for all \( r \geq 2 \), and hence if we choose \( \mu < (m+n)^{-1}(m+n-1)^{-1} \), then
\[
|C(q; \psi^*)| < \psi^*(q)^{m+n},
\]
for all sufficiently large \( q \). It now follows from the Borel–Cantelli lemma that the system of inequalities
\[
\|q \xi_i(u)\| < \psi^*(q), \quad i = 1, \ldots, m+n,
\]
has at most finitely many solutions for almost all \( u \in \Omega \), which proves Theorem 1.3.

References


Received on 9.5.1989

Representation of primes by the principal form of discriminant \(-D\) when the classnumber \(h(-D)\) is 3

by

KENNETH S. WILLIAMS* (Ottawa, Ont.) and RICHARD H. HUDSON (Columbia, S.C.)

0. Notation and preliminary result. Throughout this paper \( p \) denotes a prime \( > 3 \). We shall be concerned with binary quadratic forms \( ax^2 + bxy + cy^2 \), written \((a, b, c)\), which are integral (that is, \( a, b, c \) are integers), positive-definite (that is, \( a > 0, b^2 - 4ac < 0 \)) and primitive (that is, GCD\((a, b, c) = 1 \)). The discriminant of the form \((a, b, c)\) is the negative integer \( b^2 - 4ac \). On the set of all such forms of fixed discriminant \(-D\) \((D > 0)\), we define an equivalence relation \( \sim \) as follows: we write \((a, b, c) \sim (a', b', c')\) if there exist integers \( p, q, r, s \) with \( ps - qr = +1 \) such that
\[
a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2 = a'x^2 + b'xy + c'y^2.
\]
It is well known that there are only finitely many such equivalence classes. The number of classes is called the classnumber of forms of discriminant \(-D\) and is denoted by \( h(-D) \). The principal form of discriminant \(-D\) is the form \( p_{-D} \) given by
\[
0.1 \quad p_{-D} = \begin{cases} (1, 0, D/4), & \text{if } D \equiv 0 \pmod{4}, \\ (1, 1, (D+1)/4), & \text{if } D \equiv 3 \pmod{4}. \end{cases}
\]
A positive integer \( m \) is said to be represented by the form \((a, b, c)\) if there exist integers \( x \) and \( y \) such that \( m = ax^2 + bxy + cy^2 \). If the prime \( p \) (not dividing \( 2D \)) is represented by a form of discriminant \(-D\), it is well known that the Legendre symbol \( \left( \frac{-D}{p} \right) = +1 \). In this paper we shall be concerned with the representability of a prime \( p \) \((> 3)\) by the principal form \( p_{-D} \) of discriminant \(-D\) when \( h(-D) = 3 \).

Recent deep work of Goldfeld, Gross, Mestre, Oesterlé and Zagier (see [6], [7], [12], [13], [14], [20]) has led to the complete determination of all the imaginary quadratic fields with classnumber 3 [12: Théorème 4], namely, * Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.
The complete list of all the imaginary quadratic fields with classnumber 1 has been known for over twenty years [15], namely:

\[ Q(\sqrt{-n}) : n = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907. \]

From these results we can deduce

**Proposition.** \( h(-D) = 3 \) if and only if


**Proof.** Let \( d \) be the discriminant of the imaginary quadratic field given uniquely by

\[-D = f^2d,\]

where \( f \) is a positive integer. Then, by a formula of Gauss, we have

\[ h(-D) = h(f^2d) = h(d)\psi_d(f)/u, \]

where

\[ \psi_d(f) = f \prod_{q \mid d} \left( 1 - \left( \frac{f}{q} \right) \right), \]

and

\[ u = \begin{cases} 3, & \text{if } d = -3, \\ 2, & \text{if } d = -4, \\ 1, & \text{if } d < -4. \end{cases} \]

Note that \( q \) runs through the distinct primes dividing \( f \) and \( \left( \frac{d}{q} \right) \) is the Kronecker symbol. As \( \psi_d(f) \) is a positive integer and \( h(-3) = h(-4) = 1 \), we see that

\[ h(-D) = 3 \iff \text{ (a) } d < -4, \text{ (b) } d = -3, \text{ (c) } d = 1, \text{ or } \psi_d(f) = 1 \text{ or } \psi_d(f) = 3 \text{ or } 6 \text{ or } 9. \]

Thus, appealing to the lists of imaginary quadratic fields with classnumber 1 or 3, we see that:

(a) occurs if and only if \( D = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907, 23 \cdot 2^2, 31 \cdot 2^2; \)

(b) occurs if and only if \( D = 11 \cdot 2^2, 19 \cdot 2^2, 43 \cdot 2^2, 67 \cdot 2^2, 163 \cdot 2^2; \)

(c) cannot occur;

(d) occurs if and only if \( D = 3 \cdot 6^2, 3 \cdot 9^2. \)

This gives the twenty-five values of \( D \) listed in (0.2).

1. **Introduction.** Gauss [5] showed that 2 is congruent to a cube modulo a prime \( \equiv 1 \text{ (mod 3) if and only if there exist integers } x \text{ and } y \text{ such that } p = x^2 + 27y^2, \) that is, if and only if \( p \) is represented by the principal form of discriminant \(-108\). Moreover, when \( p = 2 \) is a cube (mod \( p \)), where \( p = 1 \) (mod 3), 2 has three distinct cube roots (mod \( p \)). If \( p = 2 \) (mod 3) then \( \left( \frac{-108}{p} \right) = \left( \frac{-3}{p} \right) = -1 \) and \( p \) is not represented by any form of discriminant \(-108\), and 2 has a unique cube root (mod \( p \)). Since every positive-definite, primitive, integral binary quadratic form of discriminant \(-108\) is equivalent to exactly one of the three forms \((1, 0, 27); (4, -2, 7); (4, 2, 7)\), Gauss' theorem can be expressed as follows:

**Theorem (Gauss).** The polynomial \( x^3 - 2 \) is

(i) the product of three distinct linear polynomials (mod \( p \)) if \( \left( \frac{-3}{p} \right) = +1 \) and \( p \) is represented by \((1, 0, 27); \)

(ii) the product of a linear polynomial and an irreducible quadratic polynomial (mod \( p \)) if \( \left( \frac{-3}{p} \right) = -1; \)

(iii) irreducible (mod \( p \)) if \( \left( \frac{-3}{p} \right) = +1 \) and \( p \) is represented by \((4, \pm 2, 7). \)

Clearly Gauss' theorem can be reformulated as a criterion for \( p \) to be represented by the principal form of discriminant \(-108\), namely,
Theorem (Gauss). The prime $p$ is represented by $(1, 0, 27)$ if and only if
\[
\left(\frac{-3}{p}\right) = +1 \text{ and } x^3 - 2 \text{ is congruent to the product of three distinct linear polynomials (mod } p).
\]

Jacobi [10] showed that if $-23$ is congruent to a cube modulo a prime $p \equiv 1 \pmod{3}$ and only if $p$ can be written in the form $4p = A^2 + 243B^2$, where $A$ and $B$ are integers. If $4p = A^2 + 243B^2$ then we have $A \equiv B \pmod{2}$ and $p = x^2 + xy + 61y^2$ with $x = \frac{1}{2}(A - B)$, $y = B$. Conversely, if $p = x^2 + xy + 61y^2$ then we have $4p = A^2 + 243B^2$ with $A = 2x + y$, $B = y$. Since every positive-definite, primitive, integral binary quadratic form of discriminant $-243$ is equivalent to exactly one of the three forms $(1, 1, 61)$, $(7, -3, 9)$, $(7, 3, 9)$, Jacobi's theorem can be restated as follows:

