TWISTS OF HYPERELLiptIC CURVES BY INTEGERS IN PROGRESSIONS MODULE $p$

DAVID KRUMM AND PAUL POLLACK

Abstract. Let $f(x)$ be a nonconstant polynomial with integer coefficients and nonzero discriminant. We study the distribution modulo primes of the set of squarefree integers $d$ such that the curve $dy^2 = f(x)$ has a nontrivial rational or integral point.

1. Introduction

Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial with nonzero discriminant, and let $C$ be the hyperelliptic curve over $\mathbb{Q}$ defined by $y^2 = f(x)$. For every squarefree integer $d$, let $C_d$ denote the quadratic twist $dy^2 = f(x)$. The main object of interest in this article is the set $S_{\mathbb{Q}}(f)$ consisting of all squarefree integers $d$ such that $C_d$ has a nontrivial rational point, i.e., an affine rational point $(x_0, y_0)$ with $y_0 \neq 0$. Specifically, we are interested in the following conjecture, which was proposed by the first author in [4].

Conjecture 1. For every large enough prime $p$, and every integer $r$ not divisible by $p$, there exist infinitely many $d \in S_{\mathbb{Q}}(f)$ such that $d \equiv r \pmod{p}$.

This conjecture is proved in [4] in the case where $\deg f \leq 2$. Furthermore, when $\deg f = 3$, or when $\deg f = 4$ and $f(x)$ has a rational root, the conjecture is shown to follow from the Parity Conjecture for elliptic curves over $\mathbb{Q}$. In this paper we explain how to leverage known results on squarefree values of polynomials and binary forms to prove the following two theorems.

First, using work of Granville [1] we show that Conjecture 1 follows from the abc conjecture; in fact, the latter can be used to prove a stronger statement. Let us denote by $S_{\mathbb{Z}}(f)$ the set of all squarefree integers $d$ such that $C_d$ has a nontrivial integral point.

Theorem 2. The abc conjecture implies that for every large enough prime $p$, and every integer $r$ not divisible by $p$, there exist infinitely many $d \in S_{\mathbb{Z}}(f)$ such that $d \equiv r \pmod{p}$.

Second, we prove an unconditional result by using work of Greaves [2].

Theorem 3. Conjecture 1 holds if every irreducible factor of $f(x)$ over $\mathbb{Q}$ has degree at most six.

2010 Mathematics Subject Classification. Primary: 11N32. Secondary: 11N36, 11G30.
Key words and phrases. Hyperelliptic curve, quadratic twist, abc conjecture.
The second author was supported by NSF award DMS-1402268.
In addition, we consider the distribution of elements of $S_Z(f)$ modulo $p$ when $p$ is a “small” prime, by which we mean that at least one of the conditions in (4) is not satisfied.

2. Assuming abc: Proof of Theorem \(^\text{2}\)

We will need the following special case of Theorem 1 in [1].

**Proposition 4** (Granville). Assume the abc conjecture is true. Let $g(x)$ be a nonconstant polynomial with integer coefficients and nonzero discriminant, and suppose that there is no prime $p$ such that $p | g(n)$ for all integers $n$. Then there exist infinitely many integers $n$ such that $g(n)$ is squarefree.

Recall that an integer $k$ is called a fixed divisor of $f(x)$ if $k | f(n)$ for every integer $n$. The set of all fixed divisors of $f(x)$ is finite, and therefore has a largest element, which we denote by $D$. It is a simple exercise to show that $D$ is maximal also in the sense that every fixed divisor of $f(x)$ divides $D$.

Let $p$ be a prime number, let $\text{ord}_p$ denote the $p$-adic valuation on $\mathbb{Z}$, and let $\varepsilon \in \{0, 1\}$ be the parity of $\text{ord}_p(D)$. For every integer $r \not\equiv 0 \pmod{p}$ and for every integer $v \geq 0$ we define a statement $S(r, v)$ as follows:

\[
\begin{align*}
(1) \quad S(r, v) \quad \text{There exist } h, x_0, y_0 \in \mathbb{Z} \text{ satisfying } \\
& \quad \begin{aligned}
& h y_0^2 \equiv f(x_0) \pmod{p^{2(v+\varepsilon)+1}}, \\
& \text{ord}_p(y_0) = v + \varepsilon, \text{ and} \\
& h \equiv r \pmod{p}.
\end{aligned}
\end{align*}
\]

The proof of the following proposition establishes the key ideas to be used throughout this article.

