MINIMALLY INTERSECTIVE POLYNOMIALS WITH ARBITRARILY LONG FACTORIZATION

Bhawesh Mishra[1]
Department of Mathematics, The Ohio State University, Columbus, Ohio
mishra.188@osu.edu

Received: 4/20/21, Accepted: 1/3/22, Published: 1/24/22

Abstract

Given a natural number $n \geq 4$, we show that there exist infinitely many polynomials $f_n(x) := (x^2 - a_1)(x^2 - a_2)\cdots(x^2 - a_n)$ such that (i) $f_n(x)$ has a root modulo every positive integer, (ii) $f_n(x)$ has no rational roots, and (iii) every proper divisor of $f_n(x)$ fails to have a root modulo some positive integer. We will call such polynomials *minimally intersective*. Our proof also shows that once $a_1, a_2, \ldots, a_{n-1}$ are chosen, the set of natural numbers a_n such that the polynomial $f_n(x) := (x^2 - a_1)(x^2 - a_2)\cdots(x^2 - a_n)$ is minimally intersective has positive asymptotic density in $\mathbb{N}$.

1. Introduction

A set $S \subset \mathbb{Z}$ is called intersective if given any set T $\subset \mathbb{Z}$ with positive upper density, one has $S \cap (T-T) \not\subseteq \{0\}$. Given a $T \subset \mathbb{Z}$, $(T-T)$ is defined as $\{t_1 - t_2 : t_1, t_2 \in T\}$ and the upper density of T is defined as

$$\overline{d}(T) := \limsup_{n\to\infty} \frac{|T \cap \{-n, \ldots, -2, -1, 0, 1, 2, \ldots, n\}|}{2n+1}.$$

A polynomial $f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ is said to be intersective if the set of its values $\{f(x_1, \ldots, x_m) : x_1, \ldots, x_m \in \mathbb{Z}\}$ is intersective. Sárközy and Furstenberg independently and concurrently proved, in [9] and [3] respectively, that for any subset T of integers with positive upper density, the set $(T - T)$ contains a perfect square. In other words, they proved that the polynomial $f(x) = x^2$ is intersective.

Kamae and Mendés-France, in [6], showed that a polynomial f of one variable is intersective if and only if $f(x) \equiv 0 \pmod{m}$ is solvable for every positive integer $m > 1$. A very special case of the polynomial Szemerédi's theorem, obtained by Bergelson, Leibman and Lesigne in [2], generalizes this fact to the polynomials of many variables. Their result implies that a polynomial $g(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$

[1]The author was partly supported by the NSF, under grant DMS-1812028.

is intersective if and only if the congruence $g(n_1, n_2, \ldots, n_k) \equiv 0 \pmod{m}$ is solvable for every $m > 1$.

Berend and Bilu, in [1], obtained a criterion for any polynomial f of one variable to be intersective. An implication of their result is that any polynomial in one variable that is intersective, but has no rational root, has to be of degree greater than 4. On the other hand, there are single-variable intersective polynomials of degree greater than 4 that have no rational roots. Hyde, Lee and Spearman obtained an infinite family of intersective polynomials of the form

$$h(x) = (x^3 - n)(x^2 + 3),$$

none of which have rational roots [5]. One can easily show that if p, q are distinct odd primes such that $p \equiv q \equiv 1 \pmod{4}$ and $\left(\frac{p}{q}\right) = +1$ then the polynomial

$$f(x) = (x^2 - p)(x^2 - q)(x^2 - pq)$$

is intersective. Hyde and Spearman generalized this result to the case when p and q are replaced by square-free integers. Let c and d be square-free integers not equal to 1, let $c_1 = \frac{c}{\gcd(c,d)}$ and $d_1 = \frac{d}{\gcd(c,d)}$. Hyde and Spearman obtained necessary and sufficient conditions for the polynomial

$$p(x) = (x^2 - c)(x^2 - d)(x^2 - c_1 d_1)$$

to be intersective but have no rational root [4]. This result was extended in [7] by obtaining a necessary and sufficient condition for polynomials of the form

$$f(x) = (x^2 - a_1)(x^2 - a_2) \cdots (x^2 - a_n)$$

to be intersective without having a rational root (see Proposition 1 below). Here $n \geq 3$ and $a_1, a_2, \ldots, a_n$ are square-free integers not equal to 1.