Theorem (Jacobi). The prime $p$ is represented by $(1, 1, 61)$ if and only if
\[
\left(\frac{-3}{p}\right) = +1 \text{ and } x^3 - 3 \text{ is congruent to the product of three distinct linear polynomials (mod } p).
\]

In this paper we generalize the results of Gauss and Jacobi to all $D > 0$ for which $h(-D) = 3$. These values of $D$ are listed in (0.2). We prove Theorem 1. Let $D$ be a positive integer such that $h(-D) = 3$. Then the prime $p \equiv 3 \pmod{4}, p \equiv D$ is represented by the principal form $D$ of discriminant $-D$ if and only if $\left(\frac{-D}{p}\right) = +1$ and $f_{-D}(x)$ is congruent to the product of three distinct linear polynomials (mod $p$), where $f_{-D}(x)$ is the monic cubic polynomial with integral coefficients listed in Table 1. Further we have
\[
\text{discriminant}(f_{-D}(x)) = \begin{cases} 
-D, & \text{if } D \equiv 3 \pmod{4} \text{ or } D \equiv 12 \pmod{32}, \\
-D/4, & \text{if } D \equiv 28 \pmod{32}.
\end{cases}
\]

<table>
<thead>
<tr>
<th>$D$</th>
<th>$f_{-D}(x)$</th>
<th>$D$</th>
<th>$f_{-D}(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>$x^3 - x + 1$</td>
<td>243</td>
<td>$x^3 - 3$</td>
</tr>
<tr>
<td>31</td>
<td>$x^3 + x + 1$</td>
<td>268</td>
<td>$x^3 + 2x^2 - 2x + 2$</td>
</tr>
<tr>
<td>44</td>
<td>$x^3 + x^2 - x + 1$</td>
<td>283</td>
<td>$x^3 + 4x + 1$</td>
</tr>
<tr>
<td>59</td>
<td>$x^3 + 2x + 1$</td>
<td>307</td>
<td>$x^3 - x^2 + 3x + 2$</td>
</tr>
<tr>
<td>76</td>
<td>$x^3 - 2x + 2$</td>
<td>331</td>
<td>$x^3 - 2x^2 + 4x + 1$</td>
</tr>
<tr>
<td>83</td>
<td>$x^3 - x^2 + 1$</td>
<td>379</td>
<td>$x^3 + x^2 + x + 4$</td>
</tr>
<tr>
<td>92</td>
<td>$x^3 - x^2 + 1$</td>
<td>499</td>
<td>$x^3 + 4x^2 + 3$</td>
</tr>
<tr>
<td>107</td>
<td>$x^3 + x^2 + 3x + 2$</td>
<td>547</td>
<td>$x^3 + x^2 - 3x + 4$</td>
</tr>
<tr>
<td>108</td>
<td>$x^3 - 2x$</td>
<td>562</td>
<td>$x^3 - x^2 - 5x + 3$</td>
</tr>
<tr>
<td>124</td>
<td>$x^3 + x + 1$</td>
<td>652</td>
<td>$x^3 + 3x^2 - 5x + 3$</td>
</tr>
<tr>
<td>139</td>
<td>$x^3 + x^2 + 2x + 2$</td>
<td>883</td>
<td>$x^3 + 5x^2 - 5x + 2$</td>
</tr>
<tr>
<td>172</td>
<td>$x^3 - x^2 + 1$</td>
<td>907</td>
<td>$x^3 + 5x^2 + x + 2$</td>
</tr>
<tr>
<td>211</td>
<td>$x^3 - 2x + 3$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We prove Theorem 2. (i) For those $D$ in (A), the Hilbert class field over $Q(\sqrt{-D})$ is $Q(\sqrt{-D}, \sqrt[3]{x_D} + \sqrt[3]{x_D^*})$, where $x_D$ is given as follows:

\[
\begin{array}{cccccc}
D & x_D & D & x_D & D & x_D \\
23 & (27 + 3\sqrt{69})/2 & 139 & (61 + 3\sqrt{417})/2 & 379 & (-101 + 3\sqrt{1137})/2 \\
31 & (27 + 3\sqrt{93})/2 & 211 & (81 + 3\sqrt{633})/2 & 499 & (-81 + 3\sqrt{1497})/2 \\
59 & (27 + 3\sqrt{177})/2 & 283 & (27 - 3\sqrt{849})/2 & 547 & (-137 + 3\sqrt{1641})/2 \\
83 & (27 + 3\sqrt{249})/2 & 307 & (79 + 3\sqrt{921})/2 & 643 & (-135 + 3\sqrt{1929})/2 \\
107 & (29 + 3\sqrt{321})/2 & 331 & (83 - 3\sqrt{993})/2 & 883 & (-529 + 3\sqrt{2699})/2 \\
23 & (27 + 3\sqrt{69})/2 & 139 & (61 + 3\sqrt{417})/2 & 379 & (-101 + 3\sqrt{1137})/2 \\
31 & (27 + 3\sqrt{93})/2 & 211 & (81 + 3\sqrt{633})/2 & 499 & (-81 + 3\sqrt{1497})/2 \\
59 & (27 + 3\sqrt{177})/2 & 283 & (27 - 3\sqrt{849})/2 & 547 & (-137 + 3\sqrt{1641})/2 \\
83 & (27 + 3\sqrt{249})/2 & 307 & (79 + 3\sqrt{921})/2 & 643 & (-135 + 3\sqrt{1929})/2 \\
107 & (29 + 3\sqrt{321})/2 & 331 & (83 - 3\sqrt{993})/2 & 883 & (-529 + 3\sqrt{2699})/2 \\
\end{array}
\]
(ii) For those $D$ in (B), the ring class field of the order $\mathbb{Z}[\sqrt{D}/4]$ in $\mathbb{Z}[-1+\sqrt{-D}/4]/2$ is

$$Q(\sqrt{-D}/4,\sqrt[3]{\beta_D}+\sqrt{\gamma_D}),$$

where

$$\beta_{44} = -19 + 3\sqrt{33},$$
$$\beta_{76} = -27 + 3\sqrt{57},$$
$$\beta_{172} = -35 + 3\sqrt{129},$$
$$\beta_{268} = -53 + 3\sqrt{201},$$
$$\beta_{652} = -135 + 3\sqrt{489}. $$

We remark that Hasse [9] has shown that the Hilbert class field over

$$Q(\sqrt{-23})$$

is solvable in integers $x$ and $y$ if and only if

$$\begin{align*}
\{u_{p-1/3} = 2 \pmod{p}, & \quad \text{if } p = 1 \pmod{3}, \\
\{u_{p+1/3} = -2k \pmod{p}, & \quad \text{if } p = 2 \pmod{3}, \\
\end{align*}$$

where the sequence of integers $\{u_n\}_{n=0,1,2,...}$ is given by

$$\begin{align*}
\{u_0 = 2, & \quad u_1 = l, \\
u_{n+2} = lu_{n+1} + k^3u_n, \quad n = 0, 1, 2,..., \\
\end{align*}$$

and the integers $k, l$ are given in Table 2:

<table>
<thead>
<tr>
<th>Table 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D$</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>44</td>
</tr>
<tr>
<td>59</td>
</tr>
<tr>
<td>76</td>
</tr>
<tr>
<td>83</td>
</tr>
<tr>
<td>107</td>
</tr>
<tr>
<td>139</td>
</tr>
<tr>
<td>172</td>
</tr>
<tr>
<td>211</td>
</tr>
<tr>
<td>268</td>
</tr>
</tbody>
</table>

The identities

$$u_{2m} = u_m^2 - 2(-1)^m k^2 u_m, \quad u_{3m} = u_m^2 - 3(-1)^m k^3 u_m,$$

are often useful in computing $u_{(p+1)/3}$ (mod $p$). We illustrate Theorem 3 with a simple example.