**Proposition 5** (Assuming abc). Let $r$ be an integer not divisible by $p$. Suppose that $S(r, v)$ holds true for some $v \geq 0$, and that $f(x)$ has an irreducible factor whose discriminant is not divisible by $p$. Then there exist infinitely many integers $d \in S_Z(f)$ such that $d \equiv r \pmod{p}$.

**Proof.** For every nonzero rational number $x$ we denote by $\text{sqf}(x)$ the squarefree part of $x$, i.e., the unique squarefree integer representing the coset of $x$ in $(\mathbb{Q}^+)/((\mathbb{Q}^+)^2)$. By definition of $\varepsilon$, we have $\text{ord}_p(D) = 2k + \varepsilon$ for some nonnegative integer $k$. Writing $D = \text{sqf}(D)t^2$, it is necessarily the case that $\text{ord}_p(t) = k$ and $\text{ord}_p(\text{sqf}(D)) = \varepsilon$; thus, we may write $t = p^k u$, where $p \nmid u$, and $\text{sqf}(D) = p^\varepsilon \delta$ for some squarefree integer $\delta$ not divisible by $p$.

Since $S(r, v)$ holds true, there exist integers $h, x_0, y_0$ satisfying the properties listed in (1). In particular, $\text{ord}_p(y_0) = v + \varepsilon$, so we may write $y_0 = p^{v+\varepsilon}z_0$, where $p \nmid z_0$. 


By the Chebotarev density theorem\textsuperscript{1}, there exists a prime \( q \nmid D \) such that \( qu \equiv z_0 \pmod{p} \) and \( f(x) \) has a simple root modulo \( q \). The latter property ensures, via Hensel’s lemma\textsuperscript{2}, that there exists \( m \in \mathbb{Z} \) such that \( q^2 \| f(m) \).

For every prime \( s \neq p \) dividing \( D \), let \( e_s = \ord_s(D) \) and let \( n_s \) be an integer such that \( f(n_s) \equiv 0 \pmod{s^{e_s+1}} \). (Such an integer must exist, for otherwise \( \lcm(s^{e_s+1}, D) = sD \) would be a fixed divisor of \( f(x) \), contradicting the maximality of \( D \).

Choose \( b \in \mathbb{Z} \) satisfying
\[
\begin{align*}
 b & \equiv x_0 \pmod{p^{2(v+\varepsilon)+1}}, \\
 b & \equiv m \pmod{q^3}, \text{ and} \\
 b & \equiv n_s \pmod{s^{e_s+1}} \text{ for every prime } s | D, s \neq p.
\end{align*}
\]

Let \( a = q^2p^{2(v+\varepsilon)+1} \prod_s s^{e_s+1} \), and define a polynomial \( g(x) \) by the equation
\[
\Delta \cdot g(x) = f(ax+b), \text{ where } \Delta = Dq^2p^{2(v-k)+\varepsilon}.
\]

Note that \( v \geq k \), so that \( \Delta \in \mathbb{Z} \). Indeed, the properties in (1) imply that \( \ord_p(f(x_0)) = 2(v+\varepsilon) \). Since \( D|f(x_0) \), then \( \ord_p(D) \leq \ord_p(f(x_0)) \), so \( 2k+\varepsilon \leq 2v+2\varepsilon \), and therefore \( k \leq v \).

We claim that \( g(x) \) satisfies all the hypotheses of Proposition\textsuperscript{4}. A Taylor expansion shows that \( f(ax+b) = f(b) + a \cdot P(x) \) for some polynomial \( P(x) \in \mathbb{Z}[x] \). Thus, in order to show that \( g(x) \in \mathbb{Z}[x] \) it suffices to show that \( \Delta \) divides both \( f(b) \) and \( a \). From the definitions it follows easily that \( \ord_\ell(a) \geq \ord_\ell(\Delta) \) for every prime \( \ell \) dividing \( \Delta \), so \( \Delta | a \). Similarly, the definition of \( b \) implies that \( \Delta | f(b) \). Hence \( g(x) \in \mathbb{Z}[x] \). Now suppose that \( \ell \) is a fixed prime divisor of \( g(x) \). We claim that \( \ell \nmid a \). If \( \ell = q \), then \( q | g(q) \), so \( q^3 | f(aq+b) \). However, \( f(aq+b) \equiv f(b) \equiv f(m) \not\equiv 0 \pmod{q^3} \). Thus \( \ell \neq q \).

