ON THE SET OF PRIMES $p$ WHICH SPLIT $X^3 + B$ MODULO $p$

JAMES G. HUARD$^1$, BLAIR K. SPEARMAN$^2$ AND KENNETH S. WILLIAMS$^3$

$^1$Department of Mathematics, Canisius College, Buffalo, New York 14208, USA
$^2$Department of Mathematics and Statistics, Okanagan University College, Kelowna, B.C., Canada, V1V 4X8
$^3$Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6

(Received 5 August 1994; after revision 24 November 1994; accepted 30 November 1994)

Let $B$ denote an integer which is not a perfect cube. It is shown, using a theorem of Iwaniec on primes represented by quadratic polynomials in two variables, that the set of primes $p$ which split the cubic $X^3 + B$ modulo $p$ cannot be characterized in terms of congruence conditions.

Let $f(x)$ be a monic polynomial with integer coefficients that is irreducible over the integers. The set of all primes $p$ such that $f(X)$ splits completely into distinct linear factors modulo $p$ is denoted by $\text{Spl}(f(X))$. If there exists a positive integer $m$ and positive integers $a_1, \ldots, a_s$ (depending only on $f(X)$) lying in distinct residue classes $\pmod{m}$ coprime with $m$, such that, except for finitely many primes, we have

$$p \in \text{Spl}(f(X)) \iff p = a_1, \ldots, a_s \pmod{m},$$

then we say that $\text{Spl}(f(X))$ is determined by congruence conditions. An abelian polynomial is a polynomial whose Galois group is abelian, that is, whose splitting field is an abelian extension of the rational number field $\mathbb{Q}$. From class field theory (see for example Wyman$^{11}$), it is known that the polynomials $f(X)$ for which $\text{Spl}(f(X))$ can be described by congruence conditions are precisely the abelian polynomials. The simplest non-abelian polynomial is $X^3 + B$, where the integer $B$ is not a perfect cube. We show without appeal to class field theory that $\text{Spl}(X^3 + B)$ cannot be described by congruence conditions. The principal tool in the proof is a deep analytic theorem of Iwaniec$^5$ on primes represented by quadratic polynomials in two integral variables. In addition we use Weber's theorem$^{10}$, as well as some results on cubic reciprocity.

*Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.
We begin with a classical theorem which has its origins in the work of Gauss, Jacobi and Eisenstein on cubic reciprocity.

Proposition 1 — Let \( p \) be a prime such that \( p \equiv 1 \pmod{3} \). Let \( L \) and \( M \) be the integers unique up to sign such that \( 4p = L^2 + 27M^2 \). Then

(i) 2 is a cube modulo \( p \) if and only if 2 divides \( M \);
(ii) 3 is a cube modulo \( p \) if and only if 3 divides \( M \);
(iii) if \( q > 3 \) is a prime divisor of \( M \) then \( q \) is a cube modulo \( p \).

PROOF: See Jacobi\(^6\).

By a form we mean a binary quadratic form \( ax^2 + bxy + cy^2 \) with integer coefficients. Its discriminant is the integer \( b^2 - 4ac \). An integer \( n \) is said to be represented by the form \( ax^2 + bxy + cy^2 \) if there exist integers \( u \) and \( v \) such that \( n = au^2 + buv + cv^2 \). The form \( ax^2 + bxy + cy^2 \) is said to be primitive if \( \gcd(a, b, c) = 1 \). It is positive-definite if and only if \( a \geq 0 \) and \( b^2 - 4ac < 0 \). We shall only be concerned with forms which are both primitive and positive-definite.

Let \( 2^r \parallel B \) and set \( B_1 = B/2^r \) so that \( B_1 \) is the odd part of \( B \). We now use Proposition 1 to show that all the primes represented by the principal form \( f(X, Y) \) of discriminant \(-108B_1^2\) belong to \( \text{Spl}(X^3 + B) \).

Proposition 2 — If \( p \) is a prime represented by the principal form \( f(X, Y) = X^2 + 27B_1^2Y^2 \) of discriminant \(-108B_1^2\) then \( p \in \text{Spl}(X^3 + B) \).

