Tokyo J. Math.
Vol. 17, No. 2, 1994

The Primes for Which an Abelian Cubic Polynomial Splits

James G. HUARD, Blair K. SPEARMAN
and Kenneth S. WILLIAMS*

Canisius College, Okanagan University College and Carleton University

(Communicated by T. Nagano)

Abstract. Let X^3+AX+B be an irreducible abelian cubic polynomial in $Z[X]$. We determine explicitly integers $a_1, \cdots, a_t, F$ such that, except for finitely many primes p,

$$x^3+Ax+B\equiv 0 \pmod p \text{ has three solutions } \Leftrightarrow p\equiv a_1, \cdots, a_t \pmod F) .$$

Let X^3+AX+B be an irreducible abelian cubic polynomial in $Z[X]$. We are interested in determining those primes p for which the congruence

$$x^3+Ax+B\equiv 0 \pmod p$$

has exactly three solutions, that is, those primes p for which X^3+AX+B splits completely into distinct linear factors modulo p. As X^3+AX+B is abelian, it is known from class field theory (see for example [6]) that, apart from a finite number of exceptions, the primes p which split X^3+AX+B modulo p lie in certain congruence classes modulo the conductor of X^3+AX+B. In this note we determine these congruence classes explicitly as well as the exceptional primes.

Let $N_p(A, B)$ denote the number of solutions $x \pmod p$ of the congruence $x^3+Ax+B\equiv 0 \pmod p$ and let $K=K(A, B)$ denote the largest positive integer such that $K^2|A$ and $K^3|B$. Since

$$N_p(A, B)=\begin{cases} N_p(A/K^2, B/K^3), & \text{if } p\nmid K, \\ 1, & \text{if } p|K, \end{cases}$$

it suffices to determine the primes p for which $N_p(A, B)=3$ under the simplifying assumption

$$K(A, B)=1 . \tag{1}$$

The irreducible polynomial X^3+AX+B is abelian if and only if its discriminant is a perfect square, that is, if and only if

Received May 19, 1993

* Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

(2) $$-4A^3-27B^2=C^2$$

for some positive integer C (see [4: Example 2, p. 308]). We see from (2) that $A<0$, $B\equiv C \pmod 2$ and $A\equiv 0$ or $2 \pmod 3$. Clearly $B\neq 0$ as X^3+AX+B is irreducible. From (1) and (2) it is easy to show that exactly one of the following occurs:

(3)(i) $$3\nmid A,$$

(3)(ii) $$3\parallel A,\ 3\nmid B,$$

(3)(iii) $$3^2\parallel A,\ 3^2\parallel B.$$

If (3) (i) holds then $3\nmid C$. If (3) (ii) holds then $3^2|C$ and, if $3^2\parallel C$, 3 divides exactly one of $B\pm(C/9)$. If (3) (iii) holds then $3^3\parallel C$ and 3 divides exactly one of $(B/9)\pm(C/27)$. It is convenient to define the integer $b=b(A, B)=0, 1, 2$ by

(4) $$\begin{cases} b=0, & \text{if } 3\nmid A \quad \text{or} \quad 3\parallel A,\ 3\nmid B,\ 3^3|C, \\ b=1, & \text{if } 3\parallel A,\ 3\nmid B,\ 3^2\parallel C,\ 3|B-(C/9) \quad \text{or} \quad 3^2\parallel A,\ 3^2\parallel B,\ 3|(B/9)+(C/27), \\ b=2, & \text{if } 3\parallel A,\ 3\nmid B,\ 3^2\parallel C,\ 3|B+(C/9) \quad \text{or} \quad 3^2\parallel A,\ 3^2\parallel B,\ 3|(B/9)-(C/27). \end{cases}$$

We note that

(5) $$b\neq 0 \iff 3\parallel A,\ 3\nmid B,\ 3^2\parallel C \quad \text{or} \quad 3^2\parallel A,\ 3^2\parallel B.$$