Suppose now that \( \ell \) is one of the primes \( s \), and let \( n \in \mathbb{Z} \). Then \( s \mid g(n) \), so \( s^{e_s+1} | f(\alpha n + b) \). However, \( f(\alpha n + b) \equiv f(b) \equiv f(n_s) \not\equiv 0 \pmod{s^{e_s+1}} \). Thus \( \ell \neq s \). Similarly, we can show that \( p \) does not divide \( g(n) \) for any integer \( n \). For if \( p | g(n) \), then \( f(\alpha n + b) \equiv 0 \pmod{p^{2(v+\varepsilon)+1}} \). However, \( f(\alpha n + b) \equiv f(b) \equiv f(x_0) \not\equiv 0 \pmod{p^{2(v+\varepsilon)+1}} \). This proves that \( \ell \nmid a \).

As shown above, neither \( p \) nor any of the primes \( s \) can divide \( g(n) \) for any integer \( n \). Thus,
\[
\gcd(g(n), pD) = 1 \text{ for every integer } n.
\]

\textsuperscript{1}See Lemma 4.4 in [4] for details. The crucial fact we use here is that if \( h(x) \) is an irreducible factor of \( f(x) \) such that \( p \nmid \disc h(x) \), then the intersection of the splitting field of \( h(x) \) and the cyclotomic field \( \mathbb{Q}(\zeta_p) \) is \( \mathbb{Q} \).

\textsuperscript{2}Let \( \alpha \) be a simple root of \( f(x) \) modulo \( q \). Hensel lifting allows us to find an integer \( \beta \) such that \( \beta \equiv \alpha \pmod{q} \) and \( f(\beta) \equiv 0 \pmod{q^3} \). Then \( m = \beta + q^2 \) satisfies \( q^2 \| f(m) \).
The last step in the proof is to show that there is a well-defined map
\[ \psi : \{ n \in \mathbb{Z} \mid g(n) \text{ is squarefree} \} \to \{ d \in S_{\mathbb{Z}}(f) \mid d \equiv r \pmod{p} \} \]
given by \( n \mapsto \delta g(n) \). Note that the domain of \( \psi \) is infinite by Proposition 4. Let \( n \in \mathbb{Z} \) be such that \( g(n) \) is squarefree. Tracking through the definitions we find that
\[ f(ax + b) = \delta g(x)(qu)^2 p^{2\epsilon+2\varepsilon}. \]
By [2] we have \( \gcd(g(n), \delta) = 1 \), so (3) implies that
\[ d := \text{sqf}(f(an + b)) = \delta g(n). \]
Reducing (3) modulo \( p^{2(\nu+\varepsilon)+1} \) and recalling that \( y_0 = p^{\nu+\varepsilon}z_0 \), we obtain
\[ d(qu)^2 p^{2\epsilon+2\varepsilon} \equiv f(b) \equiv f(x_0) \equiv h y_0^2 \equiv h p^{2\nu+2\varepsilon} z_0^2 \pmod{p^{2(\nu+\varepsilon)+1}}. \]
It follows that \( d(qu)^2 \equiv h z_0^2 \pmod{p} \). Since \( qu \equiv z_0 \pmod{p} \) by construction and \( h \equiv r \pmod{p} \) by the assumptions in (1), this implies that \( d \equiv r \pmod{p} \). Moreover, it is clear from the definitions that \( d \in S_{\mathbb{Z}}(f) \). Thus, we have shown that the map \( \psi \) is well defined.

The equation \( g(x) = g(y) \) has only finitely many integral solutions with \( x \neq y \), since the polynomial map \( x \mapsto g(x) \) is injective outside some bounded interval in the real line. Hence, the fact that the domain of \( \psi \) is infinite implies that its image is infinite as well. This completes the proof. \( \square \)

Remarks.

(i) Proposition 4 is known to hold unconditionally if every irreducible factor of \( f(x) \) has degree at most three (see [3, Chap. 4]). Our arguments show that Proposition 5 also holds unconditionally in this case.

