for all $r \geq 2$, and hence if we choose $\mu < (m+n)^{-1}(m+n-1)^{-1}$, then

$$|C(q; \psi^*)| \ll \psi^*(q)^{m+n},$$

for all sufficiently large q. It now follows from the Borel–Cantelli lemma that the system of inequalities

$$\|q\xi_i(\boldsymbol{u})\| < \psi^*(q), \quad i = 1, \ldots, m+n,$$

has at most finitely many solutions for almost all $\boldsymbol{u} \in \Omega$, which proves Theorem 1.3.

References

[1] R. C. Baker, *Metric Diophantine approximation on manifolds*, J. London Math. Soc. 14 (1976), 43–48.

[2] V. I. Bernik, *The asymptotic behaviour of the number of solutions of some systems of inequalities in the theory of Diophantine approximations of dependent quantities* (Russian), Vestsi Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk 1973 (1), 10–17.

[3] — *An analogue of Khintchine's theorem in the metric theory of Diophantine approximations of dependent quantities* (Russian), ibid. 1977 (6), 44–49.

[4] — *Applications of measure theory and Hausdorff dimension to the theory of Diophantine approximation*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge University Press, 1988.

[5] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, 1957.

[6] M. M. Dodson, B. P. Rynne and J. A. G. Vickers, *Metric Diophantine approximation and Hausdorff dimension on manifolds*, Math. Proc. Cambridge Philos. Soc. 105 (1989), 547–558.

[7] — — — *Averaging in multifrequency systems*, Nonlinearity 2 (1989), 137–148.

[8] S. Kobayashi and K. Nomizu, *Foundations of Differential Geometry II*, Interscience, New York 1969.

[9] V. G. Sprindžuk, *Metric Theory of Diophantine Approximations* (Engl. trans. R. A. Silverman), Wiley, New York 1979.

[10] — *Achievements and problems in Diophantine approximation theory*, Russian Math. Surveys 35 (1980), 1–80.

[11] E. C. Titchmarsh, *The Theory of the Riemann Zeta Function*, Oxford University Press, London 1951.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
York YO1 5DD, England
FACULTY OF MATHEMATICAL STUDIES
UNIVERSITY OF SOUTHAMPTON
Southampton S09 5NH, England

Received on 9.5.1989 (1937)

ACTA ARITHMETICA
LVII (1991)

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, $\mathrm{GCD}(a, b, c) = 1$). 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

$$p_{-D} = \begin{cases} (1, 0, D/4), & \text{if } D \equiv 0 \pmod 4, \\ (1, 1, (D+1)/4), & \text{if } D \equiv 3 \pmod 4. \end{cases} \tag{0.1}$$

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.

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

The complete list of all the imaginary quadratic fields with classnumber 1 has been known for over twenty years [15], namely,

$$Q(\sqrt{-n}):\ n = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

From these results we can deduce

PROPOSITION. $h(-D) = 3$ *if and only if*

(0.2) $D = 23, 31, 44, 59, 76, 83, 92, 107, 108, 124, 139, 172, 211, 243, 268, 283,$ $307, 331, 379, 499, 547, 643, 652, 883$ *or* 907.

Proof. Let d be the discriminant of the imaginary quadratic field given uniquely by

$$-D = f^2 d,$$

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

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

where

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

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

$$h(-D) = 3 \Leftrightarrow \text{(a) } d < -4,\ h(d) = 3,\ \psi_d(f) = 1 \quad\text{or}$$
$$\text{(b) } d < -4,\ h(d) = 1,\ \psi_d(f) = 3 \quad\text{or}$$
$$\text{(c) } \psi_{-4}(f) = 6 \quad\text{or}$$
$$\text{(d) } \psi_{-3}(f) = 9.$$

Now it is easy to check that

$$\psi_d(f) = 1 \Leftrightarrow f = 1 \text{ or } f = 2,\ d \equiv 1 \pmod 8;$$
$$\psi_d(f) = 3 \Leftrightarrow f = 2,\ d \equiv 5 \pmod 8 \text{ or}$$
$$f = 3,\ d \equiv 0 \pmod 3 \text{ or}$$
$$f = 6,\ d \equiv 1 \pmod 8,\ d \equiv 0 \pmod 3;$$
$$\psi_{-4}(f) = 6 \quad \text{cannot occur};$$
$$\psi_{-3}(f) = 9 \Leftrightarrow f = 6 \text{ or } f = 9.$$

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 $p \equiv 1 \pmod 3$ if and only if there exist integers x and y 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 2 is a cube (mod p), where $p \equiv 1 \pmod 3$, 2 has three distinct cube roots (mod p). If $p \equiv 2 \pmod 3$ 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* $\left(\frac{-3}{p}\right) = +1$ *and* x^3-2 *is congruent to the product of three distinct linear polynomials* (mod *p*).

Jacobi [10] showed that 3 is congruent to a cube modulo a prime $p \equiv 1 \pmod 3$ if 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* $\left(\frac{-3}{p}\right) = +1$ *and* x^3-3 *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 ($p > 3$, $p \nmid D$) *is represented by the principal form* p_{-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 1

D	$f_{-D}(x)$	D	$f_{-D}(x)$
23	x^3-x+1	243	x^3-3
31	x^3+x+1	268	x^3+2x^2-2x+2
44	x^3+x^2-x+1	283	x^3+4x+1
59	x^3+2x+1	307	x^3-x^2+3x+2
76	x^3-2x+2	331	x^3-2x^2+4x+1
83	x^3+x^2+x+2	379	x^3+x^2+x+4
92	x^3-x+1	499	x^3+4x+3
107	x^3+x^2+3x+2	547	x^3+x^2-3x+4
108	x^3-2	643	x^3-2x+5
124	x^3+x+1	652	x^3+3x^2-5x+3
139	x^3-x^2+x+2	883	x^3+5x^2-5x+2
172	x^3-x^2-x+3	907	x^3+5x^2+x+2
211	x^3-2x+3		

The cases $D = 108$ and $D = 243$ of the theorem are the aforementioned results of Gauss and Jacobi respectively, so these two values of D will be excluded from further consideration. Furthermore, when $D = 92$ and $D = 124$, it is easy to check that p is represented by p_{-D} if and only if it is represented by $p_{-D/4}$, as $D/4 \equiv 7 \pmod 8$. Thus we can also exclude these two values of D from further consideration. We divide the remaining 21 values of D into two lists according as $D \equiv 3 \pmod 4$ or $D \equiv 0 \pmod 4$, namely,

(A) D = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907,

(B) D = 44, 76, 172, 268, 652.

