Functiones et Approximatio
47.2 (2012), 173–182
doi: 10.7169/facm/2012.47.2.4

QUADRATIC RESIDUES AND CLASS NUMBERS

Wolfgang Knapp, Markus Köcher, Peter Schmid

Abstract: For an odd prime p let ϱ_p be the least odd prime ($\neq p$) which is a quadratic residue mod p. Using the theorems of Heegner–Baker–Stark and Siegel–Tatuzawa on the class number $h = h(-p)$ of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-p})$ it is shown that $\varrho_p < \sqrt{p}$ unless $p \in \{3, 5, 7, 17, 19, 43, 67, 163\}$, possibly with one further exceptional (large) prime $p = p_u$ (satisfying $p = 2^{h+2} - u^2$ with $h > 100$ und $5 \leqslant u < 2^{(h-5)/2}$). The exceptional prime does not exist if the Extended Riemann Hypothesis is true.

Keywords: quadratic residues, quadratic forms, class numbers, primes, Siegel–Tatuzawa.

1. Introduction

For an odd prime p let ϱ_p denote the least odd prime $q \neq p$ which is a quadratic residue mod p, that is, where the Legendre symbol $(\frac{q}{p}) = +1$. Thus $\varrho_3 = 7$, $\varrho_5 = 11 = \varrho_7$, and we shall see that $\varrho_p < p$ when $p > 7$. The results of the present paper yield that even $\varrho_p < \sqrt{p}$ up to eight or nine exceptions.

Major work on this subject has been done by Nagell many years ago. In 1923 he proved (in [6]) that $\varrho_p \leqslant \sqrt{p-4}$ if $p \equiv 1 \pmod 4$ and $p \neq 5, 17$, just using that then p is a sum of two squares of integers ($\varrho_{17} = 13$). One year earlier, in [5], he had treated the case where $p \equiv 3 \pmod 8$ assuming that the class number $h(-p)$ of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-p})$ is not trivial. By the theorem of Heegner–Baker–Stark one now knows that $h(-p) = 1$ if and only if $p \in \{3, 7, 11, 19, 43, 67, 163\}$; for (different) proofs we refer to [2, Theorem 12.34] and [8, Theorem 8.11]. One also knows from [6] that $\varrho_p = \frac{1+p}{4}$ if $h(-p) = 1$ and $p > 7$ (independent of the Heegner–Baker–Stark theorem; see also [1]). It follows that for $p \equiv 3 \pmod 8$ one has $\varrho_p < \sqrt{p}$ unless $p \in \{3, 19, 43, 67, 163\}$.

So it remains to examine the situation when $p \equiv 7 \pmod 8$. Here Nagell [7] proved that $\varrho_p < 2\sqrt{p} - 1$ for $p > 7$. It is easy to treat the case where p is a Mersenne prime. On the basis of the Siegel–Tatuzawa theorem (see Lemma 3 below) we get the following.

2010 Mathematics Subject Classification: primary: 11A15, 11E41; secondary: 11A41, 11M20, 11R29

Theorem 1. *Let the prime $p \equiv 7 \pmod 8$, $p > 7$. Then $\varrho_p < \sqrt{p}$ with at most one exception. If the exceptional prime $p = p_u$ exists (satisfying $\varrho_p \geqslant \sqrt{p}$), the L-function $L(s, \chi)$ to the real odd Dirichlet character χ with conductor p_u has a real zero in the interval $(\frac{71}{72}, 1)$, thus violating the Extended Riemann Hypothesis.*

From known properties of such L-functions [13] it is clear that the exceptional prime p_u must be fairly large (if it exists). We can describe it in some detail, thereby giving further indications that this prime possibly does not exist.

Theorem 2. *Assume the exceptional prime $p = p_u$ exists. Then $p = 2^{h+2} - u^2$ where $h = h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$ and u is an odd integer with $5 \leqslant u < 2^{(h-5)/2}$. Here $h > 100$ and $\varrho_p = 3 \cdot 2^{(h-1)/2} - u < 1.06275\sqrt{p} - u$. Moreover:*

(i) *The class number of an imaginary quadratic number field having discriminant $d \neq -p_u$ satisfies $h(d) > \frac{0.655}{18\pi}|d|^{\frac{4}{9}}$ provided $|d| \geqslant e^{18}$.*
(ii) *The quadratic polynomial $8X^2 + (8 - 2u)X + 2^{h-1} + 2 - u$ takes pairwise distinct prime values on all integers in the interval $[-2^{\frac{h-3}{2}}, 2^{\frac{h-3}{2}}]$.*

The estimate in (i) is much better than the (effective) lower bounds given by Goldfeld, Gross, Zagier and Oesterlé [9]. In proving Theorem 1 we shall establish with elementary means (avoiding computer calculations) that if $p = p_u$ exists then $h(-p) \geqslant 25$, at least. It then follows that for every imaginary quadratic number field with class number less than 25 the absolute value of its discriminant is less than e^{18}. This would provide for a (new) approach to the class number one problem (much easier than that given in [8, Theorem 8.11]). Application of a deep result of Watkins [14] yields that even $h(-p) > 100$ in Theorem 2.