(ii) The version of Proposition 4 given in [1] states that the number of positive integers \( n \leq B \) such that \( g(n) \) is squarefree is asymptotic to \( \kappa B \) (as \( B \to \infty \)) for some positive constant \( \kappa \). Modifying the proof of Proposition 5 appropriately to take advantage of this, one can show that
\[ \# \{ d \in S_{\mathbb{Z}}(f) : |d| \leq B \text{ and } d \equiv r \pmod{p} \} \gg B^{1/\deg(f)}. \]

**Corollary 6 (Assuming abc).** Let \( r \) be an integer not divisible by \( p \). Suppose that \( p \nmid D \), \( p \nmid \text{disc } f(x) \), and \( ry_0^2 \equiv f(x_0) \pmod{p} \) for some integers \( x_0, y_0 \) with \( p \nmid y_0 \). Then there exist infinitely many integers \( d \in S_{\mathbb{Z}}(f) \) such that \( d \equiv r \pmod{p} \).

**Proof.** The hypotheses imply that the statement \( S(r, 0) \) holds true. The result then follows immediately from Proposition 5. \( \square \)

**Proof of Theorem 2** Assuming the abc conjecture, we must show that for every large enough prime \( p \), and every integer \( r \) not divisible by \( p \), there exist infinitely many \( d \in S_{\mathbb{Z}}(f) \) such that \( d \equiv r \pmod{p} \). Let \( \text{lc}(f) \) be the leading coefficient of \( f(x) \), and let \( g \) be the genus of the curve \( y^2 = f(x) \). Suppose that \( p \) is a prime satisfying
\[ p \mid \text{lc}(f), \ p \nmid D, \ p \nmid \text{disc } f(x), \ \text{and } p > 4g^2 + 6g + 4. \]
Let $r$ be an integer not divisible by $p$. The Hasse-Weil bound implies that every smooth projective curve of genus $g$ defined over $\mathbb{F}_p$ has at least $2g + 5$ points defined over $\mathbb{F}_p$; in particular, this applies to the hyperelliptic curve over $\mathbb{F}_p$ defined by $ry^2 = f(x)$. This curve can have at most $2g + 4$ trivial points defined over $\mathbb{F}_p$, so it must have a nontrivial point. Applying Corollary 6 we obtain the desired result.

3. The case of small primes $p$

Let $R(p) \subseteq \mathbb{F}_p^*$ be the set consisting of all the nonzero residue classes modulo $p$ which are represented in the set $S_{\mathbb{Z}}(f)$. We have shown that if $p$ is large enough, then $R(p) = \mathbb{F}_p^*$. In this section we discuss the problem of determining $R(p)$ when $p$ is a “small” prime, meaning that the conditions (4) are not all satisfied.

Lemma 7. Let $r$ be an integer not divisible by $p$, and let $v$ be a nonnegative integer. Suppose that $S(r, v)$ holds. Then $S(a, v)$ holds for every integer $a$ in the same square class as $r$ modulo $p$.

Proof. Let $h$, $x_0$, and $y_0$ be integers satisfying the conditions in (1). Let $g$ be a primitive root modulo $p$, and let $z$ be a multiplicative inverse of $g$ modulo $p^{2(v+\varepsilon)+1}$. By hypothesis, $a \equiv rg^{2k} \pmod{p}$ for some positive integer $k$. From the definitions it follows that

- $hg^{2k}(z^ky_0)^2 \equiv hy_0^2 \equiv f(x_0) \pmod{p^{2(v+\varepsilon)+1}}$,
- $\text{ord}_p(z^ky_0) = \text{ord}_p(y_0) = v + \varepsilon$, and
- $hg^{2k} \equiv rg^{2k} \equiv a \pmod{p}$.

Hence, $S(a, v)$ holds.

Proposition 8 (Assuming abc). Suppose that $f(x)$ has an irreducible factor whose discriminant is not divisible by $p$. Then $R(p)$ is either empty or equal to one of the sets $\mathbb{F}_p^*$, $(\mathbb{F}_p^*)^2$, or $\mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$.

Proof. We claim that if $R(p)$ contains a square, then $R(p) \supseteq (\mathbb{F}_p^*)^2$. Let $a$ and $r$ be nonzero quadratic residues modulo $p$, and suppose that there exists $d \in S_{\mathbb{Z}}(f)$ such that $d \equiv r \pmod{p}$. Then we have $dy_0^2 = f(x_0)$ for some integers $x_0, y_0$ with $y_0 \neq 0$. Letting $v = \text{ord}_p(y_0) - \varepsilon$, it is easy to verify that $v \geq 0$ and $S(r, v)$ holds. By Lemma 7 $S(a, v)$ also holds. Hence, by Proposition 5 there exists $d' \in S_{\mathbb{Z}}(f)$ such that $d' \equiv a \pmod{p}$. This proves the claim. A similar argument shows that if $R(p)$ contains a nonsquare, then $R(p) \supseteq \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$.