In order to state our main result we need the notion of a cubic residue symbol. An Eisenstein integer θ is a complex number of the form $\theta=x+y\omega$, where x and y are rational integers and $\omega=(-1+\sqrt{-3})/2$ is a complex cube root of unity. Equivalently θ is of the form $(a_1+a_2\sqrt{-3})/2$, where a_1 and a_2 are rational integers with $a_1\equiv a_2$ (mod 2). The complex conjugate of θ is denoted by $\bar{\theta}$. The norm $N(\theta)$ of θ is the rational integer $\theta\bar{\theta}$. The Eisenstein integer θ is called a unit if $N(\theta)=1$. The only units are ± 1, $\pm\omega$, $\pm\omega^2$. An Eisenstein integer θ is said to be primary if $\theta\equiv -1 \pmod 3$. For each Eisenstein integer θ not divisible by $\sqrt{-3}$ there is a unique unit $\eta=\eta(\theta)$ such that $\eta\theta$ is primary. The Eisenstein primes (up to multiplication by a unit) are $\sqrt{-3}$, rational primes of the form $3n+2$, and Eisenstein integers with norm equal to a rational prime of the form $3n+1$. Each nonzero Eisenstein integer can be written uniquely as a product of a unit, a nonnegative integral power of the Eisenstein prime $\sqrt{-3}$, and nonnegative integral powers of primary Eisenstein primes. If π is an Eisenstein prime with $N(\pi)\neq 3$, and θ is an Eisenstein integer not divisible by π, then the cubic residue symbol $[\theta/\pi]_3$ is defined to be the unique cuberoot of unity such that

$$\theta^{(N(\pi)-1)/3}\equiv[\theta/\pi]_3 \pmod{\pi}.$$

The basic properties of the cubic residue symbol, extended multiplicatively to denominators not divisible by $\sqrt{-3}$, are given in [3].

Before stating and proving our main result, we introduce some notation. If a is a rational integer, the integers a' and a'' are given uniquely by

$$a=3a'+a'', \qquad a''=-1,0,1.$$

As usual ϕ denotes Euler's phi function.

We prove the following theorem.

THEOREM. *Let $X^3+AX+B\in Z[X]$ be an irreducible abelian cubic polynomial in $Z[X]$ satisfying* (1). *Let C be the positive integer given by* (2). *Let λ denote the Eisenstein integer*

$$\lambda=\tfrac{1}{2}(3B+C)+3B\omega=\tfrac{1}{2}(C+3B\sqrt{-3}) \tag{6}$$

of norm $N(\lambda)=-A^3$.

(i) *We have*

$$(\sqrt{-3})^c\|\lambda, \qquad \text{where} \quad 3^c\|A^3. \tag{7}$$

Let τ be the (possibly empty) product of primary Eisenstein primes such that $\lambda/((\sqrt{-3})^c\tau^3)$ is cubefree. Then there is a unique product ρ of primary Eisenstein primes such that

$$N(\rho)=\prod_{\substack{q(\text{prime})\equiv 1(\text{mod}\,3)\\ q\mid A,\, q\mid B}} q \quad \text{and} \quad \rho N(\rho)\mid \lambda/((\sqrt{-3})^c\tau^3). \tag{8}$$

(ii) *With b as defined in* (4), *we set*

$$F=3^{\alpha}N(\rho), \tag{9}$$

where

$$\alpha=\begin{cases} 0, & \text{if} \quad b=0, \\ 2, & \text{if} \quad b\neq 0. \end{cases} \tag{10}$$

Then $F\neq 1$ and there are $\phi(F)/3$ integers a satisfying

$$1\leq a<F, \quad \mathrm{GCD}(a,F)=1, \quad [a/\rho]_3=\omega^{ba'a''}. \tag{11}$$

(iii) *Let $a_1,\cdots,a_{\phi(F)/3}$ be the $\phi(F)/3$ integers satisfying* (11). *Then, except for finitely many primes p, we have*

$$x^3+Ax+B\equiv 0 \ (\text{mod}\, p) \text{ has } 3 \text{ solutions} \iff p\equiv a_1,\cdots,a_{\phi(F)/3} \ (\text{mod}\, F). \tag{12}$$

The exceptional primes are those primes p ($\neq 3$) such that $p\mid C$, $p\nmid F$ together with the prime 3 if $3^4\mid C$.

We note that as an exceptional prime p divides C, it divides the discriminant of the polynomial X^3+AX+B and so $N_p(A,B)\neq 3$.

Before proving this theorem we give two illustrative examples.

