Products Of Quadratic Polynomials
With Roots Modulo Any Integer

Andrea M. Hyde

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada V1V 1V7

Blair K. Spearman

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada V1V 1V7

Copyright © 2013 Andrea M. Hyde and Blair K. Spearman. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

We classify products of three quadratic polynomials, each irreducible over \( \mathbb{Q} \), which are solvable modulo \( m \) for every integer \( m > 1 \) but have no roots over the rational numbers. Polynomials with this property are known as intersective polynomials. We use Hensel’s Lemma and a refined version of Hensel’s Lemma to complete the proof.

Mathematics Subject Classification: 11R09

Keywords: Local-Global Principle, Hensel’s Lemma, Intersective Polynomials

1 Introduction

Let \( f(x) \) be a monic polynomial with integer coefficients. We are interested in intersective polynomials, that is, those polynomials \( f(x) \) which have no root
in the rational numbers but do have a root modulo all positive integers. These polynomials provide counterexamples to the local-global principle. Readers interested in more information on the local-global principle should consult [4, pp. 75-83]. A common example of this phenomenon is the following product of three quadratic polynomials.

\[ f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34). \]  

(1)

This example or others very similar appear in [1], [2], [3], [4] and [5]. We note that the three quadratic polynomials in (1) define quadratic subfields of a bicyclic quartic field

\[ \mathbb{Q}(\sqrt{2}, \sqrt{17}). \]

This type of product is necessary in order to form intersective polynomials. An explanation of this in terms of Galois theory can be found in [6] or [7]. In this paper we shall treat the general case of these products of quadratic polynomials, which we denote by \( f(x) \). Special families will be considered as corollaries. We shall confirm that

\[ f(x) \equiv 0 \pmod{m} \]

is solvable for every \( m > 1 \) by showing that for each prime \( p \) and positive integer \( j \), the congruence

\[ f(x) \equiv 0 \pmod{p^j} \]

is solvable. General solvability then follows from the Chinese Remainder Theorem. For a given prime \( p \), one of the factors of \( f(x) \) is proven to be solvable mod \( p^j \) for all positive integers \( j \). We state our main theorem next, recalling the Legendre symbol \( \left( \frac{n}{p} \right) \) which takes the values \( +1 \) if \( n \) is a quadratic residue modulo \( p \), \( -1 \) if \( n \) is a quadratic non-residue modulo \( p \), or \( 0 \) if \( p \) divides \( n \).

2 Main Result

**Theorem 2.1** Let \( a, b \) be squarefree integers, not equal to 1 such that \( ab \) is not equal to the square of an integer. Set \( \ell = \gcd(a, b) \) and define \( a_1 \) and \( b_1 \) by \( a = a_1\ell \) and \( b = b_1\ell \). Set

\[ f(x) = (x^2 - a)(x^2 - b)(x^2 - a_1b_1). \]

Then

\[ f(x) \equiv 0 \pmod{m} \]
is solvable modulo every integer \( m > 1 \) if and only if at least one of \( a, b, a_1 b_1 \) is congruent to 1 modulo 8 and for every odd prime \( p \) at least one of the Legendre symbols

\[
\left( \frac{a}{p} \right), \quad \left( \frac{b}{p} \right), \quad \left( \frac{a_1 b_1}{p} \right),
\]

has the value +1.

For the proof of our theorem we will require Hensel’s Lemma, both a standard version and a refined version.

**Theorem 2.2 (Hensel’s Lemma) (see [5, p. 87])** Suppose that \( f(x) \) is a polynomial with integral coefficients. If \( f(a) \equiv 0 \pmod{p^j} \) and \( f'(a) \not\equiv 0 \pmod{p} \), then there is a unique \( t \pmod{p} \) such that \( f(a + tp^j) \equiv 0 \pmod{p^{j+1}} \).

We call the root \( a \) nonsingular if \( f'(a) \not\equiv 0 \pmod{p} \). A nonsingular root \( a \) of \( f(x) \equiv 0 \pmod{p} \) may be lifted to a root modulo \( p^j \), \( j = 2, 3, \ldots \) by repeatedly applying Hensel’s Lemma. We employ a refined version of Hensel’s Lemma in the case of a singular root, enabling us to lift our solutions modulo arbitrarily high prime powers.

