THE CUBIC CONGRUENCE $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ AND BINARY QUADRATIC FORMS

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT

In this paper it is shown that the splitting modulo a prime p of a given monic irreducible cubic polynomial with integral coefficients is equivalent to p being represented by forms in a certain subgroup of index 3 in the form class group of discriminant equal to the discriminant of the cubic.

1. *Introduction*

In this paper we are interested in the number N of solutions $x \pmod p$ of the congruence

$$x^3+Ax^2+Bx+C\equiv 0 \pmod p, \tag{1.1}$$

where A, B, C are integers such that the cubic polynomial x^3+Ax^2+Bx+C is irreducible over the field Q of rational numbers and p is a prime greater than 3 which does not divide the discriminant D of the cubic, which we assume throughout is not a perfect square. We note that

$$D = A^2B^2-4B^3-4A^3C-27C^2+18ABC, \tag{1.2}$$

and that

$$D\equiv (AB+C)^2\equiv 0 \text{ or } 1 \pmod 4. \tag{1.3}$$

Stickelberger's parity theorem [5] asserts that the Legendre symbol $\left(\frac{D}{p}\right)$ is given by

$$\left(\frac{D}{p}\right) = (-1)^{k+1}, \tag{1.4}$$

where k is the number of irreducible factors of $x^3+Ax^2+Bx+C \pmod p$. Thus we have

$$N = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\frac{D}{p}\right) = +1, \\ 1 & \text{if } \left(\frac{D}{p}\right) = -1. \end{cases} \tag{1.5}$$

It is the purpose of this paper to use the representability or non-representability of p by the reduced, primitive, integral binary quadratic forms $(a,b,c) = ax^2+bxy+cy^2$ of discriminant $b^2-4ac = D$ to distinguish between $N=0$ and $N=3$. (Only positive-definite forms are considered when $D<0$.)

Received 15 November 1990.

1991 *Mathematics Subject Classification* 11A07.

Research of the second author was supported by grant A-7233 of the Natural Sciences and Engineering Research Council of Canada.

We let $H(D)$ (respectively $h(D)$) denote the form class group (respectively class number) of classes of primitive, integral binary quadratic forms of discriminant D. The main result of this paper is the following theorem.

THEOREM. *There is a unique subgroup $J = J(A, B, C)$ of index 3 in $H(D)$ with the following property.*

If p is any prime (greater than 3) such that $(D/p) = +1$ then $x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by one of the forms in $J(A, B, C)$.

In the special case when D is squarefree, this result has been stated by Shanks [4] without proof. The case when D is not squarefree does not seem to have been treated in the literature, and it is precisely the presence of square factors in D which adds complications to the proof. The proof of the theorem uses class field theory and is given in §3 after some preliminary results are proved in §2.

2. *Preliminary results*

Let $\theta, \theta', \theta''$ denote the three roots of the cubic polynomial $x^3 + Ax^2 + Bx + C$, so that

$$D = (\theta - \theta')^2(\theta' - \theta'')^2(\theta'' - \theta)^2, \tag{2.1}$$

and

$$\pm\sqrt{D} = (\theta - \theta')(\theta' - \theta'')(\theta'' - \theta). \tag{2.2}$$

If $D > 0$, $\theta, \theta', \theta''$ are all real, and we order them so that $\theta < \theta' < \theta''$, in which case

$$(\theta - \theta')(\theta' - \theta'')(\theta'' - \theta) > 0.$$

If $D < 0$, exactly one of $\theta, \theta', \theta''$ is real, and we choose θ to be the real root. Interchanging the complex conjugate roots θ' and θ'', if necessary, we can ensure that $(\theta - \theta')(\theta' - \theta'')(\theta'' - \theta)/\sqrt{D}$ is positive. Hence, in both cases $\theta, \theta', \theta''$ are uniquely determined and

$$\sqrt{D} = (\theta - \theta')(\theta' - \theta'')(\theta'' - \theta). \tag{2.3}$$

Further, as $\theta, \theta', \theta''$ are the roots of $x^3 + Ax^2 + Bx + C$, we have

$$\left.\begin{aligned} \theta + \theta' + \theta'' &= -A, \\ \theta\theta' + \theta'\theta'' + \theta''\theta &= B, \\ \theta\theta'\theta'' &= -C. \end{aligned}\right\} \tag{2.4}$$

We next determine $\theta' - \theta''$ in terms of θ and $\sqrt{D}$, see (2.7) below. From (2.3) we have

$$\theta' - \theta'' = \frac{\sqrt{D}}{(\theta - \theta')(\theta'' - \theta)}.$$

Appealing to the first two relations in (2.4), we obtain

$$\theta' - \theta'' = \frac{-\sqrt{D}}{B + 2A\theta + 3\theta^2}. \tag{2.5}$$

Next, by the well-known formula for the discriminant of a polynomial in terms of its derivative, we have

$$(B + 2A\theta + 3\theta^2)(B + 2A\theta' + 3\theta'^2)(B + 2A\theta'' + 3\theta''^2) = -D.$$

Thus (2.5) becomes

$$\theta'-\theta''=\frac{(B+2A\theta'+3\theta'^2)(B+2A\theta''+3\theta''^2)}{\sqrt{D}}. \tag{2.6}$$