The polynomial in (ii) would be a Frobenius–Rabinowitsch polynomial of an extraordinary kind (as there are more that 2^{50} integers in the interval $[-2^{\frac{h-3}{2}}, 2^{\frac{h-3}{2}}]$).

It should be mentioned that Linnik–Vinogradov [4] and Pintz [10] have shown, with the help of analytical methods, that $\varrho_p = O(p^{\frac{1}{4}+\varepsilon})$ for all $\varepsilon > 0$. However, such (ineffective) estimates are not helpful in the present work. On the other hand, on the basis of the Siegel–Tatuzawa theorem one might conjecture that, given any real number $c \in (\frac{1}{4}, \frac{1}{2}]$, there is an *effective* bound $\beta(c)$ such that $\varrho_p < p^c$ for $p > \beta(c)$, with at most one exception. The results obtained in this paper, together with those obtained previously by Nagell (plus the Heegner–Baker–Stark theorem) tell us that we may take $\beta(\frac{1}{2}) = 163$.

Acknowledgment. The authors thank the referee for some helpful comments.

2. Preliminaries

Let d be the discriminant of a quadratic number field, and let $\chi_d = (\frac{d}{*})$ denote the (Kronecker, Dirichlet) character associated to $K = \mathbb{Q}(\sqrt{d})$ (with conductor $|d|$; recall that every primitive real (quadratic) character $\chi \neq 1$ is of this type). Let $h(d)$ be the class number of K (in the usual sense), the order of the ideal class group $C(K)$ of K.

We only need to consider the cases where $d < 0$ (so $\chi_d(-1) = -1$; χ_d odd). Then there is an isomorphism between $C(K)$ and the form group $C(d)$ of (proper) equivalence classes of (primitive, positive definite) quadratic forms $f = aX^2 + bXY + cY^2$ over the integers with discriminant $d = b^2 - 4ac$, the latter group structure induced by composition of quadratic forms (see [2, Theorem 5.30]; there is a similar correspondence when $d > 0$ dealing with ideal classes in the narrow sense [8, Theorem 8.6]). Note that b is odd when $d \equiv 1 \pmod 4$, and even otherwise. An integer m is said to be represented by f if $f(x, y) = m$ for certain integers x, y; if one can choose here x, y relatively prime, then m is represented by f *properly* (or primitively). This makes no difference when m is square-free. Forms (properly) equivalent represent the same integers (properly).

Lemma 1. *Suppose the integer m is odd and prime to d. Then m is properly represented by some (primitive) quadratic form with discriminant d if and only if d is a quadratic residue $\bmod m$, in which case every divisor of m is thus represented too.*

This can be deduced from the literature (e.g. see Lemmas 2.3 and 2.5 in [2]). For an odd prime p let $p^* = (\frac{-1}{p})p$ (which is congruent to 1 mod 4). If $d = p^*$ then $\chi_d(q) = (\frac{p^*}{q}) = (\frac{q}{p})$ for every odd prime $q \neq p$ by quadratic reciprocity. Hence q is a quadratic residue mod p if and only if it is represented (properly) by a form with discriminant p^*.

Lemma 2. *If $d = p^*$ for some odd prime p, then $h(d)$ is odd.*

This is immediate from *genus theory* for quadratic forms (cf. [2, Theorem 6.1] and [15, Section 12]; even the class number in the narrow sense is odd).

Let $d = -p$ (with $p \equiv 3 \pmod 4$). Then *reduction theory* applies quite nicely in order to determine $h(d)$. Indeed every (positive definite) quadratic form with discriminant $-p$ is properly equivalent to a unique *reduced* form

$$f = aX^2 + bXY + cY^2.$$

This means that $|b| \leqslant a \leqslant c$ and that $b \geqslant 0$ when $|b| = a$ or $a = c$ (cf. [2, p. 27] or [15, Section 13]). Suppose we have $a = 1$. Then necessarily $b = 1$, and from $p = 4ac - b^2 = 4c - 1$ it follows that $c = \frac{1+p}{4}$. Thus $f = f_0 = X^2 + XY + \frac{1+p}{4}Y^2$ is the principal form (which is properly equivalent with $X^2 - XY + \frac{1+p}{4}Y^2$). Suppose that $f \neq f_0$ (so that $h(-p) > 1$). Then $a > 1$ (by the above). Assume that $a = c$. Then $b \geqslant 1$ (b is odd) and

$$p = 4a^2 - b^2 = (2a + b)(2a - b).$$

It follows that $p = 2a + b$ and that $2a - b = 1$. But then $2a - 1 = b \leqslant a$ and $a \leqslant 1$, a contradiction. Hence $a < c$. Assume next that $|b| = a$. Then $3 \leqslant b = a$ and $p = 4ac - a^2 = a(4c - a)$, which forces that $4c - a = 1$ and $c < a$, a contradiction. Hence $|b| < a$. Now the opposite (inverse) form $f^- = aX^2 - bXY + cY^2$ is reduced and is not properly equivalent with f. Thus all reduced non-principal quadratic forms with discriminant $-p$ appear in pairs, which gives Lemma 2 for $d < 0$. From $p = 4ac - b^2 \geqslant 4a(a+1) - (a-1)^2 = 3a^2 + 6a - 1 \geqslant 3a^2 + 11$ we get $a \leqslant \sqrt{(p-11)/3}$ (and $p > 11$).