**Theorem 2.3 (Refined Hensel’s Lemma) (see [5, p. 89])** Let \( f(x) \) be a polynomial with integral coefficients. Suppose that \( f(a) \equiv 0 \pmod{p^j} \), that \( p^\tau \parallel f'(a) \) and that \( j \geq 2\tau + 1 \). If \( b \equiv a \pmod{p^{j-\tau}} \) then \( f(b) \equiv f(a) \pmod{p^j} \) and \( p^\tau \parallel f'(b) \). Moreover there is a unique \( t \pmod{p} \) such that \( f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}} \).

As noted in [5, p. 89], since the hypotheses of the theorem apply with \( a \) replaced by \( a + tp^{j-\tau} \) and \( (\pmod{p^j}) \) replaced by \( (\pmod{p^{j+1}}) \) but with \( \tau \) unchanged, the lifting may be repeated and continues indefinitely. We require two simple lemmas for the proof of our theorem.

**Lemma 2.4** Suppose that \( p \) is an odd prime and \( r \) is a squarefree integer. Then the congruence

\[
x^2 \equiv r \pmod{p^j}
\]

is solvable for \( j = 1, 2, \ldots \) if and only if \( \left( \frac{r}{p} \right) = +1 \).

**Proof** Since \( r \) is squarefree, solvability of the given congruence requires \( p \nmid r \). Specializing to solvability mod \( p \) shows that \( \left( \frac{r}{p} \right) = +1 \)
If \( \left( \frac{r}{p} \right) = +1 \) then the congruence
\[
x^2 \equiv r \pmod{p}
\]
is solvable with integer solution \( x = x_0 \). Since
\[
x_0^2 \equiv r \pmod{p}
\]
and \( p \nmid r \) we see that \( p \nmid x_0 \) so that \( x_0 \) is a nonsingular root of this congruence. Thus we may employ Proposition 1 to lift this solution to a solution of the congruence
\[
x^2 \equiv r \pmod{p^j}
\]
for \( j = 1, 2, \ldots \), completing the proof. \( \square \)

**Lemma 2.5** Suppose that \( r \) is a squarefree integer. Then the congruence
\[
x^2 \equiv r \pmod{2^j}
\]
is solvable for \( j = 1, 2, \ldots \) if and only if \( r \equiv 1 \pmod{8} \).

**Proof** Since \( r \) is squarefree, solvability of the given congruence modulo all powers of 2 requires \( r \) to be odd. Since odd squares are congruent to 1 modulo 8, we have \( r \equiv 1 \pmod{8} \). If \( r \equiv 1 \pmod{8} \) then the congruence
\[
x^2 \equiv r \pmod{2^3}
\]
is solvable with solution \( x = 1 \). Although \( x = 1 \) is a singular root of this congruence, we may employ Proposition 2, with \( j = 3 \) and \( \tau = 1 \) and lift this root to a solution of
\[
x^2 \equiv r \pmod{2^j}
\]
modulo all powers of 2 as required. \( \square \)

We now give the proof of our theorem.

**Proof** Assume that \( f(x) = (x^2 - a)(x^2 - b)(x^2 - a_1b_1) \equiv 0 \pmod{m} \) is solvable for every integer \( m > 1 \). Then in particular this polynomial congruence is solvable modulo powers of 2 so that at least one of the factors of \( f(x) \) is solvable modulo 8. Since a congruence of the form \( x^2 \equiv r \pmod{8} \) is solvable only if \( r \equiv 1 \pmod{8} \), Lemma 2 establishes the first statement in our theorem.
Next, for any odd prime \( p \), we must have at least one of the factors of \( f(x) \), say \( (x^2 - r) \), solvable modulo \( p^j \), \( j = 1, 2, 3, \ldots \). As \( r \) is squarefree we have \( p \nmid r \) and thus \( \left( \frac{r}{p} \right) = +1 \) as required. This establishes the second statement in our theorem.