**Example.** Is the prime 1297 represented by the form $(1, 0, 19)$? Here we have $p = 1297, (p-1)/3 = 432, D = 76, k = 8, l = -2$. Making use of the above identities, we obtain successively modulo 1297

$$u_0 = 2, \quad u_1 = -2, \quad u_2 = 1028, \quad u_4 = 726, \quad u_6 = 889,$$

so that, by Theorem 3, 1297 is represented by $(1, 0, 19)$. Indeed we have $1297 = 1 \cdot 9^2 + 19 \cdot 8^2$.

2. **Proof of Theorem 1 for those $D$ listed in (A).** Throughout this section, $D$ denotes one of the integers listed in (A). Note that $D$ is a prime $\equiv 3 \pmod{4}$. 

In Section 5, we use Theorem 1 and a theorem of Cauchy [2] to give a necessary and sufficient condition for the prime $p$ to be represented by $p - D$ (in list (A) or list (B) in terms of integer sequences defined by a second order linear recurrence relation which need only be considered modulo $p$. When $D = 23$ our result agrees with that of Gurak [8]. We prove

**Theorem 3.** Let $D$ denote one of the integers in list (A) or list (B). Let $p$ be a prime ($> 3$) such that $\left(\frac{-D}{p}\right) = +1$. Then

$$p = \begin{cases} 
-2 + D^2 \gamma^2, & \text{if } D \equiv 0 \pmod{4}, \\
-2 + D \gamma^2 \left(\frac{1 + D}{4}\right)^2, & \text{if } D \equiv 3 \pmod{4}, 
\end{cases}$$

where

$$\gamma = \sqrt{27 + 3\sqrt{69}/2 + \sqrt{(-27 - 3\sqrt{69}/2) \times 2}} = -3.9741...,
\delta = \sqrt{(29 + 3\sqrt{93}/2) \times 2 + \sqrt{(29 - 3\sqrt{93}/2) \times 2}} = 3.2646...;$$

and

$$\delta = \sqrt{(29 + 3\sqrt{93}/2) \times 2 + \sqrt{(29 - 3\sqrt{93}/2) \times 2}} = 3.2646...;$$

$$y = \sqrt{(29 + 3\sqrt{93}/2) \times 2 + \sqrt{(29 - 3\sqrt{93}/2) \times 2}} = 2.0469...,
Let \( p \) be a prime \( > 3 \) with \( p \not| D \). If \( \left( \frac{-D}{p} \right) = -1 \) then \( p \) is not represented by \( p_{-p} = (1, 1, \frac{1}{2}(D+1)) \) and, as \( \text{disc}(f_{-p}(x)) = -D \), by a theorem of Stickelberger [16], \( f_{-p}(x) \) is the product of a linear polynomial and an irreducible quadratic polynomial modulo \( p \). Now suppose \( \left( \frac{-D}{p} \right) = +1 \). We must show that \( p \) is represented by \( p_{-p} = (1, 1, \frac{1}{2}(D+1)) \) if and only if \( f_{-p}(x) \) is congruent to the product of three distinct linear polynomials (mod \( p \)).

We set

\[
K_D = \mathbb{Q}(\sqrt{3D}), \quad K_F = \mathbb{Q}(\sqrt{3D}) \setminus \{0\}.
\]

Let \( G_D \) be the group defined by

\[
G_D = \{ \alpha \in K_F^\times : \alpha = A^3 \text{ for some ideal } A \text{ of } K_D \}
\]

and let \( H_D \) be the subgroup of \( G_D \) given by

\[
H_D = \{ \alpha \in K_F^\times : \alpha = \beta^3 \text{ for some } \beta \in K_F^\times \}.
\]

Then \( G_D/H_D \) is a group isomorphic with the direct sum of \( r_D + 1 \) groups of order 3, where \( r_D \) is the rank of the 3-Sylow subgroup of the class group \( H(K_D) \) of \( K_D \). Now

\[
H(K_D) \approx \begin{cases} 
\mathbb{Z}_3^r, & \text{for } D = 107, 331, 643, \\
\mathbb{Z}_1^r, & \text{for } D = 547, \\
\mathbb{Z}, & \text{otherwise},
\end{cases}
\]

so

\[
r_D = \begin{cases} 
1, & \text{for } D = 107, 331, 643, \\
0, & \text{otherwise},
\end{cases}
\]

and thus

\[
G_D/H_D \approx \begin{cases} 
\mathbb{Z}_3 \times \mathbb{Z}_3, & \text{if } D = 107, 331, 643, \\
\mathbb{Z}_3, & \text{otherwise}.
\end{cases}
\]

Let \( \varepsilon_{3D} \) denote the fundamental unit (\( > 1 \)) of \( K_D \). When \( D \neq 107, 331, 643 \), a basis for the group \( G_D/H_D \) is \( \{\varepsilon_{3D}H_D\} \). When \( D = 107, 331 \) or 643, \( H(K_D) \) is generated by the class containing the ideal \( A_D = (2, \frac{1}{2}(1 + \sqrt{3D})) \). Since

\[
A_D = \left\{ \begin{array}{ll} 
\left( \frac{1}{2}(17 + \sqrt{321}) \right), & \text{if } D = 107, \\
\left( \frac{1}{4}(31 - \sqrt{993}) \right), & \text{if } D = 331, \\
\left( \frac{1}{2}(4963 - 113\sqrt{1929}) \right) = \left( \frac{1}{2}(1258562169097 - 28655537523\sqrt{1929}) \right), & \text{if } D = 643.
\end{array} \right.
\]

Next we define \( g_{-p}(x) \) to be the monic cubic polynomial

\[
g_{-p}(x) = x^3 + \frac{a_p}{3}x^2 + \frac{b_p}{27},
\]

where the integers \( a_p \) and \( b_p \) are listed in Table 4.

Table 3

<table>
<thead>
<tr>
<th>( D )</th>
<th>( \varepsilon_{3D} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>( 2(25 + \sqrt{69})/2 )</td>
</tr>
<tr>
<td>31</td>
<td>( 2(29 + \sqrt{93})/2 )</td>
</tr>
<tr>
<td>59</td>
<td>( 62423 + 4692\sqrt{177} )</td>
</tr>
<tr>
<td>83</td>
<td>( 8553815 + 542076\sqrt{249} )</td>
</tr>
<tr>
<td>107</td>
<td>( 215 + 12\sqrt{321} )</td>
</tr>
<tr>
<td>139</td>
<td>( 85322647 + 4178268\sqrt{417} )</td>
</tr>
<tr>
<td>211</td>
<td>( 440772247 + 17519124\sqrt{633} )</td>
</tr>
<tr>
<td>283</td>
<td>( 1501654712948695 + 515365630476\sqrt{849} )</td>
</tr>
<tr>
<td>307</td>
<td>( 2522057712835735 + 83104627139412\sqrt{921} )</td>
</tr>
<tr>
<td>331</td>
<td>( 2647 + 84\sqrt{993} )</td>
</tr>
<tr>
<td>379</td>
<td>( 650468934487 + 19290626292\sqrt{1137} )</td>
</tr>
<tr>
<td>499</td>
<td>( 22516718751127 + 581964130932\sqrt{1497} )</td>
</tr>
<tr>
<td>547</td>
<td>( 4375 + 108\sqrt{1641} )</td>
</tr>
<tr>
<td>643</td>
<td>( 126794455 + 2886916\sqrt{1929} )</td>
</tr>
<tr>
<td>883</td>
<td>( 99736649218553790682248535 + 1937821608115448210697276\sqrt{2649} )</td>
</tr>
<tr>
<td>907</td>
<td>( 5231287949706796270736288215 + 10028693419599623931686388\sqrt{2721} )</td>
</tr>
</tbody>
</table>
Table 4

