C. R. Math. Rep. Acad. Sci. Canada Vol. **27**, (1), 2005 pp. 20–24

EISENSTEIN EQUATIONS AND CENTRAL NORMS

R. A. MOLLIN

Presented by M. Ram Murty, FRSC

Abstract. Central norms are given definition according to the infrastructure of the underlying order under discussion, which we define in the introductory section below. We relate these central norms in the simple continued fraction expansion of $\sqrt{D}$ to solutions of the Eisenstein equation $x^2 - Dy^2 = -4$, with $\gcd(x, y) = 1$. This provides a criterion for central norms to be 4 in the presence of certain congruence conditions on the fundamental unit of the underlying real quadratic order $\mathbb{Z}[\sqrt{D}]$.

1. **Introduction.** As early as 1844, Eisenstein studied the equation cited above. In this note, we look at it from a different perspective that intertwines the continued fraction expansion with the fundamental unit of the associated quadratic order and central norms when the equation under consideration has solutions.

Typically the aforementioned equation is considered when D is an odd positive integer, not a perfect square. In that instance, we know that the equation will have a solution only if $D \equiv 5 \pmod 8$, in which case there is a solution to $|x^2 - Dy^2| = 4$ with $\gcd(x, y) = 1$, if and only if the fundamental unit of $\mathbb{Z}[(1 + \sqrt{D})/2]$ is not in the order $\mathbb{Z}[\sqrt{D}]$. Moreover, the period length of the simple continued fraction expansion of $(1 + \sqrt{D})/2$ must be odd. Since we are interested in central norms we are interested in even period lengths. Thus, we look at the case where the Eisenstein equation is solvable for even D. Some nice work relating these solutions to continued fraction expansions of $\sqrt{D}$ has been done by Kaplan and Williams in [1], for instance (see also [3, Exercise 2.1.14, p. 59]). In the case where D is even and the equation

$$x^2 - Dy^2 = -4 \quad \text{with} \quad \gcd(x, y) = 1 \tag{1}$$

has solutions, the aforementioned results tell us that $D \equiv 4, 8 \pmod{16}$—see [1, p. 170]. Moreover, if $D \equiv 4, 8 \pmod{16}$, the equation (1) has solutions if and only if the period length of the simple continued fraction expansion of $\sqrt{D/4}$ is odd. However, if equation (1) is solvable, then the period length of the simple continued fraction expansion of $\sqrt{D}$ is even. It is this scenario that we will study.

2. **Notation and preliminaries.** The symbol, $\ell(\sqrt{D})$, will denote the period length of the simple continued fraction expansion of $\sqrt{D}$ where $D > 1$ is an integer that is not a perfect square.

Received by the editors on June 14, 2004.
AMS subject classification: Primary: 11D09, 11R11, 11A55; secondary: 11R29.
Keywords: Eisenstein equations, continued fractions, central norms.

Two important sequences are the following: $A_{-2} = 0$, $A_{-1} = 1$, $A_j = q_j A_{j-1} + A_{j-2}$ (for $j \geq 0$), and $B_{-2} = 1$, $B_{-1} = 0$, $B_j = q_j B_{j-1} + B_{j-2}$ (for $j \geq 0$), where q_j is the j-th partial quotient in the simple continued fraction expansion of $\sqrt{D}$. In fact, A_j/B_j is the j-th convergent for $\sqrt{D}$.

We will also need the following facts (which can be found in most introductory texts in number theory, such as [4]. Also, see [3] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \tag{2}$$

Also,

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j. \tag{3}$$

In particular,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell, \tag{4}$$

and $(A_{\ell-1}, B_{\ell-1})$ is the fundamental solution of the Pell equation

$$x^2 - Dy^2 = (-1)^\ell. \tag{5}$$

When ℓ is even, $Q_{\ell/2}$ is called the *central norm*, (via equation (3)), where

$$Q_{\ell/2} \mid 2D. \tag{6}$$

In the following (which we need in the next section), and all subsequent results, the notation for the A_j, B_j, Q_j and so forth apply to the above-developed notation for the continued fraction expansion of $\sqrt{D}$.