Note that if $f(x)$ is an intersective polynomial then for every polynomial $g(x)$, $f(x)g(x)$ is also intersective. Therefore, one could always get more examples of intersective polynomials by multiplying a given intersective polynomial $f(x)$ by any polynomial $g(x)$. The topic of this article is to show the existence of, and construct, a particular type of intersective polynomial, which is defined below.

Definition 1. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be *minimally intersective* if it satisfies the following two conditions:

1. $f(x)$ is intersective but $f(x)$ does not have a rational root;
2. none of the proper divisors of $f(x)$ is intersective.

Minimally intersective polynomials can be thought of as genuinely new examples of intersective polynomials because they are not obtained by adjoining factors to

an already intersective polynomials. The result in this article shows that for every $n \geq 4$, there exist minimally intersective polynomials with n quadratic factors.

Given an integer n and a prime p we will denote the group of quadratic residues modulo p by Q_p and the Legendre symbol of n with respect to p by $\left(\frac{n}{p}\right)$. Similarly, $p^a \mid\mid n$ $(a \geq 1)$ will denote that p^a is the highest power of prime p dividing the integer n, (a, b) will denote the greatest common divisor of two natural numbers a and b, and $\text{rad}(x)$ will denote the square-free part of natural number x. The asymptotic density of a set $A \subset \mathbb{N}$ is defined as:

$$\lim_{n\to\infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n}.$$

Let p be an odd prime, $e \geq 1$ and $a \in \mathbb{Z}$ such that $p \nmid a$. Then a is a square modulo p^e if and only if $\left(\frac{a}{p}\right) = +1$. This fact is an immediate consequence of Hensel's lemma for the polynomial $(x^2 - a)$. The main result of this article is the following theorem.

Theorem 1. *For every $n \geq 4$, natural numbers $\{a_i\}_{i=1}^n$ can be chosen such that the polynomial $f_n(x) := (x^2 - a_1) \cdots (x^2 - a_n)$ is minimally intersective. In fact, once $a_1, a_2, \ldots, a_{n-1}$ are chosen, the set of natural numbers a_n for which $f_n(x)$ is minimally intersective, has positive asymptotic density.*

We will collect some preliminary results in Section 2. In Section 3, we shall describe a process to find square-free integers $a_1, \ldots, a_n$ that define the polynomials $f_n(x)$ for the corresponding $n \geq 4$. Section 4 contains proof that the polynomial $f_n(x)$ thus obtained is intersective. The proof that $f_n(x)$ is minimally intersective is contained in Section 5. Section 6 contains an explicit example of $f_4(x)$ and $f_5(x)$ each.

2. Preliminaries

We will repeatedly utilize the following characterization of intersectivity of polynomials consisting of quadratic factors that is proved in [7].

Proposition 1. *Let $n \geq 3$ and let $a_1, a_2, \ldots, a_n$ be distinct nonzero square-free integers, none of which is 1. Then the polynomial $f(x) = \prod_{i=1}^n (x^2 - a_i)$ is intersective if and only if the following conditions are satisfied.*

1. *There exists $T \subset \{1, 2, \ldots, n\}$ of odd cardinality such that:*
   (a) *the product $\prod_{j\in T} a_j$ is a perfect square, and*
   (b) *for every $j \in T$ and for every odd prime p dividing a_j, there exists $i \in \{1, \ldots, n\}$, $i \neq j$, such that $\left(\frac{a_i}{p}\right) = +1$.*

2. One of the a_i is of the form $8m+1$ for some $m \in \mathbb{Z}$ and $m \neq 0$.

We will also use the following classical result about distribution of square-free integers in an arithmetic progressions that was originally proved in [8].