EXAMPLE 1. We consider the irreducible abelian cubic $X^3-21X-17$. Here $A=-21=-3\cdot 7$, $B=-17$ and by (2) $C=171=3^2\cdot 19$. From (4), (8), (10), (9) we see respectively that $b=1$, $\rho=1$, $\alpha=2$, $F=9$. By (11) the $\phi(F)/3=2$ integers a_1, a_2 are the solutions a of

$$1\le a<9\,,\quad \mathrm{GCD}(a,9)=1\,,\quad \omega^{a'a''}=1\,.$$

The following table

a	1	2	4	5	7	8
a'	0	1	1	2	2	3
a''	1	-1	1	-1	1	-1
$\omega^{a'a''}$	1	ω^2	ω	ω	ω^2	1

shows that $a_1=1$, $a_2=8$. By Theorem (iii) the only exceptional prime is $p=19$, so that for a prime $p\ne 19$ we have

$$x^3-21x-17\equiv 0 \pmod p \text{ has 3 solutions} \quad\Leftrightarrow\quad p\equiv 1, 8 \pmod 9)\,.$$

EXAMPLE 2. We consider the irreducible abelian cubic $X^3-21X+35$. Here $A=-21=-3\cdot 7$, $B=35=5\cdot 7$ and by (2) $C=63=3^2\cdot 7$. Thus from (6) we have $\lambda=\frac{1}{2}(63+105\sqrt{-3})$. By (7) we see that $(\sqrt{-3})^3\|\lambda$. Further, as

$$\frac{\lambda}{(\sqrt{-3})^3}=\frac{-35+7\sqrt{-3}}{2}=\omega^2\left(\frac{1+3\sqrt{-3}}{3}\right)\left(\frac{1-3\sqrt{-3}}{2}\right)^2,$$

we see by (8) that $\tau=1$ and $\rho=\frac{1}{2}(1-3\sqrt{-3})$. From (4), (10), (9) we deduce respectively $b=2$, $\alpha=2$, $F=3^2\cdot 7=63$. By (11) the $\phi(F)/3=12$ integers $a_1,\cdots,a_{12}$ are the solutions a of

$$1\le a<63\,,\quad \mathrm{GCD}(a,63)=1\,,\quad \left[\frac{a}{\frac{1}{2}(1-3\sqrt{-3})}\right]_3=\omega^{2a'a''}\,.$$

Clearly we have

$$\omega^{2a'a''}=\begin{cases}1\,, & \text{if } a\equiv \pm 1 \pmod 9\,,\\ \omega\,, & \text{if } a\equiv \pm 2 \pmod 9\,,\\ \omega^2\,, & \text{if } a\equiv \pm 4 \pmod 9\,,\end{cases}$$

and, as $N(\rho)=7$ and $\omega\equiv 2 \pmod \rho$, we have

$$\left[\frac{a}{\rho}\right]_3=\begin{cases}1\,, & \text{if } a\equiv \pm 1 \pmod 7\,,\\ \omega\,, & \text{if } a\equiv \pm 3 \pmod 7\,,\\ \omega^2\,, & \text{if } a\equiv \pm 2 \pmod 7\,.\end{cases}$$

Thus the required a's must satisfy

$$\left\{\begin{array}{l} a\equiv \pm 1 \pmod 9 \\ a\equiv \pm 1 \pmod 7 \end{array}\right\} \quad \text{or} \quad \left\{\begin{array}{l} a\equiv \pm 2 \pmod 9 \\ a\equiv \pm 3 \pmod 7 \end{array}\right\} \quad \text{or} \quad \left\{\begin{array}{l} a\equiv \pm 4 \pmod 9 \\ a\equiv \pm 2 \pmod 7 \end{array}\right\}.$$

Hence $a_1=1$, $a_2=5$, $a_3=8$, $a_4=11$, $a_5=23$, $a_6=25$, $a_7=38$, $a_8=40$, $a_9=52$, $a_{10}=55$, $a_{11}=58$, $a_{12}=62$. By Theorem (iii) there are no exceptional primes. Thus for all primes p we have

$$\begin{aligned} &x^3-21x+35\equiv 0 \pmod p \text{ has 3 solutions} \\ &\quad \Leftrightarrow \quad p\equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}\,. \end{aligned}$$

Proof of Theorem. We begin by noting the following easily proved consequences of (1), (2) and (6).

(13) If p is a prime $\neq 3$ then $p^2 \nmid \lambda$.

(14) If p is a prime such that $p|\lambda$ then $p\not\equiv 2 \pmod 3$.

(15) If p is a prime such that $p|A$ then $p\not\equiv 2 \pmod 3$.