PROOF: Let \( p \) be a prime represented by the form \( X^2 + 27B_1^2Y^2 \) so that \( p \equiv 1 \pmod{3} \) and \( p \nmid B \). Proposition 1 ensures that every prime divisor of \( B \) is a cube modulo \( p \), so that \( X^3 + B \) has at least one root \( \pmod{p} \). But, as \( p \equiv 1 \pmod{3} \), it must have three roots \( \pmod{p} \), and so \( p \in \text{Spl}(X^3 + B) \). ■

Let \( g(X, Y) \) be a primitive, positive-definite quadratic form of discriminant \(-108B_1^2\) that represents a square modulo \( l \) for each odd prime \( l \cdot \) dividing \( 108B_1^2 \). It then follows from the theory of genera of binary quadratic forms that \( g(X, Y) \) belongs to the principal genus, see for example Hua\(^4\) (§12.6). The next result guarantees the existence of such a form \( g(X, Y) \) which represents only primes which are not in \( \text{Spl}(X^3 + B) \).

Proposition 3 — There is a primitive positive-definite form \( g(X, Y) \) in the principal genus of discriminant \(-108B_1^2\) with the property that if \( p \) is a prime represented by \( g(X, Y) \) then \( p \notin \text{Spl}(X^3 + B) \).

PROOF: We consider two cases according as \( B_1 \) is a perfect cube or not.

(i) \( B_1 \) is a perfect cube: In this case we take \( g(X, Y) = 4X^2 + 2B_1XY + 7B_1^2Y^2 \), which is a primitive, positive-definite form of discriminant \(-108B_1^2\). Since \( g(X, Y) \) represents 4, \( g(X, Y) \) is in the principal genus. Let \( p \) be a prime represented by \( g(X, Y) \) so there are integers \( u \) and \( v \) such that \( p = g(u, v) \). Then we have \( 4p = L^2 + 27M^2 \) with \( L = 4u + B_1v \), \( M = B_1v \). We note that \( p \equiv 1 \pmod{3} \) and \( p \nmid B_1 \). As \( M \) is odd, 2 is not a cube \( \pmod{p} \) by Proposition 1(i), and thus \( B \) is not a cube \( \pmod{p} \). Hence the congruence \( x^3 + B \equiv 0 \pmod{p} \) is insolvable and so \( p \notin \text{Spl}(X^3 + B) \).
(ii) $B_1$ is not a perfect cube: In this case $B_1$ has at least one odd prime divisor $q$ for which $3 \nmid \alpha$ where $q^\alpha \mid B_1$. We set $B_2 = B_1/q^\alpha$ so that $q \nmid B_2$. We consider two subcases: (a) $q = 3$ and (b) $q \neq 3$.

(a) $q = 3$. Here we take

$$g(X, Y) = 3^{2a}X^2 + 2 \cdot 3^aXY + (1 + 27B_2^2)Y^2,$$

which is a primitive, positive-definite form of discriminant $-108B_1^2$. Since $g(X, Y)$ represents $3^{2a}$ and $1 + 27B_2^2$, $g$ is in the principal genus. If $p$ is a prime represented by $g(X, Y)$ then there exist integers $u$ and $v$ such that $p = g(u, v)$. Then we have $4p = L^2 + 27M^2$ with $L = 2 \cdot 3^a u + 2v$, $M = 2B_2 v$. We note that $p \equiv 1 \pmod{3}$, $p \nmid B_1$, $3 \nmid M$ and $2B_2 \mid M$. By Proposition 1, 3 is not a cube modulo $p$ but every other prime divisor of $B$ is a cube modulo $p$. Hence the congruence $x^3 + B \equiv 0 \pmod{p}$ is insolvable, and $p \not\in \text{Spl}(X^3 + B)$.

(b) $q \neq 3$. The number $n_q$ of values of $s \pmod{q}$ for which the Legendre symbol

$$\left( \frac{s^2 + 27B_2^2}{q} \right)$$

has the value 1 is given by

$$n_q = \sum_{s^2 + 27B_2^2 \equiv 0 \pmod{q}} \frac{1}{2} \left( 1 + \left( \frac{s^2 + 27B_2^2}{q} \right) \right).$$