From (2.4) we obtain

$$\begin{gathered}\theta'+\theta''=-A-\theta,\\ \theta'\theta''=B+A\theta+\theta^2,\\ \theta'^2+\theta''^2=(A^2-2B)-\theta^2,\\ \theta'\theta''(\theta'+\theta'')=(C-AB)-A^2\theta-A\theta^2,\\ \theta'^2\theta''^2=(B^2-AC)+(AB-C)\theta+B\theta^2,\end{gathered}$$

so that (2.6) becomes

$$\theta'-\theta''=((4B^2-A^2B-3AC)+(-2A^3+7AB-9C)\theta+(-2A^2+6B)\theta^2)/\sqrt{D}. \tag{2.7}$$

Then, using $\theta'+\theta''=-A-\theta$, we see that

$$\left.\begin{aligned}\theta'&=\frac{-A}{2}-\frac{\theta}{2}+\frac{((4B^2-A^2B-3AC)+(-2A^3+7AB-9C)\theta+(-2A^2+6B)\theta^2)}{2\sqrt{D}},\\ \theta''&=\frac{-A}{2}-\frac{\theta}{2}-\frac{((4B^2-A^2B-3AC)+(-2A^3+7AB-9C)\theta+(-2A^2+6B)\theta^2)}{2\sqrt{D}}.\end{aligned}\right\} \tag{2.8}$$

We set

$$K=Q(\sqrt{D}), \qquad L=K(\theta)=Q(\sqrt{D},\theta), \tag{2.9}$$

$$C=Q(\theta), \quad C'=Q(\theta'), C''=Q(\theta''). \tag{2.10}$$

LEMMA 1. *L is a cyclic cubic extension of K.*

Proof. The expressions for θ' and θ'' in (2.8) show that

$$L=K(\theta)=K(\theta')=K(\theta''),$$

so that L/K is normal. Moreover we have $[L:K]=3$ and $\mathrm{Gal}(L/K)$ is a cyclic group of order 3. Thus L is a cyclic cubic extension of K.

LEMMA 2. *L is a dihedral extension of Q.*

Proof. Let σ be the automorphism of L given by

$$\left.\begin{aligned}\sigma(\theta)&=\theta',\\ \sigma(\sqrt{D})&=\sqrt{D},\end{aligned}\right\} \tag{2.11}$$

and let τ be the automorphism of L given by

$$\left.\begin{aligned}\tau(\theta)&=\theta,\\ \tau(\sqrt{D})&=-\sqrt{D}.\end{aligned}\right\} \tag{2.12}$$

Then we have $\sigma(\theta')=\theta'', \sigma(\theta'')=\theta, \tau(\theta')=\theta'', \tau(\theta'')=\theta'$ and

$$\sigma^3=\tau^2=1, \qquad \sigma^2\tau=\tau\sigma, \tag{2.13}$$

and

$$\mathrm{Gal}(L/Q)=\{1,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau\}=D_3, \tag{2.14}$$

where, for $n\geqslant 3$, D_n denotes the dihedral group of order $2n$. Thus L is a dihedral extension of Q.

If F is an algebraic number field, we write $d(F)$ for the discriminant of F.

LEMMA 3. *There is a positive integer g such that*

$$D = g^2 d(K).$$

Proof. Let $D = D_1 m^2$, where D_1 is a squarefree integer and m is a positive integer. Moreover we have

$$m \equiv 0 \pmod 2, \qquad \text{if } D \equiv 0 \pmod 4.$$

We note that

$$\begin{aligned} d(K) = d(Q(\sqrt{D})) &= d(Q(\sqrt{(D_1 m^2)})) = d(Q(\sqrt{D_1})) \\ &= \begin{cases} D_1 & \text{if } D_1 \equiv 1 \pmod 4, \\ 4D_1 & \text{if } D_1 \equiv 2,3 \pmod 4, \end{cases} \\ &= \begin{cases} D/m^2 & \text{if } D_1 \equiv 1 \pmod 4, \\ 4D/m^2 & \text{if } D_1 \equiv 2,3 \pmod 4, \end{cases} \\ &= D/g^2, \end{aligned}$$

where g is the positive integer given by

$$g = \begin{cases} m & \text{if } D_1 \equiv 1 \pmod 4 \\ m/2 & \text{if } D_1 \equiv 2,3 \pmod 4. \end{cases}$$

If a and b are integers with $a \neq 0$ we write $a \mid b$ to mean a divides b.

LEMMA 4. $d(L) \mid g^6 d(K)^3$.

Proof. Clearly the discriminant $d(L)$ divides the discriminant $d(1, \theta, \theta^2, \theta', \theta\theta', \theta^2\theta')$ of the set $\{1, \theta, \theta^2, \theta', \theta\theta', \theta^2\theta'\}$ of integers of L. We have

$$d(1,\theta,\theta^2,\theta',\theta\theta',\theta^2\theta') = \begin{vmatrix} 1 & \theta & \theta^2 & \theta' & \theta\theta' & \theta^2\theta' \\ 1 & \theta' & \theta'^2 & \theta'' & \theta'\theta'' & \theta'^2\theta'' \\ 1 & \theta'' & \theta''^2 & \theta & \theta''\theta & \theta''^2\theta \\ 1 & \theta & \theta^2 & \theta'' & \theta\theta'' & \theta^2\theta'' \\ 1 & \theta' & \theta'^2 & \theta & \theta'\theta & \theta'^2\theta \\ 1 & \theta'' & \theta''^2 & \theta' & \theta''\theta' & \theta''^2\theta' \end{vmatrix}^2$$