(16) If p is a prime $\neq 3$ then

$$p|A,\ p|B \quad \Leftrightarrow \quad p|\lambda\,.$$

(17) If p is a prime $\neq 3$ then

$$p|A,\ p\nmid B \quad \Leftrightarrow \quad \text{there exists an Eisenstein prime } \pi \text{ dividing } p \text{ such that } \pi\nmid\lambda,\ \bar{\pi}|\lambda\,.$$

We also note that λ is not the cube of an Eisenstein integer, otherwise,

$$\tfrac{1}{2}(C+3B\sqrt{-3})=(\tfrac{1}{2}(g+h\sqrt{-3}))^3\,,$$

for some integers g and h, so that

$$A=(-g^2-3h^2)/4\,, \quad B=(g^2h-h^3)/4\,, \quad C=(g^3-9gh^2)/4\,,$$

and thus

$$X^3+AX+B=(X-h)(X^2+hX+(h^2-g^2)/4)\,,$$

contradicting that X^3+AX+B is irreducible in $Z[X]$.

Proof of (i). Suppose $(\sqrt{-3})^x\|\lambda$. Then $(\sqrt{-3})^x\|\bar{\lambda}$ and so $(\sqrt{-3})^{2x}\|\lambda\bar{\lambda}$, that is $3^x\|N(\lambda)=-A^3$, showing that $x=c$, as required.

We now prove (8). We let μ denote the product of primary Eisenstein primes such that $\lambda/((\sqrt{-3})^c\mu)$ is a unit, say,

(18) $$\frac{\lambda/(\sqrt{-3})^c}{\mu}=(-1)^a\omega^e\,, \qquad a=0, 1\,, \quad e=0, 1, 2\,.$$

We first prove that $e=b$. We consider the Eisenstein integer $\lambda_1=\frac{1}{2}(x+y\sqrt{-3})$ given by

$$\lambda_1=\lambda/(\sqrt{-3})^c=\begin{cases}\frac{1}{2}(C+3B\sqrt{-3}), & \text{if } 3\nmid A,\\ \dfrac{1}{2}\left(-B+\dfrac{C}{9}\sqrt{-3}\right), & \text{if } 3\| A,\\ \dfrac{1}{2}\left(-\dfrac{C}{27}-\dfrac{B}{9}\sqrt{-3}\right), & \text{if } 3^2\| A.\end{cases} \tag{19}$$

From (18) we have

$$\lambda=(-1)^a\omega^e(\sqrt{-3})^c\mu, \tag{20}$$

and as μ is a product of primary Eisenstein integers we have

$$\mu\equiv\pm 1 \pmod 3, \tag{21}$$

and

$$\lambda_1=(-1)^a\omega^e\mu\equiv\pm\omega^e \pmod 3. \tag{22}$$

Then, as $3\nmid x$, we have

$$\begin{cases} e=0 & \Leftrightarrow \quad 3\mid y\\ e=1 & \Leftrightarrow \quad 3\mid x+y,\ 3\nmid y\\ e=2 & \Leftrightarrow \quad 3\mid x-y,\ 3\nmid y,\end{cases} \tag{23}$$

and appealing to (4) and (19) we obtain $e=b$ as asserted. By the definition of τ we have $\tau^3|\mu$ and μ/τ^3 is cubefree. We let F_1 denote the largest positive integer dividing μ/τ^3, and set

$$\rho=\mu/(\tau^3F_1). \tag{24}$$

Clearly ρ is a product of primary Eisenstein primes, and

$$\lambda=(-1)^a\omega^b(\sqrt{-3})^c\mu, \qquad \mu=F_1\rho\tau^3. \tag{25}$$

We show that ρ is the unique Eisenstein integer satisfying (8). This will be done in four steps:

(a) $$N(\rho)=F_1,$$

(b) $$F_1=\prod_{\substack{q(\text{prime})\equiv 1 \pmod 3\\ q|A,\, q|B}} q,$$

(c) $$\rho N(\rho)\mid \lambda/((\sqrt{-3})^c\tau^3),$$

(d) ρ is the unique product of primary Eisenstein primes having property (8).

Proof of (a). From (25) we have $N(\mu)=F_1^2N(\rho)N(\tau)^3$. As $N(\mu)$ is a cube, $F_1^2N(\rho)$ is also a cube. Clearly F_1 is cubefree, so that to prove $N(\rho)=F_1$ it suffices to prove that $N(\rho)$ is cubefree. Suppose not. Then there exists a prime p such that

$$p^3 \mid N(\rho) \mid N(\mu) = -A^3/3^c,$$

so that $p|A$ and $p\neq 3$. Hence, by (15), we have $p\equiv 1 \pmod 3$, say $p=\pi\bar{\pi}$, where π and $\bar{\pi}$ are conjugate Eisenstein primes. Then $\pi^3\bar{\pi}^3|\rho\bar{\rho}$, and as ρ is not divisible by a rational integer, we have $\pi^3|\rho$ or $\bar{\pi}^3|\rho$, contradicting that ρ is cubefree. Thus we have $F_1=N(\rho)$, which is (a), and by (25)