Let us derive Nagell's [5] results for $p \equiv 3 \pmod 8$. Assume $h(-p) > 1$ and let $f \neq f_0$ as above. Then all coefficients a, b, c of f must be odd now, thus $|b| \leqslant a - 2$ and $c \geqslant a + 2$ and so

$$p = 4ac - b^2 \geqslant 4a(a+2) - (a-2)^2 = 3a^2 + 12a - 4.$$

If q is an (odd) prime dividing $a = f(1,0)$, then q is a quadratic residue mod p by Lemma 1 and therefore $\varrho_p \leqslant q \leqslant a$. This yields Nagell's estimate $\varrho_p \leqslant \sqrt{\frac{p+16}{3}} - 2$. One checks that here equality holds if and only if $a = 3$ and $p = 59$.

If $h(-p) = 1$ and $p > 7$, then $p \equiv 3 \pmod 8$ and $\varrho_p = \frac{1+p}{4}$. For then ϱ_p splits and is the norm of an integer in $\mathbb{Q}(\sqrt{-p})$, which forces that $\varrho_p \geqslant \frac{1+p}{4}$. On the other hand, $\frac{1+p}{4} = f_0(0,1)$ is an odd integer whose prime divisors are squares mod p by Lemma 1.

Lemma 3 (Siegel–Tatuzawa). *Let d be negative (χ_d odd). Then, given $0 < \varepsilon < \frac{1}{2}$, we have $h(d) > \frac{0.655 \cdot \varepsilon}{\pi} |d|^{\frac{1}{2} - \varepsilon}$ whenever $|d| \geqslant \max(e^{\frac{1}{\varepsilon}}, e^{11.2})$, with at most one exception.*

Improving Siegel's work [11] Tatuzawa [12] has shown that $L(1, \chi) > 0.655 \cdot \varepsilon \cdot k^{-\varepsilon}$ whenever χ is a real Dirichlet character with conductor $k \geqslant \max(e^{\frac{1}{\varepsilon}}, e^{11.2})$, with at most one exception. This gives the lemma in view of the class number formula [8, p. 436]. If there is an exceptional character χ the L-function $L(s, \chi)$ has a real zero in the interval $(1 - \frac{\varepsilon}{4}, 1)$ [12, Lemma 9], thus contradicting the Extended Riemann Hypothesis. It is known (see [13]) that $L(s, \chi)$ has no positive real zero if χ is odd and $k \leqslant 3 \cdot 10^8$.

Lemma 4. *Let $p = 2^q - 1$ be a Mersenne prime with $q > 3$ (also prime). Then $\varrho_p = 5$ if $q \equiv 1 \pmod 4$ and $\varrho_p = 7$ if $q \equiv 11 \pmod{12}$. Moreover, in the remaining cases $\varrho_p = 11$ or 13 depending on whether $q \equiv 7, 43 \pmod{60}$ or $q \equiv 19, 31 \pmod{60}$.*

Proof. Note that 2^q is divisible by 4 and so $p \equiv 3 \pmod 4$. Since q is odd, $2^q \equiv 2 \pmod 3$ and so $(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{1}{3}) = -1$. Hence $\varrho_p \geqslant 5$. If $q \equiv 1 \pmod 4$ then $2^q \equiv 2 \pmod 5$ and $(\frac{5}{p}) = (\frac{p}{5}) = (\frac{1}{5}) = 1$. On the other hand, if $q \equiv 3 \pmod 4$ then $2^q \equiv 3 \pmod 5$ and $(\frac{5}{p}) = -1$. Thus $\varrho_p = 5$ if and only if $q \equiv 1 \pmod 4$. Let $q \equiv 3 \pmod 4$ in what follows. Then either $q \equiv 7$ or 11 mod 12 (as we assumed that $q > 3$).

If $q \equiv 11 \pmod{12}$ then $q \equiv 5 \pmod 6$ and $2^q \equiv 2^5 \equiv 4 \pmod 7$, whence $(\frac{7}{p}) = -(\frac{p}{7}) = -(\frac{3}{7}) = 1$, by quadratic reciprocity, so that $\varrho_p = 7$. If $q \equiv 7 \pmod{12}$ then $2^q \equiv 2 \pmod 7$ and $(\frac{7}{p}) = -(\frac{p}{7}) = -(\frac{1}{7}) = -1$, implying that $\varrho_p > 7$.

So let $p \equiv 7 \pmod{12}$. Then $2^q \equiv 2^7 \equiv 11 \pmod{13}$ and $(\frac{13}{p}) = (\frac{p}{13}) = (\frac{10}{13}) = 1$. Hence either $\varrho_p = 13$ or $\varrho_p = 11$ in this case. Observe that $q \equiv 7, 19, 31$ or 43

mod 60. If $q \equiv 7 \pmod{60}$ then $q \equiv 7 \pmod{10}$ and $2^q \equiv 2^7 \equiv 7 \pmod{11}$, so that $(\frac{11}{p}) = -(\frac{p}{11}) = -(\frac{6}{11}) = 1$ and $\varrho_p = 11$. If $q \equiv 19 \pmod{60}$ then $2^q \equiv 2^9 \equiv 6 \pmod{11}$ and $(\frac{11}{p}) = -(\frac{p}{11}) = -(\frac{5}{11}) = -1$. If $q \equiv 31 \pmod{60}$ then $2^q \equiv 2 \pmod{11}$ and $(\frac{11}{p}) = -(\frac{p}{11}) = -(\frac{1}{11}) = -1$. Finally, for $q \equiv 43 \pmod{60}$ we have $2^q \equiv 8 \pmod{11}$ and $(\frac{11}{p}) = -(\frac{p}{11}) = -(\frac{7}{11}) = 1$. This completes the proof. ■