The proof of Theorem 1 for the 16 values of D listed in (A) is based on a theorem of Weinberger [18] and is given in Section 2. For the 5 values of D listed in (B), Weinberger's theorem does not apply and we give a proof (in § 3) using Artin's reciprocity law instead. We remark that the existence of such a polynomial $f_{-D}(x)$ is known by class field theory (see [3: Theorem 9.2 and Ex. 9.3]). Our Theorem 1 gives such a polynomial $f_{-D}(x)$ explicitly for all D with $h(-D) = 3$, and furthermore shows that $f_{-D}(x)$ may be chosen with discriminant $-D/4$ or $-D$ according as $D \equiv 28 \pmod{32}$ or not. In future work it is planned to determine $f_{-D}(x)$ explicitly when $h(-D)$ = 4, 5, 6, 7 and 8, assuming that the known lists of such D are complete. For general D not much is known about $f_{-D}(x)$ or its discriminant.

The case $D = 124$ of Theorem 1 was treated by Kronecker [11], who showed that p is represented by (1, 0, 31) if and only if the congruence

$$(x^3-10x)^2+31(x^2-1)^2 \equiv 0 \pmod p$$

is solvable. It is easy to check that this is equivalent to our result, namely, p ($\nmid 2\cdot 3\cdot 31$) is represented by (1, 0, 31) if and only if $\left(\frac{-31}{p}\right) = +1$ and the congruence $x^3+x+1 \equiv 0 \pmod p$ is solvable. Appealing to Theorem 1, a sextic polynomial analogous to that of Kronecker for $D = 124$ can be found for each D in (0.2).

In Section 4, we use Theorem 1 to construct explicitly some class fields. We prove

THEOREM 2. (i) *For those D in* (A), *the Hilbert class field over* $Q(\sqrt{-D})$ *is*

$$Q(\sqrt{-D}, \sqrt[3]{\varkappa_D}+\sqrt[3]{\varkappa_D'}),$$

where $\varkappa_D$ *is given as follows:*

D	$\varkappa_D$	D	$\varkappa_D$	D	$\varkappa_D$
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	$(-47+3\sqrt{249})/2$	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	$(-529+3\sqrt{2649})/2$
				907	$(-259+3\sqrt{2721})/2$

(ii) *For those D in* (B), *the ring class field of the order* $Z[\sqrt{-D/4}]$ *in* $Z[(-1+\sqrt{-D/4})/2]$ *is*

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

where

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

We remark that Hasse [9] has shown that the Hilbert class field over $Q(\sqrt{-23})$ is

$$Q(\sqrt{-23}, \sqrt[3]{(25+3\sqrt{69})/2}+\sqrt[3]{(25-3\sqrt{69})/2})$$

and the Hilbert class field over $Q(\sqrt{-31})$ is

$$Q(\sqrt{-31}, \sqrt[3]{(29+3\sqrt{93})/2}+\sqrt[3]{(29-3\sqrt{93})/2}).$$

Our results for $D = 23$ and $D = 31$ agree with those of Hasse since $\beta = (\alpha-9)/\alpha$ for

$$\begin{cases} \alpha = \sqrt[3]{(-27+3\sqrt{69})/2}+\sqrt[3]{(-27-3\sqrt{69})/2} = -3.9741\ldots, \\ \beta = \sqrt[3]{(25+3\sqrt{69})/2}+\sqrt[3]{(25-3\sqrt{69})/2} = 3.2646\ldots; \end{cases}$$

and $\delta = (-\gamma-9)/\gamma$ for

$$\begin{cases} \gamma = \sqrt[3]{(-27+3\sqrt{93})/2}+\sqrt[3]{(-27-3\sqrt{93})/2} = -2.0469\ldots, \\ \delta = \sqrt[3]{(29+3\sqrt{93})/2}+\sqrt[3]{(29-3\sqrt{93})/2} = 3.3967\ldots \end{cases}$$

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} (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*

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

is solvable in integers x and y if and only if

$$\begin{cases} u_{(p-1)/3} \equiv 2 \pmod p, & \text{if } p \equiv 1 \pmod 3, \\ u_{(p+1)/3} \equiv -2k \pmod p, & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

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

$$\begin{cases} u_0 = 2, \quad u_1 = l, \\ u_{n+2} = lu_{n+1}+k^3u_n, \quad n = 0, 1, 2, \ldots, \end{cases}$$

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

Table 2

D	k	l	D	k	l
23	-1	$+25$	283	$+12$	$+27$
31	-1	$+29$	307	$+8$	-79
44	-4	-38	331	$+8$	$+83$
59	-4	-43	379	$+2$	$+101$
76	$+8$	-2	499	$+12$	$+81$
83	$+2$	-47	547	-10	$+137$
107	$+8$	$+29$	643	-6	$+135$
139	$+2$	-61	652	$+20$	$+196$
172	-4	$+70$	883	-40	$+529$
211	-6	-81	907	-22	$+259$
268	-10	$+106$			

The identities

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

are often useful in computing $u_{(p\pm 1)/3} \pmod p$. 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

$$u_0 \equiv 2, \quad u_1 \equiv -2, \quad u_2 \equiv 1028, \quad u_4 \equiv 726, \quad u_8 \equiv 889,$$
$$u_{16} \equiv 904, \quad u_{48} \equiv 544, \quad u_{144} \equiv 1296, \quad u_{432} \equiv 2,$$

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 $\equiv 3 \pmod 4$.