Suppose that $R(p)$ is nonempty. If $R(p)$ contains only squares, then the above argument implies that $R(p) = (\mathbb{F}_p^*)^2$; similarly, if $R(p)$ contains only nonsquares, then $R(p) = \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$. Finally, if $R(p)$ contains both a square and a nonsquare, then $R(p) = \mathbb{F}_p^*$.

We now provide examples in which the various possibilities of Proposition 8 occur with small primes $p$. 

□
Example 9. Let $p$ be any prime such that $p \equiv 3 \pmod{4}$, and consider the polynomial $f(x) = (x^2 + 1)(x^p - x)^2 + p)$. Note that $f(x)$ has a repeated root modulo $p$, so that $p | \text{disc } f(x)$, and $p$ is a small prime for $f(x)$. We have $\text{ord}_p(f(n)) = 1$ for every integer $n$, which implies that $p | \text{sqf}(f(n))$ for all $n$. Hence, every element of $S_\mathbb{Z}(f)$ is divisible by $p$, and $R(p) = \emptyset$.

Example 10. Let $p$ be an arbitrary prime, and consider the polynomial $f(x) = x^p - x + 1$. Note that $p$ is small for $f(x)$. We claim that $R(p) = (\mathbb{F}_p^*)^2$. Let $r$ be an integer not divisible by $p$, and suppose that $d \in S_\mathbb{Z}(f)$ satisfies $d \equiv r \pmod{p}$. Then $d y_0^2 = x_0^p - x_0 + 1$ for some integers $x_0, y_0$. Reducing modulo $p$ we obtain $r y_0^2 \equiv 1 \pmod{p}$, from which it follows that $r$ is a square modulo $p$. Thus, $R(p) \subseteq (\mathbb{F}_p^*)^2$. Conversely, if $r$ is a nonzero square modulo $p$, then $r y_0^2 \equiv 1 \pmod{p}$ for some integer $y_0$ and for every integer $x_0$. Since $p \nmid D = 1$ and $p \nmid \text{disc } f(x)$, Corollary 4 implies that there exists $d \in S_\mathbb{Z}(f)$ such that $d \equiv r \pmod{p}$. Hence, $R(p) = (\mathbb{F}_p^*)^2$, as claimed. A similar argument shows that if we define $f(x) = x^p - x + a$, where $a$ is a quadratic nonresidue modulo $p$, then $R(p) = \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$.

Example 11. Let $p$ be prime, let $v$ be a nonnegative integer, and consider $f(x) = x(x^p - x)^{2^{v+2}} + p^{2^{v+1}} x$. We will show that $R(p) = \mathbb{F}_p^*$. Note that $p | \text{disc } f(x)$, so $p$ is small for $f(x)$. Clearly, $p^{2^{v+1}}$ is a fixed divisor of $f(x)$, so $p^{2^{v+1}} | D$; in fact $p^{2^{v+1}} | D$ since $p^{2^{v+2}} | f(1)$. In particular, the parity of $\text{ord}_p(D)$ is $\varepsilon = 1$. The statement $S(r, v)$ can now be seen to hold for every integer $r \not\equiv 0 \pmod{p}$: indeed, $r(p^{v+1})^2 \equiv f(rp) \pmod{p^{2^{v+2}}}$. Moreover, $f(x)$ has an irreducible factor (namely, $x$) whose discriminant is not divisible by $p$. Thus, by Proposition 5, there exists $d \in S_\mathbb{Z}(f)$ such that $d \equiv r \pmod{p}$. We conclude that $R(p) = \mathbb{F}_p^*$.

In the last example we show that when the discriminant condition in Proposition 8 is not satisfied, the conclusion may not hold.