Proposition 2. *Let $a, b \in \mathbb{N}$ such that (a, b) is square-free. Then the density of the set of square-free natural numbers congruent to b modulo a is $\frac{6}{\pi^2} \prod_{p|a} \left(1 - \frac{1}{p^2}\right)^{-1}$.*

For the sake of brevity, we will present the following elementary fact (without proof) as a lemma.

Lemma 1. *Let $n \geq 3$ and let $a_1, a_2, \ldots, a_n$ be distinct square-free nonzero integers, none of which is equal to 1. Then $\prod_{i=1}^{n} a_i$ is a perfect square if and only if for every $j \in \{1, 2, \ldots, n\}$, $a_j = rad\left(\prod_{i=1, i\neq j}^{n} a_i\right)$.*

Now we will state and prove some elementary number-theoretic lemmas that we shall repeatedly utilize in our proofs.

Lemma 2. *Let p be an odd prime and let $a \in \mathbb{Z}$ be a square-free integer. If $\left(\frac{a}{p}\right) \neq +1$ then a cannot be a square modulo p^2.*

Proof. If $p \nmid a$ then $\left(\frac{a}{p}\right) \neq +1$ implies that a cannot be a square modulo p^2. On the other hand, if $p \mid a$ then $p \mid\mid a$ because a is square-free.

Assume for the sake of contradiction that a is a square modulo p^2 , i.e., $x^2 \equiv a \pmod{p^2}$ for some $x \in \mathbb{Z}$. Then we have $p^2 \mid (x^2 - a)$, i.e., $p \mid (x^2 - a)$. Since $p \mid a$ and $p \mid (x^2 - a)$ we have that $p \mid x^2$ implying $p^2 \mid x^2$. However, $p^2 \mid (x^2 - a)$ and $p^2 \mid x^2$ gives that $p^2 \mid a$, contradicting that a is square-free. Therefore, a cannot be a square modulo p^2. □

Lemma 3. *Let $k, m \in \mathbb{N}$, let p be a prime and let $f(x) = \prod_{i=1}^{m}(x^2 - a_i) \in \mathbb{Z}[x]$. If $(x^2 - a_i) \equiv 0 \ (mod\, p^k)$ is not solvable for any $1 \leq i \leq m$ then $f(x) \equiv 0 \ (mod\, p^{km})$ is not solvable.*

Proof. For the sake of contradiction, assume that $f(x) \equiv 0 \pmod{p^{km}}$ is solvable for some $x \in \mathbb{Z}$, i.e., $p^{km} \mid (x^2 - a_1) \cdots (x^2 - a_m)$. Then we must have $p^k \mid (x^2 - a_j)$, for some $j \in \{1, 2, \ldots, m\}$.

However $p^k \mid (x^2 - a_j)$ implies that $(x^2 - a_j) \equiv 0 \pmod{p^k}$ is solvable, a contradiction to the fact that $(x^2 - a_i) \equiv 0 \pmod{p^k}$ is not solvable for any i. Therefore, we have the result. □

Lemma 4. *Let $k \geq 3$ and let $a_1, \ldots, a_k$ be distinct, nonzero square-free integers. Suppose that for each $1 \leq m \leq k$ and for every $T \subset \{1, 2, \ldots, m\}$, $a_m > rad\left(\prod_{j\in T, j\neq m} a_j\right)$. Then for any subset $S \subseteq \{1, 2, \ldots, k\}$, $\prod_{j\in S} a_j$ is not a perfect square.*

Proof. For the sake of contradiction, assume that there is an $S \subseteq \{1, 2, \ldots, k\}$ such that $\prod_{j \in S} a_j$ is a perfect square. Then using Lemma 1, we have that

$$a_{j_0} = \text{rad}\,\Big(\prod_{j \in S, j \neq j_0} a_j\Big),$$

where $j_0 = \max S$. This is a contradiction to our assumption for $m = j_0$ and $T = S \subset \{1, 2, \ldots, j_0\}$. Hence we have the result. □

3. Finding $a_1, a_2, \ldots, a_n$ such that $f_n(x) = \prod_{i=1}^{n}(x^2 - a_i)$

In this section, we will show the existence of natural numbers $a_1, a_2, \ldots, a_n$ that will define the polynomial $f_n(x) = (x^2 - a_1)(x^2 - a_2)\cdots(x^2 - a_n)$. Each of the integers $a_1, \ldots, a_n$ will be square-free and not equal to 1. They can be chosen in accordance with the following steps.