Let p be a prime >3 with $p \nmid D$. If $\left(\frac{-D}{p}\right) = -1$ then p is not represented by $p_{-D} = (1, 1, \frac{1}{4}(D+1))$ and, as $\operatorname{discrim}(f_{-D}(x)) = -D$, by a theorem of Stickelberger [16], $f_{-D}(x)$ 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 $p_{-D} = (1, 1, \frac{1}{4}(D+1))$ if and only if $f_{-D}(x)$ is congruent to the product of three distinct linear polynomials (mod p).

We set

(2.1) $$K_D = Q(\sqrt{3D}), \quad K_D^* = Q(\sqrt{3D})\backslash\{0\}.$$

Let G_D be the group defined by

(2.2) $$G_D = \{\alpha \in K_D^*: (\alpha) = A^3 \text{ for some ideal } A \text{ of } K_D\}$$

and let H_D be the subgroup of G_D given by

(2.3) $$H_D = \{\alpha \in K_D^*: \alpha = \beta^3 \text{ for some } \beta \in K_D^*\}.$$

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 classgroup $H(K_D)$ of K_D. Now

(2.4) $$H(K_D) \simeq \begin{cases} Z_3, & \text{for } D = 107, 331, 643, \\ Z_5, & \text{for } D = 547, \\ Z_1, & \text{otherwise,} \end{cases}$$

so

(2.5) $$r_D = \begin{cases} 1, & \text{for } D = 107, 331, 643, \\ 0, & \text{otherwise,} \end{cases}$$

and thus

(2.6) $$G_D/H_D \simeq \begin{cases} Z_3 \times Z_3, & \text{if } D = 107, 331, 643, \\ Z_3, & \text{otherwise.} \end{cases}$$

Let ε_{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

$$A_D^3 = \begin{cases} (\frac{1}{2}(17+\sqrt{321})), & \text{if } D = 107, \\ (\frac{1}{2}(31-\sqrt{993})), & \text{if } D = 331, \\ (\frac{1}{2}(4963-113\sqrt{1929})) = (\frac{1}{2}(1258562169097-28655537523\sqrt{1929})), & \\ & \text{if } D = 643. \end{cases}$$

a basis for G_D/H_D is given by $\{\varepsilon_{3D}H_D, \mu_{3D}H_D\}$, where

$$\mu_{3D} = \begin{cases} (\frac{1}{2}(17+\sqrt{321})), & \text{if } D = 107, \\ (\frac{1}{2}(31-\sqrt{993})), & \text{if } D = 331, \\ (\frac{1}{2}(1258562169097-28655537523\sqrt{1929})), & \text{if } D = 643. \end{cases}$$

Hence, for every nonzero integer α of K_D, there is a unique integer γ_{3D} of K_D, a unique integer r ($=0, 1, 2$), and, if $D = 107$, 331 or 643, a unique integer s ($=0, 1, 2$), such that

(2.7) $$\begin{cases} \alpha\varepsilon_{3D}^r = \gamma_{3D}^3, & \text{if } D \neq 107, 331, 643, \\ \alpha\varepsilon_{3D}^r\mu_{3D}^s = \gamma_{3D}^3, & \text{if } D = 107, 331, 643. \end{cases}$$

The choice of generator μ_{3D} of A_D^3 with large coefficients in the case $D = 643$ is so that when α is taken to be α_D (see (2.12)) we have $r = 0$ and $s = 1$ (see Table 6 and (2.13)). The values of ε_{3D} for those D under consideration are taken from the table of Wada [17] and are listed in Table 3.

Table 3

D	ε_{3D}
23	$(25+3\sqrt{69})/2$
31	$(29+3\sqrt{93})/2$
59	$62423+4692\sqrt{177}$
83	$8553815+542076\sqrt{249}$
107	$215+12\sqrt{321}$
139	$85322647+4178268\sqrt{417}$
211	$440772247+17519124\sqrt{633}$
283	$1501654712948695+51536656330476\sqrt{849}$
307	$2522057712835735+83104627139412\sqrt{921}$
331	$2647+84\sqrt{993}$
379	$650468934487+19290626292\sqrt{1137}$
499	$22516718751127+581961430932\sqrt{1497}$
547	$4375+108\sqrt{1641}$
643	$126794455+2886916\sqrt{1929}$
883	$9973664921855379068224853 5+19378216081154482106972 76\sqrt{2649}$
907	$523128794970679627073628821 5+10028693419599962339168638 8\sqrt{2721}$

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

(2.8) $$g_{-D}(x) = x^3 + \frac{a_D}{3}x + \frac{b_D}{27},$$

where the integers a_D and b_D are listed in Table 4.