THEOREM 1. *Let D be a positive integer that is not a perfect square. Then $\ell = \ell(\sqrt{D})$ is even if and only if one of the following two conditions occurs.*

(i) *There exists a factorization $D = ab$ with $1 < a < b$ such that the following equation has an integral solution (x, y).*

$$ax^2 - by^2 = \pm 1. \tag{7}$$

Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of equation (7).

(a) $Q_{\ell/2} = a$.

(b) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.

(c) $A_{\ell-1} = r^2 a + s^2 b$ *and* $B_{\ell-1} = 2rs$.

(d) $r^2 a - s^2 b = (-1)^{\ell/2}$.

(ii) *There exists a factorization* $D = ab$ *with* $1 \leq a < b$ *such that the following equation has an integral solution* (x, y) *with* xy *odd.*

$$ax^2 - by^2 = \pm 2 \tag{8}$$

Moreover, in this case each of the following holds, where $(x, y) = (r, s)$ *is the fundamental solution of equation* (8).

(a) $Q_{\ell/2} = 2a$.

(b) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.

(c) $2A_{\ell-1} = r^2a + s^2b$ *and* $B_{\ell-1} = rs$.

(d) $r^2a - s^2b = 2(-1)^{\ell/2}$.

PROOF. All of this is proved in [5]. ∎

3. **Central norms and Eisenstein.** Lagrange is attributed with having proved that if $D = p$ is an odd prime, and (x_0, y_0) is the fundamental solution of the Pell equation $x^2 - Dy^2 = 1$, then $x_0 \equiv 1 \pmod{p}$ if and only if $p \equiv 7 \pmod{8}$. Related results may be found in [1, Lemma 3, p. 174]. The following are the even analogues of this result applied to Eisenstein (rather than Pell) equations.

THEOREM 2. *Let* $D = 4c$ *where* c *is an odd integer that is not a perfect square, and* $\ell' = \ell(\sqrt{2c})$. *Also assume that* (x_0, y_0) *is the fundamental solution of equation* (1). *Then the following are equivalent*

(i) $A_{\ell'-1} \equiv 1 \pmod{2c}$.

(ii) $\ell = \ell(\sqrt{D})$ *is even,* $Q_{\ell/2} = 4$, $\ell/2$ *is odd,* ℓ' *is even with* $Q_{\ell'/2} = 2$, *and* $\ell'/2$ *is even.*

(iii) *The Diophantine equation*

$$X^2 - 2cY^2 = 2 \tag{9}$$

has a solution.

PROOF. First we assume that part (i) holds. If ℓ' is odd, then by equation (3), $A_{\ell'-1} \equiv -1 \pmod{2c}$, a contradiction, so ℓ' is even. By Theorem 1 either $2c = ab$ with $1 < a < b$ and equation (7) holds, or $2c = ab$ with $1 \leq a < b$ equation (8) holding. We will assume only the former case, and prove that $Q_{\ell'/2} = 2$. The other case is argued similarly. It follows from part (i) of Theorem 1 that

$$1 \equiv A_{\ell'-1} \equiv r^2a + s^2b \equiv (-1)^{\ell'/2} + 2s^2b \pmod{2c}. \tag{10}$$

If $\ell'/2$ is odd, then it follows from equation (10) that $b \mid 2$, which is impossible. Hence, $\ell'/2$ is even, so from equation (10), $a \mid 2s^2$. Therefore, it follows from equation (2) and part (i) (b) of Theorem 1 that $a = 2$. Thus, by part (i) (a) of that theorem, $Q_{\ell'/2} = 2$.

If $x_0/2$ is odd, then by equation (1), $D/4$ is even, a contradiction. Thus $x_0/2$ is even, so $4(x_0/4)^2 - Dy_0^2/4 = -1$. It now follows from Theorem 1 that ℓ is even, $Q_{\ell/2} = 4$, and $\ell/2$ is odd since $x_0 = A_{\ell/2-1}$.

Now we assume part (ii). Since $Q_{\ell'/2} = 2$ and $\ell'/2$ is even, then it follows from equation (3) that part (iii) holds.