Example 12. Let $p$ be an odd prime, and let $f(x)$ be the $p$-th cyclotomic polynomial. Then $f(x)$ is irreducible and $p | \text{disc } f(x)$. We will show that $R(p) = \{1\}$. Clearly $1 \in R(p)$ because the curve $y^2 = f(x)$ has a nontrivial integral point, namely $(0, 1)$. Now suppose that $d \in S_\mathbb{Z}(\mathbb{Z})$ is not divisible by $p$. We have $d > 0$ because $f(x)$ only takes positive values for $x \in \mathbb{R}$. If $q$ is any prime dividing $d$, then $f(x)$ has a simple root modulo $q$. Let $K$ denote the cyclotomic field $\mathbb{Q}[x]/(f(x))$. By the Dedekind-Kummer theorem in algebraic number theory (Proposition 8.3 in [], some prime (and therefore every prime) of $\mathcal{O}_K$ lying over $(q)$ has ramification index and residue degree equal to 1. Hence, $q$ splits completely in $K$. It follows that $q \equiv 1 \pmod{p}$ (see Corollary 10.4 in [], for instance). Since $d > 0$ and every prime divisor of $d$ is congruent to 1 modulo $p$, then $d \equiv 1 \pmod{p}$. Therefore, $R(p) = \{1\}$. 


4. An unconditional result: proof of Theorem 3

We will need the following special case of the main theorem in [2].

**Proposition 13** (Greaves). Let \( F(x, y) \in \mathbb{Z}[x, y] \) be a binary form of degree \( d \) with nonzero discriminant, and suppose that the coefficient of \( y^d \) in \( F(x, y) \) is nonzero. Let \( A, B, M \) be integers with \( M > 0 \). Assume that for every prime \( \ell \) there exist integers \( \alpha \) and \( \beta \) such that

\[
\alpha \equiv A \pmod{M}, \quad \beta \equiv B \pmod{M}, \quad \text{and} \quad \ell^2 \nmid F(\alpha, \beta).
\]

If every irreducible factor of \( F(x, y) \) has degree at most six, then there exist infinitely many pairs of integers \( \alpha, \beta \) such that \( \alpha \equiv A \pmod{M}, \beta \equiv B \pmod{M} \), and \( F(\alpha, \beta) \) is squarefree.

**Remark.** The result in [2] assumes that \( F(x, y) \) has nonzero terms in both \( x^d \) and \( y^d \). To obtain Proposition 13, one should apply the result of [2] with \( F(x, y) \) replaced with \( F(x, kx + y) \) for an integer \( k \) chosen so that the coefficient of \( x^d \) is nonzero.

**Proposition 14.** Let \( r \) be an integer not divisible by \( p \). Suppose that \( S(r, v) \) holds true for some \( v \geq 0 \), and that \( f(x) \) has an irreducible factor whose discriminant is not divisible by \( p \). Moreover, suppose that \( \deg f \geq 3 \) and that every irreducible factor of \( f(x) \) has degree at most six. Then there exist infinitely many integers \( d \in S_\mathbb{Q}(f) \) such that \( d \equiv r \pmod{p} \).

**Proof.** The hypotheses allow us to define a polynomial \( g(x) \) as in the proof of Proposition 5. We will use here the notation introduced in that proof. Let \( G(x, y) \) be the homogenization of \( g(x) \), \( \sigma = \deg g \), and \( F(x, y) = y^\sigma G(x, y) \), where \( \sigma \in \{0, 1\} \) is the parity of \( \sigma \). We have \( \Disc F \neq 0 \) since \( \Disc g(x) \neq 0 \). Note that \( g(0) = f(b)/\Delta \), and \( f(b) \neq 0 \) because \( f(b) \equiv f(m) \neq 0 \pmod{q^3} \). It follows that the coefficient of \( y^{\sigma+\sigma} \) in \( F(x, y) \) is nonzero.

We will apply Proposition 14 with \( A = q, B = 1, M = pD \). We must show that for every prime \( \ell \) there exist \( \alpha, \beta \in \mathbb{Z} \) satisfying (5). By (2) we have \( \gcd(g(q), pD) = 1 \). Thus, if \( \ell \nmid pD \), then \( \ell \nmid g(q) = F(q, 1) \), so we may take \( \alpha = q, \beta = 1 \). For \( \ell = q \), we have \( q \nmid g(q) = F(q, 1) \), as shown in the proof of Proposition 5. Suppose now that \( \ell \mid pqD \), so that \( \ell \nmid a \). We claim that there exists \( \alpha \equiv q \pmod{pD} \) such that \( \ell \nmid F(\alpha, 1) \). If not, then \( \ell \mid f(aa + b) \) for every such \( \alpha \). Since \( a \) is invertible modulo \( \ell \), this implies that \( \ell \) is a fixed divisor of \( f(x) \), and hence divides \( D \), which is a contradiction.

