GLASNIK MATEMATIČKI
Vol. 40(60)(2005), 21 – 27

A NOTE ON CLASS NUMBER ONE CRITERIA OF ŠIROLA FOR REAL QUADRATIC FIELDS

P.G. Walsh
University of Ottawa, Canada

Abstract. In [6], Širola gives two necessary and sufficient conditions for the class number of a real quadratic field to be equal to one. The purpose of this note is to remark that the equivalence of these conditions can be proved by using an elementary result of Nagell, which itself is a simple consequence of the fact that the Pell equation $X^2 - dY^2 = 1$ always has solutions in positive integers when $d > 1$ is squarefree.

1. Introduction

For a positive squarefree integer $d > 1$, let $\mathbf{Q}(\sqrt{d})$ denote the real quadratic field associated to d, and let $h(d)$ denote the class number of the ring of integers of $\mathbf{Q}(\sqrt{d})$. In [6], Širola provides necessary and sufficient conditions for $h(d) = 1$ in terms of the existence of solutions of certain Pell equations of the type $x^2 - dy^2 = \pm 4^\delta p$ and $x^2 - dy^2 = 4^\delta p^2$, where p ranges over the primes in Π, where Π is defined as the set of primes in $\mathbf{Z}$ for which the Legendre symbol $(d/p) = 1$. The proof of this result is somewhat involved, appealing to class group and ideal theoretic results from the theory of quadratic fields.

Our objective here is twofold. First, we point out that the equivalence of $h(d)$ to the solvability of Pell equations of the type $x^2 - dy^2 = \pm 4^\delta p$ is well known, and that in fact, one can simply take Π to be the finite set of primes p which satisfy $(d/p) = 1$ and $p < \sqrt{d}$. The second, and main point of this note, is to show that the equivalence between the condition $h(d) = 1$ and the solvability to Pell equations of the type $x^2 - dy^2 = 4^\delta p^2$ can easily be obtained using a simple result of Nagell concerning the form of $\sqrt{\epsilon_d}$, where $\epsilon_d = T + U\sqrt{d}$ is the minimal unit greater than 1, of norm 1, in the order

2000 *Mathematics Subject Classification.* 11D09, 11R11, 11R29.
Key words and phrases. Quadratic field, Pellian equation.

$\mathbf{Z}(\sqrt{\mathbf{d}})$, i.e. $(x, y) = (T, U)$ is the minimal solution in positive integers to the Pell equation $x^2 - dy^2 = 1$.

In what follows $d > 1$ will represent a squarefree positive integer, and $B_d = \sqrt{d}/2$ if $d \equiv 2, 3 \pmod 4$, while $B_d = \sqrt{d}$ if $d \equiv 1 \pmod 4$. We let $\Pi_1(d)$ denote the set of primes for which $2 < p < B_d$ and $(d/p) = 1$. Also, we define $\Pi^*(d) = \Pi_1(d)$ if either d is a prime with $d \neq 1 \pmod 8$, $d = 2q$ with q prime and $q \equiv 3 \pmod 4$, or $d = qr$ with q, r primes satisfying $q \equiv 3 \pmod 8$, $r \equiv 7 \pmod 8$, and we define $\Pi^*(d) = \Pi_1(d) \cup \{2\}$ if either d is a prime with $d \equiv 1 \pmod 8$, or $d = qr$ with q, r primes satisfying $q \equiv r \equiv 3$ or $7 \pmod 8$.

In the statement of our theorem, we make reference to the following two Pell-type equations. Here, δ represents an integer in $\{0, 1\}$.

$$X^2 - dY^2 = \pm 4^\delta p, \tag{1}$$

$$X^2 - dY^2 = 4^\delta p^2. \tag{2}$$

For $\delta \in \{0, 1\}$, a solution (X, Y) to equation (2) is referred to as 2^δ-*proper* provided that $\gcd(X, Y)$ divides 2^δ.

Our main goal then is to prove the following refinement of the main theorem of [6], noting that our primary purpose is not just to refine the result, but to exhibit a proof which is considerably more straightforward.

THEOREM 1.1. *The following conditions are equivalent*

1. $h(d) = 1$.
2. *For each prime* $p \in \Pi^*(d)$, *equation (1) has a positive integer solution* (X, Y).
3. *For each prime* $p \in \Pi^*(d)$, *equation (2) has a* 2*-proper solution* (X, Y).

2. Some Preliminary Results

It is well known that for a given squarefree positive integer $d > 1$, the Pell equation $x^2 - dy^2 = 1$ is solvable in positive integers x, y, and that every such solution can be generated from a minimal solution (T, U) by simply identifying this minimal solution with the unit $\epsilon_d = T + U\sqrt{d}$, and taking powers of this unit. In so doing, one sees that every positive integer solution (x, y) of $x^2 - dy^2 = 1$ is of the form $(x, y) = (T_k, U_k)$, where $\epsilon_d^k = T_k + U_k\sqrt{d}$ for some positive integer k.