1. Pick distinct odd primes p_1 and p_2. For each $i = 1, 2$ pick nonzero elements $b_i, c_i \in \left(\mathbb{Z}/p_i\mathbb{Z}\right)^*$ such that $c_i \in Q_{p_i}$ $b_i \notin Q_{p_i}$. Set $a_1 = p_1 p_2$.

   We can choose a_1 as any square-free odd natural number that has at least two odd prime factors and choose p_1, p_2 as two odd primes dividing a_1. For the sake of brevity, we choose a_1 to be a product of two odd primes.

2. Pick square-free $a_2 \in \mathbb{N}$ such that $a_2 > a_1$ and $a_2 \equiv b_j \pmod{p_j}$ for $j = 1, 2$. Any integer a_2 satisfying $a_2 \equiv b_j \pmod{p_j}$ for $j = 1, 2$ above is unique modulo $p_1 p_2$, as a consequence of the Chinese remainder theorem.

   Since $p_1 \neq p_2$, we have that $p_1 p_2$ is square-free and hence infinitely many square-free a_2 exist, by Proposition 2. We pick a square-free a_2 greater than a_1. Also note that since $(b_j, p_j) = 1$ for every $j = 1, 2$ we have that $(a_2, p_j) = 1$ for $j = 1, 2$.

3. For any $i \leq n - 3$, after choosing $a_1, \ldots, a_{i-1}$, choose a square-free integer a_i such that:

   - $a_i \equiv b_j \pmod{p_j}$ for $j = 1, 2$ and
   - for every $A \subset \{1, \ldots, i - 1\}$, a_i is greater than the rad $\left(\prod_{j \in A} a_j\right)$.

   Exactly as in step 2, a square free a_i satisfying the above exists as a consequence of Proposition 2 and $(a_i, p_j) = 1$ for $j = 1, 2$.

4. Choose a square-free natural number a_{n-2} that satisfies the following requirements.

- $$a_{n-2} \equiv \begin{cases} b_1 \pmod{p_1}; & \text{if } n \text{ is even} \\ c_1 \pmod{p_1}; & \text{if } n \text{ is odd} \end{cases}$$
- $a_{n-2} \equiv b_2 \pmod{p_2}$
- a_{n-2} is greater than rad $\left(\prod_{j\in T} a_j\right)$, for any $T \subset \{1, \ldots, n-3\}$.

Such a square-free a_{n-2} exists, again due to Proposition 2. Similarly, we also have $(a_{n-2}, p_j) = 1$ for $j = 1, 2$.

5. Define a square-free natural number a_{n-1} as:

$$a_{n-1} = \begin{cases} \text{rad } \left(\prod_{i=1}^{n-2} a_j\right); & \text{if } n \text{ is even} \\ \text{rad } \left(\prod_{i=1}^{n-3} a_j\right); & \text{if } n \text{ is odd.} \end{cases}$$

6. Choose all the odd primes $p_1, \ldots, p_M$ dividing any of $a_1, \ldots, a_{n-1}$ and pick $c_j \in Q_{p_j}$ for every $1 \leq j \leq M$. Now, pick a square-free natural number a_n that satisfies the following.

   - $a_n \equiv c_j \pmod{p_j}$ for any $2 \leq j \leq M$
   - $$a_n \equiv \begin{cases} c_1 \pmod{p_1}; & \text{if } n \text{ is even} \\ b_1 \pmod{p_1}; & \text{if } n \text{ is odd} \end{cases}$$
   - $a_n \equiv 1 \pmod 8$
   - For any subset $S \subset \{1, 2, \ldots, n-1\}$, $a_n >$ rad $\left(\prod_{j\in S} a_j\right)$.