$$= (\theta''-\theta')^2(\theta-\theta'')^2(\theta'-\theta)^2 \begin{vmatrix} 1 & \theta & \theta^2 & \theta' & \theta\theta' & \theta^2\theta' \\ 1 & \theta' & \theta'^2 & \theta'' & \theta'\theta'' & \theta'^2\theta'' \\ 1 & \theta'' & \theta''^2 & \theta & \theta''\theta & \theta''^2\theta \\ 0 & 0 & 0 & 1 & \theta & \theta^2 \\ 0 & 0 & 0 & 1 & \theta' & \theta'^2 \\ 0 & 0 & 0 & 1 & \theta'' & \theta''^2 \end{vmatrix}^2$$

$$= (\theta-\theta')^6(\theta'-\theta'')^6(\theta''-\theta)^6$$

$$= D^3,$$

so that

$$d(L) \mid D^3.$$

The required result now follows from Lemma 3.

If E and F are algebraic number fields with $E \subseteq F$, the discriminant (respectively conductor) of the extension F/E is denoted by $d(F/E)$ (respectively $f(F/E)$). The ring of integers of the field E is denoted by O_E.

LEMMA 5. *There exists a rational integer f such that*

$$d(L/K) = (fO_K)^2.$$

Proof. See [3, Théorème 3.5].

LEMMA 6. $d(L/K) = f(L/K)^2$.

Proof. This follows immediately from [1, Corollary 17.29] as L/K is cyclic by Lemma 1.

LEMMA 7. $f(L/K) = fO_K$.

Proof. This follows from Lemmas 5 and 6.

LEMMA 8. $f^2 \mid g^3$.

Proof. By the discriminant relation [1, Theorem 17.3] for the tower of fields $Q \subset K \subset L$, we have

$$d(L) = d(K)^3 N_{K/Q}(d(L/K)).$$

Appealing to Lemma 5, we obtain

$$d(L) = d(K)^3 f^4. \tag{2.15}$$

From (2.15) and Lemma 4, we deduce that $f^4 \mid g^6$ so that $f^2 \mid g^3$.

LEMMA 9. $d(C) = 3^{2\rho} h^2 d(K)$, *where $\rho = 0, 1, 2$ and h is a positive integer not divisible by* 3.

Proof. See [3, Théorème 2.3].

If a and b are integers (with $a \neq 0$) such that $a^k \mid b, a^{k+1} \nmid b$, for some non-negative integer k, we write $a^k \parallel b$.

LEMMA 10. *If $3^\alpha \parallel f$ then $\alpha \leqslant 2$.*

Proof. We define the non-negative integers l, c and k by

$$3^l \parallel d(L), \quad 3^c \parallel d(C), \quad 3^k \parallel d(K),$$

and note that $k = 0, 1$. From (2.15) we obtain

$$l = 3k + 4\alpha. \tag{2.16}$$

By the discriminant relation for the tower of fields $Q \subset C \subset L$, we have

$$d(L) = d(C)^2 N_{C/Q}(d(L/C)). \tag{2.17}$$

Further, as

$$w_k = \tfrac{1}{2}(d(K) + \sqrt{(d(K))}) \in O_K \subset O_L, \tag{2.18}$$

we have

$$d(L/C)\left|\begin{vmatrix} 1 & w_k \\ 1 & \tau(w_k) \end{vmatrix}\right|^2 = d(K),$$

so that

$$N_{C/Q}(d(L/C)) \mid d(K)^3,$$

and thus by (2.17)

$$d(L) \mid d(C)^2 d(K)^3,$$

giving

$$l \leqslant 2c + 3k. \tag{2.19}$$

Hence, from (2.16) and (2.19), we deduce that

$$2\alpha \leqslant c.$$

Next, from Lemma 9, we obtain

$$c = 2\rho + k \leqslant 2 \cdot 2 + 1 = 5,$$

so that

$$\alpha \leqslant 2.$$

LEMMA 11. *$f \mid g g_1$, where $g_1 = g/3^\beta$, $3^\beta \parallel g$.*

Proof. Let $f = 3^\alpha f_1, g = 3^\beta g_1$, where $\alpha \geqslant 0, \beta \geqslant 0$, $3 \nmid f_1$, $3 \nmid g_1$. By Lemma 8 we have $2\alpha \leqslant 3\beta$ and $f_1^2 \mid g_1^3$. Thus $f_1 \mid g_1^2$ and, as $\alpha \leqslant 2$ by Lemma 10, we have $\alpha \leqslant \beta$. Hence we have

$$f = 3^\alpha f_1 \mid 3^\beta g_1^2 = g g_1.$$

3. *Proof of Theorem*

Throughout this section p denotes a prime such that $p > 3$ and $\left(\frac{D}{p}\right) = +1$, so that by Lemma 3 $\left(\frac{d(K)}{p}\right) = 1$ and $p \nmid g$. In addition $\mathfrak{P}$ denotes a prime ideal of O_K dividing p, so that $N_{K/Q}(\mathfrak{P}) = p$. We also let $\tilde{\mathfrak{P}}$ be a prime in O_L lying above $\mathfrak{P}$. As L/K is an abelian extension (Lemma 1) and as $\mathfrak{P} \nmid g$, $\mathfrak{P}$ is unramified in L by Lemmas 7 and 8 and the Artin symbol $\left(\frac{L(K)}{\mathfrak{P}}\right)$ is defined. Since $\left(\frac{L(K)}{\mathfrak{P}}\right)$ is an automorphism of $\mathrm{Gal}(L/K) = \langle \sigma \rangle \simeq Z/3Z$, we have

$$\left(\frac{L/K}{\mathfrak{P}}\right) = \sigma^{e(\mathfrak{P})}, \qquad e(\mathfrak{P}) = 0, 1, 2. \tag{3.1}$$