It is easy to show that if $p = 2^{2^n}+1$ is a Fermat prime with $n \geqslant 1$, then $\varrho_p = 11$ if n is odd, and $\varrho_p = 13$ if n is even. (From $2^{2^n} \equiv 1 \pmod{15}$ it follows that $(\frac{3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$ and $(\frac{5}{p}) = (\frac{p}{5}) = (\frac{2}{5}) = -1$. Similarly, from $2^{2^n} \equiv 2, 4 \pmod{7}$ we get $(\frac{7}{p}) = -1$, so that $\varrho_p \geqslant 11$. If $n \geqslant 2$ is even, then $2^{2^n} \equiv 3 \pmod{13}$, whence $p \equiv 4 \pmod{13}$ and $(\frac{13}{p}) = (\frac{p}{13}) = 1$. Use finally that $2^{2^n} \equiv 4, 5, 3, 9 \pmod{11}$ for $n \equiv 1, 2, 3, 0 \pmod{4}$, respectively.)

Suppose we have $p \equiv 1 \pmod{4}$ but p is not a Fermat prime. Let us show Nagell's [6] upper bound $\varrho_p \leqslant \sqrt{p-4}$ in this case. There are unique positive integers a, b such that $p = a^2 + 4b^2$ (Fermat). Using quadratic reciprocity we see that $\varrho_p \leqslant a \leqslant \sqrt{p-4b^2}$ when $a > 1$ (as a is odd), and if $a = 1$ then b is divisible by some odd prime (being a square mod p) and so $\varrho_p \leqslant b = \frac{1}{2}\sqrt{p-1}$.

Arguing as in the next section one gets the estimate $\varrho_p < \frac{1}{2}\sqrt{p}$ if $p \equiv 5 \pmod{8}$ and $h(p) > 1$; use that 2 remains prime in $\mathbb{Q}(\sqrt{p})$ and that the Minkowski constant of this number field is $\frac{1}{2}$.

3. The Minkowski bound

Let the prime $p \equiv 7 \pmod{8}$ in what follows, and let $K = \mathbb{Q}(\sqrt{-p})$. By a classical result of Minkowski (and Dirichlet) in every ideal class of K there is an (integral) ideal $\mathfrak{a}$ with (absolute) norm $\mathrm{N}\mathfrak{a} < \frac{2}{\pi}\sqrt{\mathrm{p}}$ (see [8, Lemma 2.3]). This estimate will be crucial for our approach.

Proposition 1. *Let $p \equiv 7 \pmod{8}$ and $h = h(-p)$. Assume that $\varrho_p \geqslant \frac{2}{\pi}\sqrt{p}$. Then the ideal class group $C(K)$ of $K = \mathbb{Q}(\sqrt{-p})$ is cyclic and $p = 2^{h+2} - u^2$ for some positive (odd) integer $u < \sqrt{p}$.*

Proof. We may assume that $p > 7$. Then $h > 1$ (as is easily seen; see below). Since $-p \equiv 1 \pmod{8}$, the prime $(2) = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K. Let $0 \neq \alpha = \frac{x+y\sqrt{-p}}{2}$ be an integer in K, where $x, y \in \mathbb{Z}$ have the same parity. Then its norm $\mathrm{N}(\alpha) = \frac{\mathrm{x}^2+\mathrm{py}^2}{4}$ cannot be equal to 2. So $\mathfrak{p}$ (and its complex conjugate $\bar{\mathfrak{p}}$) cannot be principal ideals (having norm 2). Let $h_0 \leqslant h$ be the order of the ideal class $[\mathfrak{p}]$ of $\mathfrak{p}$. Then $h_0 > 1$ and $\mathfrak{p}^{h_0} = (\alpha)$, with $\alpha = \frac{x+y\sqrt{-p}}{2}$ as above. Since $\bar{\mathfrak{p}}^{h_0} = (\bar{\alpha})$ is different from (α), we have $y \neq 0$ (and $y^2 \geqslant 4$ if $x = 0$). Observe that $2^h \geqslant 2^{h_0} = \frac{x^2+py^2}{4}$.

