plus) or M (for minus), depending on the choice of sign. Assume $j \neq 0$, $u \neq 0$, $\Delta \neq 0$, because these cases are trivial. Observe then that $\operatorname{sgn}(t) = \operatorname{sgn}(j)$. Since $\Delta = b^2 - 4ac$ implies $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$, ignore triples for which this condition does not hold.

Part (b). Assume first that u is odd. If j is odd, $\Delta \equiv 3 \pmod 4$. If j is even, $\Delta \equiv 0 \pmod 4$.

In the P case for even j, $(B, AC) = \big(uj + 2\operatorname{sgn}(u), 1 + |u|\, j - j/2\big)$ satisfies all criteria. The first two conformances are obvious. The third may be checked by noting that $|B/2AC| < |u|$, insofar as $\Lambda_T(B, AC) < \Lambda_G(\Delta)$ iff the normed eigenvalue difference of T is less than that of G. The fourth may be checked by noting the monotone properties of $b/2ac$ with Δ constant, and observing that $(b, ac) = (uj, -j/2)$ violates (i).

In the M case for even j, the corresponding pair is $(B, AC) = (uj, j/2)$. For this example $|B/2AC| = |u|$, and the pair $(b, ac) = \big(uj - 2\operatorname{sgn}(u), 1 - |u|\, j + j/2\big)$ violates (i).

Assume next that u is even. If $j \equiv 0 \pmod 4$, then the analysis exhibited for the case u odd, j even, applies. Simply let $j = 4k = 2\hat{\jmath}$. Then $t = u^2(4k)/2 \pm 1 = u^2\hat{\jmath} \pm 1$, and $\Delta = \big(u(4k)/2\big)^2 \pm 4k = (u\hat{\jmath})^2 \pm 2\hat{\jmath}$. If $j \equiv 2 \pmod 4$, then $\Delta \equiv 2 \pmod 4$.

It remains, therefore, to examine the P and M cases for $j \equiv (2 \mp 1) \pmod 4$ with u even. For these cases $\Delta \equiv \big(1 \mp 1 + u \pmod 2 + j\big) \pmod 4$. If Δ is reachable, $(B, AC) = \big(uj/2 + \operatorname{sgn}(u), (1 + |u|\, j \mp j)/4\big)$ satisfies the criteria. $|B/AC| < |u|$, and $(b, ac) = \big(uj/2 - \operatorname{sgn}(u), (1 - |u|\, j \mp j)/4\big)$ violates (i). □

Corollary 4.2. $\Lambda_T = \Lambda_G$ *implies* $\Delta \equiv 0 \pmod 4$. *Equivalently,* $\Delta \equiv 1 \pmod 4$ *implies* $\Lambda_T < \Lambda_G$.

5. Examples

Example 5.1. *Let* $f(x, y) = x^2 - 3xy + y^2 - x + y = 0$. *Then*

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ -3 & 8 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$G^3 = T^3$, *for* $(t, u, \Delta) = (9, -4, 5)$. G^2 *is required because* G *does not have integral entries. A complete set of solutions is obtained by transforming* $(0, 0)$ *and* $(1, 0)$ *by powers of* T. *These solutions are of the form* $(u_{2k-1}u_{2k}, u_{2k}u_{2k+1})$ *and* $(u_{2k+1}u_{2k+2}, u_{2k}u_{2k+1})$, *where* u_j *is an element of the bi-directional Fibonacci sequence:* $u_0 = 0$, $u_1 = 1$, $u_j = u_{j-2} + u_{j-1}$.