Table 4

D	a_D	b_D	D	a_D	b_D
23	−1	−25	307	+8	+79
31	−1	−29	331	+8	−83
59	−4	+43	379	+2	−101
83	+2	+47	499	+12	−81
107	+8	−29	547	−10	−137
139	+2	+61	643	−6	−135
211	−6	+81	883	−40	−529
283	+12	−27	907	−22	−259

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

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

as

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

and

$$4a_D^3 + b_D^2 = 27D. \tag{2.9}$$

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

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

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

Table 5

D	d	e	t	u	v	w	D	d	e	t	u	v	w
23	1	3	1	−3	3	0	307	0	0	3	−1	0	3
31	1	3	−1	−3	3	0	331	1	0	−3	2	0	3
59	0	3	2	3	3	0	379	1	0	−3	−1	0	3
83	0	0	3	1	0	3	499	1	0	−1	0	0	1
107	1	0	−3	−1	0	3	547	1	0	−3	−1	0	3
139	0	0	3	−1	0	3	643	1	0	−1	0	0	1
211	0	0	1	0	0	1	883	1	0	−3	−5	0	3
283	1	0	−1	0	0	1	907	1	0	−3	−5	0	3

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

Table 5, as in each case we have

$$\left(t^3 + \frac{a_D}{3}tv^2 + \frac{b_D}{27}v^3\right)^2 = \pm(tw-uv)^3. \tag{2.11}$$

Set

$$\alpha_D = \tfrac{1}{2}(b_D + 3\sqrt{3D}), \tag{2.12}$$

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

Table 6

D	r	s	u_D	v_D
23	1		−2	0
31	1		−2	0
59	1		+173	+13
83	1		+931	+59
107	1	0	+17	+1
139	1		+2185	+107
211	1		+4101	+163
283	1		+449331	+15421
307	1		+754117	+24849
331	1	0	+31	+1
379	1		+4687	+139
499	1		+92433	+2389
547	1		−41	−1
643	0	1	−55164	+1256
883	1		−3343018627	−64952791
907	1		−8124416167	−155749941

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

Summarizing we have

$$\begin{cases} \alpha_D \varepsilon_{3D} = \gamma_{3D}^3, & \text{for } D \neq 643, \\ \alpha_D \mu_{3D} = \gamma_{3D}^3, & \text{for } D = 643. \end{cases} \tag{2.13}$$

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 $\operatorname{discrim}(g_{-D}(x)) = -D$ 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 α_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 $\alpha_D \not\equiv 0 \pmod{\mathfrak{p}}$, otherwise $p \mid a_D$, 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), α_D is a cube $\pmod{\mathfrak{p}}$ if and only if ε_{3D} (if $D \neq 643$), μ_{3D} (if $D = 643$) is a cube $\pmod{\mathfrak{p}}$.

Let $H(-9D)$ denote the group of classes of primitive, positive-definite, binary quadratic forms of discriminant $-9D$, so that, for those 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], ε_{3D} (if $D \neq 643$), μ_{3D} (if $D = 643$) is a cube $\pmod{\mathfrak{p}}$ if and only if $N(\mathfrak{p})$ is represented by one of the forms in the subgroup of sixth powers in $H(-9D)$, that is, by

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

In view of the identities

$$x^2+xy+\frac{(9D+1)}{4}y^2 \equiv (x-y)^2+(x-y)(3y)+\frac{(D+1)}{4}(3y)^2,$$

$$9x^2+9xy+\frac{(D+9)}{4}y^2 \equiv (3x+y)^2+(3x+y)\,y+\frac{(D+1)}{4}y^2,$$

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

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

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

$$N(\mathfrak{p}) = x^2+xy+\tfrac{1}{4}(D+1)\,y^2,$$

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 $N(\mathfrak{p})$ is represented by $(1, 1, \frac{1}{4}(9D+1))$ as

$$N(\mathfrak{p}) = \left(x+\frac{y}{3}\right)^2+\left(x+\frac{y}{3}\right)\left(\frac{y}{3}\right)+\frac{(9D+1)}{4}\left(\frac{y}{3}\right)^2.$$

If (ii) holds then $N(\mathfrak{p})$ is represented by $(9, 9, \frac{1}{4}(D+9))$ as

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

This completes the proof when $p \equiv 1 \pmod 3$ as in this case $N(\mathfrak{p}) = p$. When $p \equiv 2 \pmod 3$, we have $N(\mathfrak{p}) = p^2$, 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 is represented by (1, 1, 223) if and only if $\varepsilon_{33} = 23+4\sqrt{33}$ is a cube $\pmod{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of $Q(\sqrt{33})$ with $N(\mathfrak{p}) = p$.

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 bicyclic biquadratic field $Q(\sqrt{-3}, \sqrt{-D^*})$. If $\theta \in L_D$ the conjugates of θ are $\theta, \theta', \bar\theta, \bar\theta'$, where

$$(3.1)\qquad \begin{cases} \theta = a+b\sqrt{-3}+c\sqrt{-D^*}+d\sqrt{3D^*}, \\ \theta' = a-b\sqrt{-3}+c\sqrt{-D^*}-d\sqrt{3D^*}, \\ \bar\theta = a-b\sqrt{-3}-c\sqrt{-D^*}+d\sqrt{3D^*}, \\ \bar\theta' = a+b\sqrt{-3}-c\sqrt{-D^*}-d\sqrt{3D^*}, \end{cases}$$

where $a, b, c, d \in Q$. 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 discrim $(f_{-D}(x)) = -D$, 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

$$(3.2)\qquad g_{-D}(x) = x^3+\frac{a_D}{3}x+\frac{b_D}{27},$$

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

Table 7

D	a_D	b_D
44	-4	$+38$
76	$+8$	$+2$
172	-4	-70
268	-10	-106
652	$+20$	-196

We note that

$$\text{discrim}(g_{-D}(x)) = (-4a_D^3 - b_D^2)/27 = \begin{cases} -D, & \text{if } D \neq 652, \\ -4D, & \text{if } D = 652, \end{cases} \tag{3.3}$$

and that

$$f_{-D}(x) = \frac{1}{d}(vx+w)^e g_{-D}\left(\frac{tx+u}{vx+w}\right), \tag{3.4}$$

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

Table 8

D	d	e	t	u	v	w
44	$+1$	0	$+3$	$+1$	0	$+3$
76	$+27$	$+3$	$+1$	$+2$	$+3$	-3
172	-1	0	-3	$+1$	0	$+3$
268	-1	0	-3	-2	0	$+3$
652	-108	$+3$	-4	-2	-3	$+3$