We state the following consequence of this fact, possibly due to Nagell [4], which seems not to be as well known as it should. The formulation we provide appears in [7], and differs somewhat from that of Nagell, but is equivalent to Nagell's theorem.

LEMMA 2.1. *There exists a unique (possibly trivial) factorization $d = rs$ with the property that*

$$\sqrt{\epsilon_d} = \frac{u\sqrt{r} + v\sqrt{s}}{\sqrt{c}},$$

where $c \in \{1, 2\}$, $(r, s) \neq (1, d)$ if $c = 1$, and u and v are coprime positive integers for which

$$u^2 r - v^2 s = c. \tag{3}$$

Consequently, among all quadratic equations of the form (3) (with $rs = d$ and $c \in \{1, 2\}$), only the equations $X^2 - dY^2 = 1$ and $rX^2 - sY^2 = c$ are solvable in positive integers.

PROOF. As defined above, let (T, U) denote the minimal solution in positive integers to the Pell equation $X^2 - dY^2 = 1$, so that $T^2 - 1 = (T+1)(T-1) = dU^2$. Assume first that T is even, then $T+1 = ru^2, T-1 = sv^2$ for integers r, s, u, v satisfying $d = rs$, $u^2 r - v^2 s = c$, with $c = 2$. If T is odd, then $(T + 1)/2 = ru^2, (T - 1)/2 = sv^2$ for integers r, s, u, v satisfying $d = rs$, $u^2 r - v^2 s = c$, with $c = 1$. In either case it is trivial to see that $\sqrt{\epsilon_d} = \frac{u\sqrt{r}+v\sqrt{s}}{\sqrt{c}}$, and the fact that $(r, s) \neq (1, d)$ if $c = 1$ follows from the minimality of the solution (T, U) to $X^2 - dY^2 = 1$. The last part of the lemma is a consequence of the relation $\sqrt{\epsilon_d} = \frac{u\sqrt{r}+v\sqrt{s}}{\sqrt{c}}$. □

The last part of Lemma 2.1 was proved by K. Petr [5]. We use Lemma 2.1 to deduce the following three results.

LEMMA 2.2. *If $d \equiv 3 \pmod 4$ is prime, then the equation*

$$x^2 - dy^2 = (-1)^{(d+1)/4} \cdot 2$$

is solvable in odd positive integers x, y.

PROOF. Since $d \equiv 3 \pmod 4$, the equation $x^2 - dy^2 = -1$ cannot be solvable, which implies that the value of c from Lemma 2.1 is equal to 2. Lemma 2.1 shows that the equation $x^2 - dy^2 = \pm 2$ is solvable, and since x and y are clearly odd, the sign of -1 is determined by the congruence class of d modulo 8. □

LEMMA 2.3. *If $q \equiv 3 \pmod 4$ is prime, then the equation*

$$2x^2 - qy^2 = (-1)^{(q+1)/4}$$

is solvable in positive integers x, y.

PROOF. Applying Lemma 2.1 to $d = 2q$, we see first of all that $c = 1$, and so there is a factorization $d = rs$, $(r, s) \neq (1, d)$, for which $rx^2 - sy^2 = 1$ is solvable in positive integers. Since $q \equiv 3 \pmod 4$, we have that $(r, s) \neq (d, 1)$, and so either $(r, s) = (2, q)$ or $(r, s) = (q, 2)$. If $q \equiv 3 \pmod 8$, then it is easy

to see that $(r,s) = (q,2)$ by considering the equation $rx^2 - sy^2 = 1$ modulo 8. Similarly, if $q \equiv 7 \pmod 8$, then $(r,s) = (2,q)$, and the result follows. □

We remark that this lemma appears as Corollary 1.7 in [6]. We have therefore provided a proof of this result which does not appeal to the structure of class groups and related ideal-theoretic considerations.

LEMMA 2.4. *If q and r are primes satisfying $q \equiv r \equiv 3 \pmod 4$, then the equation*

$$qX^2 - rY^2 = \pm 1$$

is solvable in positive integers X, Y.

PROOF. Since $q \equiv r \equiv 3 \pmod 4$, it is evident that $c = 1$, and furthermore, since these primes are 3 modulo 4, the equation $X^2 - qrY^2 = -1$ is not solvable. Therefore, the only remaining possibilities are those in the statement of the lemma. □

The reader should be aware that the results above have been known for quite some time, even to Legendre and Dirichlet. For more on the history of the Pell equation, the reader is referred to the wonderful survey of Lemmermeyer [1], and also to a recent paper of Mollin [3].