Example 5.2. *Let* $g(x, y) = x^2 + 3xy - y^2 + x - y = 0$. *Then*

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & -3 \\ -3 & -10 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} -1 \\ -4 \end{pmatrix}$$

$G = T^3$, *for* $(t, u, \Delta) = (-649, -180, 13)$. *A complete set of solutions is obtained by transforming* $(0, 0)$ *and* $(0, -1)$. *Basic solutions are found by searching between points and their transforms by* G^2, *because eigenvalues are negative.*

6. Applicability and Performance of the Fast Quadratic Transform

Table 1 illustrates the extent of applicability and relative performance of the FQT for values of $\Delta \le 200$. Column 1, labeled 'Δ', lists values for which there exists a pair (b, ac) such that $ac|b^2$. An asterisk (*) indicates that $\Delta|t + 1$ for a minimal $t > 0$ Pellian solution. Column 2, labeled 'r', lists the residue modulo 4 of the square-free factor of Δ. Columns 3 through 6, labeled 'pairs $(|b|, ac)$' list all pairs for which $ac|b^2$, in increasing order on ac. Column 7, labeled 'p', lists the power $p = \log \Lambda_G / \log \Lambda_T$, for the pair (b, ac) flagged with a dagger '†'. This is the minimum power over all qualifying pairs. Column 8, labeled 'q', lists the period of the continued fraction expansion for $\sqrt{\Delta}$.

The number of pairs represented, 93 for 52 of 86 possible Δ's, is an index of applicability of the FQT. The power 'p' and the period 'q' are indices of relative performance.

7. Future Research

Further efforts are justified to advance the theory of several fronts. Included are:

(a) extensions to solution algorithms for inhomogeneous quadratic forms of more than two variables. This problem relates to the general quadratic programming problem in integers, insofar as quadratic forms are boundaries of inequality-constrained regions.

(b) investigations into relationships between G and T involving the theory of indefinite quadratic forms. One conjecture is that the power $p = \log \Lambda_G / \log \Lambda_T$, given $ac|b^2$, must be a positive integer if the square-free factor of Δ is congruent to 2 or 3 (mod 4), and must be of the form $3j/2 > 0$ or unity if the named residue is 1. A second

conjecture is that $\Delta | t_0 + 1 > 0$ implies $\Delta \equiv 1 \pmod 4$, and that $\Delta | t_0 - 1 > 0$ is impossible. The conjectures are true for $\Delta \leq 5000$.

(c) inquiries concerning the employment of integer search techniques to aid in solving continuous problems
(d) solving quadratics of more than two variables
(e) solving mathematical programming problems with inequality quadratic constraints
(f) providing examples which reduce to the requirement of solving problems of the above types

Table 1: Data from the Fast Quadratic Transform

Δ	r	pairs $(\lvert b\rvert, ac)$				p	q
*5	1		(1,-1)	†(3,1)	(5,5)	1.5	1
8	2		(2,-1)	†(4,2)		1.0	2
12	3		(2,-2)	†(4,1)	(6,6)	1.0	2
*13	1		†(3,-1)			3.0	5
20	1	(2,-4)	†(4,-1)	(6,4)		1.0	2
21	1		(3,-3)	†(5,1)	(7,7)	1.5	6
24	2		(4,-2)	†(6,3)		1.0	2
28	3			†(6,2)		2.0	4
29	1		†(5,-1)			3.0	5
32	2		(4,-4)	†(6,1)	(8,8)	1.0	4
40	2		†(6,-1)			1.0	2
44	3		†(6,-2)			2.0	8
45	1		(5,-5)	†(7,1)	(9,9)	1.5	6
48	3	(4,-8)	(6,-3)	†(8,4)		1.0	2
52	1		†(6,-4)			3.0	6
*53	1		†(7,-1)			3.0	5
56	2			†(8,2)		1.0	2
60	3		(6,-6)	†(8,1)	(10,10)	1.0	4
68	1		†(8,-1)			1.0	2
69	1			†(9,3)		3.0	8
72	2	(6,-9)	†(8,-2)			1.0	2
77	1		(7,-7)	†(9,1)	(11,11)	1.5	6
80	1		(8,-4)	†(10,5)	(12,16)	1.0	2
84	1	(6,-12)		†(10,4)		1.5	2
*85	1		†(9,-1)			3.0	5
92	3			†(10,2)		2.0	8
93	1		†(9,-3)			3.0	10
96	2		(8,-8)	†(10,1)	(12,12)	1.0	4
104	2		†(10,-1)			1.0	2
108	3		†(10,-2)	(12,9)		2.0	8
112	3			†(12,8)		2.0	6
116	1		†(10,-4)			3.0	10