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

$$\left[\frac{\mu_D}{\lambda_D}\right]_3 = 1, \tag{3.5}$$

where

$$\mu_D = \begin{cases} 19+3\sqrt{33}, & \text{if } D = 44, \\ 1+3\sqrt{57}, & \text{if } D = 76, \\ -35+3\sqrt{129}, & \text{if } D = 172, \\ -53+3\sqrt{201}, & \text{if } D = 268, \\ -98+6\sqrt{489}, & \text{if } D = 652, \end{cases} \tag{3.6}$$

and λ_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:

$$3 = \begin{cases} -\pi_D^2 \bar{\pi}_D'^2, & \text{if } D = 44, \\ -\pi_D^2, & \text{if } D = 76, 172, 268, 652, \end{cases} \tag{3.7}$$

where

$$\pi_D = \begin{cases} \frac{1}{2}(1+2\sqrt{-3}+\sqrt{-11}), & \text{if } D = 44, \\ \sqrt{-3}, & \text{if } D = 76, 172, 268, 652. \end{cases} \tag{3.8}$$

By Artin's reciprocity law, we have

$$\left[\frac{\mu_D}{\lambda_D}\right]_3 = \begin{cases} \left(\frac{\mu_D, \lambda_D}{\pi_D}\right)_3 \left(\frac{\mu_D, \lambda_D}{\bar{\pi}_D'}\right)_3 \left[\frac{\lambda_D}{\mu_D}\right]_3, & \text{if } D = 44, \\ \left(\frac{\mu_D, \lambda_D}{\pi_D}\right)_3 \left[\frac{\lambda_D}{\mu_D}\right]_3, & \text{if } D \neq 44, \end{cases} \tag{3.9}$$

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

$$\mu_D \equiv 1 \pmod{(\sqrt{-3})^3}, \tag{3.10}$$

so that

$$\left(\frac{\mu_D, \lambda_D}{\pi_D}\right)_3 = \left(\frac{\mu_D, \lambda_D}{\bar{\pi}_D'}\right)_3 = 1. \tag{3.11}$$

Thus (3.9) reduces to

$$\left[\frac{\mu_D}{\lambda_D}\right]_3 = \left[\frac{\lambda_D}{\mu_D}\right]_3. \tag{3.12}$$

Next we observe that

$$\mu_D = \omega_D \theta_D \bar{\theta}_D'^2 \gamma_D^3, \tag{3.13}$$

where $\gamma_D \in R_D$, ω_D is a unit of R_D, and θ_D is the prime divisor of 2 in R_D given by

$$(3.14)\qquad \theta_D = \begin{cases} \tfrac{1}{2}(\sqrt{-3}+\sqrt{-11}), & \text{if } D = 44,\\ \tfrac{1}{2}(3\sqrt{-3}+\sqrt{-19}), & \text{if } D = 76,\\ \tfrac{1}{2}(19\sqrt{-3}+5\sqrt{-43}), & \text{if } D = 172,\\ \tfrac{1}{2}(5\sqrt{-3}+\sqrt{-67}), & \text{if } D = 268,\\ \tfrac{1}{2}(715\sqrt{-3}+97\sqrt{-163}), & \text{if } D = 652. \end{cases}$$

We note that

$$(3.15)\qquad \theta_D\bar{\theta}_D = \begin{cases} 2, & \text{if } D = 44,\\ -2, & \text{if } D \neq 44. \end{cases}$$

Appealing to (3.13) we see that

$$(3.16)\qquad \left[\frac{\lambda_D}{\mu_D}\right]_3 = \left[\frac{\lambda_D}{\theta_D}\right]_3 \left[\frac{\lambda_D}{\bar{\theta}_D}\right]_3^2.$$

Thus we have shown:

$$(3.17)\qquad p \text{ is represented by } p_{-D} \Leftrightarrow \left[\frac{\lambda_D}{\theta_D}\right]_3 = \left[\frac{\lambda_D}{\bar{\theta}_D}\right]_3.$$

From (3.14) and (3.15) we obtain

$$\pm\theta_D^3\bar{\theta}_D = 2\theta_D^2 = \begin{cases} -7-\sqrt{33}, & \text{if } D = 44,\\ -23-3\sqrt{57}, & \text{if } D = 76,\\ -1579-95\sqrt{129}, & \text{if } D = 172,\\ -71-5\sqrt{201}, & \text{if } D = 268,\\ -1533671-69355\sqrt{489}, & \text{if } D = 652, \end{cases}$$

from which we see that

$$(3.18)\qquad \begin{cases} \sqrt{3D^*} \equiv r_D \pmod{\theta_D^3},\\ \sqrt{3D^*} \equiv -r_D \pmod{\bar{\theta}_D^3}, \end{cases}$$

where

$$(3.19)\qquad r_D = \begin{cases} 1, & \text{if } D = 44,\\ 3, & \text{if } D = 76, 172, 652,\\ 5, & \text{if } D = 268. \end{cases}$$

Multiplying (3.18) by $\sqrt{-3}$, we obtain

$$(3.20)\qquad \begin{cases} \sqrt{-D^*} \equiv 3r_D\sqrt{-3} \pmod{\theta_D^3},\\ \sqrt{-D^*} \equiv -3r_D\sqrt{-3} \pmod{\bar{\theta}_D^3}. \end{cases}$$

Next, as λ_D is a prime divisor of p in R_D, we have

$$(3.21)\qquad p = \begin{cases} \lambda_D\bar{\lambda}_D\lambda'_D\bar{\lambda}'_D, & \text{if } p \equiv 1 \pmod 3,\\ \lambda_D\bar{\lambda}_D, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