   Any integer a_{n_0} that satisfies the above conditions is unique modulo $(8p_1 \cdots p_M)$, as a consequence of the Chinese remainder theorem. In other words, if a_{n_0} satisfies above congruences then any integer in the arithmetic progression $\left(8p_1 \cdots p_M\right)\mathbb{N} + a_{n_0}\right)$ also satisfies those congruences.

   Since a_{n_0} is odd and $(c_i, p_i) = 1$ for $i = 1, 2, \ldots, M$, $\left(a_{n_0}, 8p_1 \cdots p_M\right)$ is square-free. Hence the set of square-free natural numbers a_n that satisfy above congruences is of positive density, as a consequence of Proposition 2. We choose a square-free a_n such that for any $S \subset \{1, 2, \ldots, n-1\}$:

$$a_n > \text{rad } \left(\prod_{j\in S} a_j\right)$$

7. Define $f_n(x) := (x^2 - a_1)(x^2 - a_2) \cdots (x^2 - a_n)$.

4. Proof that $f_n(x)$ is Intersective

In this section, we shall prove that $f_n(x)$ has roots modulo every integer, by showing that $f_n(x)$ satisfies the conditions in Proposition 1.

1. Condition 1(a) of Proposition 1 holds for $f_n(x)$ because $\prod_{j\in T} a_j$ is a perfect square, where

$$T = \begin{cases} \{1, 2, \ldots, n-2, n-1\} & ; \text{if } n \text{ is even} \\ \{1, 2, \ldots, n-4, n-3, n-1\} & ; \text{if } n \text{ is odd.} \end{cases}$$

   This follows from Step 5 of Section 3 and Lemma 1.

2. Let $j \in T$ and p be any odd prime dividing a_j, then from the step 6 of Section 3 it follows that $p = p_j$ for some $1 \leq j \leq M$. It also follows from steps 4 and 6 of Section 3 that:

$$\begin{cases} \left(\frac{a_n}{p}\right) = +1 & \text{if } j \neq 1 \text{ or } n \text{ is even} \\ \left(\frac{a_{n-2}}{p}\right) = +1 & \text{if } j = 1 \text{ and } n \text{ is odd.} \end{cases}$$

   Therefore the condition 1(b) of Proposition 1 is also satisfied for $f_n(x)$.

3. The condition 2 of the Proposition 1 is satisfied for $f_n(x)$ because a_n is chosen to be square-free and equivalent to 1 modulo 8 (in Step 6 of Section 3).

5. Proof that $f_n(x)$ is Minimally Intersective

In this section, we shall prove that if we remove any quadratic factors from $f_n(x)$, the resulting polynomial $g_n(x)$ will fail to be intersective. To show that $g_n(x)$ is not intersective, we will show that $g_n(x)$ fails to satisfy the necessary conditions in Proposition 1. We will separate the proofs into parts according to the quadratic factor that is being removed from $f_n(x)$.

- **Removing $(x^2 - a_r)$ for any $1 \leq r \leq (n-3)$**

  In Section 3, we chose the square-free integers $a_1, a_2 \ldots, a_{r-1}, a_{r+1}, \ldots, a_{n-2}, a_n$ such that they satisfy the assumption of Lemma 4. Therefore, for any subset $S \subset \{1, 2, \ldots, r-1, r+1, \ldots, n-2, n\}$, $\prod_{j\in S} a_j$ cannot a perfect square.

  Hence, if there exists a set $S \subset \{1, 2, \ldots, r-1, r+1, \ldots, n\}$ such that $\prod_{j\in S} a_j$ is a perfect square, then $(n-1) \in S$. If $n \in S$, then by Lemma 1, we must have that $a_n = \text{rad}\left(\prod_{j\in S, j\neq n} a_j\right)$, which is a contradiction to the way a_n was chosen in the step 6 of Section 3.