$$\mu=\rho N(\rho)\tau^3. \tag{26}$$

Proof of (b). We begin by showing that $F_1=N(\rho)$ is squarefree. Suppose not. Then, by an argument similar to that in the proof of (a), there is an Eisenstein prime π such that $\pi^2|\rho$. Hence $\pi^4|\rho N(\rho)$, contradicting that $F_1\rho$ is cubefree. Next we show that for any prime p, we have

$$p|A,\ p|B,\ p\equiv 1 \pmod 3 \quad\Leftrightarrow\quad p|N(\rho),$$

completing the proof of (b) as F_1 is squarefree.

We have appealing to (13), (16), (20) and (26)

$$\begin{aligned}
&p|A,\ p|B,\ p\equiv 1 \pmod 3\\
&\quad\Rightarrow p|\lambda,\ p^3\nmid\lambda\\
&\quad\Rightarrow \exists \text{ some Eisenstein prime } \pi \text{ dividing } p \text{ with } \pi|\lambda,\ \pi^3\nmid\lambda\\
&\quad\Rightarrow \pi|\rho N(\rho)\\
&\quad\Rightarrow p|N(\rho)^3\\
&\quad\Rightarrow p|N(\rho),
\end{aligned}$$

and appealing to (14), (16), (20), (26)

$$p|N(\rho)\Rightarrow p|\mu\,,\, p\neq 3\Rightarrow p|\lambda\Rightarrow p\equiv 1 \pmod 3),\, p|A,\, p|B\,.$$

This completes the proof of (b). From (9) and (b) we see that

$$F=3^\alpha F_1\,. \tag{27}$$

Proof of (c). From (18) we have $\mu|\lambda/(\sqrt{-3})^c$. But by (26) $\mu=\rho N(\rho)\tau^3$ so that $\rho N(\rho)\mid\lambda/((\sqrt{-3})^c\tau^3)$, which is (c).

Proof of (d). Suppose that ρ_1 is a product of primary Eisenstein primes such that

$$\rho_1 N(\rho_1)\mid\lambda/((\sqrt{-3})^c\tau^3)\,,\qquad N(\rho_1)=F_1\,.$$

As

$$\lambda=(-1)^a\omega^b(\sqrt{-3})^c\rho N(\rho)\tau^3\,,$$

we have

$$\rho_1 N(\rho_1)|\rho N(\rho)\,,\qquad N(\rho_1)=N(\rho)\,,$$

so that $\rho_1|\rho$, say, $\rho=\kappa\rho_1$. As $N(\rho)=N(\rho_1)$, κ is a unit, and so as both ρ and ρ_1 are products of primary Eisenstein primes we have $\rho=\rho_1$. This completes the proof of (d).

Proof of (ii). We first prove that $F\neq 1$. Suppose on the contrary that $F=1$. Then, by (9), we see that $\alpha=0$ and $N(\rho)=1$. As $\alpha=0$, by (10), we have $b=0$ and so by (4)

$$\begin{array}{ll}\text{either} & \text{(I) } 3\nmid A\,,\\ \text{or} & \text{(II) } 3\| A,\ 3\nmid B,\ 3^3|C\,.\end{array}$$

As $N(\rho)=1$, by (8), we see that

either (III) there are no primes $q\equiv 1 \pmod 3$ dividing A,

or (IV) there are primes $q\equiv 1 \pmod 3$ dividing A none of which divide B.

Recall that $A<0$ and that by (15) A has no prime divisors $\equiv 2 \pmod 3$. Also recall that $C>0$.

If (I) and (III) hold then $A=-1$. By (2) we see that $B=0$, $C=2$, which contradicts $B\neq 0$.

If (II) and (III) hold then $A=-3$. By (2) we see that $B=\pm 1$, $C=9$, which contradicts $3^3|C$.