Now assume that $\varrho_p \geqslant \frac{2}{\pi}\sqrt{p}$. Let $\mathfrak{a}$ be an ideal of K with norm $\mathrm{N}\mathfrak{a} < \frac{2}{\pi}\sqrt{\mathrm{p}}$. Suppose $\mathfrak{q} \neq \mathfrak{p}, \bar{\mathfrak{p}}$ is a prime ideal of K appearing in $\mathfrak{a}$. Then $\mathfrak{q}|q$ where q is an odd rational prime, and we assert that $\mathfrak{q} = (q)$ is principal. Clearly $q \leqslant \mathrm{N}\mathfrak{q} < \frac{2}{\pi}\sqrt{\mathrm{p}}$

and so $(\frac{q}{p}) = -1$ by assumption. But then $(\frac{-p}{q}) = -1$ by quadratic reciprocity. Hence the assertion. This shows that $C(K)$ is generated by $[\mathfrak{p}]$ (or $[\bar{\mathfrak{p}}] = [\mathfrak{p}]^{-1}$). In particular, $h = h_0$ in the notation introduced above, and this is odd by Lemma 2. For ideals $\mathfrak{p}^i\bar{\mathfrak{p}}^j$ in $[\mathfrak{p}]^{(h-1)/2}$ we have $i - j = (h-1)/2$ and $\mathrm{N}(\mathfrak{p}^{\mathrm{i}}\bar{\mathfrak{p}}^{\mathrm{j}}) = 2^{\mathrm{i}+\mathrm{j}}$. Hence the minimal norm of ideals in this class equals $2^{(h-1)/2}$. Consequently

$$2^{(h-1)/2} < \frac{2}{\pi}\sqrt{p}$$

and, therefore, $2^h < \frac{8}{\pi^2}p < p$. Comparing this with the identity $2^h = 2^{h_0} = \frac{x^2+py^2}{4}$ obtained before, this forces that $y^2 = 1$ and that $u = |x|$ is a positive odd integer. Hence $u^2 + p = 2^{h+2} < \frac{32}{\pi^2}p$, giving $u < \frac{3}{2}\sqrt{p}$. We have to improve this upper bound.

One knows that $2X^2 - Y^2$ is the unique (primitive) quadratic form with discriminant 8, up to proper equivalence (see [15, p. 81]). From $(\frac{8}{p}) = 1$ and Lemma 1 we infer that $p = 2a^2 - b^2$ for positive integers a, b. Here $a = 2a_0$ must be even and b odd (as $p \equiv 7 \,(\mathrm{mod}\, 8)$), and by Theorem 1 in [3] we can choose a, b such that $b < \sqrt{p}$. Assume there is an odd prime q dividing a_0. Then $(\frac{q}{p}) = (\frac{-p}{q}) = (\frac{b^2}{q}) = 1$ and $\varrho_p \leqslant q \leqslant a_0 = \sqrt{(p+b^2)/8} < \frac{1}{2}\sqrt{p}$, against our assumption. Hence $a_0 = 2^n$ and $p = 2^{2n+3} - b^2$ for some integer $n \geqslant 1$. We claim that $h+2 = 2n+3$ and $u = b$. Otherwise $h + 2 \leqslant 2n+1$, implying that $p < 2^{h+2} \leqslant 2^{2n+1} = (p+b^2)/4 < p/2$, or $h+2 \geqslant 2n+5$ and this implies that $p > 2^h \geqslant 2^{2n+3} = p + b^2 > p$. In both cases we get a contradiction. Hence $u = b < \sqrt{p}$, as desired. ∎

Remark. We have $\varrho_p \geqslant \frac{2}{\pi}\sqrt{p}$ for the Mersenne primes $p = 7, 31, 127$ (Lemma 4) and also for $p \in \{103, 463, 487\}$ ($\varrho_{103} = 7$, $\varrho_{463} = 17$, $\varrho_{487} = 19$). One can deduce from Lemma 3 that these are the only primes $p \equiv 7 \,(\mathrm{mod}\, 8)$ where this happens, with at most one exception, where the possible exceptional prime will be the same as that described in Theorems 1, 2 (provided p_u exists). We do not go into details but remark that the elementary approach to our theorems given below applies also in this case (with a bit more effort).

4. Towards the exceptional prime

Let $p \equiv 7 \,(\mathrm{mod}\, 8)$, $p > 7$ and $h = h(-p)$. Assume in what follows that $\varrho_p \geqslant \sqrt{p}$. By Lemma 2 we know that h is odd, and $h > 1$ (as $p > 7$). Let $h = 2n+1$ ($n \geqslant 1$). From Proposition 1 it follows that $p = 2^{2n+3} - u^2$ for some positive odd integer $u < \sqrt{p}$. In particular $2^{2n+2} < p < 2^{2n+3}$.

For any integer r with $1 \leqslant r \leqslant n$ let u_r be the least positive (odd) integer such that 2^{r+2} is a divisor of $u_r^2 + p$. Then 2^{r+2} also divides $(2^{r+1} - u_r)^2 + p$ (as $r+2 \geqslant 3$) and so $|2^{r+1} - u_r| \geqslant u_r$. Since $u_r - 2^{r+1} < u_r$, we must have $2^{r+1} - u_r \geqslant u_r$ and hence $u_r < 2^r$ (as u_r is odd). By definition $u_1 = 1$ (as $p \equiv 7 \,(\mathrm{mod}\, 8)$) and $1 = u_1 \leqslant u_2 \leqslant \ldots \leqslant u_n \leqslant u$. Let $c_r = \frac{u_r^2+p}{2^{r+2}}$ ($1 \leqslant r \leqslant n$).