3. Proof of Theorem reft1

The equivalence of conditions 1. and 2. is well known, and can be found for instance as Theorem 5.2.1 on p.158 of [2]. The essential ingredient in proving this equivalence is the fact that the class group of the ring of integers in $\mathbf{Q}(\sqrt{d})$ is generated by all noninert primitive ideals whose norm does not exceed the so-called Minkowski bound, which is no larger than $(4/\pi)\sqrt{d}$. Clearly condition 2. implies condition 3., as a solution (x,y) to equation (1) corresponds to an element $\tau = x + y\sqrt{d}$, and so squaring τ yields an element whose coefficients give rise to a solution of equation (2). Thus, we need only prove that condition 3. implies condition 2. For each odd prime p under consideration, we will deal only with the case that $\delta = 0$. That is to say, for a given odd prime $p \in \Pi^*(d)$, we will assume that the equation

$$X^2 - dY^2 = p^2 \tag{4}$$

is solvable in coprime integers, and show that this assumption either leads to a contradiction, or to a solution of the equation $X^2 - dY^2 = \pm p$. The case $\delta = 1$ can be dealt with using precisely the same arguments.

In what follows, (x,y) will denote a positive integer solution to (4) with $\gcd(x,y) = 1$. Furthermore, if y is odd, then the factorization $(x-p)(x+p) = dy^2$ implies the existence of integers m, n, u, v, with u, v odd, such that $x - p = mu^2, x + p = nv^2, d = mn, y = uv$, and so

$$nv^2 - mu^2 = 2p. \tag{5}$$

In the case that y is even, then there exist integers m, n, u, v such that $x - p = 2mu^2, x + p = 2nv^2, d = mn, y = 2uv$, and hence in this case

$$nv^2 - mu^2 = p. \tag{6}$$

Case 1a: $d \not\equiv 1 \pmod 8$ prime, and y odd.

In this case, the integers u, v, n, m in equation (5) are all odd. Note that since d is prime, either $(m, n) = (1, d)$ or $(d, 1)$. This implies that $n \equiv m \pm 2 \pmod 8$, from which we deduce that $d = nm \equiv 3$ or $7 \pmod 8$. By Lemma 2.2, the equation $X^2 - dY^2 = \pm 2$ is solvable, and so we let (x_1, y_1) denote a solution of this equation. If we define $x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})(u\sqrt{m} + v\sqrt{n})$, then it follows that x_2 and y_2 are even, and $(x_2/2)^2 - d(y_2/2)^2 = \pm p$.

Case 1b: $d \not\equiv 1 \pmod 8$ prime, and y even.

In this case, since d is prime, $(m, n) = (1, d)$ or $(d, 1)$, and so equation (6) gives the desired result.

Case 2a: $d \equiv 1 \pmod 8$ prime, and y odd.

Assume first that p is odd. As argued in case 1a, the assumption that y is odd leads to the conclusion that $d = nm \equiv 3 \pmod 8$.

Now assume that $p = 2$. If (x, y) is a 2-proper solution to $X^2 - dY^2 = 4p^2 = 16$ with y odd, then there are odd integers u, v, with $y = uv$, such that $x \pm 4 = du^2, x \mp 4 = v^2$, and so $v^2 - du^2 = \pm 4p$ as desired.

If $X^2 - dY^2 = p^2 = 4$ has a solution in coprime integers (x, y), then again we contradict the fact that $d \equiv 1 \pmod 8$.

Case 2b: $d \equiv 1 \pmod 8$ prime, and y even.

Assume first that p is odd. As in case 1b, since d is prime, equation (6) gives the desired result.

Now assume that $p = 2$. If (x, y) is a 2-proper solution to $X^2 - dY^2 = 4p^2 = 16$ with y even, then $x/2$ and $y/2$ are odd integers satisfying $(x/2)^2 - d(y/2)^2 = 4$, showing that $d \neq 1 \pmod 8$, and so $X^2 - dY^2 = 4p^2 = 16$ cannot be solvable with y even.

Case 3a: $d = 2q$, $q \equiv 3 \pmod 4$ prime, and y odd.

In this case, since one of m or n is even, equation (5) shows that not both u and v can be odd, hence y cannot be odd.

Case 3b: $d = 2q$, $q \equiv 3 \pmod 3$ prime, and y even.

In this case, equation (6) implies that one of the equations $X^2 - 2qY^2 = \pm p$, $2X^2 - qY^2 = \pm p$ is solvable in positive integers. If the first of these two equations is solvable, we have the desired result. Therefore, assume rather that $2X^2 - qY^2 = \pm p$ is solvable, and let (u, v) be a solution in positive integers. By Lemma 2.3, the equation $2X^2 - qY^2 = \pm 1$ is solvable in positive

integers, and so if we let (x_1, y_1) denote a solution of this equation, and put $(x_2+y_2\sqrt{2q}) = (x_1\sqrt{2}+y_1\sqrt{q})(u\sqrt{2}+v\sqrt{q})$, then $x_2^2-(2q)y_2^2 = \pm p$, as desired.