Now the number of solutions $s \pmod{q}$ of $s^2 \equiv -27B_2^2 \pmod{q}$ is

$$1 + \left( \frac{-27B_2^2}{q} \right) = 1 + \left( \frac{-3}{q} \right),$$

and by a classical result (see for example Hua, Theorem 8.2, p. 174)

$$\sum_{s=0}^{q-1} \left( \frac{s^2 + 27B_2^2}{q} \right) = -1,$$

so that

$$n_q = \frac{1}{2} \left( q - \left( 1 + \left( \frac{-3}{q} \right) \right) + (-1) \right) = \begin{cases} (q-3)/2, & \text{if } q \equiv 1 \pmod{3}, \\ (q-1)/2, & \text{if } q \equiv 2 \pmod{3}. \end{cases}$$

Let $s_1, ..., s_{n_q}$ denote these $n_q$ values of $s$.

We recall the definition of the cubic residue symbol: Let $E$ be the ring of Eisenstein integers; that is, the ring of integers of the field $\mathbb{Q}(\sqrt{-3})$. If $q \equiv 2 \pmod{3}$, then $q$ remains prime in $E$. If $q \equiv 1 \pmod{3}$, then $q = \lambda \overline{\lambda}$, where $\lambda$ is a prime in $E$. Let $\mu$ be a prime in $E$ dividing $q$ and let $\alpha \in E$ with $\mu \nmid \alpha$. The cubic residue symbol $[\alpha/\mu]_3$ is the unique cube root of unity such that

$$\alpha^{(N(\mu) - 1)/3} = [\alpha/\mu]_3 \pmod{\mu},$$
where the norm $N(\mu) = \mu \overline{\mu}$. If $q \equiv 1 \pmod{3}$, then $[\alpha/q] = [\alpha/\lambda]_3 [\alpha/\lambda_3]_3$.

We show that at least one of the cubic residue symbols

$$\left[ \frac{s_1 + 3B_2\sqrt{-3}}{q} \right]_3, \ldots, \left[ \frac{s_n + 3B_2\sqrt{-3}}{q} \right]_3$$

is not equal to 1. Suppose on the contrary that

$$\left[ \frac{s_j + 3B_2\sqrt{-3}}{q} \right] = 1, \quad j = 1, 2, \ldots, n_q$$

Then the $n_q(q-1)$ Eisenstein integers

$$k(s_j + 3B_2\sqrt{-3}) \mod q, \quad k = 1, 2, \ldots, q-1; \quad j = 1, 2, \ldots, n_q$$

are distinct modulo $q$ and satisfy

$$\left[ \frac{k(s_j + 3B_2\sqrt{-3})}{q} \right] = 1.$$

The number $R$ of reduced residue classes of Eisenstein integers (mod $q$) is

$$R = \begin{cases} (q-1)^2, & \text{if } q \equiv 1 \pmod{3}, \\ q^2-1, & \text{if } q \equiv 2 \pmod{3}, \end{cases}$$

and there are exactly $\frac{1}{3}R$ residue classes $\lambda$ (mod $q$) for which $\left[ \frac{\lambda}{q} \right] = 1$. Therefore we have

$$n_q(q-1) \leq \frac{1}{3}R,$$

that is

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

equivalently

$$\begin{cases} q \leq 7, & \text{if } q \equiv 1 \pmod{3}, \\ q \leq 5, & \text{if } q \equiv 2 \pmod{3}. \end{cases}$$

Hence for $q > 7$ there exists an integer $s$ such that

$$\left( \frac{s^2 + 27B_2^2}{q} \right) = 1, \quad \left[ \frac{s + 3B_2\sqrt{-3}}{q} \right] = 1. \quad \ldots \ (1)$$

In fact (1) holds for $q = 5$ and $q = 7$ if we take $s = -3B_2$. We now appeal to the Chinese remainder theorem to define an integer $r$ by

$$r \equiv 4 \pmod{6}, \quad r = s \pmod{q}, \quad r \equiv 1 \pmod{B_2}. \quad \ldots \ (2)$$
The congruences are consistent since if \( 3 \mid B_2 \) the third congruence implies \( r = 1 \) (mod 3). Define the form \( g(X, Y) \) of discriminant \(-108B_1^2\) by

\[
g(X, Y) = q^{2a} X^2 + 2q^a r XY + (r^2 + 27B_2^2) Y^2.
\]

Note that \( g(X, Y) \) is primitive as \( q \nmid r^2 + 27B_2^2 \) in view of (1) and (2). It is clearly positive-definite. As \( g(X, Y) \) represents \( q^{2a} \) and \( r^2 + 27B_2^2 \), by (1) and (2), \( g(X, Y) \) is in the principal genus.