Proposition 2. *Under the above assumptions, the quadratic forms $f_r = 2^rX^2 + u_rXY + c_rY^2$, together with their opposites f_r^- and the principal form f_0, are* *precisely all the distinct reduced forms with discriminant* $-p$ $(1 \leqslant r \leqslant n)$. *The coefficients* c_r *are strictly decreasing, with* $c_1 = \frac{1+p}{8} > c_2 > \cdots > c_n = 2^{n+1}$. *Moreover:*

(i) *Each odd integer in the interval* $(1, p)$ *which is properly represented by* f_0 *or some form* f_r *is a prime.*

(ii) *We have* $5 \leqslant u = u_n < (3 - \sqrt{7})2^{n-1} < 2^{n-2}$, *and* u *is divisible only by primes congruent* 5 *or* 7 *mod* 8.

(iii) $2^{2n} - u^2 = (2^n - u)(2^n + u)$ *is divisible only by primes congruent* 3 *mod* 4. *In particular,* $u \equiv 3, 5$ *or* 7 *mod* 10 *when* n *is odd, and* $u \equiv 1, 5$ *or* 9 *mod* 10 *otherwise.*

Proof. Clearly $c_r > 2^{2n+2-r-2} \geqslant 2^n$ (as $p > 2^{2n+2}$). In particular $c_r > 2^r$ for each r and so f_r is reduced. Now recall that $h = 2n + 1$ and that there are just h distinct reduced forms with discriminant $-p$. This gives the first assertion. Of course $f_1 = 2X^2 + XY + \frac{1+p}{8}Y^2$. Let us consider $f_n = 2^n X^2 + u_n XY + c_n Y^2$. We know that $u_n < 2^n < \frac{1}{2}\sqrt{p}$ and that $c_n > 2^n$. On the other hand $u_n \leqslant u$ (by definition) and so

$$c_n = \frac{u_n^2 + p}{2^{n+2}} \leqslant \frac{u^2 + p}{2^{n+2}} = 2^{n+1} < \sqrt{p}.$$

If there is an odd prime q dividing $c_n = f_n(0, 1)$, then q is a quadratic residue mod p by Lemma 1. We infer that c_n must be a power of 2, and this implies that $c_n = 2^{n+1}$ and that $u = u_n$. By Lemma 4 and assumption we also have $u > 1$.

If $u_r = u_{r+1}$ for some r, then $c_r = 2c_{r+1}$. Suppose $u_r < u_{r+1}$. This means that $2^r < u_{r+1} < 2^{r+1}$, by definition of reduced forms. Hence $u_{r+1} - 2^r < 2^{r+1} - 2^r = 2^r$. Since 2^{r+2} is a divisor of both $u_r^2 + p$ and $u_{r+1}^2 + p$, it divides $u_{r+1}^2 - u_r^2 = (u_{r+1} - u_r)(u_{r+1} + u_r)$. Since u_r and u_{r+1} are odd, 2^{r+1} is a divisor of just one of $u_{r+1} - u_r$ or $u_{r+1} + u_r$ (the other one being $\equiv 2 \,(\mathrm{mod}\, 4)$). Using that $u_r < 2^r$, $u_{r+1} < 2^{r+1}$ are positive we infer that $u_r = 2^{r+1} - u_{r+1}$. We derive that

$$c_r = \frac{(2^{r+1} - u_{r+1})^2 + p}{2^{r+2}} = 2c_{r+1} - (u_{r+1} - 2^r) > 2c_{r+1} - 2^r > c_{r+1}.$$

So the sequence $\{c_r\}$ is strictly decreasing with r.

(i) Let f be any quadratic form with discriminant $-p$, and let x, y be relatively prime integers such that the odd part, say m, of $f(x, y)$ is greater than 1 and less than p. Then each (odd) prime q dividing m is a square mod p by Lemma 1. Assume m is no prime. Then we may arrange matters such that $q \leqslant \frac{m}{q}$ and so $q^2 \leqslant m < p$. But then $\varrho_p \leqslant q < \sqrt{p}$, against our general assumption. Hence $m = q$ is a prime.

(ii) We know already that $u = u_n$. Let $w = f_n(1, -1) = 3 \cdot 2^n - u$. By (i) w is an (odd) prime, and $(\frac{w}{p}) = 1$ by Lemma 1. Thus $w^2 > p = 2^{2n+3} - u^2$ by assumption. It follows that $u^2 - 3 \cdot 2^n u + 2^{2n-1} > 0$, yielding that $u < (3 - \sqrt{7})2^{n-1} < 2^{n-2}$. Let q be an (odd) prime dividing u. Then $q \leqslant u < \sqrt{p}$ and so $(\frac{q}{p}) = (\frac{-p}{q}) = (\frac{-2}{q}) = -1$, whence $q \equiv 5, 7 \,(\mathrm{mod}\, 8)$. This also shows that $u \geqslant 5$, and that $n \geqslant 5$ (at least).