If (I) and (IV) hold then $A=-q_1\cdots q_s$, where the q_i are $s\ (\geq 1)$ primes $\equiv 1 \pmod 3$ which do not divide B. We have $q_i=\pi_i\bar{\pi}_i$, where π_i and $\bar{\pi}_i$ are distinct conjugate primary Eisenstein primes. Now

$$\pi_i^3\bar{\pi}_i^3 \mid q_i^3 \mid A^3 \mid \tfrac{1}{2}(C+3B\sqrt{-3})\times\tfrac{1}{2}(C-3B\sqrt{-3})$$

and

$$\pi_i,\ \bar{\pi}_i\nmid \mathrm{GCD}(\tfrac{1}{2}(C+3B\sqrt{-3})\,,\ \tfrac{1}{2}(C-3B\sqrt{-3}))\,,$$

so we can choose π_i without loss of generality such that $\pi_i^3|\frac{1}{2}(C+3B\sqrt{-3})$. Hence

$$\tfrac{1}{2}(C+3B\sqrt{-3})=\varepsilon\pi_1^3\cdots\pi_s^3\,,\qquad \tfrac{1}{2}(C-3B\sqrt{-3})=\bar{\varepsilon}\bar{\pi}_1^3\cdots\bar{\pi}_s^3\,,$$

where ε is a unit. As the π_i are primary and $\frac{1}{2}(C+3B\sqrt{-3})\equiv\pm 1 \pmod 3$ we have $\varepsilon\equiv\pm 1 \pmod 3$ so that $\varepsilon=\pm 1$. Set $\Omega=\pi_1\cdots\pi_s$. Then

$$A=-\Omega\bar{\Omega}\,,\qquad B=\varepsilon(\Omega^3-\bar{\Omega}^3)/3\sqrt{-3}\,,$$

and thus

$$X^3+AX+B=X^3-\Omega\bar{\Omega}X+\frac{\varepsilon}{3\sqrt{-3}}(\Omega^3-\bar{\Omega}^3)$$

$$=\left(X-\varepsilon\frac{(\Omega-\bar{\Omega})}{\sqrt{-3}}\right)\left(X^2+\varepsilon\frac{(\Omega-\bar{\Omega})}{\sqrt{-3}}X-\frac{1}{3}(\Omega^2+\Omega\bar{\Omega}+\bar{\Omega}^2)\right),$$

which contradicts that X^3+AX+B is irreducible.

If (II) and (IV) hold then $A=-3q_1\cdots q_s$, where the q_i are s (≥ 1) primes $\equiv 1 \pmod 3$ which do not divide B. Arguing as in the previous case, we see that

$$A=-3\Omega\bar{\Omega}\,,\quad \tfrac{1}{2}(C+3B\sqrt{-3})=\varepsilon(\sqrt{-3})^3\Omega^3\,,\quad \tfrac{1}{2}(C-3B\sqrt{-3}=-\varepsilon(\sqrt{-3})^3\bar{\Omega}^3\,,$$

where $\varepsilon=\pm 1$ and $\Omega=\pi_1\cdots\pi_s$. Hence $B=-\varepsilon(\Omega^3+\bar{\Omega}^3)$ and so

$$\begin{aligned}X^3+AX+B&=X^3-3\Omega\bar{\Omega}X-\varepsilon(\Omega^3+\bar{\Omega}^3)\\&=(X-\varepsilon(\Omega+\bar{\Omega}))(X^2+\varepsilon(\Omega+\bar{\Omega})X+(\Omega^2-\Omega\bar{\Omega}+\bar{\Omega}^2))\,,\end{aligned}$$

which contradicts that X^3+AX+B is irreducible.

This completes the proof that $F\neq 1$. Then, from (8), (9) and (10), we see that $\phi(F)\equiv 0 \pmod 3$.

Next we suppose that there are t integers satisfying (11), say $a_1,\cdots,a_t$, and show that $t=\phi(F)/3$. Let G denote the multiplicative group of reduced residue classes modulo F and H the multiplicative group of cube roots of unity. We consider the homomorphism $\theta: G\to H$ given by

$$\theta(\tilde{k})=[k/\rho]_3\omega^{-bk'k''}\,,$$

where $\tilde{k}$ denotes the residue class modulo F of the integer k coprime with F. If $b=0$, θ is onto since $\rho\neq 1$ is cubefree. If $b\neq 0$, θ is onto since for $v=3F_1\pm 1$, $\theta(\tilde{v})=\omega^{\pm bF_1}\neq 1$. Hence $t=\operatorname{card}\{\tilde{a}_1,\cdots,\tilde{a}_t\}=|\ker\theta|=|G|/|H|=\phi(F)/3$ as asserted.

This completes the proof of (ii).