Let \( p \) be a prime represented by \( g(X, Y) \) so that \( p = 1 \) (mod 3) and \( p \nmid B_2 \), and there are integers \( u \) and \( v \) such that \( p = g(u, v) \). Thus \( p = \pi \overline{\pi} \), where \( \pi \) is the Eisenstein prime

\[
\pi = (q^{a}u + rv) + 3B_2v \sqrt{-3} \equiv \pm 1 \pmod{3}.
\]

Note that

\[
\pi = v(r + 3B_2\sqrt{-3}) = v(s + 3B_2\sqrt{-3}) \pmod{q}.
\]

Then, by Eisenstein's law of cubic reciprocity\(^3\), we have

\[
\left[ \frac{q}{\pi} \right]_3 = \left[ \frac{\pi}{q} \right]_3 = \left[ \frac{v(s + 3B_2\sqrt{-3})}{q} \right]_3 = \left[ \frac{s + 3B_2\sqrt{-3}}{q} \right]_3 = 1,
\]

so that \( q \) is not cube modulo \( p \). As \( 4p = L^2 + 27M^2 \) with \( L = 2q^a u + 2rv \) and \( M = 2B_2v \), Proposition 1 shows that every prime divisor of \( B \) other than \( q \) is a cube modulo \( q \). Hence the congruence \( x^3 + B \equiv 0 \pmod{p} \) is insolvable and \( p \notin \text{Spl}(x^3 + B) \).

Our next result relates the form \( f(X, Y) = X^2 + 27B_1^2 Y^2 \) of Proposition 2 and the form \( g(X, Y) \) of Proposition 3.

**Proposition 4** — Let \( f(X, Y) \) and \( g(X, Y) \) be the forms specified in Propositions 2 and 3. Then, for each positive integer \( m \) there exist integers \( r, s, t, u \) with \( \text{GCD}(ru - st, m) = 1 \) such that

\[
f(X, Y) \equiv g(rX + sY, tX + uY) \pmod{m}.
\]

**Proof:** Since \( f(X, Y) \) is the principal form of discriminant \(-108B_1^2\), it belongs to the principal genus. By Proposition 3, \( g(X, Y) \) also belongs to the principal genus. Hence, by Theorem 3.21 (p. 58) of Cox\(^2\) or §12.5, Exercise 4 of Hua\(^4\), the assertion follows.

The next result is needed in order to apply a theorem of Iwaniec\(^5\) in the proof of our Theorem. Although Proposition 5 is stated for arbitrary forms \( f(X, Y) \) and \( g(X, Y) \) it will be applied with \( f(X, Y) \) and \( g(X, Y) \) as in Propositions 2, 3 and 4.

**Proposition 5** — Let \( f(X, Y) \) and \( g(X, Y) \) be primitive, positive-definite, integral binary quadratic forms of the same discriminant \( D \) for which there exist integers \( r, s, t, u, m \) with \( m \) even and \( \text{GCD}(ru - st, m) = 1 \) such that

\[
f(X, Y) \equiv g(rX + sY, tX + uY) \pmod{m}.
\]
Let \( x \) and \( y \) be integers such that
\[
\gcd(f(x, y), m) = 1.
\]
Set
\[
h(X, Y) = g(rx + sy + mX, tx + uy + mY).
\]
Then \( h(X, Y) \) is a quadratic polynomial in \( X \) and \( Y \) with coefficients such that
(i) \( h(X, Y) \) is primitive,
(ii) \( h(X, Y) \) is irreducible over \( \mathbb{Q} \),
(iii) \( h(X, Y) \) represents arbitrarily large odd integers,
(iv) \( \frac{\partial h}{\partial X}, \frac{\partial h}{\partial Y} \) are linearly independent over \( \mathbb{Q} \).

**PROOF:** We set \( G = rx + sy, H = tx + uy \).

(i) Clearly all the coefficients of \( h(X, Y) \) are divisible by \( m \) except possibly the constant term \( g(G, H) \). However \( g(G, H) = f(x, y) \) (mod \( m \)) and so is coprime with \( m \). Thus \( h(X, Y) \) is primitive.