On the other hand, assuming that \( p \) is an odd prime and one of \( (a^p) \), \( (b^p) \), \( (a_1b_1^p) \) has the value +1, we may use Lemma 1 to deduce solvability of a factor of \( f(x) \) and hence \( f(x) \) modulo \( p^j \), \( j = 1, 2, 3, \ldots \). Similarly, assuming that the constant term of one of the factors of \( f(x) \) is of the form \( 8k + 1 \) we may use Lemma 2 to conclude that this factor is solvable modulo \( 2^j \), \( j = 1, 2, 3, \ldots \) and conclude that \( f(x) \) is solvable modulo \( 2^j \), \( j = 1, 2, 3, \ldots \).

Solvability modulo \( m \) for any positive integer \( m \) follows from the Chinese Remainder Theorem. This concludes the proof of our theorem. \[ \square \]

3 Corollaries

We use our theorem to construct three simple families of polynomials, solvable modulo every positive integer \( m \).

**Corollary 3.1** Let \( n \) be an odd squarefree integer with \( n \neq 1 \). Then

\[
f(x) = (x^2 - 2)(x^2 - n)(x^2 - 2n)
\]

is solvable modulo \( m \) for every positive integer \( m \) if and only if the prime factors of \( n \) have the form \( 8k \pm 1 \) and \( n \equiv 1(\text{mod } 8) \).

**Proof** If \( f(x) \) has a root modulo every positive integer \( m \), then our theorem requires that one factor of \( f(x) \) have constant term with the form \( 8k + 1 \). Clearly this term must be \( n \). Suppose that \( p \) is an odd prime. Our theorem implies that one of the Legendre symbols

\[
\left( \frac{2}{p} \right), \left( \frac{n}{p} \right), \left( \frac{2n}{p} \right)
\]

has the value +1. This is automatic if \( p \nmid n \) by multiplicativity of the Legendre symbol. If \( p \mid n \) then from our theorem we deduce that

\[
\left( \frac{2}{p} \right) = 1
\]
implying that
\[ p \equiv \pm 1 \pmod{8}. \]
Reversing the argument clearly shows that \( f(x) \) is solvable modulo \( p' \), for all primes \( p \) and all positive integers \( j \). General solvability modulo \( m \) follows from the Chinese Remainder Theorem.

The proofs of the next two corollaries are similar to the proof of Corollary 3.1.

**Corollary 3.2** Let \( n \) be a squarefree integer with \( n \neq \pm 1 \). Then
\[ f(x) = (x^2 + 1)(x^2 - n)(x^2 + n) \]
is solvable modulo \( m \) for every positive integer if and only if the prime factors of \( n \) have the form \( 4k + 1 \) and \( n \equiv \pm 1 \pmod{8} \).

**Corollary 3.3** Let \( n \) be an odd squarefree integer with \( n \neq 1 \). Then
\[ f(x) = (x^2 + 2)(x^2 - n)(x^2 + 2n) \]
is solvable modulo \( m \) for every positive integer if and only if the prime factors of \( n \) have the form \( 8k + 1 \) or \( 8k + 3 \) and \( n \equiv 1 \pmod{8} \).

We finish by giving some examples of polynomials obtained from our corollaries.

<table>
<thead>
<tr>
<th>( n )</th>
<th>Corollary</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>3.1</td>
<td>((x^2 - 2)(x^2 - 17)(x^2 - 34))</td>
</tr>
<tr>
<td>(-7)</td>
<td>3.1</td>
<td>((x^2 - 2)(x^2 + 7)(x^2 + 14))</td>
</tr>
<tr>
<td>17</td>
<td>3.2</td>
<td>((x^2 + 1)(x^2 - 17)(x^2 + 17))</td>
</tr>
<tr>
<td>(-41)</td>
<td>3.2</td>
<td>((x^2 + 1)(x^2 + 41)(x^2 - 41))</td>
</tr>
<tr>
<td>17</td>
<td>3.3</td>
<td>((x^2 + 2)(x^2 - 17)(x^2 + 34))</td>
</tr>
<tr>
<td>33</td>
<td>3.3</td>
<td>((x^2 + 2)(x^2 - 33)(x^2 + 66))</td>
</tr>
</tbody>
</table>

**References**


Received: May 30, 2013