Therefore $n-1 = \max S$ and by Lemma 1 we have that

$$a_{n-1} = \text{ rad } \Big(\prod_{j \in S, j \neq (n-1)} a_j \Big).$$

This, along with Step 5 of Section 3 implies

$$\text{rad } \Big(\prod_{j \in S, j \neq (n-1)} a_j \Big) = \begin{cases} \text{rad } \left(\prod_{i=1}^{n-2} a_j \right) & ; \text{if } n \text{ is even} \\ \text{rad } \left(\prod_{i=1}^{n-3} a_j \right) & ; \text{if } n \text{ is odd.} \end{cases}$$

Hence we obtain that

$$\begin{cases} \prod_{j \in S, j \neq (n-1)} a_j \times \prod_{i=1}^{n-2} a_j \text{ is a perfect square} & ; \text{if } n \text{ is even} \\ \prod_{j \in S, j \neq (n-1)} a_j \times \prod_{i=1}^{n-3} a_j \text{ is a perfect square} & ; \text{if } n \text{ is odd.} \end{cases}$$

Since $r \notin S$ but $r \in \{1, 2, \ldots, n-3\}$, the two factors above are not equal, regardless of whether n is odd or even. Therefore, we could disregard all a_j appearing in both the multiplicands above.

After disregarding the common a_j appearing in both the multiplicands, we are still left with a product of distinct a_j that is a perfect square. Let r_0 be the largest such that a_{r_0} remaining in this product. Then using Lemma 1 we have that

$$a_{r_0} = \text{ rad } \left(a_{j_1} \times \cdots \times a_{j_l} \right),$$

where $j_1, \ldots, j_l \in \{1, 2, \ldots, r_0 - 1\}$. Since a_{r_0} was chosen from the product of a_j with $j \leq n-2$, we have that $r_0 \leq n-2$. This is a contradiction to how $a_1, a_2, \ldots, a_{n-2}$ were chosen in Steps 1, 2, 3 and 4 of Section 3. Specifically, for $i \leq n-2$, we had chosen a_i to be greater than the square-free part of any sub-product of $a_1, \ldots, a_{i-1}$.

Therefore if we remove $(x^2 - a_r)$ for any $1 \leq r \leq (n-3)$ then for the resulting polynomial $g_n(x) := \frac{f_n(x)}{(x^2 - a_r)}$, the condition $1(a)$ of Proposition 1 will not be satisfied. Hence, $g_n(x)$ is not intersective.

- **Removing $(x^2 - a_{n-2})$ from $f_n(x)$**

  If n is even, then removing $(x^2 - a_{n-2})$ from $f_n(x)$ will again result in a polynomial $g_n(x) := \frac{f_n(x)}{(x^2 - a_{n-2})}$ not satisfying the condition $1(a)$ of Proposition 1. The proof of this is exactly analogous to the previous case of removing $(x^2 - a_r)$ for $1 \leq r \leq (n-3)$. Therefore, we assume that n is odd.

  – Since $\left(\frac{a_1}{p_1}\right) = 0 \neq +1$, $(x^2 - a_1) \equiv 0 \pmod{p_1^2}$ is not solvable. This follows from Lemma 2.

- Since for any $2 \leq i \leq n-3$ or $i = n$ $\left(\frac{a_i}{p_1}\right) = -1 \neq +1$ from step 2, 3 and 6 of Section 3, $(x^2 - a_i) \equiv 0 \pmod{p_1^2}$ is not solvable . This again follows from Lemma 2.
- $(x^2 - a_{n-1}) \equiv 0 \pmod{p_1^2}$ is not solvable because $\left(\frac{a_{n-1}}{p_1}\right) = 0 \neq +1$. This follows from Lemma 2 again.

So for the resulting polynomial

$$g_n(x) = (x^2 - a_1) \cdots (x^2 - a_{n-3})(x^2 - a_{n-1})(x^2 - a_n)$$

the congruence

$$g_n(x) \equiv 0 \pmod{p_1^{2(n-1)}}$$

is not solvable. This last assertion follows from Lemma 3 for $k = 2$, $m = (n-1)$ and $p = p_1$. Hence, $g_n(x)$ is not intersective.