(ii) As \( g(G, H) \) is coprime with \( m \), not both of \( G \) and \( H \) are zero. If \( G \neq 0 \) (resp. \( H \neq 0 \), \( h(0, Y) \) (resp. \( h(X, 0) \)) is irreducible over \( \mathbb{Q} \) as its discriminant \( G^2 m^2 D \) (resp. \( H^2 m^2 D \)) is negative, proving that \( h(X, Y) \) is irreducible over \( \mathbb{Q} \).

(iii) \( h(X, 0) \) has positive leading coefficient and so \( h(k, 0) \) takes arbitrarily large integral values. These integers are odd as \( h(k, 0) = g(G, H) = f(x, y) \) (mod \( m \)).

(iv) Suppose there exist \( k, l \in \mathbb{Q} \) (not both zero) such that
\[
k \frac{\partial h}{\partial X} + l \frac{\partial h}{\partial Y} = 0.
\]
Then, as
\[
h(X, Y) = m^2 g(X, Y) + mX \frac{\partial g}{\partial X} (G, H) + mY \frac{\partial g}{\partial Y} (G, H) + g(G, H),
\]
we have
\[
m \left( k \frac{\partial g}{\partial X} + l \frac{\partial g}{\partial Y} \right) + \left( k \frac{\partial g}{\partial X} (G, H) + l \frac{\partial g}{\partial Y} (G, H) \right) = 0.
\]
As \( \frac{\partial g}{\partial X}, \frac{\partial g}{\partial Y} \) are linear forms in \( X, Y \), and \( 1, X, Y \) are linearly independent over \( \mathbb{Q} \), we see that
\[
k \frac{\partial g}{\partial X} + l \frac{\partial g}{\partial Y} = 0,
\]
contradicting that \( g \) genuinely depends on both \( X \) and \( Y \). Hence \( \frac{\partial h}{\partial X} \) and \( \frac{\partial h}{\partial Y} \) are linearly independent over \( \mathbb{Q} \).

We are now ready to prove the main result of this paper. The proof follows ideas used in Spearman and Williams.9.
Theorem — If $B$ is an integer which is not a perfect cube then $\text{Spl}(X^3 + B)$ cannot be described by congruence conditions.

PROOF: We suppose that $\text{Spl}(X^3 + B)$ can be described by congruence conditions, that is, there exist positive integers $s, a_1, \ldots, a_s, m$ with $\text{GCD}(a_i, m) = 1$ and the $a_i$ lying in distinct residue classes modulo $m$ such that, except for finitely many primes $p$,

$$p \in \text{Spl}(X^3 + B) \iff p = a_1, \ldots, a_s \pmod{m}.$$  \hspace{1cm} \ldots (3)

In addition, by enlarging the set of exceptional primes to include the prime 2 if necessary, we may take $m$ to be even, since for $m$ odd each congruence $p = a_i \pmod{m}$ is equivalent to $p = a_i' \pmod{2m}$, where $a_i' = a_i$ if $a_i$ is odd, $a_i' = a_i + m$, if $a_i$ is even. By Weber's theorem\footnote{10} the form $X^2 + 27B^2Y^2$ represents infinitely many primes.

(An elementary proof of Weber's theorem is given in Briggs\footnote{1}.) We choose one of these primes $p_0$ which is not exceptional. By Proposition 2 we have $p_0 \in \text{Spl}(X^3 + B)$, and so by (3) $p_0 = a_i \pmod{m}$ for some $i$ with $1 \leq i \leq s$, that is $p_0$ belongs to the arithmetic progression $A(a_i, m) = \{a_i + km : k = 0, 1, 2, \ldots\}$. Let $g(X, Y)$ be the form given in Proposition 3. By Proposition 4 there exist integers $r, s, t, u$ with $\text{GCD}(ru - st, m) = 1$ such that $f(X, Y) = g(rX + sY, tX + uY) \pmod{m}$. Let $x$ and $y$ be integers such that $p_0 = f(x, y)$. Set $h(X, Y) = g(rx + sy + mX, tx + uy + mY)$. Then, by Proposition 5, $h(X, Y)$ is primitive, irreducible over $\mathbb{Q}$, represents arbitrarily large odd integers, and genuinely depends on both $X$ and $Y$, so that by Iwaniec’s theorem\footnote{5} $h(X, Y)$ represents infinitely many primes. Choose $p_1$ to be one of these which is not exceptional. Thus $p_1 \in A(a_i, m)$. However, as $p_1$ is represented by $g(X, Y)$, by Proposition 2, $p_1 \not\in \text{Spl}(X^3 + B)$, contradicting (3).