(continued)

*$\Delta | t_0 + 1 > 0$

†Used to compute p

Table 1 (continued)

Δ	r	pairs $(\lvert b\rvert, ac)$				p	q
117	1		(9,-9)	†(11,1)	(13,13)	1.5	6
120	2		(10,-5)	†(12,6)		1.0	2
*125	1		†(11,-1)		(15,25)	3.0	5
128	2	(8,-16)		†(12,4)		2.0	4
132	1			†(12,3)		1.0	2
136	2			†(12,2)		1.0	4
140	3		(10,-10)	†(12,1)	(14,14)	1.0	4
148	1		†(12,-1)			1.0	2
152	2		†(12,-2)			1.0	2
156	2		†(12,-3)			1.0	2
160	2		†(12,-4)			2.0	8
165	1		(11,-11)	†(13,1)	(15,15)	1.5	6
168	2		(12,-6)	†(14,7)		1.0	2
*173	1		†(13,-1)			3.0	5
176	3		†(12,-8)			2.0	4
180	1	(10,-20)	(12,-9)	†(14,4)		1.5	4
188	3			†(14,2)		2.0	8
189	1			†(15,9)		1.5	4
192	3		(12,-12)	†(14,1)	(16,16)	1.0	4
200	2		†(14,-1)			1.0	2

*$\Delta | t_0 + 1 > 0$
†Used to compute p

Notes

1. This equation has a long and illustrious history. Dickson (25, Vol. 2, pp. 341–400) gives numerous references. Gel'fond (36, pp. 33–46) and Mordell (74, 53–65) relate more recent developments. Other sources are Barlow (6, pp. 245–295), Carmichael (9, pp. 34–35), and Skolem (98, 42–47).

2. Mordell (74, p. 57) discusses the restrictions in greater detail.

3. Classical interest in the so-called Pell equation was restimulated by the letter of Fermat (22). Important advances followed by Euler (32; 33; 34), including the introduction of automorphic solution transforms. Lagrange (53; 54) developed the first proofs of an infinitude of solutions. Gauss (35, pp. 163–200, and pp. 215–216) contributed further insights on indefinite forms and the relationship to the general second degree equation. The next major breakthrough in understanding was the unit theorem of Dirichlet (29). The first significant computational advance was that of Lehmer (61; 62), stating in part some results which may have been known to Legendre. Extensive historical coverage was provided by Heath (43, pp. 277–292), Dickson (25, Vol. 2, pp. 341–400), Ore (81), F. Châtelet (15), Shanks (93), and LeVeque (67).

Material specifically on the Pell equation appears in Barlow (6, pp. 245–295), Serret (92, pp. 7–85), Chrystal (18, pp. 482–490), Sommer (99, p. 104), Heath (43, pp. 277–292), Carmichael (9, pp. 26–33), Landau (55, pp. 57–64), Perron (82, pp. 102–110), Bachmann (5, pp. 175–199), Skolem (98, pp. 42–47), Dickson (28, pp. 80–87), Uspensky and Heaslet (103, pp. 346–369), Lehmer (63, pp. 55–57), Scholz (91, pp. 107–113), Davenport (19, pp. 107–111), Jones (50, pp. 71–73 and pp. 96–104), LeVeque (66, Vol. 1, pp. 137–158), Landau (56, pp. 76–84), Holzer (47, Vol. 1, pp. 157–187), Gel'fond (36, pp. 19–32), Pisot (83), Nagell (75), Sierpiński (97, pp. 305–309), McCoy (72, pp. 96–142), Niven and Zuckermann (77, pp. 175–181), and Mordell (74, pp. 53–65).