(iii) Consider $p = 2^{2n+2} + (2^{2n+2} - u^2)$. We have $2^{n+1} + u < \sqrt{p}$, because $u < 2^{n-2}$, $u^2 + 2^{n+1}u < 2^{2n-4} + 2^{2n-1} < 2^{2n}$ and so $2^{2n+2} + 2^{n+2}u + u^2 < p = 2^{2n+3} - u^2$. If q is an odd prime dividing $2^{2n+2} - u^2 = (2^{n+1} - u)(2^{n+1} + u)$, then $(\frac{q}{p}) = (\frac{-p}{q}) = (\frac{-1}{q}) = -1$ and so $q \equiv 3 \,(\mathrm{mod}\, 4)$ (as $\varrho_p \geqslant \sqrt{p}$ by assumption). Let n be odd. Then $2^{n+1} \equiv pm4 \,(\mathrm{mod}\, 10)$ and so one of $2^{n+1}pmu$ is divisible by 5 if $u \equiv pm1 \,(\mathrm{mod}\, 10)$, which cannot happen. Hence $u \equiv 3, 5$ or 7 mod 10 in this case. Similarly, $u \equiv 1, 5$ or 9 mod 10 when n is even. The proof is complete. ■

5. Proof of Theorem 1

Keep the assumptions and notation introduced in the preceding section. We prove that we must have $n \geqslant 12$ ($h = h(-p) = 2n + 1$). We know already that $n \geqslant 5$. In our argumentation we ignore that $2^{2n+3} - u^2$ may be no prime (using a table of the primes up to 10,000 only). Mostly we argue by verifying that one of $w = f_n(1, -1) = 3 \cdot 2^n - u$ or $w' = f_n(1, 1) = 3 \cdot 2^n + u$ is not prime, contrary to statement (i) in Proposition 2. Of course $w = w(n, u)$ and $w' = w'(n, u)$ depend on n and u. Fortunately $u = u(n)$ is quite restricted by Proposition 2.

Assume that $n = 5$. Then $u < (3 - \sqrt{7}) \cdot 2^4 < 6$ and so necessarily $u = 5$ (where $p = 2^{13} - 25 = 8167$ actually is a prime). But here $w = 3 \cdot 2^5 - 25 = 7 \cdot 13$ is no prime. For $n = 6$ we have $u < 12$ but $u \neq 7, 11$ by Proposition 2, and $w = 3 \cdot 2^6 - u$ is no prime for $u = 5, 9$.

Let $n = 7$. Then $u < 23$, and by Proposition 2 only the possibilities $u = 5, 7, 13$ remain. Now $w = 3 \cdot 2^7 - u$ is not prime for $u = 7, 13$ (namely $13 \cdot 29$ and $7 \cdot 53$, respectively). For $u = 5$ both w and w' are primes, but $9 \cdot 2^{n-1} - u$ equals $31 \cdot 37$ for $n = 7$, $u = 5$.

Let $n = 8$. Then $u < 46$, and we have to examine the cases $u = 5, 25, 29, 31$ (Proposition 2). Here $w = 3 \cdot 2^8 - u$ is no prime for $u = 5, 31$ (namely $7 \cdot 109$ resp. $11 \cdot 67$), and $w' = 3 \cdot 2^8 + 25 = 13 \cdot 161$. Finally, $2^{n+1} + u = 2^9 + 29 = 541$ is a prime congruent 1 mod 4 (and so $\varrho_p \leqslant 541 < \sqrt{p}$); alternately, $f_{n-1}(3, 1) = 17 \cdot 2^{n-1} + 3u = 31 \cdot 73$ for $n = 8$, $u = 29$ (and so $\varrho_p \leqslant 31$).

Let $n = 9$. Then $u < 91$ and $u = 5, 7, 13, 23, 25, 35, 37, 43, 47$ or 53 (Proposition 2). Here one of w, w' is no prime for $u \in \{5, 7, 23, 25, 35, 37\}$. Also, $9 \cdot 2^8 + u$ is not prime for $u = 13, 43$ and 47.

Let $n = 10$. Then $u < 182$ and $u = 5, 25, 29, 31, 49, 61, 71, 79, 91, 101, 109, 115, 125, 131, 139, 145, 149, 151, 155, 161, 169, 175, 179$ or 181 (Proposition 2). Here one of w, w' is not prime except when $u \in \{5, 109, 115\}$. Also, $9 \cdot 2^9 - u$ is not prime for $u = 109, 115$, and $2^{11} + 5 = 2053$ is a prime congruent 1 mod 4.

Let $n = 11$. Then $u < 363$ and $u = 5, 7, 13, 23, 25, 35, 37, 43, 47, 53$, 65, 103, 115, 125, 127, 155, 157, 167, 173, 175, 185, 197, 203, 217, 223, 233, 235, 235, 263, 265, $277, 293, 305, 317, 325, 343$ or 355 (Proposition 2). Here one of w, w' is no prime unless $u \in \{23, 157, 217, 277, 305\}$. But $9 \cdot 2^{10} - u$ is not prime for $u \in \{23, 277, 305\}$. Further $2^{12} - 157 = 3 \cdot 13 \cdot 101$ with $13 \equiv 1 \,(\mathrm{mod}\, 4)$. Finally, $f_{n-2}(1, -1)$ equals $13 \cdot 1283$ for $n = 11$ and $u = 217$. Consequently $n \geqslant 12$, as desired.