<table>
<thead>
<tr>
<th>$D$</th>
<th>$a_D$</th>
<th>$b_D$</th>
<th>$D$</th>
<th>$a_D$</th>
<th>$b_D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>-1</td>
<td>-25</td>
<td>307</td>
<td>+8</td>
<td>+79</td>
</tr>
<tr>
<td>31</td>
<td>-1</td>
<td>-29</td>
<td>331</td>
<td>+8</td>
<td>-83</td>
</tr>
<tr>
<td>59</td>
<td>-4</td>
<td>+43</td>
<td>379</td>
<td>+2</td>
<td>-101</td>
</tr>
<tr>
<td>83</td>
<td>+2</td>
<td>+47</td>
<td>499</td>
<td>+12</td>
<td>-81</td>
</tr>
<tr>
<td>107</td>
<td>+8</td>
<td>-29</td>
<td>547</td>
<td>-10</td>
<td>-137</td>
</tr>
<tr>
<td>139</td>
<td>+2</td>
<td>+61</td>
<td>643</td>
<td>-6</td>
<td>-135</td>
</tr>
<tr>
<td>211</td>
<td>-6</td>
<td>+81</td>
<td>883</td>
<td>-40</td>
<td>-529</td>
</tr>
<tr>
<td>283</td>
<td>+12</td>
<td>-27</td>
<td>907</td>
<td>-22</td>
<td>-259</td>
</tr>
</tbody>
</table>

The integers $a_D$ and $b_D$ were chosen so that the polynomials $f_{-D}(x)$ and $g_{-D}(x)$ have the same discriminant as well as the same number of roots (mod $p$). It is clear that

$$\text{discrim}(f_{-D}(x)) = \text{discrim}(g_{-D}(x))$$

as

$$\text{discrim}(f_{-D}(x)) = -D, \quad \text{discrim}(g_{-D}(x)) = (-4a_D^3 - b_D^2)/27,$$

and

$$(2.9) \quad 4a_D^2 + b_D^2 = 27D.$$ 

It is also clear that $f_{-D}(x)$ and $g_{-D}(x)$ have the same number of roots (mod $p$) as

$$(2.10) \quad f_{-D}(x) = (-1)^d x^e g_{-D}(\frac{tx + u}{x + w}),$$

where the integers $d (= 0, 1)$, $e (= 0, 3)$, $t$, $u$, $v$, $w$ are given in Table 5.

Table 5

<table>
<thead>
<tr>
<th>$D$</th>
<th>$d$</th>
<th>$e$</th>
<th>$t$</th>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
<th>$D$</th>
<th>$d$</th>
<th>$e$</th>
<th>$t$</th>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>1</td>
<td>3</td>
<td>-3</td>
<td>3</td>
<td>0</td>
<td>307</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>3</td>
<td>-1</td>
<td>-3</td>
<td>3</td>
<td>331</td>
<td>1</td>
<td>-3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>0</td>
<td>3</td>
<td>-1</td>
<td>-3</td>
<td>3</td>
<td>379</td>
<td>1</td>
<td>-3</td>
<td>0</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>499</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>1</td>
<td>0</td>
<td>-3</td>
<td>-1</td>
<td>0</td>
<td>3</td>
<td>547</td>
<td>1</td>
<td>-3</td>
<td>-1</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>643</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>211</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>883</td>
<td>1</td>
<td>-3</td>
<td>-5</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>283</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>907</td>
<td>1</td>
<td>-3</td>
<td>-5</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

We can also see that $\text{discrim}(f_{-D}(x)) = \text{discrim}(g_{-D}(x))$ from (2.10) and

$$\gamma_{3D} = \frac{\sqrt{3D}}{3},$$

as in each case we have

$$\left(\frac{t^3 + a_D^2 u^2 + b_D v^2}{3}\right)^2 = \pm (r - uw)^3.$$ 

Set

$$(2.12) \quad \gamma_{3D} = \frac{1}{2}(b_D + 3\sqrt{3}D),$$

so that by (2.9) $\gamma_{3D}$ is of norm $(-a_D)^3$. For each $D$, we determine the values of $r$, $s$ and $\gamma_{3D} = \frac{1}{2}(u_D + v_D\sqrt{3}D)$ in (2.7) when $\alpha = \alpha_D$. These are listed in Table 6.

Table 6

<table>
<thead>
<tr>
<th>$D$</th>
<th>$r$</th>
<th>$s$</th>
<th>$u_D$</th>
<th>$v_D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>1</td>
<td>-1</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>1</td>
<td>-2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>59</td>
<td>1</td>
<td>+173</td>
<td>+13</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>1</td>
<td>+931</td>
<td>+59</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>1</td>
<td>0</td>
<td>+17</td>
<td>+1</td>
</tr>
<tr>
<td>139</td>
<td>1</td>
<td>+2185</td>
<td>+107</td>
<td></td>
</tr>
<tr>
<td>211</td>
<td>1</td>
<td>+4101</td>
<td>+163</td>
<td></td>
</tr>
<tr>
<td>283</td>
<td>1</td>
<td>+449331</td>
<td>+15421</td>
<td></td>
</tr>
<tr>
<td>307</td>
<td>1</td>
<td>+754117</td>
<td>+24849</td>
<td></td>
</tr>
<tr>
<td>331</td>
<td>1</td>
<td>0</td>
<td>+31</td>
<td>+1</td>
</tr>
<tr>
<td>379</td>
<td>1</td>
<td>+4687</td>
<td>+139</td>
<td></td>
</tr>
<tr>
<td>499</td>
<td>1</td>
<td>+92433</td>
<td>+2389</td>
<td></td>
</tr>
<tr>
<td>547</td>
<td>1</td>
<td>-41</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>643</td>
<td>1</td>
<td>-55164</td>
<td>+1256</td>
<td></td>
</tr>
<tr>
<td>883</td>
<td>1</td>
<td>-3343018627</td>
<td>-64952791</td>
<td></td>
</tr>
<tr>
<td>907</td>
<td>1</td>
<td>-8124416167</td>
<td>-155749941</td>
<td></td>
</tr>
</tbody>
</table>

It is no coincidence that $r = 1$ for $D = 643$, this is a consequence of the choice of sign of $b_D$.

Summarizing we have

$$(2.13) \quad \begin{cases} 
\gamma_{3D} = \gamma_D, & \text{for } D \neq 643, \\
\gamma_{p3D} = \gamma_{3D}, & \text{for } D = 643.
\end{cases}$$

In view of (2.10), $f_{-D}(x)$ is the product of three distinct linear polynomials (mod $p$) if and only if $g_{-D}(x)$ is the product of three distinct linear polynomials (mod $p$). By a theorem of Dickson [4], as $\text{discrim}(g_{-D}(x)) = -D$ and

$$\left(\frac{-D}{p}\right) = +1,$$

the polynomial $g_{-D}(x)$ is the product of three distinct linear polynomials (mod $p$) if and only if $\alpha_D$ is congruent to a cube (mod $p$), where $p$
is a prime ideal of the ring of integers of \( K_D \) which divides \( p \). We note that \( \alpha_p \neq 0 \pmod{p} \), otherwise \( p | \alpha_p \), which is seen to be impossible from Table 4 remembering that \( p > 3 \) and \( \left( \frac{-D}{p} \right) = +1 \). In view of (2.13), \( \alpha_p \) is a cube (mod \( p \)) if and only if \( \varepsilon_p \) (if \( D \neq 643 \)), \( \mu(p) \) (if \( D = 643 \)) is a cube (mod \( p \)).