- **Removing $(x^2 - a_{n-1})$ from $f_n(x)$**

In this case, we note that $a_1, \ldots, a_{n-2}, a_n$ satisfies the hypothesis of Lemma 4 and hence for every subset $S \subset \{1, 2, \ldots, n-2, n\}$, the product $\prod_{j \in S} a_j$ is not a perfect square.

Therefore the polynomial $g_n(x) := \frac{f_n(x)}{(x^2 - a_{n-1})}$ does not satisfy the condition $1(a)$ of Proposition 1 and hence is not intersective.

- **Removing $(x^2 - a_n)$ from $f_n(x)$**

If n is even, then note the following.

- Since $\left(\frac{a_1}{p_1}\right) = 0 \neq +1$, $(x^2 - a_1) \equiv 0 \pmod{p_1^2}$ is not solvable. This follows from Lemma 2.
- Since for any $2 \leq i \leq n-2$ $\left(\frac{a_1}{p_1}\right) = -1 \neq +1$ from step 3 and 4 of Section 3, $(x^2 - a_i) \equiv 0 \pmod{p_1^2}$ is not solvable . This follows again from Lemma 2.
- $(x^2 - a_{n-1}) \equiv 0 \pmod{p_1^2}$ is not solvable because $\left(\frac{a_{n-1}}{p_1}\right) = 0 \neq +1$. This follows again from Lemma 2.

Therefore, for the resulting polynomial $g_n(x) = (x^2 - a_1) \cdots (x^2 - a_{n-2})(x^2 - a_{n-1})$ we have that the congruence

$$g_n(x) \equiv 0 \pmod{p_1^{2(n-1)}}$$

is not solvable This last assertion follows from Lemma 3 for $k = 2$, $m = (n-1)$ and $p = p_1$; hence, $g_n(x)$ is not intersective.

If n is odd, then we have the following implications.

- Since $\left(\frac{a_1}{p_2}\right) = 0 \neq +1$, $(x^2 - a_1) \equiv 0 \pmod{p_2^2}$ is not solvable. This follows from Lemma 2.
- Since for any $2 \leq i \leq n-2$ $\left(\frac{a_1}{p_2}\right) = -1 \neq +1$ from step 3 and 4 of Section 3, $(x^2 - a_i) \equiv 0 \pmod{p_2^2}$ is not solvable. This follows again from Lemma 2.
- $(x^2 - a_{n-1}) \equiv 0 \pmod{p_2^2}$ is not solvable because $\left(\frac{a_{n-1}}{p_2}\right) = 0 \neq +1$. This follows again from Lemma 2.

Therefore, when n is odd, for the resulting polynomial

$$g_n(x) = (x^2 - a_1) \cdots (x^2 - a_{n-2})(x^2 - a_{n-1})$$

we have that the congruence

$$g_n(x) \equiv 0 \pmod{p_2^{2(n-1)}}$$

is not solvable. This last assertion again follows from Lemma 3 for $k = 2$, $m = (n-1)$ and $p = p_2$; hence $g_n(x)$ is not intersective.

6. Some Examples

We shall construct an explicit example of minimally intersective $f_4(x)$ and then another of a minimally intersective $f_5(x)$.

6.1. An Example of Minimally Intersective $f_4(x)$

1. We pick $p_1 = 3$ and $p_2 = 5$. And, we pick $c_1 = 1 \in Q_3$, $b_1 = 2 \notin Q_3$, $c_2 = 1 \in Q_5$ and $b_2 = 2 \notin Q_5$. We define $a_1 = p_1 p_2 = 15$.
2. Now we pick a square-free integer $a_2 > 15$ such that $a_2 \equiv 2 \pmod 3$ and $a_2 \equiv 2 \pmod 5$. We pick $a_2 = 17$.
3. Since $n = 4$ is even and $n - 1 = 3$, we take $a_3 = \text{rad}\ (a_1 \times a_2) = \text{rad}\ (15 \times 17) = 255$.
4. Now we take all the primes $p_1 = 3, p_2 = 5, p_3 = 17$ that divides any one of the a_1, a_2, a_3. Then for every $1 \leq j \leq 3$, we take $c_j \in Q_{p_j}$. Here we take $c_1 = 1$, $c_2 = 1$ and $c_3 = 2$.