As λ_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, if $p \equiv 2 \pmod 3$, such that

$$(3.22)\qquad \lambda_D = \begin{cases} \tfrac{1}{4}(x_0+x_1\sqrt{-3}+x_2\sqrt{-D^*}+x_3\sqrt{3D^*}), & \text{if } p \equiv 1 \pmod 3,\\ \tfrac{1}{2}(x_0+x_1\sqrt{-D^*}), & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

with

$$(3.23)\qquad \begin{cases} \begin{Bmatrix} x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod 2\\ x_0-x_1+x_2+x_3 \equiv 0 \pmod 4 \end{Bmatrix}, & \text{if } p \equiv 1 \pmod 3,\\ x_0 \equiv x_1 \pmod 2, & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

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

$$(3.24)\qquad \tfrac{1}{2}(u+v\sqrt{-D^*}) = \begin{cases} \lambda_D\lambda'_D, & \text{if } p \equiv 1 \pmod 3,\\ \lambda_D, & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

so that u and v are integers such that

$$(3.25)\qquad u = \begin{cases} (x_0^2+3x_1^2-D^*x_2^2-3D^*x_3^2)/8, & \text{if } p \equiv 1 \pmod 3,\\ x_0, & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

$$(3.26)\qquad v = \begin{cases} (x_0x_2-3x_1x_3)/4, & \text{if } p \equiv 1 \pmod 3,\\ x_1, & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

and

$$(3.27)\qquad 4p = u^2+D^*v^2, \quad u \equiv v \pmod 2.$$

Clearly p is represented by p_{-D} if and only if $u \equiv v \equiv 0 \pmod 2$. Thus, in view of (3.17), we must show that

$$(3.28)\qquad \left[\frac{\lambda_D}{\theta_D}\right]_3 = \left[\frac{\lambda_D}{\bar{\theta}_D}\right]_3 \Leftrightarrow \begin{cases} x_0x_2-3x_1x_3 \equiv 0 \pmod 8, & \text{if } p \equiv 1 \pmod 3,\\ x_1 \equiv 0 \pmod 2, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Next, as θ_D is a prime divisor of 2 and λ_D is a prime divisor of the odd prime p, we have $\lambda_D \nmid \theta_D$ and

$$(3.29)\qquad \lambda_D^3 \equiv \lambda_D^{N(\theta_D)-1} \equiv 1 \pmod{\theta_D},$$

showing that

$$(3.30)\qquad \lambda_D \equiv 1, \omega \text{ or } \omega^2 \pmod{\theta_D},$$

where $\omega=(-1+\sqrt{-3})/2$. Appealing to (3.18) and (3.20), we obtain for $p\equiv 1 \pmod 3$

$$(3.31)\qquad \lambda_D\equiv\begin{cases}1 \pmod{\theta_D}, & \text{if } E\equiv 0 \pmod 4,\ F\equiv 4 \pmod 8,\\ \omega \pmod{\theta_D}, & \text{if } E\equiv 2 \pmod 4,\ F\equiv 4 \pmod 8,\\ \omega^2 \pmod{\theta_D}, & \text{if } E\equiv 2 \pmod 4,\ F\equiv 0 \pmod 8,\end{cases}$$

where

$$(3.32)\qquad E=x_0+rx_3,\quad F=x_0-x_1-3rx_2+rx_3;$$

and for $p\equiv 2 \pmod 3$

$$(3.33)\qquad \lambda_D\equiv\begin{cases}1 \pmod{\theta_D}, & \text{if } x_0\equiv x_1\equiv 0 \pmod 2,\ x_0+rx_1\equiv 2 \pmod 4,\\ \omega \pmod{\theta_D}, & \text{if } x_0\equiv x_1\equiv 1 \pmod 2,\ x_0+rx_1\equiv 2 \pmod 4,\\ \omega^2 \pmod{\theta_D}, & \text{if } x_0\equiv x_1\equiv 1 \pmod 2,\ x_0+rx_1\equiv 0 \pmod 4.\end{cases}$$

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)

$$\left[\frac{\lambda_D}{\theta_D}\right]_3=\left[\frac{\lambda_D}{\theta'_D}\right]_3$$

$$\Leftrightarrow \begin{Bmatrix}\lambda_D\equiv 1 \pmod{\theta_D}\\ \lambda_D\equiv 1 \pmod{\theta'_D}\end{Bmatrix} \text{ or } \begin{Bmatrix}\lambda_D\equiv \omega \pmod{\theta_D}\\ \lambda_D\equiv \omega \pmod{\theta'_D}\end{Bmatrix} \text{ or } \begin{Bmatrix}\lambda_D\equiv \omega^2 \pmod{\theta_D}\\ \lambda_D\equiv \omega^2 \pmod{\theta'_D}\end{Bmatrix}$$

$$\Leftrightarrow \begin{Bmatrix}x_0\equiv -rx_3 \pmod 4\\ x_0-x_1-3rx_2+rx_3\equiv 4 \pmod 8\\ x_0\equiv rx_3 \pmod 4\\ x_0+x_1-3rx_2-rx_3\equiv 4 \pmod 8\end{Bmatrix} \text{ or }$$

$$\begin{Bmatrix}x_0+2\equiv -rx_3 \pmod 4\\ x_0-x_1-3rx_2+rx_3\equiv 4 \pmod 8\\ x_0+2\equiv rx_3 \pmod 4\\ x_0+x_1-3rx_2-rx_3\equiv 0 \pmod 8\end{Bmatrix} \text{ or }$$

$$\begin{Bmatrix}x_0+2\equiv -rx_3 \pmod 4\\ x_0-x_1-3rx_2+rx_3\equiv 0 \pmod 8\\ x_0+2\equiv rx_3 \pmod 4\\ x_0+x_1-3rx_2-rx_3\equiv 4 \pmod 8\end{Bmatrix}$$