Further, for all $\alpha \in O_L$, we have

$$\sigma^{e(\mathfrak{P})}(\alpha) = \left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N_{K/Q}(\mathfrak{P})} \pmod{\tilde{\mathfrak{P}}}. \tag{3.2}$$

LEMMA 12. *$x^3+Ax^2+Bx+C\equiv 0 \pmod p$ has three solutions if and only if $e(\mathfrak{P})=0$.*

Proof. If $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ has three solutions then p splits completely in O_L. Then $N_{L/Q}(\tilde{\mathfrak{P}})=p$ and, appealing to (3.2) and Fermat's theorem, for any $\alpha\in O_L$ we have

$$\sigma^{e(\mathfrak{P})}(\alpha)\equiv \alpha^{N_{K/Q}(\mathfrak{P})}\equiv \alpha^p\equiv \alpha \pmod{\tilde{\mathfrak{P}}}.$$

By the uniqueness of the Artin symbol, we see that $\sigma^{e(\mathfrak{P})}$ is the identity automorphism, that is, $e(\mathfrak{P})=0$.

On the other hand, if $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ does not have three solutions, then as $\left(\frac{D}{p}\right)=+1$ and $p>3$, it does not have any solutions. Thus $\mathfrak{P}$ remains a prime ideal $\tilde{\mathfrak{P}}$ in O_L with $N_{L/Q}(\tilde{\mathfrak{P}})=p^3$. Since $(O_L/\mathfrak{P})^*$ is a cyclic group of order p^3-1, there exists an element α of O_L of order p^3-1 modulo $\tilde{\mathfrak{P}}$. Clearly we have $\alpha^p\not\equiv\alpha \pmod{\tilde{\mathfrak{P}}}$. Now suppose that $e(\mathfrak{P})=0$. Then, by (3.2), we have

$$\alpha=\sigma^{e(\mathfrak{P})}(\alpha)\equiv \alpha^{N_{K/Q}(\mathfrak{P})}\equiv \alpha^p \pmod{\tilde{\mathfrak{P}}},$$

which is a contradiction. Hence $e(\mathfrak{P})\neq 0$ in this case.

Next we define for any non-zero ideals M of O_K the group $I_K(M)$ by

$I_K(M)$ = group of all fractional ideal of O_K which are relatively prime to M.

We also set

$P_{K,Z}(M)$ = subgroup of $I_K(M)$ generated by principal ideals αO_K with $\alpha\in O_K$ and $\alpha\equiv a \pmod M$ for some integer a coprime with M

and

$P_{K,1}(M)$ = subgroup of $I_K(M)$ generated by principal ideals αO_K with $\alpha\in O_K$ and $\alpha\equiv 1 \pmod M$.

If $M=\alpha O_K$ we write $I_K(\alpha)$ for $I_K(\alpha O_K)$, $P_{K,Z}(\alpha)$ for $P_{K,Z}(\alpha O_K)$, and $P_{K,1}(\alpha)$ for $P_{K,1}(\alpha O_K)$. If M is divisible by all primes of K which ramify in L (note that the extension L/K has no ramified infinite primes) and I is a prime ideal O_K not dividing M, the Artin symbol $\left(\frac{L(K)}{I}\right)\in \mathrm{Gal}(L/K)$ is defined, and can be extended by multiplicativity to a homomorphism

$$\Phi_{L/K,M}: I_K(M)\longrightarrow \mathrm{Gal}(L/K),$$

which is called the Artin map for the extension $K\subset L$ and the ideal M.

We denote the order $[1, nw_K]$ of index n in O_K by O_n, so that $O_1=O_K$. (We defined w_K in (2.18).) The discriminant of O_n is $n^2d(K)$. We also let $C(O_n)$ denote the ideal class group of the order O_n, $h(O_n)=|C(O_n)|$ the class number of the order O_n, and F_n the ring class field of the order O_n.

LEMMA 13. $L\subseteq F_{gg_1}$.

Proof. By Lemmas 7 and 11, we have

$$f(L/K) \mid gg_1 O_K,$$

and so, by the conductor theorem (see for example [2, Theorem 8.5, p. 162]),

$$H = \ker(\Phi_{L/K, gg_1})$$

is a congruence subgroup for gg_1, that is,

$$P_{K,1}(gg_1) \subseteq H \subseteq I_K(gg_1),$$

and, by the Artin reciprocity theorem (see for example [2, Theorem 8.2, p. 161]), the Artin map $\Phi_{L/K, gg_1}$ induces an isomorphism

$$I_K(gg_1)/H \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Next we show that if $\alpha, \beta \in O_K$ are prime to g then

$$\alpha \equiv \beta \pmod{gg_1 O_K} \Longrightarrow (\alpha O_K \in H \longleftrightarrow \beta O_K \in H). \tag{3.3}$$

We choose $\gamma \in O_K$ such that $\alpha\gamma \equiv 1 \pmod{gg_1 O_K}$. Then we have $\beta\gamma \equiv 1 \pmod{gg_1 O_K}$, and so $\alpha\gamma O_K$ and $\beta\gamma O_K$ both belong to $P_{K,1}(gg_1) \subseteq H$, which proves (3.3).