Sources relating to the Dirichlet Unit Theorem and consequences include Minkowski (73, pp. 137–147), Ore (80, pp. 63–69), Hasse (40, p. 262), Pollard (84, pp. 125–141), Hall (37, p. 124), Artin (3), Pisot (83), O'Meara (79, p. 77), Borevič and Šafarevič (8, pp. 107–123), Eichler (31, pp. 98–108), Samuel (88), and Hasse (42, p.516)

General material on units obtains in Hilbert (45, pp. 284–285), Weber (108, Vol. 2, pp. 670–684), Sommer (99, pp. 98–107), Minkowski (73, pp. 137–147), Reid (85, pp. 403–426), Hecke (44, pp. 127–217), Bachmann (5, pp. 175-199), Ore (80, pp. 63–69), Jung (51), Weyl (112, pp. 168–175), Lehmer (63, pp. 75–77), Hasse (40, pp. 282–289), Pollard (84, pp. 71–78), Hardy and Wright (39, pp. 204–217), Hall (37, pp. 123–132), Behnke (7, pp. 157–165), LeVeque (66, Vol. 2, pp. 74–81), Holzer (47, Vol. 1, pp. 157–187), Pisot (83), Chowla (16), A. Robinson (86, pp. 40–56), Borevič and Šafarevič (8, pp. 107–123), Eichler (31, pp. 98–108), Hasse (42, pp. 399–415), and Hilbert (46, pp. 98–109).

The standard works on continued fractions are Perron (82) and Khintchine (52). Other references are Barlow (6, pp. 261–316), Serret (92, pp. 7–85), Chrystal (18, pp. 423–527), Weber (108, Vol. 1, pp. 358–407), Wall (105), Davenport (19, pp. 79–114), Hardy and Wright (39, pp. 129–153), Jones (50, pp. 76–104), Niven (76, pp. 51–67), Olds (78, pp. 88–122), Sierpiński (97, pp. 282–314), McCoy (72, pp. 96–142), Niven and Zuckermann (77, pp. 151–181), and Lehmer (64, pp. 138–141)

Related treatment of quadratic fields or forms exists in Hilbert (45, pp. 280–324), Sommer (99), Dickson (25, Vol. 3, pp. 1–59), Hecke (44, pp. 173–217), Dickson (26, pp. 64–88),

Dickson (27, pp. 99–116 and pp. 175–180), Steinitz (100), Jung (51), Weyl (112, pp. 141–222), Siegel (94), Jones (49, pp. 139–185), Pollard (84, pp. 71–81), Eichler (30), Hardy and Wright (39, pp. 204–217), Artin (3), Cassels (10, pp. 256–303), Watson (107), Weiss (111, pp. 233–254), Deskins (24, pp. 360–414), Lang (59, pp. 55–57), Chowla (16), Borevič and Šafarevič (8, pp. 107–123), Artin (4, pp. 297–306), and Scharlau (90).

Automorphisms are examined by Bachmann (5, pp. 175–199), Dickson (28, pp. 80–87), Scholz (91, pp. 107–113), Jones (49, p. 147), Eichler (30), Cassels (10, pp. 256–303), and Watson (106, pp. 123–134).

Ideals are examined by Dedekind (23), Hilbert (45), Sommer (99), Hecke (44), Mann (71), A. Châtelet (13; 14), and others.

Researches involving topics of important, but peripheral, interest are Weil (109) on rational points of curves of arbitrary genus, Siegel (95; 96), Ankeny, Artin, and Chowla (2), Lang (57) for curves of genus exceeding zero, Watson (107) with simplifications on Siegel (95), Davenport, Lewis, and Schinzel (21), Cassels (11) with good bibliography, Chowla (17) on sums of squares, Samuel (89), Lewis (70), and J. Robinson (87).

The following are general works on allied topics. In algebra: Jacobson (48), Zariski and Samuel (113). In algebraic numbers: Hancock (38) and Lang (60). In class fields: Hilbert (45), Hasse (41), and Swinnerton-Dyer (101). In geometry: van der Waerden (104), Weil (110), and Lang (58).

Recent conference proceedings, advancing thoughts on topical problems such as the Mordell Conjecture, include American Mathematical Society (1), Cassels and Fröhlich (12), LeVeque (68), LeVeque and Straus (69), and Turán (102).

On theory relevant to quadratic programming in integers are: Davenport (20) and Lekkerkerker (65) on star bodies.