Proof of (iii). Let p denote a prime such that $p\nmid 3C$, and let π be an Eisenstein prime such that $\pi|p$, $\pi\nmid\lambda$. By class field theory, or appealing to [2], we know that $N_p(A,B)=3\Leftrightarrow[\lambda/\pi]_3=1$. From (25) we see that

$$\left[\frac{\lambda}{\pi}\right]_3=\left[\frac{\omega}{\pi}\right]_3^b\left[\frac{\mu}{\pi}\right]_3=\omega^{b(N(\pi)-1)/3}\left[\frac{\mu}{\pi}\right]_3=\omega^{bp'}\left[\frac{\mu}{\pi}\right]_3.$$

As $\mu=\rho N(\rho)\tau^3$ we have (appealing to the law of cubic reciprocity)

$$\begin{aligned}\left[\frac{\mu}{\pi}\right]_3&=\left[\frac{\rho^2\bar{\rho}\tau^3}{\pi}\right]_3=\left[\frac{\rho^2\bar{\rho}}{\pi}\right]_3=\left[\frac{\rho}{\pi}\right]_3^2\left[\frac{\bar{\rho}}{\pi}\right]_3=\left[\frac{\bar{\rho}}{\bar{\pi}}\right]_3\left[\frac{\bar{\rho}}{\pi}\right]_3\\&=\left[\frac{\bar{\rho}}{N(\pi)}\right]_3=\left[\frac{N(\pi)}{\bar{\rho}}\right]_3=\left[\frac{p}{\bar{\rho}}\right]_3^h=\left[\frac{p}{\rho}\right]_3^{-h},\end{aligned}$$

where $N(\pi)=p^h$. As $p''=h=1$ for $p\equiv 1 \pmod 3$ and $p''=-1$, $h=2$ for $p\equiv 2 \pmod 3$, we have

$$\left[\frac{\lambda}{\pi}\right]_3=1 \Leftrightarrow \omega^{bp'}\left[\frac{p}{\rho}\right]_3^{-h}=1 \Leftrightarrow \left[\frac{p}{\rho}\right]_3^{h}=\omega^{bp'}$$
$$\Leftrightarrow \left[\frac{p}{\rho}\right]_3^{p''}=\omega^{bp'} \Leftrightarrow \left[\frac{p}{\rho}\right]_3=\omega^{bp'p''} .$$

Since ρ is not divisible by a rational prime, $N(\rho)$ is squarefree, and $3\nmid N(\rho)$, an easy calculation shows that the value of the quantity $[k/\rho]_3\omega^{-bk'k''}$, where k is a fixed integer coprime with

$$\left\{\begin{array}{ll} N(\rho), & \text{if } 3\mid b \\ 9N(\rho), & \text{if } 3\nmid b \end{array}\right\}=3^{\alpha}N(\rho)=3^{\alpha}F_1=F,$$

is determined by the residue class of k modulo F. Hence $[\lambda/\pi]_3=1$ if and only if $p\equiv a_i$ (mod F) for some i, $1\le i\le\phi(F)/3$. Thus for a prime p not dividing $3C$, we have $N_p(A, B)=3$ if and only if $p\equiv a_i$ (mod F) for some i, $1\le i\le\phi(F)/3$.

It remains to determine the set of exceptional primes, that is the set $E(A, B)$ given by

$$E(A, B)=\{p\,(\text{prime}) \mid N_p(A, B)\neq 3,\ p\equiv a_i \ (\text{mod } F) \text{ for some } i, \text{ or}$$
$$N_p(A, B)=3,\ p\not\equiv a_i \ (\text{mod } F) \text{ for any } i\} .$$

It suffices to consider the primes p dividing $3C$. First we consider the prime 3. We observe that X^3+AX+B splits modulo 3 if and only if $A\equiv -1$ (mod 3), $B\equiv 0$ (mod 3), that is, if and only if $3\nmid A$, $3\mid B$.

If $b=0$ we see from (4) that $N_3(A, B)=3$ if and only if $3\mid B$. Next, by (11), (25), (19), and the result

$$\left[\frac{3}{\beta}\right]_3=\omega^{\mp 2y/3}, \qquad \text{if} \quad \beta=\frac{1}{2}(x+y\sqrt{-3})\equiv \pm 1 \ (\text{mod } 3),$$

we have

$$3\equiv a_i \ (\text{mod } F) \text{ for some } i \Leftrightarrow \left[\frac{3}{\rho}\right]_3=1 \Leftrightarrow \left[\frac{3}{\mu}\right]_3=1 \Leftrightarrow \left[\frac{3}{\lambda_1}\right]_3=1$$
$$\Leftrightarrow \left\{\begin{array}{ll} 3\mid B, & \text{if } 3\nmid A, \\ 81\mid C, & \text{if } 3\,\|\,A . \end{array}\right.$$

If $3\nmid A$ we have $3\notin E(A, B)$. From (4) we see that if $3\,\|\,A$, then $3\nmid B$, so $3\in E(A, B)\Leftrightarrow 81\mid C$.