Now we assume part (iii) and complete the proof by showing that part (i) holds. By part (ii) of Theorem 1, ℓ' is even, $A_{\ell'-1} = (A_{\ell'/2-1}^2 + B_{\ell'/2-1}^2 2c)/2$ and $Q_{\ell'/2} = 2$. Thus, $2A_{\ell'-1} \equiv A_{\ell'/2-1}^2 \pmod{2c}$, and $A_{\ell'/2-1}^2 - B_{\ell'/2-1}^2 2c = 2$, which implies that $A_{\ell'/2-1}^2 \equiv 2 \pmod{2c}$. Hence, $A_{\ell'-1} \equiv 1 \pmod{2c}$. ∎

Example 1. If $D = 68 = 4 \cdot 17 = 4c$, then $\ell = 2$, $Q_{\ell/2} = 4$, $\ell' = 4$, $Q_{\ell'/2} = 2$, $A_{\ell'-1} = 35 \equiv 1 \pmod{2c}$. Also, $6^2 - 2c = 2$, and $8^2 - D = -4$.

Remark 1. The case $D \equiv 8 \pmod{16}$ has no analogue for Theorem 2. The reason is that for $D = 8c$, c odd, $\ell(\sqrt{2c})$ is necessarily odd when there is a solution to equation (1).

Remark 2. When $D = 2c$ for c odd, if $x_0 \not\equiv \pm 1 \pmod{2c}$, then $Q_{\ell/2} \neq 2$. This follows from Theorem 1. We will use this fact in what follows.

We provide the following as a consequence of the above. This generalizes the main result in [6].

Theorem 3. *Let D be a positive integer that is one of the following types.*

(i) *$D = 2c$ where $c \equiv 3 \pmod{8}$ and c is divisible only by primes congruent to 1 or 3 modulo 8.*
(ii) *$D = 2c$, where $c \equiv 1 \pmod{8}$ and c is divisible only by primes congruent to 1 or 7 modulo 8, with at least one prime congruent to 7 modulo 8 among them.*

Suppose that (x_0, y_0) is the fundamental solution of $x^2 - Dy^2 = 1$, with $x_0 \not\equiv \pm 1 \pmod{D}$. Then

$$2x^2 - cy^2 = (-1)^{(c-1)/2} \tag{11}$$

is not solvable for any integers x, y, but

$$2x^2 - cy^2 \equiv (-1)^{(c-1)/2} \pmod{n} \tag{12}$$

is solvable for all $n \geq 1$.

Proof. This follows by the same proof as in [6] where the fact that $Q_{\ell/2} \neq 2$ is achieved via the above rather than by assuming D is a certain Richaud–Degert type, where $\ell = \ell(\sqrt{2c})$. ∎

EXAMPLE 2. If $D = 372198 = 2c = 2 \cdot 3 \cdot 17 \cdot 41 \cdot 89$, a non-Richaud–Degert type, then $Q_{\ell/2} \neq 2$ so equation (11) is not solvable. However,

$$2x^2 - 186099y^2 \equiv -1 \pmod{n}$$

is solvable for all $n \geq 1$.

See also the related work by Kimura and Williams, [2], which motivated the more general work in [6].

ACKNOWLEDGEMENTS. The author's research is supported by NSERC Canada grant # A8484.

REFERENCES

1. P. Kaplan and K. S. Williams, *Pell's equations $x^2 = my^2 = -1, -4$ and continued fractions.* J. Number Theory **23** (1990), 169–182.
2. N. Kimura and K. S. Williams, *Infinitely many unsolvable Diophantine equations $f(x_1, x_2) = 0$ such that $f(x_1, x_2) \equiv 0 \pmod{m}$ is solvable for every m.* Amer. Math. Monthly, to appear.
3. R. A. Mollin, *Quadratics.* CRC Press, Boca Raton–London–New York–Washington D.C., 1996.
4. _____, *Fundamental Number Theory with Applications.* CRC Press, Boca Raton–London–New York–Washington D.C., 1998.
5. _____, *A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$.* JP J. Algebra Number Theory Appl. **4** (2004), 159–207.
6. _____, *Infinitely many quadratic Diophantine equations solvable everywhere locally, but not solvable globally.* JP J. Algebra Number Theory Appl., to appear.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
Canada, T2N 1N4
website: http://www.math.ucalgary.ca/∼ramollin/
email: ramollin@math.ucalgary.ca