Let \( H(-9D) \) denote the group of classes of primitive, positive-definite, binary quadratic forms of discriminant \(-9D\), so that, for these \( D \) under consideration, \( H(-9D) \) is cyclic of order 12 (resp. 6) if \( D \equiv 1 \pmod{3} \) (resp. \( D \equiv 2 \pmod{3} \)). As the 3-Sylow subgroup of \( H(-9D) \) is of order 3, by a theorem of Weinberger [18], \( \varepsilon_p \) (if \( D \neq 643 \)), \( \mu(p) \) (if \( D = 643 \)) is a cube (mod \( p \)) if and only if \( N(p) \) is represented by one of the forms in the subgroup of sixth powers in \( H(-9D) \), that is, by

\[
(2.14) \begin{cases} 
(1, 1, \frac{4(D+1)}{3}) \text{ or } (9, 9, \frac{4(D+9)}{3}), & \text{if } D \equiv 1 \pmod{3}, \\
(1, 1, \frac{4(D+1)}{3}), & \text{if } D \equiv 2 \pmod{3}.
\end{cases}
\]

In view of the identities

\[
x^2 + xy + \frac{(D+1)}{4} y^2 = (x-y)^2 + (x-y) (3y) \frac{(D+1)}{4} (3y)^2,
\]

\[
9x^2 + 9xy + \frac{(D+9)}{4} y^2 = (3x+y)^2 + (3x+y) y \frac{(D+9)}{4} y^2,
\]

it is clear that if \( N(p) \) is represented by \((1, 1, \frac{4(D+1)}{3}) \) or \((9, 9, \frac{4(D+9)}{3}) \) it is represented by \( p_{-D} = (1, 1, \frac{4(D+1)}{3}) \). In order to treat the converse, we first show that \( N(p) \equiv 1 \pmod{3} \). We have

\[
N(p) = \begin{cases} 
p, & \text{if } \left( \frac{3D}{p} \right) = 1, \\
p^2, & \text{if } \left( \frac{3D}{p} \right) = -1.
\end{cases}
\]

Recalling that \( \left( \frac{-D}{p} \right) = 1 \), the condition \( \left( \frac{3D}{p} \right) = 1 \) (resp. \(-1 \)) is equivalent to \( p \equiv 1 \pmod{3} \) (resp. \( D \equiv 2 \) \( \pmod{3} \)). Hence we have \( N(p) \equiv 1 \pmod{3} \). Thus, if \( N(p) \) is represented by \( p_{-D} = (1, 1, \frac{4(D+1)}{3}) \), then

\[
N(p) = x^2 + xy + \frac{4(D+1)}{3} y^2,
\]

with either (i) \( y \equiv 0 \pmod{3} \), or (ii) \( x \equiv y \not\equiv 0 \pmod{3} \), \( D \equiv 1 \pmod{3} \). If (i) holds then \( N(p) \) is represented by \((1, 1, \frac{4(D+1)}{3}) \) as

\[
N(p) = \left( x + \frac{y}{3} \right)^2 + \left( x + \frac{y}{3} \right) \frac{(D+1)}{4} \left( \frac{y}{3} \right)^2.
\]

If (ii) holds then \( N(p) \) is represented by \((9, 9, \frac{4(D+9)}{3}) \) as

\[
N(p) = 9 \left( \frac{x-y}{3} \right)^2 + 9 \left( \frac{x-y}{3} \right) y + \frac{4(D+9)}{3} y^2.
\]

This completes the proof when \( p \equiv 1 \pmod{3} \) as in this case \( N(p) = p \). When \( p \equiv 2 \pmod{3} \), we have \( N(p) \equiv p^2 \), and since there are exactly three inequivalent forms of discriminant \(-D, p^2 \) is represented by \( p_{-D} \) if and only if \( p \) is represented by \( p_{-D} \).

This completes the proof of Theorem 1 for those \( D \) listed in (A).

We conclude this section by noting that when \( D = 44 \), and \( p \) is a prime \( \equiv 1 \pmod{3} \) with \( \left( \frac{-44}{p} \right) = 1 \), Weinberger’s theorem [18] gives a necessary and sufficient condition for \( p \) to be represented by the form \((1, 1, 223) \), namely

\[
p \text{ is represented by } (1, 1, 223) \text{ if and only if } \varepsilon_5 = 23 + 4 \sqrt{33} \text{ is a cube (mod } p) \text{, where } p \text{ is a prime ideal of } O(\sqrt{33}) \text{ with } N(p) = p.
\]

This result is not relevant to Theorem 1. Similar remarks apply to the other values of \( D \) in (B). Thus a different approach is needed to prove Theorem 1 for those \( D \) in (B), and this is done in the next section.

3. Proof of Theorem 1 for those \( D \) listed in (B). Throughout this section, \( D \) is one of the five integers listed in (B). Note that \( D = 4D^* \), where \( D^* \) is a prime \( \equiv 3 \pmod{8} \). Let \( L_D \) denote the binary bicuadratic field \( Q(\sqrt{-3}, \sqrt{-D^*}) \). If \( \theta \in L_D \) the conjugates of \( \theta \) are \( \theta, \theta^*, \theta^* \), where

\[
(3.1) \begin{cases} 
\theta = a + b \sqrt{-3} + c \sqrt{-D^*} + d \sqrt{3D^*}, \\
\theta = -a - b \sqrt{-3} + c \sqrt{-D^*} - d \sqrt{3D^*}, \\
\theta = -a + b \sqrt{-3} - c \sqrt{-D^*} + d \sqrt{3D^*}, \\
\theta = a - b \sqrt{-3} - c \sqrt{-D^*} - d \sqrt{3D^*},
\end{cases}
\]

where \( a, b, c, d \in \mathbb{Q} \). The ring of integers of \( L_D \) is denoted by \( R_D \). It is known that \( R_D \) is a unique factorization domain [1].

Let \( p \) be a prime \( > 3 \) not dividing \( D \). If \( \left( \frac{-D}{p} \right) = -1 \), \( p \) is not represented by \( p_{-D} = (1, 0, D/4) \), and, as discriminant \( f_{-D}(x) = -D \), by a theorem of Stickelberger [16], \( f_{-D}(x) \) is the product of a linear polynomial and an irreducible quadratic (mod \( p \)).

Suppose now that \( \left( \frac{-D}{p} \right) = +1 \). We must show that \( p \) is represented by \( p_{-D} = (1, 0, D/4) \) if and only if \( f_{-D}(x) \) is congruent to the product of three distinct linear polynomials (mod \( p \)). Define

\[
(3.2) \quad g_{-D}(x) = x^2 + \frac{a_D}{3} x + \frac{b_D}{27},
\]

where the integers \( a_D \) and \( b_D \) are given in Table 7.
Table 7

<table>
<thead>
<tr>
<th>$D$</th>
<th>$a_D$</th>
<th>$b_D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>-4</td>
<td>+38</td>
</tr>
<tr>
<td>76</td>
<td>+8</td>
<td>+2</td>
</tr>
<tr>
<td>172</td>
<td>-4</td>
<td>-70</td>
</tr>
<tr>
<td>268</td>
<td>-10</td>
<td>-106</td>
</tr>
<tr>
<td>652</td>
<td>+20</td>
<td>-196</td>
</tr>
</tbody>
</table>

We note that

\[ \text{discrim}(g_D(x)) = \frac{-4a_D^3 - b_D^3}{27} = \begin{cases} -D, & \text{if } D \neq 652, \\ -4D, & \text{if } D = 652, \end{cases} \]

and that

\[ f_D(x) = \frac{1}{d}(ux + w)^3 g_D\left( \frac{tx + u}{ux + w} \right), \]

where the integers $d$, $e$ ($= 0, 3$), $t$, $u$, $v$, $w$ are given in Table 8.