4. See Note 3, Paragraph 3, for references to Dirichlet. Pollard (84, p. 45) relates to Gel'fond's work.

References

[1] American Mathematical Society, *Institute in the theory of numbers*, Providence, 1959.

[2] N. Ankeny, E. Artin, and S. Chowla, *The class number of real quadratic number fields*, Ann. of Math. **56** (1952), no. 2, 479–493, MR 14; 251.

[3] E. Artin, *Theory of algebraic numbers*, Striker, Göttingen, 1959, Translated by B. Striker. MR 24; A1884.

[4] ———, *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967, Notes of 1950–1951 lectures at Princeton University. MR 38; 5742.

[5] P. Bachmann, *Grundlehren der neueren Zahlentheorie*, de Gruyter, Berlin, 1931.

[6] P. Barlow, *An elementary investigation of the theory of numbers*, Johnson, London, 1811.

[7] H. Behnke, *Vorlesungen über allgemeine Zahlentheorie*, Aschendorff, Münster, 1956, MR 18; 15.

[8] Z. Borevič and I. Šafarevič, *Number theory*, Academic, New York, 1966, MR 33; 4001.

[9] R. Carmichael, *Diophantine analysis*, Mathematical Monographs, no. 16, Wiley, New York, 1915.

[10] J. Cassels, *An introduction to the geometry of numbers*, Springer, Berlin, 1959, MR 28; 1175.

[11] ———, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291, MR 33; 7299.

[12] J. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Thompson, Washington, 1967, MR 35; 6500.

[13] A. Châtelet, *L'arithmétique des corps quadratiques*, Enseignement Math. **6** (1960), no. 2, 81–139, MR 23; A2414a.

[14] ———, *Les corps quadratiques*, Enseignement Math. **6** (1960), no. 2, 161–193, MR 23; A2414b.

[15] F. Châtelet, *Introduction à l'analyse diophantienne*, Enseignement Math. **6** (1960), no. 2, 3–17, MR 23; A2370.

[16] S. Chowla, *Note on the units of a real quadratic field*, Proc. Amer. Math. Soc. **16** (1965), 551, MR 32; 4114.

[17] ———, *Problems in elementary number theory*, J. Reine Angew. Math. **222** (1966), 71–74, MR 32; 4081.

[18] G. Chrystal, *Algebra*, Adam and Black, Edinburgh, 1889, 2 Vols., reprinted 1959. Chelsea: New York.

[19] H. Davenport, *Higher arithmetic*, Hutchinson, London, 1952, MR 14; 352.

[20] ———, *Analytic methods for diophantine equations and diophantine inequalities*, University of Michigan, Ann Arbor, 1963, MR 28; 3002.

[21] H. Davenport, D. Lewis, and A. Schinzel, *Quadratic diophantine equations with a parameter*, Acta Arith. **11** (1965-1966), 353–358, MR 32; 2373.

[22] P. de Fermat, *Letter to Lord Brouncker and John Wallis*, Œuvres de Fermat, vol. 2 (1894), Tannery & Henry, Paris, 1657, pp. 333–335.

[23] R. Dedekind (ed.), *Vorlesungen über Zahlentheorie von P. G. Lejeune-Dirichlet*, 4th ed., Viewig, Brunswick, 1871.

[24] W. Deskins, *Abstract algebra*, MacMillan, New York, 1964, MR 33; 7216.

[25] L. Dickson, *History of the theory of numbers*, Carnegie Institute, Washington, 1919–1923, 3 Vols., Vol. 2 reprinted 1952. New York: Chelsea.