The next step is to prove that for any ideal $A \in I_K(gg_1)$, we have

$$N_{K/Q}(A)\, O_K \in H. \tag{3.4}$$

As L is a dihedral extension of Q (Lemma 2), for $A \in I_K(gg_1)$ we have $\tau(A)\, H = (AH)^{-1}$, and so $A\tau(A) \in H$. Since $A\tau(A) = N_{K/Q}(A)\, O_K$, we have (3.4).

Now we prove that

$$\text{if } r \text{ is a prime} \not\mid g \text{ then } rO_K \in H. \tag{3.5}$$

First we treat the case when r splits or ramifies in K. In this case $r = N_{K/Q}(R)$ for some prime ideal R of O_K. Then, by (3.4), we have

$$rO_K = N_{K/Q}(R)\, O_K \in H.$$

Secondly we treat the case when r remains prime in K, so that $(d(K)/r) = -1$. Thus r splits as $rO_L = RR'R''$ in L, where R, R' and R'' are prime ideals of O_L with norms r and r^2 respectively. Then, for all $\alpha \in O_L$, we have

$$\left(\frac{L/K}{rO_K}\right)(\alpha) \equiv \alpha^{N_{K/Q}(r)} \equiv \alpha^{r^2} \equiv \alpha \pmod{R},$$

and so $\left(\dfrac{L/K}{rO_K}\right) = 1$ and thus $rO_K \in H$. This completes the proof of (3.5).

We see immediately from (3.5) by multiplicativity that

$$\text{if } c \text{ is an integer coprime with } g \text{ then } cO_K \in H. \tag{3.6}$$

Next we show that

$$P_{K,Z}(gg_1) \subseteq H. \tag{3.7}$$

If $\alpha O_K \in P_{K,Z}(gg_1)$, so that $\alpha \equiv c \pmod{gg_1}$ for some integer c coprime with gg_1, we deduce from (3.3) and (3.6) that $\alpha O_K \in H$. This proves (3.7).

Finally we show that $L \subseteq F_{gg_1}$. We have established the chain of inclusions

$$P_{K,1}(gg_1) \subseteq P_{K,Z}(gg_1) = \ker(\Phi_{F_{gg_1}/K, gg_1}) \subseteq \ker(\Phi_{L/K, gg_1}) = H.$$

Thus, by [2, Corollary 8.7], we have $L \subseteq F_{gg_1}$.

In fact a stronger result than Lemma 13 is true. We prove the following.

LEMMA 14. $L \subseteq F_g$.

Proof. For convenience we treat the cases $D < 0$ and $D > 0$ separately.

Case (i): $D < 0$. By Gauss's formula for the class number of an order in an imaginary quadratic field (see for example [**1**, Corollary 15.40]), we have

$$h(O_g) = \frac{h(O_K)g}{u} \prod_{q|g} \left(1 - \left(\frac{d(K)}{q}\right)\frac{1}{q}\right)$$

and

$$h(O_{gg_1}) = \frac{h(O_K)gg_1}{u} \prod_{q|g} \left(1 - \left(\frac{d(K)}{q}\right)\frac{1}{q}\right),$$

where q runs through all the primes dividing g and

$$u = \begin{cases} 3 & \text{if } d(K) = -3, \\ 2 & \text{if } d(K) = -4, \\ 1 & \text{otherwise} \end{cases}$$

so that

$$h(O_{gg_1}) = g_1 h(O_g).$$

Then, because of the isomorphisms $H(D) \simeq C(O_g)$ and $H(Dg_1^2) \simeq C(O_{gg_1})$, we have

$$h(Dg_1^2) = g_1 h(D).$$

Since $3 \nmid g_1$ and $H(D)$ is a surjective image of $H(Dg_1^2)$, it follows that the 3-parts of $H(D)$ and $H(Dg_1^2)$ are isomorphic. Now, as F_g (respectively F_{gg_1}) is the ring class field of the order O_g (respectively O_{gg_1}) we have

$$H(D) \simeq C(O_g) \simeq I_K(g)/P_{K,Z}(g) \simeq \mathrm{Gal}(F_g/K)$$

and

$$H(Dg_1^2) \simeq C(O_{gg_1}) \simeq I_K(gg_1)/P_{K,Z}(gg_1) \simeq \mathrm{Gal}(F_{gg_1}/K),$$

so that the 3-parts of $\mathrm{Gal}(F_g/K)$ and $\mathrm{Gal}(F_{gg_1}/K)$ are isomorphic. Thus, by Galois theory, F_g/K and F_{gg_1}/K contain the same number of subfields of degree 3 over K. Since $F_g \subseteq F_{gg_1}$ (as $O_{gg_1} \subseteq O_g$) and $K \subset L \subseteq F_{gg_1}$, $[L:K] = 3$, it follows that $L \subseteq F_g$.