We next use the Theorem to exhibit without class field theory a wider class of cubic polynomials $c(X)$ for which $\text{Spl}(c(X))$ cannot be described by congruence conditions.

Corollary — Let $A$ and $B$ be integers such that $X^3 + AX + B$ is an irreducible cubic polynomial for which there is a nonzero integer $C$ such that $-4A^3 - 27B^2 = -3C^2$. Then $\text{Spl}(X^3 + AX + B)$ cannot be described by congruence conditions.

PROOF: We begin by recalling the Stickelberger parity theorem (Narkiewicz\footnote{8}, Theorem 4.5, p. 153). Let $f(X)$ be a monic irreducible polynomial of degree $n$ with integer coefficients. Let $p$ denote an odd prime not dividing the discriminant $D$ of $f(X)$, and suppose

$$f(X) = f_1(X) \ldots f_r(X) \pmod{p},$$

where the $f_i(X)$ are polynomials with integer coefficients which are irreducible $\pmod{p}$.

Then

$$\left(\frac{D}{p}\right) = (-1)^{n-r}.$$  \hspace{1cm} \ldots (4)
We are now ready to prove the Corollary. Let $H$ be the splitting field of $f(X) = X^3 + AX + B$ and $r_1, r_2, r_3 \in H$ the roots of $f(X)$. As $D = ((r_1 - r_2)(r_2 - r_3)(r_3 - r_1))^2 = -3C^2$ we see that $Q(\sqrt[3]{-3}) \subseteq H$ and $[H : Q(\sqrt[3]{-3})] = 3$.

Next we show that if $p \in \text{Spl}(f(X))$ then $p = 1 \pmod{3}$. As $p \in \text{Spl}(f(X))$ we have $p \nmid 3C$ and by (4) $\left(\frac{-3C^2}{p}\right) = (-1)^{3^3 - 3} = 1$, so $p = 1 \pmod{3}$.

As $D = -3C^2 < 0$, $f(X)$ has exactly one real root, say $r_1$, so that the other roots $r_2, r_3$ form a conjugate pair, say $r_2, \overline{r}_2$ and we set $s = r_1 + r_2 \omega + r_3 \omega^2$. The real number $s$ is called a Lagrange resolvent and generates $H$ over $Q(\sqrt[3]{-3})$ (Jacobson$^7$, Lemma 3, p. 245). The minimal polynomial of $s$ over $Q(\sqrt[3]{-3})$ is $X^3 - s^3$, so that $s^3 \in Q(\sqrt[3]{-3})$, $s \notin Q(\sqrt[3]{-3})$. As $s^3$ is a real algebraic integer, $s^3$ must in fact be a rational integer $M$, and $H$ is the splitting field of $X^3 - M$. Then, for $p \nmid -3C^2M$, we have

$$p \in \text{Spl}(X^3 + AX + B)$$

$\Leftrightarrow p = 1 \pmod{3}$ and $X^3 + AX + B = 0 \pmod{p}$ has three distinct solutions

$\Leftrightarrow x^3 + Ax + B = 0 \pmod{\pi}$ has three distinct solutions where $\pi$ is an Eisenstein prime with $\pi \overline{\pi} = p$

$\Leftrightarrow$ in the ring of integers of $H$, the ideal generated by $\pi$ is the product of three distinct prime ideals and $p = \pi \overline{\pi}$

$\Leftrightarrow x^3 - M = 0 \pmod{\pi}$ has three distinct solutions and $p = \pi \overline{\pi}$

$\Leftrightarrow x^3 - M = 0 \pmod{p}$ has three distinct solutions (as residue classes $\pmod{\pi}$ can be taken to be integers).

Hence $\text{Spl}(X^3 + AX + B) = \text{Spl}(X^3 - M)$ except possibly for a finite set of primes. The result now follows from the Theorem.

---

**REFERENCES**