[26] ———, *Modern algebraic theories*, Sanborn, Chicago, 1926.
[27] ———, *Introduction to the theory of numbers*, University of Chicago, Chicago, 1929.
[28] ———, *Modern elementary theory of numbers*, University of Chicago, Chicago, 1939, MR 1; 65.
[29] L. Dirichlet, *Zur Theorie der komplexen Einheiten*, Werke (1889), vol. 1, Reimer, Berlin, 1846, p. 639 ff.
[30] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Springer, Berlin, 1952, MR 14; 540.
[31] ———, *Introduction to the theory of algebraic numbers and functions*, Academic, New York, 1966, MR 35; 160.
[32] L. Euler, *Letter IX of L. Euler to C. Goldbach*, Correspondance Mathématique et Physique de Quelques Célèbres Géometres du XVIIIième Siècle, vol. 1 (1843), 1732, p. 37 ff.
[33] ———, *De solutione problematum diophantœorum per numeros integros*, Commentarii Academiæ Scientiarum Imperialis Petropolitanæ, vol. 6 (1738), 1732–1733, p. 175 ff.
[34] ———, *De usu novi algorithmi in problemate Pelliano solvendo*, Novi Commentarii Academiæ Scientiarum Imperialis Petropolitanæ, vol. 11 (1765), 1759, p. 98 ff.
[35] C. Gauss, *Disquisitiones arithmeticæ*, Fleischer, Leipzig, 1801.
[36] A. Gel'fond, *The solution of equations in integers*, Freeman, San Francisco, 1961, MR 25; 5025.
[37] M. Hall, *Units*, Introduction to Algebraic Number Theory (H. Mann, ed.), Ohio State University, Columbus, 1955, pp. 123–132.
[38] H. Hancock, *Foundations of the theory of algebraic numbers*, MacMillan, New York, 1931–1932, 2 Vols.
[39] G. Hardy and E. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford, London, 1960, MR 16; 673.
[40] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer, Berlin, 1964, MR 32; 5569.
[41] ———, *History of class field theory*, Algebraic Number Theory (J. Cassels and A. Fröhlich, eds.), Thompson, Washington, 1967, MR 36; 1417, pp. 266–279.
[42] ———, *Zahlentheorie*, 3rd ed., Akademie, Berlin, 1969, MR 40; 7185.
[43] T. Heath, *Diophantus of Alexandria*, Cambridge University, Cambridge, 1910.
[44] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademie, Leipzig, 1923, Reprinted 1948. New York: Chelsea.
[45] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung **4** (1894–1895), 175–546.
[46] ———, *Die Theorie der algebraischen Zahlkörper*, Gesammelte Abhandlungen, vol. 1, Springer, Berlin, 2nd ed., 1970, pp. 63–361.
[47] L. Holzer, *Zahlentheorie*, Mathematisch-Naturwissenschaftliche Bibliothek, no. 13–14, Teubner, Leipzig, 1959, 2 Vols.
[48] N. Jacobson, *Lectures in abstract algebra*, Van Nostrand, Toronto and Princeton, 1951–1964, 3 Vols. MR 12; 794, MR 14; 837, MR 30; 3087.
[49] B. Jones, *The arithmetic theory of quadratic forms*, Carus Mathematical Monographs, no. 10, Mathematical Association of America, Buffalo, 1950, MR 12; 244.
[50] ———, *The theory of numbers*, Holt, Rinehart, and Winston, New York, 1955, MR 16; 673.