Case (ii): $D > 0$. By Gauss's formula for the class number of an order in a real quadratic field (see for example [**1**, Corollary 15.40]), we have

$$h(O_g) = \frac{h(O_K)g \log \varepsilon_1}{\log \varepsilon_g} \prod_{q|g} \left(1 - \left(\frac{d(K)}{q}\right)\frac{1}{q}\right)$$

and

$$h(O_{gg_1}) = \frac{h(O_K)gg_1 \log \varepsilon_1}{\log \varepsilon_{gg_1}} \prod_{q|g} \left(1 - \left(\frac{d(K)}{q}\right)\frac{1}{q}\right),$$

where ε_n denotes the fundamental unit (greater than 1) of the order O_n and q runs through all the primes dividing g, so that

$$\frac{h(O_{gg_1})}{h(O_g)} = g_1 \frac{\log \varepsilon_g}{\log \varepsilon_{gg_1}}. \tag{3.8}$$

Next let $\varepsilon_1^{u_g}\,(u_g > 0)$ (respectively $\varepsilon_1^{u_{gg_1}}(u_{gg_1} > 0)$) denote the least power of ε_1 which belongs to O_g (respectively O_{gg_1}). Then (by [1, Corollary 15.40]) we have

$$\varepsilon_g = \varepsilon_1^{u_g}, \qquad \varepsilon_{gg_1} = \varepsilon_1^{u_{gg_1}}. \tag{3.9}$$

A straightforward argument using the minimality of u_g shows that $u_g \mid u_{gg_1}$, so that $v = u_{gg_1}/u_g$ is a positive integer. Then, from (3.8) and (3.9), we deduce that

$$h(O_{gg_1}) = g_1 h(O_g)/v. \tag{3.10}$$

Further, because of the isomorphisms

$$H(D) \simeq C^+(O_g), \qquad H(Dg_1^2) \simeq C^+(O_{gg_1}),$$

where $C^+(O_n)$ denotes the strict ideal class group of the order O_n, and the equalities

$$h^+(O_g) = |C^+(O_g)| = \begin{cases} h(O_g) & \text{if } N_{K/Q}(\varepsilon_g) = -1, \\ 2h(O_g) & \text{if } N_{K/Q}(\varepsilon_g) = +1, \end{cases}$$

$$h^+(O_{gg_1}) = |C^+(O_{gg_1})| = \begin{cases} h(O_{gg_1}) & \text{if } N_{K/Q}(\varepsilon_{gg_1}) = -1, \\ 2h(O_{gg_1}) & \text{if } N_{K/Q}(\varepsilon_{gg_1}) = +1, \end{cases}$$

we have

$$h(Dg_1^2) = ug_1 h(D)/v, \tag{3.11}$$

where

$$u = \begin{cases} 1 & \text{if } N_{K/Q}(\varepsilon_g) = N_{K/Q}(\varepsilon_{gg_1}), \\ 2 & \text{if } N_{K/Q}(\varepsilon_g) = -1, \quad N_{K/Q}(\varepsilon_{gg_1}) = 1. \end{cases}$$

We note that the case $N_{K/Q}(\varepsilon_g) = +1$, $N_{K/Q}(\varepsilon_{gg_1}) = -1$ cannot occur as $u_g \mid u_{gg_1}$. Let $3^r \parallel H(D)$, $3^s \parallel h(Dg_1^2)$, $3^t \parallel v$. Then, from (3.11), as $3 \nmid u$, $3 \nmid g_1$, we have $s = r - t$. But $H(D)$ is a surjective image of $H(Dg_1^2)$, so that $s \geqslant r$. Hence we have $t = 0$ and $s = r$. Since $3^r \parallel h(Dg_1^2)$, $3^r \parallel h(D)$ and $H(D)$ is a surjective image of $H(Dg_1^2)$, we see that the 3-parts of $H(D)$ and $H(Dg_1^2)$ are isomorphic. From the following isomorphisms

$$\begin{cases} H(D) \simeq C^+(O_g), \\ C^+(O_g)/E_g \simeq C(O_g) \simeq I_K(g)/P_{K,Z}(g) \simeq \mathrm{Gal}\,(F_g/K), \end{cases}$$

and

$$\begin{cases} H(Dg_1^2) \simeq C^+(O_{gg_1}), \\ C^+(O_{gg_1})/E_{gg_1} \simeq C(O_{gg_1}) \simeq I_K(gg_1)/P_{K,Z}(gg_1) \simeq \mathrm{Gal}\,(F_{gg_1}/K), \end{cases}$$

where E_g (respectively E_{gg_1}) denotes the subgroup generated by the strict class containing the principal ideal $\sqrt{DO_g}$ (respectively $\sqrt{DO_{gg_1}}$) (note that $|E_g| = 1$ or 2, $|E_{gg_1}| = 1$ or 2), we see that $\mathrm{Gal}\,(F_g/K)$ and $\mathrm{Gal}\,(F_{gg_1}/K)$ have the same 3-part. Then, exactly as in the case when $D < 0$, we can conclude that $L \subseteq F_g$.

LEMMA 15. *There exists a unique subgroup $M \equiv M(A, B, C)$ of index 3 in $I_K(g)$ such that*

$$e(\mathfrak{P}) = 0 \Longleftrightarrow \mathfrak{P} \in M(A, B, C).$$

Proof. As $L \subseteq F_g$ (Lemma 14) and $\mathrm{Gal}(F_g/K) \simeq I_K(g)/P_{K,Z}(g)$, by the classification theorem of class field theory there exists a unique subgroup $M \equiv M(A,B,C)$ of $I_K(g)$ with

$$P_{K,Z}(g) \subseteq M \subseteq I_K(g)$$

and

$$I_K(g)/M \simeq \mathrm{Gal}(L/K),$$

where the isomorphism is induced by the Artin map $\Phi_{L/K,g}$. Thus we see that

$$e(\mathfrak{P}) = 0 \Longleftrightarrow \left(\frac{L/K}{\mathfrak{P}}\right) = 1 \Longleftrightarrow \mathfrak{P} \in M(A,B,C),$$

proving Lemma 15.