Table 8

<table>
<thead>
<tr>
<th>$D$</th>
<th>$d$</th>
<th>$e$</th>
<th>$t$</th>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>+1</td>
<td>0</td>
<td>+3</td>
<td>+1</td>
<td>0</td>
<td>+3</td>
</tr>
<tr>
<td>76</td>
<td>+27</td>
<td>+3</td>
<td>+1</td>
<td>+2</td>
<td>+3</td>
<td>-3</td>
</tr>
<tr>
<td>172</td>
<td>-1</td>
<td>0</td>
<td>-3</td>
<td>+1</td>
<td>0</td>
<td>+3</td>
</tr>
<tr>
<td>268</td>
<td>-1</td>
<td>0</td>
<td>-3</td>
<td>-2</td>
<td>0</td>
<td>+3</td>
</tr>
<tr>
<td>652</td>
<td>-108</td>
<td>+3</td>
<td>-4</td>
<td>-2</td>
<td>-3</td>
<td>+3</td>
</tr>
</tbody>
</table>

From (3.4) we see that $f_D(x)$ is congruent to the product of three distinct linear polynomials (mod $p$) if and only if $g_D(x)$ is the product of three distinct linear polynomials (mod $p$). By (3.3) we have

\[ \left( \frac{\text{discrim}(g_D)}{p} \right) = \left( \frac{-D}{p} \right) = +1, \]

so that by a theorem of Dickson [4], $g_D(x)$ is the product of three distinct linear polynomials (mod $p$) if and only if

\[ \left[ \frac{\mu_D}{\lambda_D} \right]_3 = 1, \]

where

\[ \lambda_D = \begin{cases} 19 + 3\sqrt{33}, & \text{if } D = 44, \\ 1 + 3\sqrt{57}, & \text{if } D = 76, \\ -35 + 3\sqrt{129}, & \text{if } D = 172, \\ -53 + 3\sqrt{201}, & \text{if } D = 268, \\ -98 + 6\sqrt{489}, & \text{if } D = 652, \end{cases} \]

and $\lambda_D$ is a prime divisor of $p$ in $R_D$. (The symbol $\left[ \frac{\mu}{\lambda} \right]_3$ in (3.5) is the cubic Legendre symbol.) The prime factorization of the prime 3 in $R_D$ is given as follows:

\[ \lambda_D = \begin{cases} \frac{1}{2}(1+2\sqrt{-3} + \sqrt{-11}), & \text{if } D = 44, \\ \sqrt{-3}, & \text{if } D = 76, 172, 268, 652, \end{cases} \]

By Artin's reciprocity law, we have

\[ \left[ \frac{\mu_D}{\lambda_D} \right]_3 = \left( \frac{\mu_D}{\pi_D} \right)_3 \left( \frac{\mu_D}{\pi_D} \right)_3 \left( \frac{\lambda_D}{\pi_D} \right)_3, \]

if $D = 44$, if $D \neq 44$,

\[ \left( \frac{\mu_D}{\pi_D} \right)_3 = \left( \frac{\mu_D}{\pi_D} \right)_3 \left( \frac{\lambda_D}{\pi_D} \right)_3, \]

if $D = 44$, if $D \neq 44$,

where $\left( \frac{a, b}{\pi} \right)_3$ is the cubic Hilbert symbol. From (3.6) we see that

\[ \left( \frac{\mu_D}{\pi_D} \right)_3 = 1, \]

so that

\[ \left( \frac{\mu_D}{\pi_D} \right)_3 = \left( \frac{\mu_D}{\pi_D} \right)_3 \left( \frac{\lambda_D}{\pi_D} \right)_3 = 1. \]

Thus (3.9) reduces to

\[ \left[ \frac{\mu_D}{\lambda_D} \right]_3 = \left[ \frac{\lambda_D}{\mu_D} \right]_3. \]

Next we observe that

\[ \mu_D = \omega_D, \theta_D \gamma_D, \]

where $\gamma_D \in R_D$, $\omega_D$ is a unit of $R_D$, and $\theta_D$ is the prime divisor of 2 in $R_D$ given by
Next, as \( \lambda_D \) is a prime divisor of \( p \) in \( R_n \), we have
\[
(3.21) \quad p = \left\{ \begin{array}{ll}
\lambda_D \lambda_D^*, & \text{if } p \equiv 1 \pmod{3}, \\
\lambda_D^*, & \text{if } p \equiv 2 \pmod{3}.
\end{array} \right.
\]

As \( \lambda_D \) is an integer of \( Q(\sqrt{-3}, \sqrt{-D^*}) \), if \( p \equiv 1 \pmod{3} \), and of \( Q(\sqrt{-D^*}) \), if \( p \equiv 2 \pmod{3} \), there are integers \( x_0, x_1, x_2, x_3 \), if \( p \equiv 1 \pmod{3} \), and integers \( x_0, x_1, x_2 \), if \( p \equiv 2 \pmod{3} \), such that
\[
(3.22) \quad \lambda_D = \left\{ \begin{array}{ll}
\frac{1}{2}(x_0 + x_1 \sqrt{-3} + x_2 \sqrt{-D^*} + x_3 \sqrt{3D^*}), & \text{if } p \equiv 1 \pmod{3}, \\
\left(\frac{x_0 + x_1 \sqrt{-D^*}}{2}\right), & \text{if } p \equiv 2 \pmod{3},
\end{array} \right.
\]
with
\[
(3.23) \quad \left\{ \begin{array}{ll}
x_0 = x_1 = x_2 = x_3 \pmod{2}, & \text{if } p \equiv 1 \pmod{3}, \\
x_0 - x_1 + x_2 + x_3 = 0 \pmod{4}, & \text{if } p \equiv 2 \pmod{3},
\end{array} \right.
\]
see [14]. (Note that \( \sqrt{m_1 n_1} \) should be replaced by \( \sqrt{m_1 \sqrt{n_1}} \) in Theorem 1 of [19]).

Set
\[
(3.24) \quad \frac{1}{2}(u + v \sqrt{-D^*}) = \left\{ \begin{array}{ll}
\lambda_D \lambda_D^*, & \text{if } p \equiv 1 \pmod{3}, \\
\lambda_D^*, & \text{if } p \equiv 2 \pmod{3},
\end{array} \right.
\]
so that \( u \) and \( v \) are integers such that
\[
(3.25) \quad u = \left\{ \begin{array}{ll}
x_0^3 + 3x_1^2 - D^* x_2^3 - 3D^* x_3^2 / 8, & \text{if } p \equiv 1 \pmod{3}, \\
x_0, & \text{if } p \equiv 2 \pmod{3},
\end{array} \right.
\]
\[
(3.26) \quad v = \left\{ \begin{array}{ll}
x_0 x_2 - 3x_1 x_3 / 4, & \text{if } p \equiv 1 \pmod{3}, \\
x_1, & \text{if } p \equiv 2 \pmod{3},
\end{array} \right.
\]
and
\[
(3.27) \quad 4p = u^2 + D^* v^2, \quad u = v \pmod{2}.
\]
Clearly \( p \) is represented by \( p_D \) if and only if \( u = v = 0 \pmod{2} \). Thus, in view of (3.17), we must show that
\[
(3.28) \quad \left[ \begin{array}{l}
\lambda_D \\
\theta_D
\end{array} \right] \equiv \left[ \begin{array}{l}
\lambda_D \\
\theta_D
\end{array} \right] \Rightarrow \left\{ \begin{array}{ll}
x_0 x_2 - 3x_1 x_3 = 0 \pmod{8}, & \text{if } p \equiv 1 \pmod{3}, \\
x_1 = 0 \pmod{2}, & \text{if } p \equiv 2 \pmod{3}.
\end{array} \right.
\]
Next, as \( \theta_D \) is a prime divisor of 2 and \( \lambda_D \) is a prime divisor of the odd prime \( p \), we have \( \lambda_D \neq \theta_D \) and
\[
(3.29) \quad \lambda_D^2 = \lambda_D^{(\theta_D)^{-1}} = 1 \pmod{\theta_D},
\]
showing that
\[
(3.30) \quad \lambda_D = 1, \omega \text{ or } \omega^2 \pmod{\theta_D},
\]
where $\omega = (-1 + \sqrt{-3})/2$. Appealing to (3.18) and (3.20), we obtain for $p \equiv 1 \pmod{3}$