[51] H. Jung, *Einführung in die Theorie der quadratischen Zahlkörper*, Jänecke, Leipzig, 1936.
[52] A. Khintchine, *Continued fractions*, 3rd ed., Noordhoff, Groningen, 1963, Translated by P. Wynn. MR 28; 5038.
[53] J. Lagrange, *Sur la solution des problèmes inteterminés du second degré*, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin **23 (1769)** (1768), 165–310.
[54] ———, *Nouvelle méthod pour résoudre les problèmes indeterminés in nombres entiers*, Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin **24 (1770)** (1770), 181–256.
[55] E. Landau, *Vorlesungen über Zahlentheorie*, Hirzel, Leipzig, 1927, 3 Vols. Sec. 1 of Vol. 1 reprinted 1950. New York: Chelsea.
[56] ———, *Elementary number theory*, Vorlesungen über Zahlentheorie, vol. 1, Sec. 1, Chelsea, New York, 1958, Translated by J. Goodman. MR 19; 1159.
[57] S. Lang, *Integral points on curves*, Inst. Hautes Etudes Sci. Publ. Math. **6** (1960), 27–43, MR 24; A86.
[58] ———, *Diophantine geometry*, Interscience, New York, 1962, MR 26; 119.
[59] ———, *Algebraic numbers*, Addison-Wesley, Reading, 1964, MR 28; 3974.
[60] ———, *Algebraic numbers*, Addison-Wesley, New York, 1970.
[61] D. Lehmer, *On the indeterminate equation* $t^2 - p^2Du^2 = 1$, Annals of Math. **27** (1926), 471–476.
[62] ———, *On the multiple solutions of the Pell equation*, Annals of Math. **30** (1928), 66–72.
[63] ———, *Guide to tables in the theory of numbers*, National Research Council, Washington, 1941, MR 2; 247.
[64] ———, *Computer technology applied to the theory of numbers*, Studies in Number Theory (W. LeVeque, ed.), MAA Studies in Mathematics, vol. 6, Mathematical Association of America, Buffalo, 1969, MR 40; 84, pp. 117–151.
[65] C. Lekkerkerker, *Geometry of numbers*, Bibliotheca Mathematica, no. 8, Wolters-Noordhoff, Groningen, 1969.
[66] W. LeVeque, *Topics in number theory*, Addison-Wesley, Reading, 1956, 2 Vols. MR 18; 283.
[67] ———, *A brief survey of diophantine equations*, Studies in Number Theory (W. LeVeque, ed.), MAA Studies in Mathematics, vol. 6, Mathematical Association of America, Buffalo, 1969, MR 40; 4201, pp. 4–24.
[68] W. LeVeque (ed.), *Studies in number theory*, MAA Studies in Mathematics, vol. 6, Mathematical Association of America, Buffalo, 1969, MR 39; 1388.
[69] W. LeVeque and G. Straus, *Number theory*, Proceedings of Symposia in Pure Mathematics (Providence) (W. LeVeque and G. Straus, eds.), no. 12, American Mathematical Society, 1969, MR 40; 2592.
[70] D. Lewis, *Diophantine equations: p-adic methods*, Studies in Number Theory (W. LeVeque, ed.), MAA Studies in Mathematics, vol. 6, Mathematical Association of America, Buffalo, 1969, MR 39; 2699, pp. 25–75.
[71] H. Mann, *Introduction to algebraic number theory*, Ohio State University, Columbus, 1955, MR 17; 240.
[72] Neal H. McCoy, *The theory of numbers*, MacMillan, New York, 1965, MR 32; 78.