We are now ready to prove the theorem.

Proof of theorem. Let $\mu: I_K(g) \to C(O_g)$ be the standard homomorphism passing from ideals to ideal classes and let $\lambda: C^+(O_g) \to H(D)$ be the standard isomorphism between ideal classes and form classes. We have

$$C^+(O_g) = \begin{cases} C(O_g) & \text{if } D < 0 \text{ or } D > 0, N_{K/Q}(\varepsilon_g) = -1, \\ C(O_g) \cup \sqrt{D}C(O_g) & \text{if } D > 0, N_{K/Q}(\varepsilon_g) = +1, \end{cases}$$

and set

$$J = J(A,B,C) = \begin{cases} \lambda(\mu(M(A,B,C))) & \text{if } D < 0 \text{ or } D > 0, N_{K/Q}(\varepsilon_g) = -1, \\ \lambda(\mu(M(A,B,C)) \cup \sqrt{D}\mu(M(A,B,C))) & \text{if } D > 0, N_{K/Q}(\varepsilon_g) = +1. \end{cases}$$

Clearly J is of index 3 in $H(D)$. We have $\mathfrak{P} \in M(A,B,C)$ if and only if $p = N_{K/Q}(\mathfrak{P})$ is represented by a form in J. The presence of $\sqrt{D}\mu(M)$ in the definition of J guarantees that p (and not just $\pm p$) is represented by a form in J in the case when $D > 0$, $N_{K/Q}(\varepsilon_g) = +1$. The theorem now follows from Lemmas 12 and 15.

COROLLARY 1. *If $H(D)$ has 3-rank equal to 1 then $x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by the cube of a form of discriminant D.*

Proof. This is clear from the theorem as $H(D)$ contains a unique subgroup of index 3, namely the subgroup of cubes, which must therefore be $J(A,B,C)$.

COROLLARY 2. *Let D be the discriminant of a monic irreducible cubic polynomial $f(x)$ with integral coefficients. Let p be a prime ($p > 3, p \nmid D$) which is represented by the cube of a form in $H(D)$. Then $f(x)$ splits into three linear factors modulo p.*

Proof. The subgroup of cubes of $H(D)$ is contained in every subgroup of index 3 in $H(D)$. The result now follows from the theorem.

The next two corollaries show that in certain circumstances the splitting of $x^3 + Ax^2 + Bx + C$ modulo p can be characterized using forms of discriminant smaller than D in absolute value. Before stating these corollaries we introduce notation for

the Gauss surjective homomorphism between form class groups. If E is an integer $\equiv 0, 1 \pmod 4$ and F is a positive integer we let $\kappa = \kappa(EF^2, E)$ denote the surjective homomorphism

$$\kappa: H(EF^2) \longrightarrow H(E)$$

given by

$$\kappa([a, bF, cF^2]) = [a, b, c],$$

where $[a, b, c]$ denotes the class of the form (a, b, c).

COROLLARY 3. *If E is an integer such that*
(i) $E \equiv 0, 1 \pmod 4$,
(ii) $D = EF^2$ *for some integer* $F > 1$,
(iii) $[H(E): \kappa(J(A, B, C))] = 3$,
then $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ has three solutions if and only if p is represented by a form in $\kappa(J(A, B, C))$.

Proof. Suppose that $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ has three solutions. Then, by the theorem, p is represented by a form in $J(A, B, C)$. Replacing this form by an equivalent one, if necessary, we may suppose that it is of the form (a, bF, cF^2), so that $p = ax^2 + bFxy + cF^2y^2$ for some integers x and y, and thus $p = ax^2 + bx(Fy) + c(Fy)^2$ is represented by the form (a, b, c) in $\kappa(J(A, B, C))$.

Suppose now that p is represented by a form (a, b, c) in $\kappa(J(A, B, C))$. We may suppose that $\kappa([a, bF, cF^2]) = [a, b, c]$. Now, as $\left(\frac{D}{p}\right) = +1$, p is represented by some form class in $H(D)$. Without loss of generality this form class may be taken as $[a_1, b_1F, c_1F^2]$. Using the Gauss map $\kappa: H(D) \to H(E)$ we see that p is represented by $[a_1, b_1, c_1]$ in $H(E)$. It follows that for some choice of sign $[a, \pm b, c] = [a_1, b_1, c_1]$. Hence we have

$$[a_1, b_1F, c_1F^2] = [a, \pm bF, cF^2] \circ [r, s, t],$$

where $[r, s, t] \in \ker \kappa$. Since

$$[H(D): J(A, B, C)] = [H(E): \kappa(J(A, B, C))] = 3,$$

elementary group theory shows that $\ker \kappa \subseteq J(A, B, C)$. Thus p is represented by $[a_1, b_1F, c_1F^2] \in J(A, B, C)$, and so, by the theorem, $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ has three solutions.

COROLLARY 4. *If E is an integer such that*
(i) $E \equiv 0, 1 \pmod 4$,
(ii) $D = EF^2$ *for some integer* $F > 1$,
(iii) 3*-rank of* $H(D) =$ 3*-rank of* $H(E)$,
then $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ has three solutions if and only if p is represented by a form in $\kappa(J(A, B, C))$.