$$\lambda_p = \begin{cases} 1 \pmod{\theta_p}, & \text{if } E \equiv 0 \pmod{4}, F \equiv 4 \pmod{8}, \\ \omega \pmod{\theta_p}, & \text{if } E \equiv 2 \pmod{4}, F \equiv 4 \pmod{8}, \\ \omega^2 \pmod{\theta_p}, & \text{if } E \equiv 2 \pmod{4}, F \equiv 0 \pmod{8}, \end{cases}$$

where

$$E = x_0 + r x_3, \quad F = x_0 - x_1 - 3 r x_2 + r x_3;$$

and for $p \equiv 2 \pmod{3}$

$$\lambda_p = \begin{cases} 1 \pmod{\theta_p}, & \text{if } x_0 \equiv x_1 \equiv 0 \pmod{2}, x_0 + r x_1 \equiv 2 \pmod{4}, \\ \omega \pmod{\theta_p}, & \text{if } x_0 \equiv x_1 \equiv 1 \pmod{2}, x_0 + r x_1 \equiv 2 \pmod{4}, \\ \omega^2 \pmod{\theta_p}, & \text{if } x_0 \equiv x_1 \equiv 1 \pmod{2}, x_0 + r x_1 \equiv 0 \pmod{4}. \end{cases}$$

We now treat the two cases $p \equiv 1 \pmod{3}$ and $p \equiv 2 \pmod{3}$ separately.

**Case (i):** $p \equiv 1 \pmod{3}$. We have by (3.31)

$$\left[ \frac{\lambda_p}{\theta_p} \right]_{p = 1} = \left[ \frac{\lambda_p}{\theta_p} \right]_{p = 3}$$

or $\lambda_p \equiv 1 \pmod{\theta_p}$ or $\lambda_p \equiv \omega \pmod{\theta_p}$ or $\lambda_p \equiv \omega^2 \pmod{\theta_p}$

$$\Rightarrow \begin{cases} x_0 = - r x_3 \pmod{4} \\ x_0 - x_1 - 3 r x_2 + r x_3 \equiv 4 \pmod{8} \\ x_0 + x_1 - 3 r x_2 - r x_3 \equiv 4 \pmod{8} \end{cases}$$

and

$$\Rightarrow \begin{cases} x_0 + 2 \equiv - r x_3 \pmod{4} \\ x_0 - x_1 - 3 r x_2 + r x_3 \equiv 4 \pmod{8} \\ x_0 + x_1 - 3 r x_2 - r x_3 \equiv 0 \pmod{8} \end{cases}$$

or

$$\Rightarrow \begin{cases} x_0 + 2 \equiv - r x_3 \pmod{4} \\ x_0 - x_1 - 3 r x_2 + r x_3 \equiv 0 \pmod{8} \\ x_0 + 2 \equiv r x_3 \pmod{4} \end{cases}$$

It should be noted that if $x_0 \equiv x_1 \equiv x_2 \equiv x_3 \equiv 0 \pmod{2}$, with $x_i \equiv 2 y_i$ (i = 0, 1, 2, 3), then by (2.23), we have

$$\Rightarrow \begin{cases} y_0 = y_1 = y_2 = y_3 \pmod{2}, y_0 - y_1 - 3 y_2 + y_3 \equiv 2 \pmod{4}, y_0 + y_1 - 3 y_2 - y_3 \equiv 0 \pmod{4} \end{cases}$$

or

$$\Rightarrow \begin{cases} y_0 + y_1 + y_2 + y_3 \equiv 0 \pmod{2} \end{cases}$$

In view of (2.28) we must show that the assertion

$$\Rightarrow \begin{cases} x_0 x_2 - 3 x_1 x_3 \equiv 0 \pmod{8} \end{cases}$$

is equivalent to

$$\Rightarrow \begin{cases} x_i = 2 y_i \pmod{2}, \text{ say } x_i = 2 y_i \pmod{2}, \text{ if } i = 0, 1, 2, 3 \text{ and } y_0 = y_1 = y_2 = y_3 \pmod{2}, y_0 - y_1 - 3 y_2 + y_3 \equiv 2 \pmod{4}, y_0 + y_1 - 3 y_2 - y_3 \equiv 0 \pmod{4} \end{cases}$$

under (2.23). It is clear that (3.36) implies (3.35) as

$$x_0 x_2 - 3 x_1 x_3 = 4 (y_0 y_2 - 3 y_1 y_3) = 4 (y_0 y_2 - 3 y_0 y_2) \equiv 0 \pmod{8}.$$

Next we assume that (3.35) holds and begin by showing that the $x_i$ are all even. We suppose that this is not the case, so that by (2.23) the $x_i$ are all odd, say $x_i = 2 z_i + 1$ (i = 0, 1, 2, 3). Then, from (3.35), we have

$$2 (x_0 x_2 + x_1 x_3) + (x_0 + x_1 + x_2 + x_3) \equiv 1 \pmod{4}.$$

Further, as $u \equiv v \equiv 0 \pmod{2}$, by (2.27) we see that $u + v \equiv 2 \pmod{4}$, and so by (3.25) and (3.26), we have

$$(x_0^2 + 3 x_1^2 - 3 D* x_2^2 + 3 D* x_3^2) + 2 (x_0 x_2 - 3 x_1 x_3) \equiv 16 \pmod{32},$$