$$\Leftrightarrow \begin{Bmatrix}x_0\equiv x_1\equiv x_2\equiv x_3\equiv 0 \pmod 2,\ \text{say } x_i=2y_i\ (i=0,1,2,3)\\ \text{and}\\ y_0\equiv y_3 \pmod 2,\ y_0-y_1-3ry_2+ry_3\equiv 2 \pmod 4,\ y_0+y_1-3ry_2-ry_3\equiv 2 \pmod 4\\ \text{or}\\ y_0+1\equiv y_3 \pmod 2,\ y_0-y_1-3ry_2+ry_3\equiv 2 \pmod 4,\ y_0+y_1-3ry_2-ry_3\equiv 0 \pmod 4\\ \text{or}\\ y_0+1\equiv y_3 \pmod 2,\ y_0-y_1-3ry_2+ry_3\equiv 0 \pmod 4,\ y_0+y_1-3ry_2-ry_3\equiv 2 \pmod 4\end{Bmatrix}$$

$$\Leftrightarrow \begin{Bmatrix}y_0\equiv y_1\equiv y_2\equiv y_3 \pmod 2,\ y_0-y_1+ry_2+ry_3\equiv 2 \pmod 4\\ \text{or}\\ y_0\equiv y_3+1 \pmod 2,\ y_0-y_1-3ry_2+ry_3\equiv y_0+y_1-3ry_2-ry_3+2 \pmod 4\end{Bmatrix}$$

$$\Leftrightarrow \begin{Bmatrix}y_0\equiv y_1\equiv y_2\equiv y_3 \pmod 2,\ y_0-y_1-y_2-y_3\equiv 2 \pmod 4\\ \text{or}\\ y_0\equiv y_1\equiv y_2+1\equiv y_3+1 \pmod 2\end{Bmatrix}.$$

It should be noted that if $x_0\equiv x_1\equiv x_2\equiv x_3\equiv 0 \pmod 2$, with $x_i=2y_i$ $(i=0,1,2,3)$, then by (3.23), we have

$$(3.34)\qquad y_0+y_1+y_2+y_3\equiv 0 \pmod 2.$$

In view of (3.28) we must show that the assertion

$$(3.35)\qquad x_0x_2-3x_1x_3\equiv 0 \pmod 8$$

is equivalent to

$$(3.36)\qquad \begin{cases}x_i=2y_i\ (i=0,1,2,3) \text{ and}\\ y_0\equiv y_1\equiv y_2\equiv y_3 \pmod 2,\ y_0-y_1-y_2-y_3\equiv 2 \pmod 4, \text{ or}\\ y_0\equiv y_1\equiv y_2+1\equiv y_3+1 \pmod 2,\end{cases}$$

under (3.23). It is clear that (3.36) implies (3.35) as

$$x_0x_2-3x_1x_3=4(y_0y_2-3y_1y_3)\equiv 4(y_0y_2-3y_0y_2)\equiv 0 \pmod 8.$$

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 (3.23) the x_i are all odd, say $x_i=2z_i+1$ $(i=0,1,2,3)$. Then, from (3.35), we have

$$(3.37)\qquad 2(z_0z_2+z_1z_3)+(z_0+z_1+z_2+z_3)\equiv 1 \pmod 4.$$

Further, as $u\equiv v\equiv 0 \pmod 2$, by (3.27) we see that $u+v\equiv 2 \pmod 4$, and so by (3.25) and (3.26), we have

$$(x_0^2+3x_1^2-D^*x_2^2-3D^*x_3^2)+2(x_0x_2-3x_1x_3)\equiv 16 \pmod{32},$$

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

$$(3.38)\qquad (z_0^2+3z_1^2-3z_2^2-z_3^2)+2(z_0z_2+z_1z_3)+2(z_0-z_2+2z_3)\equiv 7 \pmod 8.$$

From (3.37) we deduce

$$(2z_1+1)z_3 \equiv 1-z_0-z_1-z_2+2z_0z_2 \pmod 4. \tag{3.39}$$

Multiplying (3.39) by $(2z_1+1)$, we obtain

$$z_3 \equiv 1-(z_0+z_1+z_2)+2(z_0z_1+z_1z_2+z_2z_0) \pmod 4, \tag{3.40}$$

so that

$$\begin{cases} z_3 \equiv 1-A+2B \pmod 4, \\ z_3^2 \equiv 1+A^2-2A+4AB \pmod 8, \end{cases} \tag{3.41}$$

where

$$A = z_0+z_1+z_2, \quad B = z_0z_1+z_1z_2+z_2z_0. \tag{3.42}$$

Using (3.41) in (3.38), we obtain

$$3+4(z_0+z_2)\big((z_0z_1+z_1z_2+z_2z_0)-z_1\big) \equiv 7 \pmod 8,$$

that is

$$(z_0+z_2)(z_0z_1+z_1z_2+z_2z_0-z_1) \equiv 1 \pmod 2,$$

showing that

$$z_0+z_2 \equiv z_0z_1+z_1z_2+z_2z_0-z_1 \equiv 1 \pmod 2,$$

which gives the contradiction

$$z_0+z_2 \equiv z_0z_2 \equiv 1 \pmod 2.$$

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

$$y_0^2-y_1^2+y_2^2-y_3^2 \equiv 0 \pmod 4, \tag{3.43}$$

$$y_0y_2+y_1y_3 \equiv 0 \pmod 2, \tag{3.44}$$

$$y_0^2+3y_1^2-3y_2^2-y_3^2+2y_0y_2+2y_1y_3 \equiv 4 \pmod 8. \tag{3.45}$$

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

$$y_0 \equiv y_1+1 \equiv y_2+1 \equiv y_3 \pmod 2. \tag{3.46}$$

If $y_0 \equiv 0 \pmod 2$ then (3.45) and (3.46) give

$$y_0^2-y_3^2+2y_0+2y_3 \equiv 4 \pmod 8,$$

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

$$y_1^2+y_2^2+2y_1+2y_2 \equiv 4 \pmod 8,$$

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 $y_1 \equiv y_2+1 \pmod 2$ we are finished. Otherwise $y_1 \equiv y_2 \pmod 2$ 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