[73] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1910, Reprinted 1953. New York: Chelsea.
[74] L. Mordell, *Diophantine equations*, Academic, New York, 1969, MR 40; 2600.
[75] T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York, 1964, MR 30; 4714.
[76] I. Niven, *Irrational numbers*, Carus Mathematical Monographs, no. 11, Mathematical Association of America, Buffalo, 1956, MR 18; 195.
[77] I. Niven and H. Zuckerman, *An introduction to the theory of numbers*, 2nd ed., Wiley, New York, 1966, MR 33; 3981.
[78] C. Olds, *Continued fractions*, New Mathematical Library, no. 9, Random House, New York, 1963, MR 26; 3672.
[79] O. O'Meara, *Introduction to quadratic forms*, Springer, Berlin, 1963, MR 27; 2485.
[80] Ø. Ore, *Les corps algébriques et la théorie des idéaux*, Mémoires des Sciences Mathématiques, no. 64, Gauthier-Villars, Paris, 1934.
[81] ———, *Number theory and its history*, McGraw-Hill, New York, 1948, MR 10; 100.
[82] O. Perron, *Die Lehre von den Kettenbrüchen*, 3rd ed., Teubner, Stuttgart, 1957, MR 19; 25.
[83] C. Pisot, *Introduction à la théorie des nombres algébriques*, Enseignement Math. **8** (1962), no. 2, 238–251, MR 27; 1434.
[84] H. Pollard, *The theory of algebraic numbers*, Carus Mathematical Monographs, no. 9, Mathematical Association of America, Buffalo, 1950, MR 12; 243.
[85] L. Reid, *The elements of the theory of algebraic numbers*, MacMillan, New York, 1910.
[86] A. Robinson, *Numbers and ideals*, Holden-Day, San Francisco, 1965, MR 32; 79.
[87] J. Robinson, *Diophantine decision problems*, Studies in Number Theory (W. LeVeque, ed.), MAA Studies in Mathematics, vol. 6, Mathematical Association of America, Buffalo, 1969, MR 39; 5364, pp. 76–116.
[88] P. Samuel, *Qu'est-ce qu'une quadratique?*, Enseignement Math. **13** (1967), no. 2, 129–130, MR 36; 6410.
[89] ———, *Théorie algébrique des nombres*, Hermann, Paris, 1967, MR 35; 6643.
[90] Winfried Scharlau, *Quadratic forms*, Queen's Papers on Pure and Applied Mathematics, no. 22, Queen's University, Kingston, 1969.
[91] A. Scholz, *Einführung in die Zahlentheorie*, de Gruyter, Berlin, 1945, MR 11; 159.
[92] J. Serret, *Cours d'algèbre supérieure*, 5th ed., Gauthier-Villars, Paris, 1885, 2 Vols.
[93] D. Shanks, *Solved and unsolved problems in number theory*, Spartan, Washington, 1962, MR 28; 3952.
[94] C. Siegel, *Equivalence of quadratic forms*, Amer. J. Math. **63** (1941), 658–680, MR 3; 163.
[95] ———, *Indefinite quadratische Formen und Funktionentheorie, I.*, Math. Ann. **124** (1951), 17–54, MR 16; 800.
[96] ———, *Indefinite quadratische Formen und Funktionentheorie, II.*, Math. Ann. **124** (1952), 364–387, MR 16; 801.
[97] W. Sierpiński, *Elementary theory of numbers*, Naukowe, Warsaw, 1964, Translated by A. Hulanicki. MR 31; 116.
[98] T. Skolem, *Diophantische Gleichungen*, Springer, Berlin, 1938, Reprinted 1950. New York: Chelsea.
[99] J. Sommer, *Vorlesungen über Zahlentheorie*, Teubner, Leipzig, 1907.

[100] E. Steinitz, *Algebraische Theorie der Körper*, de Gruyter, Berlin, 1930, Reprinted 1950. New York: Chelsea.
[101] H. Swinnerton-Dyer, *An application of computing to class field theory*, Algebraic Number Theory (J. Cassels and A. Fröhlich, eds.), Thompson, Washington, 1967, MR 36; 2595, pp. 280–291.
[102] P. Turán (ed.), *Number theory and analysis, a collection of papers in honor of edmund landau (1877–1938)*, Plenum, New York, 1969, MR 41; 3200b.
[103] J. Uspensky and M. Heaslet (eds.), *Elementary number theory*, McGraw-Hill, New York, 1939, MR 1; 38.
[104] B. van der Waerden, *Einführung in die algebraische Geometrie*, Springer, Berlin, 1939, Reprinted 1945. New York: Dover. MR 7; 476.
[105] H. Wall, *Analytic theory of continued fractions*, Van Nostrand, New York, 1948, MR 10; 32.
[106] G Watson, *Integral quadratic forms*, Cambridge University, Cambridge, 1960, MR 22; 9475.
[107] G. Watson, *Indefinite quadratic diophantine equations*, Mathematika **8** (1961), 32–38, MR 24; A79.
[108] H. Weber, *Lehrbuch der Algebra*, Vieweg, Brunswick, 1896, 2 Vols.
[109] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1928), 281–315.
[110] ———, *Foundations of algebraic geometry*, American Mathematical Society, New York, 1946, MR 9; 303.
[111] E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963, MR 28; 3021.
[112] H. Weyl, *Algebraic theory of numbers*, Annals of Mathematics Studies, no. 1, Princeton University, Princeton, 1940, MR 2; 37.
[113] O. Zariski and P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, 1958–1960, MR 19; 833, MR 22; 11006.

(Paul C. Kettler)
Centre of Mathematics for Applications
Department of Mathematics
University of Oslo
P.O. Box 1053, Blindern
N–0316 Oslo
Norway
E-mail address: paulck@math.uio.no
URL: http://www.math.uio.no/∼paulck/