If $b\neq 0$, then, by (4), we see that $N_3(A, B)\neq 3$. Moreover, by (4), (10) and (9), we have $9\mid F$, so that $3\not\equiv a_i$ (mod F) for any i. Hence, in this case, we have $81\nmid C$ and $3\notin E(A, B)$.

Combining cases we see that

$$3 \in E(A, B) \Leftrightarrow 81 | C .$$

Next we consider primes p $(\neq 3)$ dividing C. If $p|A$ (so that $p \equiv 1 \pmod 3$) then $p|B$ and so $p|F$ showing that $p \not\equiv a_i \pmod F$ for any i. Clearly $N_p(A, B) \neq 3$ in this case, so that $p \notin E(A, B)$.

If $p \nmid A$ then $p \nmid F$. As $p|C$ we have $p|\operatorname{disc}(X^3+AX+B)$ and so $N_p(A, B) \neq 3$. However, we show that $[p/\rho]_3 = \omega^{bp'p''}$ so that $p \equiv a_i \pmod F$ for some i and thus $p \in E(A, B)$. Since $p \nmid A$, we have $\mathrm{GCD}(p, \lambda)=1$ as $N(\lambda)=-A^3$, and

$$\left[\frac{p}{\rho}\right]_3 = \left[\frac{\rho}{p}\right]_3 = \left[\frac{F_1\rho\tau^3}{p}\right]_3 = \left[\frac{\mu}{p}\right]_3 = \left[\frac{\omega^{-b}\lambda}{p}\right]_3 = \left[\frac{\omega}{p}\right]_3^{-b}\left[\frac{\lambda}{p}\right]_3$$

$$= \omega^{bp'p''}\left[\frac{\frac{1}{2}(3B+C)+3B\omega}{p}\right]_3 = \omega^{bp'p''}\left[\frac{\frac{1}{2}(3B+C)}{p}\right]_3 = \omega^{bp'p''}$$

as asserted. This completes the proof of the theorem. □

Let L denote the cubic field $Q(\theta)$, where θ is any root of the cubic equation $x^3+Ax+B=0$. By a result of Llorente and Nart [5: Theorem 2] the discriminant $d(L)$ of L is given by

$$d(L) = 3^{2\alpha} \prod_{\substack{q(\text{prime}) \equiv 1 \pmod 3 \\ q|A,\, q|B}} q^2 .$$

Further, by the conductor-discriminant formula for a cyclic cubic field [1: Corollary 17.29], we have $d(L)=f(L)^2$, where $f(L)$ is the conductor of L, that is, the conductor of X^3+AX+B. This shows that F (as in (9)) is the conductor of X^3+AX+B.

We conclude by remarking that if F is a prime, the set $\{a_1, \cdots, a_{\phi(F)/3}\}$ consists precisely of the nonzero cubes modulo F. This is clear, for if F is a prime, we have $\alpha=b=0$ and as ρ is an Eisenstein prime of norm F_1, $[a_i/\rho]_3=1$ if and only if a_i is a nonzero cube modulo F.

For example consider the irreducible abelian cubic $X^3-31X+62$. We have $A=-31$, $B=62$, $C=124$, $b=0$, $\alpha=0$, $F=31$, $E(A, B)=\{2\}$, so that for $p \neq 2$

$$\begin{aligned} x^3-31x+62 \equiv 0 \pmod p \text{ has 3 solutions} \\ \Leftrightarrow p \equiv \text{nonzero cube} \pmod{31} \\ \Leftrightarrow p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31} . \end{aligned}$$

References

[1] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer (1978).

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

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer (1982).

[4] S. LANG, *Algebra* (2nd ed.), Addison-Wesley (1984).

[5] P. LLORENTE and E. NART, Effective determination of the decomposition of the rational primes in a cubic field, Proc. Amer. Math. Soc. **87** (1983), 579–585.

[6] B. F. WYMAN, What is a reciprocity law?, Amer. Math. Monthly **79** (1972), 571–586.

Present Addresses:
JAMES G. HUARD
DEPARTMENT OF MATHEMATICS, CANISIUS COLLEGE,
BUFFALO, NY 14208, USA.

BLAIR K. SPEARMAN
DEPARTMENT OF MATHEMATICS, OKANAGAN UNIVERSITY COLLEGE,
KELOWNA, B.C. V1Y 4X8, CANADA.

KENNETH S. WILLIAMS
DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY,
OTTAWA, ONTARIO K1S 5B6, CANADA.