Proof. By elementary group theory the preservation of the 3-rank ensures that all the elements of $\ker \kappa$ are cubes. Since cubes are contained in any subgroup of index 3, in particular they are contained in $J(A, B, C)$. It now follows that $\ker \kappa \subseteq J(A, B, C)$ and a simple argument shows that $[H(E): \kappa(J(A, B, C))] = 3$, and the result follows from Corollary 3.

The following example shows that if E is an integer satisfying conditions (i) and (ii) of Corollary 3, the hypothesis (iii) cannot be weakened to $h(E) \equiv 0 \pmod 3$.

EXAMPLE 1. Let $A = -6$, $B = 3$, $C = -5$. Here $D = -3159$. We take $E = -351$ so that $F = 3$. The group $H(-3159) = U \times V \times W$, where U (respectively V, W) is a cyclic group of order 3 (respectively 3, 4) generated by [16, 13, 52] (respectively [22, 19, 40], [8, 3, 99]) and the subgroup $J(-6, 3, -5) = V \times W$. However, $\kappa(J(-6, 3, -5)) = H(-351)$ and therefore it is impossible to use the representation of p by forms of discriminant -351 to characterize the splitting of $x^3 - 6x^2 + 3x - 5$ modulo p. The prime 367 is represented by the principal form $(1, 1, 88)$ of discriminant -351 but $x^3 - 6x^2 + 3x - 5$ does not split modulo 367. However the prime 3163 is also represented by the principal form and does split the cubic:

$$x^3 - 6x^2 + 3x - 5 \equiv (x - 1419)(x - 2379)(x - 2534) \pmod{3163}.$$

We conclude with three further examples.

EXAMPLE 2. Let $A = 3$, $B = 7$, $C = 13$. Here $D = -1984$ and $H(-1984) = U \times V \times W$, where U (respectively V, W) is a cyclic group of order 2 (respectively 2, 3) generated by $(16, 0, 31)$ (respectively $(16, 16, 35)$, $(20, 4, 25)$). The group $H(-1984)$ contains a unique subgroup of index 3, namely $U \times V$, so that by the theorem $J(3, 7, 13) = U \times V$. Taking $E = -31$, $F = 8$, we see that conditions (i), (ii), and (iii) of Corollary 4 are satisfied since $h(-31) = 3$. Hence $x^3 + 3x^2 + 7x + 13 \equiv 0 \pmod p$ has three solutions if and only if p is represented by $(1, 1, 8)$.

EXAMPLE 3. Let $A = 0$, $B = -9$, $C = 1$. Here we have $D = 2889 = EF^2$ with $E = 321$, $F = 3$, and 3-rank of $H(2889) =$ 3-rank of $H(321) = 1$. Moreover $H(321) \simeq Z_6$ has a unique subgroup of index 3 so that, by Corollary 4, $x^3 - 9x + 1 \equiv 0 \pmod p$ has three solutions if and only if p is represented by either $(1, 1, -80)$ or $(-1, 1, 80)$.

EXAMPLE 4. The polynomials

$$f_1(x) = x^3 - 4x^2 + 8x + 5,$$
$$f_2(x) = x^3 - 3x^2 + 5x + 8,$$
$$f_3(x) = x^3 - 2x^2 + 10x - 1,$$
$$f_4(x) = x^3 - 16x + 27$$

all have discriminant $D = -3299$. Here $H(-3299) = U \times V$, where U is a cyclic group of order 3 generated by $u = (23, 17, 39)$ and V is a cyclic group of order 9 generated by $v = (29, 23, 33)$. The group $H(-3299)$ contains four subgroups of index 3, namely, $\langle v \rangle$, $\langle uv \rangle$, $\langle uv^2 \rangle$, $\langle u, v^3 \rangle$, and it is easy to check that

$$J(-4, 8, 5) = \langle uv \rangle, \qquad J(-3, 5, 8) = \langle u, v^3 \rangle,$$
$$J(-2, 10, -1) = \langle v \rangle, \qquad J(0, -16, 27) = \langle uv^2 \rangle.$$

The intersection of these four subgroups is the subgroup of cubes, namely, $S = \langle v^3 \rangle$.

The theorem gives: all four cubics $f_1(x)$, $f_2(x)$, $f_3(x)$, $f_4(x)$ split modulo p if and only if p is represented by the cube of a form in $H(-3299)$, that is, by $(1, 1, 825)$, $(27, \pm 7, 31)$.

Acknowledgement. The authors would like to thank Mr Serge Elinitsky (Carleton University) and Mr Nicholas Buck (College of New Caledonia) for writing and running some computer programs for them in connection with this research.

References

1. HARVEY COHN, *A classical invitation to algebraic numbers and class fields* (Springer, New York, 1978).
2. DAVID A. COX, 'Primes of the form x^2+ny^2', *Fermat, class field theory and complex multiplication* (Wiley, New York, 1989).
3. JACQUES MARTINET and JEAN-JACQUES PAYAN, 'Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne', *J. Reine Angew. Math.* 228 (1967) 15–37.
4. DANIEL SHANKS, 'A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)', *Proceedings, Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing* (Louisiana State University, Baton Rouge, 1976) 15–40. Congressus Numerantium XVII, Utilitas Math. Winnipeg, Man., 1976.
5. L. STICKELBERGER, 'Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper', *Verhandlungen des ersten internationalen Mathematiker Kongresses in Zürich* 1897 (Leipzig, 1898) 182–193.

Department of Mathematics
Okanagan College
Kelowna
British Columbia
Canada V1Y 4X8

Department of Mathematics and Statistics
Carleton University
Ottawa
Ontario
Canada K1S 5B6