Now we apply Lemma 3, picking $\varepsilon = \frac{1}{18}$. Then

$$p > 2^{2n+2} \geqslant 2^{26} \geqslant \max(e^{18}, e^{11.2}) = e^{18}$$

but $h = 2n + 1 < \frac{0.655}{18\pi} p^{\frac{1}{2} - \frac{1}{18}}$, because

$$2n + 1 < \frac{0.655}{18\pi} (2^{\frac{4}{9}})^{2n+2}$$

for $n \geqslant 12$. Thus $\chi = (\frac{-p}{*})$ must be the unique (exceptional) primitive real Dirichlet character with conductor $|d| = p \geqslant e^{18}$ which possibly exists by virtue of the Siegel–Tatuzawa theorem. By [12, Lemma 9] $L(s, \chi)$ has a real zero in the interval $(\frac{71}{72}, 1)$, which violates the Extended Riemann Hypothesis. This completes the proof of Theorem 1.

6. Proof of Theorem 2

Assume the large exceptional prime $p = p_u$ exists (with $\varrho_p \geqslant \sqrt{p}$). Then $p = 2^{h+2} - u^2$ where $h = h(-p)$ and u is a positive odd integer (Proposition 1). In view of Proposition 2 we know that $5 \leqslant u < (3 - \sqrt{7}) 2^{(h-3)/2} < 2^{(h-5)/2}$. In the course of the proof for Theorem 1 we have shown that $h \geqslant 25$ and, therefore, $p > 2^{26}$. But if $h(d) \leqslant 100$ for some negative fundamental discriminant d, then $|d| \leqslant 2^{22}$ by the work of Watkins [14]. Thus we even have $h > 100$.

It follows from Proposition 2 that $\varrho_p = f_n(1, -1) = 3 \cdot 2^{(h-1)/2} - u$. Define the real number t through $3 \cdot 2^{(h-1)/2} = t\sqrt{p}$. Then $9 \cdot 2^{h-1} = t^2 p = t^2(2^{h+2} - u^2) > t^2(2^{h+2} - (3 - \sqrt{7})^2 2^{h-3})$ and $t < 1.06275$. Thus $\varrho_p < 1.06275\sqrt{p} - u$, as asserted.

(i) By the Siegel–Tatuzawa theorem (Lemma 3), for every negative fundamental discriminant $d \neq -p$ with $|d| \geqslant e^{18}$ we have $h(d) > \frac{0.655}{18\pi} |d|^{\frac{4}{9}}$.

(ii) Consider the quadratic form $f = 2X^2 + uXY + 2^{h-1}Y^2$. This form is properly equivalent with the reduced form f_1 when $u \equiv 1 \pmod 4$ and with f_1^- otherwise (in the notation of Proposition 2). The class of each of f, f_1, f_1^- generates the form class group $C(-p)$ (as these forms correspond to one of the prime ideals above 2 in $\mathbb{Q}(\sqrt{-p})$ described in Proposition 1). The quadratic polynomial

$$f(2X + 1, -1) = 8X^2 + (8 - 2u)X + 2^{h-1} + 2 - u$$

takes only odd (positive) values on integers. It follows from statement (i) of Proposition 2 that this polynomial takes prime values on all integers in $[-2^{(h-3)/2}, 2^{(h-3)/2}]$ (as these values are less than p). These primes are pairwise distinct, because if the polynomial takes the same value on integers $x \neq y$, then we get $x + y = \frac{2u-8}{8}$, which is impossible. We are done.

References

[1] S. Chowla, J.R. Cowles, M.J. Cowles, *The least prime quadratic residue and the class number*, J. Number Theory **22** (1986), 1–3.

[2] D.A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley, New York , 1989.

[3] A. Gica, *A proof of a conjecture of additive number theory*, J. Number Theory **94** (2002), 80–89.

[4] Y.V. Linnik, A.I. Vinogradov, *Hyperelliptic curves and the least prime quadratic residue*, Doklady Akad. Nauk SSSR **168** (1966), 259–261.

[5] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamb. **1** (1922), 140–150.

[6] T. Nagell, *Zahlentheoretische Notizen II*, Videnskapsselskapets Skrifter. I. Mat.-naturv. Klasse (1923), 7–10.

[7] T. Nagell, *Sur les restes et les non-restes quadratiques suivant un module premier*, Ark. Mat. **1** (1950), 185-193.

[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, New York, 1990.

[9] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Astérisque **121-122** (1985), 309–323.

[10] J. Pintz, *Elementary methods in the theory of L-functions VI, On the least prime quadratic residue (mod p)*, Acta Arith. **32** (1977), 173–178.

[11] C.L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.

[12] T. Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. **21** (1951), 169–178.

[13] M. Watkins, *Real zeros of real odd Dirichlet L-functions*, Math. Comp. **73** (2004), 415–423.

[14] M. Watkins, *Class numbers of imaginary quadratic number fields*, Math. Comp. **73** (2004), 907–938.

[15] D.B. Zagier, *Zetafunktionen und und quadratische Körper*, Springer, New York, 1981.

Addresses: Wolfgang Knapp, Markus Köcher, Peter Schmid: Mathematisches Institut, Universität Tübingen, Auf der Morgenstelle 10, 72076 Tübingen, Germany.

E-mail: wolfgang.knapp@uni-tuebingen.de, markus.koecher@t-online.de, peter.schmid@uni-tuebingen.de

Received: 3 September 2011