and so (as $D^* \equiv 3 \pmod{8}$) we obtain

$$(x_0^2 + 3 x_1^2 - 3 x_2^2 - x_3^2) + 2 (x_0 x_2 + z_1 x_3) + 2 (x_0 - z_2 + 2 z_3) \equiv 7 \pmod{8}.$$
From (3.37) we deduce
\[(2x_1 + 1)z_3 = 1 - x_0 - x_1 - x_2 + 2x_0z_2 \pmod{4}.
\]
Multiplying (3.39) by \((2x_1 + 1)\), we obtain
\[z_3 = 1 - (x_0 + x_1 + x_2) + 2(x_0x_1 + x_1x_2 + x_2z_0) \pmod{4},
\]
so that
\[
\begin{cases}
  z_3 = 1 - \frac{A}{4} + 2B \pmod{4}, \\
  z_3 = 1 + A^2 - 2A + 4AB \pmod{8},
\end{cases}
\]
where
\[A = x_0 + x_1 + x_2, \quad B = x_0z_1 + x_1z_2 + x_2z_0.\]
Using (3.41) in (3.38), we obtain
\[3 + 4(x_0 + x_2)(x_0z_1 + x_1z_2 + x_2z_0 - x_1) \equiv 7 \pmod{8},
\]
that is
\[(x_0 + x_2)(x_0z_1 + x_1z_2 + x_2z_0 - x_1) \equiv 1 \pmod{2},
\]
showing that
\[x_0 + x_2 = x_0z_1 + x_1z_2 + x_2z_0 - x_1 \equiv 1 \pmod{2},
\]
which gives the contradiction
\[x_0 + x_2 = x_0z_1 = x_0 \pmod{2}.
\]
This completes the proof that (3.35) implies that all the \(x_i\) are even, say \(x_i = 2y_i\) \((i = 0, 1, 2, 3)\). We complete the proof in the case \(p \equiv 1 \pmod{3}\) by showing that we must have either
\[y_0 \equiv y_1 \equiv y_2 \equiv y_3 \pmod{2}, \quad y_0 - y_1 - y_2 - y_3 \equiv 2 \pmod{4}.
\]
or
\[y_0 \equiv y_1 \equiv y_2 + 1 \equiv y_3 + 1 \pmod{2}.
\]
As \(u \equiv 0 \pmod{2}, v \equiv 0 \pmod{2}, u + v \equiv 2 \pmod{4}\) we have
\begin{align*}
(3.43) & \quad y_0 + y_2 + y_1 + y_3 \equiv 0 \pmod{4}, \\
(3.44) & \quad y_0y_2 + y_1y_3 \equiv 0 \pmod{2}, \\
(3.45) & \quad y_0^3 + y_1^3 + y_2^3 + y_3^3 \equiv 0 \pmod{4}(mod 8).
\end{align*}
We begin by showing that \(y_0 \equiv y_1 \pmod{2}\). Suppose not, so that we have \(y_0 \equiv y_1 + 1 \pmod{2}\). Next, (3.34) gives \(y_2 \equiv y_3 + 1 \pmod{2}\). Then, from either (3.43) or (3.44), we deduce that \(y_1 \equiv y_3 + 1 \pmod{2}\). Thus we have
\[y_0 \equiv y_1 + 1 \equiv y_2 + 1 \equiv y_3 \pmod{2}.
\]
If \(y_0 \equiv 0 \pmod{2}\) then (3.45) and (3.46) give
\[y_0^3 - y_2^3 + 2y_0 + 2y_3 \equiv 4 \pmod{8},
\]
which gives the contradiction
\[0 \equiv (y_0 + 1)^2 - (y_3 - 1)^2 \equiv 4 \pmod{8}.
\]
If \(y_0 \equiv 1 \pmod{2}\) then (3.45) and (3.46) give
\[y_0^3 + y_2^3 + 2y_1 + 2y_2 \equiv 4 \pmod{8},
\]
which gives the contradiction
\[2 \equiv (y_1 + 1)^2 + (y_2 + 1)^2 \equiv 6 \pmod{8}.
\]
Hence we must have
\[y_0 \equiv y_1 \pmod{2},
\]
and so, by (3.34), we also have
\[y_2 \equiv y_3 \pmod{2}.
\]
If \(y_1 \equiv y_2 \equiv 1 \pmod{2}\) we are finished. Otherwise \(y_1 \equiv y_3 \pmod{2}\) and we must show that \(y_0 - y_1 - y_2 - y_3 \equiv 2 \pmod{4}\). We have
\[y_0 \equiv y_1 \equiv y_2 \equiv y_3 \pmod{2}.
\]
If \(y_0 \equiv y_1 \equiv y_2 \equiv y_3 \equiv 1 \pmod{2}\) then (3.45) gives
\[y_0y_2 + y_1y_3 \equiv 2 \pmod{4},
\]
and thus
\[y_0 - y_1 - y_2 - y_3 \equiv 2y_0 - (y_0 + y_1 + y_2 + y_3) \pmod{4} \equiv 2 - (y_0 + 1)(y_0 + 1) - (y_1 + 1)(y_1 + 1) + (y_0y_2 + y_1y_3)
\]
\[\equiv 2 - 0 - 0 + 2 \pmod{4} \equiv 2 \pmod{4},
\]
as required. If \(y_0 \equiv y_1 \equiv y_2 \equiv y_3 \equiv 0 \pmod{2}\) then (3.45) gives (remembering that \(n^2 \equiv 2n \pmod{8}\) when \(n\) is even)
\[y_0 - y_1 - y_2 - y_3 \equiv 2 \pmod{4},
\]
and thus
\[y_0 - y_1 - y_2 - y_3 \equiv (y_0 - y_1 + y_2 - y_3) - 2y_2 \equiv 2 \pmod{4},
\]
as required. This completes the proof when \(p \equiv 1 \pmod{3}\).
Case (ii): $p \equiv 2 \pmod{3}$. As $\lambda_D = \lambda_D$ and $\delta_D = -\delta_D$, we have \[
\begin{align*}
\frac{\lambda_D}{\theta_D},
\end{align*}
\]
and so \[
\begin{align*}
\frac{\lambda_D}{\theta_D} = \frac{\lambda_D}{\theta_D}
\end{align*}
\]
holds if and only if \[
\begin{align*}
\frac{\lambda_D}{\theta_D} = 1
\end{align*}
\]
that is, if and only if $\lambda_D = 1 \pmod{\theta_D}$. By (3.33) this condition is equivalent to $x_0 = x_1 \equiv 0 \pmod{2}$, $x_0 + r x_1 = 2 \pmod{4}$, which by (3.25), (3.26) and (3.27) is equivalent to $u = v = 0 \pmod{2}$ as required.

The proof of Theorem 1 is now complete.

4. Proof of Theorem 2. Since $2/\sqrt{x_0} + \sqrt{x_0}$ is the real root of $27/(-x)(x-3)/r$, where $r$ is the coefficient of $x^2$ in $f(x)$, Theorem 2 follows immediately from Theorem 1 and [3: Theorem 9.2, Exercise 9.3].

5. Proof of Theorem 3. Theorem 3 follows from Theorem 1 and the following theorem (which is essentially due to Cauchy [2]) with $k = A_1 = a_D$, $l = -B = -b_D$ (see (2.8) and (3.2)).

**THEOREM** (Cauchy). Let $A$ and $B$ be integers and let $p$ be a prime such that
\[
\begin{align*}
p > 3, \quad p | AB, \quad \left(-\frac{4A^3 - 27B^2}{p}\right) = +1.
\end{align*}
\]
Define an integer $A_1$, by $A = 3A_1 \pmod{p}$. Let \{$u_n$\}$_{n=0,1,2,...}$ be the sequence of integers defined by
\[
\begin{align*}
u_{n+2} + Bu_{n+1} + A_1^2 u_n = 0, \quad u_0 = 2, \quad u_1 = -B.
\end{align*}
\]
Then $x^3 + Ax + B$ is congruent to the product of three distinct linear polynomials \((\pmod{p})\) if
\[
\begin{align*}
\begin{cases}
u_{(p-1)/3} \equiv 2 \pmod{p}, & \text{if } p = 3 \pmod{3}, \\
\nu_{(p+1)/3} \equiv -2A_1 \pmod{p}, & \text{if } p = 2 \pmod{3},
\end{cases}
\end{align*}
\]
and $x^3 + Ax + B$ is irreducible \((\pmod{p})\) if
\[
\begin{align*}
\begin{cases}
u_{(p-1)/3} \equiv -1 \pmod{p}, & \text{if } p = 3 \pmod{3}, \\
\nu_{(p+1)/3} \equiv A_1 \pmod{p}, & \text{if } p = 2 \pmod{3}.
\end{cases}
\end{align*}
\]

6. Acknowledgement. The authors would like to thank Dr. Kenneth Hardy (Carleton University) and Mr. Nicholas Buck (College of New Caledonia) for doing some computing for them in connection with this research.

References

[17] H. Wada, A table of ideal class numbers and fundamental units of real quadratic number fields $Q(i/\sqrt{m})$ ($2 \leq m \leq 8192$), Sophia University, Tokyo, Japan.