Case 4a: $d = qr$, $q \equiv 3 \pmod 8$, $r \equiv 7 \pmod 8$ primes, and y odd.

In this case, $d \equiv 1 \pmod 8$, and hence y cannot be odd, as argued earlier.

Case 4b: $d = qr$, $q \equiv 3 \pmod 8$, $r \equiv 7 \pmod 8$ primes, and y even.

Assume first that p is odd. Since y is even, the factorization $(x-p)(x+p) = dy^2$ implies that $x-p = 2mu^2$ and $x+p = 2nv^2$, with $d = mn, y = 2uv$, and so $nv^2 - mu^2 = p$. If $(m,n) = (1,d)$ or $(d,1)$, the result is proved. Therefore assume that $(m,n) = (q,r)$, so that $qv^2 - ru^2 = p$. By Lemma 2.4, we let (x_1, y_1) denote a solution to $qX^2 - rY^2 = 1$, and put $x_2 + y_2\sqrt{d} = (v\sqrt{q} + u\sqrt{r})(x_1\sqrt{q} + y_1\sqrt{r})$. It is clear that $X_2^2 - dy_2^2 = p$ as desired.

Case 5a: $d = qr$, $q \equiv r \equiv 3$ or $7 \pmod 8$ primes, and y odd.

Assume first that p is odd. In this case, $d \equiv 1 \pmod 8$, and hence y cannot be odd, as argued earlier.

Now assume that $p = 2$. Consider first the case $\delta = 1$. If (x,y) are odd integers satisfying $x^2 - dy^2 = 4p^2 = 16$, then there are odd integers m, n, u, v satisfying $d = mn, y = uv$ for which $x - 4 = mu^2, x + 4 = nv^2$, and so $nv^2 - mu^2 = 8$. If $(n,m) = (1,d)$ or $(d,1)$, we have the desired result. If $(n,m) = (q,r)$ say, then we appeal to Lemma 2.4 by letting (x_1, y_1) be a positive integer solution to $qX^2 - rY^2 = \pm 1$, and putting $x_2 + y_2\sqrt{d} = (x_1\sqrt{q} + y_1\sqrt{r})(v\sqrt{q} + u\sqrt{r})$, as it is easily verified that by doing so, $x_2^2 - dy_2^2 = \pm 8$, as desired.

For the case $\delta = 0$, suppose that there are odd positive integers (x,y) satisfying $x^2 - dy^2 = p^2 = 4$, then we contradict the fact that $d = qr \equiv 1 \pmod 8$.

Case 5b: $d = qr$, $q \equiv r \equiv 3$ or $7 \pmod 8$ primes, and y even.

In the case that p is odd the argument is identical to that of case 4b. Now assume that $p = 2$. For the case $\delta = 1$, suppose that (x,y) is a 2-proper solution of $x^2 - dy^2 = 4p^2 = 16$ with y even. It follows that $(x/2, y/2)$ are odd integers satisfying $(x/2)^2 - d(y/2)^2 = 4$, again contradicting the fact that $d = qr \equiv 1 \pmod 8$. For the case $\delta = 0$, if (x,y) is a solution in coprime integers to $x^2 - dy^2 = p^2 = 4$, then once again we contradict the fact that $d = qr \equiv 1 \pmod 8$.

Acknowledgements.

The author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

References

[1] F. Lemmermeyer, *Higher Descent on Conics. I. From Legendre to Selmer,* `arXiv:math.NT/0311309`.
[2] R.A. Mollin, Quadratics, CRC Press, New York, 1995.
[3] R.A. Mollin, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$, JP Journal algebra, Number Theory and Appl. **4** (2004), 159-207.
[4] T. Nagell, *On a special class of Diophantine equations of the second degree,* Ark. Math. **3** (1954), 51-65.
[5] K. Petr, *On Pellian equation,* Časopis Pěst. Mat. Fys. **56** (1927), 57-66 (in Czech).
[6] B. Širola, *Class number one quadratic fields and solvability of some Pellian equations,* Acta. Math. Hungarica **104** (2004), 127-142.
[7] P.G. Walsh, *The Pell Equation and Powerful Numbers,* Master's Thesis, University of Calgary, 1988.

P.G. Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario
Canada K1N 6N5
E-mail: `gwalsh@mathstat.uottawa.ca`

Received: `8.10.2004.`
Revised: `12.11.2004.`