$$\begin{aligned} y_0-y_1-y_2-y_3 &\equiv 2y_0-(y_0+y_1+y_2+y_3) \pmod 4 \\ &\equiv 2-(y_0+1)(y_2+1)-(y_1+1)(y_3+1)+(y_0y_2+y_1y_3) \\ &\quad +2 \pmod 4 \\ &\equiv 2-0-0+2+2 \pmod 4 \\ &\equiv 2 \pmod 4, \end{aligned}$$

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 $\overline{\theta}'_D = -\theta'_D$, we have $\left[\frac{\lambda_D}{\overline{\theta}'_D}\right]_3 = \left[\frac{\lambda_D}{\theta_D}\right]_3^2$, and so $\left[\frac{\lambda_D}{\overline{\theta}'_D}\right]_3 = \left[\frac{\lambda_D}{\theta_D}\right]_3$ holds if and only if $\left[\frac{\lambda_D}{\theta_D}\right]_3 = 1$, that is, if and only if $\lambda_D \equiv 1 \pmod{\theta_D}$. By (3.33) this condition is equivalent to $x_0 \equiv x_1 \equiv 0 \pmod 2$, $x_0 + rx_1 \equiv 2 \pmod 4$, which by (3.25), (3.26) and (3.27) is equivalent to $u \equiv v \equiv 0 \pmod 2$ as required.

The proof of Theorem 1 is now complete.

4. Proof of Theorem 2. Since $\sqrt[3]{\varkappa_D} + \sqrt[3]{\varkappa'_D}$ is the real root of $27f_{-D}((x-r)/3)$, where r is the coefficient of x^2 in $f_{-D}(x)$, 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*

$$p > 3, \quad p \nmid AB, \quad \left(\frac{-4A^3 - 27B^2}{p}\right) = +1.$$

Define an integer A_1 by $A \equiv 3A_1 \pmod p$. Let $\{u_n\}_{n=0,1,2,\dots}$ be the sequence of integers defined by

$$u_{n+2} + Bu_{n+1} - A_1^3 u_n = 0,$$

$$u_0 = 2, \quad u_1 = -B.$$

Then $x^3 + Ax + B$ is congruent to the product of three distinct linear polynomials $\pmod p$ *if*

$$\begin{cases} u_{(p-1)/3} \equiv 2 \pmod p, & p \equiv 1 \pmod 3, \\ u_{(p+1)/3} \equiv -2A_1 \pmod p, & p \equiv 2 \pmod 3, \end{cases}$$

and $x^3 + Ax + B$ is irreducible $\pmod p$ *if*

$$\begin{cases} u_{(p-1)/3} \equiv -1 \pmod p, & p \equiv 1 \pmod 3, \\ u_{(p+1)/3} \equiv A_1 \pmod p, & p \equiv 2 \pmod 3. \end{cases}$$

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

[1] E. Brown and C. J. Parry, *The imaginary bicyclic biquadratic fields with classnumber* 1, J. Reine Angew. Math. 266 (1974), 118–120.

[2] A. Cauchy, Exercices de Mathématiques 4 (1829), 274–292. (*Oeuvres* (2), 9, 326–333.)

[3] David A. Cox, *Primes of the form x^2+ny^2 in From Fermat to Class Field Theory and Complex Multiplication*, John Wiley and Sons, New York 1989.

[4] L. E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bull. Amer. Math. Soc. 13 (1906), 1–8.

[5] C. F. Gauss, *Theoria Residuorum Biquadraticorum, Commentatio Prima*, in *Werke*, II (1876), 65–92.

[6] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. 13 (1985), 23–37.

[7] B. Gross and D. Zagier, *Points de Heegner et derivées de fonctions L*, C. R. Acad. Sci. Paris 297 (1983), 85–87.

[8] S. Gurak, *On the representation theory for full decomposable forms*, J. Number Theory 13 (1981), 421–442.

[9] H. Hasse, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante* −47, Acta Arith. 9 (1964), 419–434.

[10] C. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math. 2 (1827), 66–69.

[11] L. Kronecker, *Werke*, Vol. II, p. 93 and pp. 97–101, Vol. IV, pp. 123–129, Chelsea Publishing Co., New York, N.Y., 1968.

[12] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proc. Int. Conf. on Class Numbers and Fund. Units, June 24–28, 1986, Katata, Japan, pp. 217–242.

[13] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Séminaire Nicolas Bourbaki, 1983–1984, Exp. 631.

[14] — *Nombres des classes des corps quadratiques imaginaires*, Astérisque 121–122 (1985), 309–323.

[15] H. M. Stark, *A complete determination of the complex quadratic fields with classnumber one*, Michigan Math. J. 14 (1967), 1–27.

[16] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress, Zürich (1897), 182–193.

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

[18] P. J. Weinberger, *The cubic character of quadratic units*, Proc. 1972 Number Theory Conference, University of Colorado, Aug. 14–18, 1972, pp. 241–242.

[19] K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. 13 (1970), 519–526.

[20] D. Zagier, *L-series of elliptic curves, the Birch–Swinnerton-Dyer conjecture, and the class number problem of Gauss*, Notices Amer. Math. Soc. 31 (1984), 739–743.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada K1S 5B6

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, South Carolina, U.S.A. 29208

Received on 22.5.1989
and in revised form on 19.9.1989 (1938)