Let \( P \) be the set of all pairs of integers \( (\alpha, \beta) \) such that \( \alpha \equiv q \pmod{pD} \), \( \beta \equiv 1 \pmod{pD} \), and \( F(\alpha, \beta) \) is squarefree. By Proposition 13, \( P \) is an infinite set. We claim that there is a well-defined map

\[
\psi : P \to \{d \in S_\mathbb{Q}(f) \mid d \equiv r \pmod{p}\}, \quad (\alpha, \beta) \mapsto F(\alpha, \beta) \delta.
\]

Given \((\alpha, \beta) \in P\), let \( \lambda = \alpha/\beta \) and \( d = F(\alpha, \beta) \delta \). Then \( \beta^{\sigma+\sigma} g(\lambda) = F(\alpha, \beta) \), so \( sqf(g(\lambda)) = F(\alpha, \beta) \). Note that \( F(\alpha, \beta) \) is relatively prime to \( D \): if \( \ell \) is a prime dividing \( D \), then \( \ell \nmid g(q) = F(q, 1) \), and therefore \( \ell \nmid F(\alpha, \beta) \) since
\[ F(\alpha, \beta) \equiv F(q, 1) \pmod{\ell}. \] Thus \(d\) is squarefree. Using (3) we obtain
\[ \beta^{\theta + \sigma} f(a \lambda + b) = d(\ell)^2 \ell^{2\nu + 2\varepsilon}, \]
from which it follows that \(\text{sqf}(f(a \lambda + b)) = d\), and therefore \(d \in S_Q(f)\). We claim that \(d \equiv r \pmod{p}\). Since \(\beta\) is a unit modulo \(p\), \(\lambda\) belongs to the local ring \(\mathbb{Z}(p)\). In this ring we have the congruence
\[ a \lambda + b \equiv b \pmod{p^2(v + \varepsilon) + 1}; \]
hence, by the displayed equation above,
\[ d(\ell)^2 \ell^{2\nu + 2\varepsilon} \equiv \beta^{\theta + \sigma} f(b) \pmod{p^2(v + \varepsilon) + 1}. \]
The definition of \(b\) implies that \(f(b) \equiv h z_0^2 p^{2(v + \varepsilon)} \pmod{p^2(v + \varepsilon) + 1}\). It follows that \(d(\ell)^2 \equiv \beta^{\theta + \sigma} h z_0^2 \equiv \beta^{\theta + \sigma} r z_0^2 \pmod{p}\). Since \(qu \equiv z_0 \pmod{p}\) and \(\beta \equiv 1 \pmod{p}\), we obtain \(d \equiv r \pmod{p}\), as claimed. This proves that the map \(\psi\) is well defined.

Proof of Theorem 3. Assuming that every irreducible factor of \(f(x)\) has degree at most six, we must show that for every large enough prime \(p\), and every integer \(r\) not divisible by \(p\), there exist infinitely many \(d \in S_Q(f)\) such that \(d \equiv r \pmod{p}\).

By the results of [4] mentioned in the introduction, we may assume that \(\deg f \geq 3\). As seen in the proof of Theorem 2 if \(p\) satisfies the conditions (4), then \(S(r, 0)\) holds for every integer \(r \not\equiv 0 \pmod{p}\). Applying Proposition 14 we obtain the desired result. □

References

[1] Andrew Granville, ABC allows us to count squarefrees, Internat. Math. Res. Notices 19 (1998), 991–1009.
[2] George Greaves, Power-free values of binary forms, Quart. J. Math. Oxford Ser. (2) 43 (1992), no. 169, 45–65.
[3] Christopher Hooley, Applications of sieve methods to the theory of numbers, Cambridge Tracts in Mathematics, vol. 70, Cambridge University Press, Cambridge-New York-Melbourne, 1976.
[4] David Krumm, Squarefree parts of polynomial values, J. Théor. Nombres Bordeaux 28 (2016), no. 3, 699–724.
[5] Jürgen Neukirch, Algebraic number theory, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999.

Mathematics Department, Reed College
E-mail address: dkrumm@reed.edu
URL: http://maths.dk

Department of Mathematics, University of Georgia
E-mail address: pollack@uga.edu
URL: http://pollack.uga.edu