   Then we solve for a square-free a_4 such that $a_4 > \text{rad}\ (\prod_J a_j)$ for every $J \subseteq \{1, 2, 3\}$, $a_4 \equiv c_j \pmod{p_j}$ for every $j = 1, 2, 3$ and $a_4 \equiv 1 \pmod 8$.

   By Proposition 2, infinitely many such square-free a_4 exists. We choose $a_4 = 2161$, which is a prime and hence square-free. Therefore,

$$f_4(x) = (x^2 - 15)(x^2 - 17)(x^2 - 255)(x^2 - 2161)$$

   is minimally intersective.

6.2. An Example of Minimally Intersective $f_5(x)$

1. As in 6.1, take $p_1 = 3$, $p_2 = 5$, $c_1 = 1 \in Q_3$, $c_2 = 1 \in Q_5$, $b_1 = 2 \notin Q_3$, $b_2 = 2 \notin Q_5$, $a_1 = 15$ and $a_2 = 17$.

2. Pick a square-free integer $a_3 > 15 \times 17 = 255$ such that $a_2 \equiv 2 \pmod 3$ and $a_2 \equiv 2 \pmod 5$. We choose $a_3 = 557$, which is a prime and hence square-free.

3. Define a_4 to be rad $(a_1 \times a_2) = 15 \times 17 = 255$ and hence $a_4 = 255$.

4. Pick all the odd primes $p_1 = 3, p_2 = 5, p_3 = 17, p_4 = 557$ that divide any one of the a_1, a_2, a_3, a_4. Then take $c_1 = 1$, $c_2 = 1$, $c_3 = 2$ and $c_4 = 6$ which are in Q_{p_j} for $j = 1, 2, 3, 4$ respectively.

   Now choose a square-free a_5 such that $a_5 > \prod_J a_j$ for all $J \subset \{1, 2, 3, 4\}$, $a_5 \equiv c_j \pmod{p_j}$ for $j = 1, 2, 3, 4$ and $a_5 \equiv 1 \pmod 8$.

   Any such a_5 has to be of the form $587641 + 142035k$ for some $k \in \mathbb{Z}$. We take $a_5 = 587641 + 142035(2) = 871711$, which is square-free since its prime-factorization is 29×30059. Therefore,

$$f_5(x) = (x^2 - 15)(x^2 - 17)(x^2 - 557)(x^2 - 255)(x^2 - 871711)$$

   is minimally intersective.

References

[1] D. Berend and Y. Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.* **124** (1996), 1663–1671.

[2] V. Bergelson, A. Leibman and E. Lesigne, Intersective polynomials and polynomial Szemerédi theorem, *Adv. Math.* **219** (2008), 369–388.

[3] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. d'Analyse Math.* **71** (1977), 204–256.

[4] A. M. Hyde and B. K. Spearman, Products of quadratic polynomials with roots modulo any integer, *Int. Math. Forum.* **8** (2013), 1225–1231.

[5] A. M. Hyde, D. P. Lee and B. K. Spearman, Polynomials $(x^3 - n)(x^2 + 3)$ solvable modulo any integer, *Amer. Math. Monthly.* **121** (2014), 355–358.

[6] T. Kamae and M. Mendés-France, Van der Corput's difference theorem, *Israel. J. Math.* **31** (1978), 335–342.

[7] B. Mishra, Polynomials consisting of quadratic factors with roots modulo any positive integer, *To Appear in Amer. Math. Monthly* (Accepted 02.24.2021), `https://arxiv.org/abs/2102.08379v1`.

[8] K. Prachar, Uber die kleinste quadratfreie einer arithmetischen reihe, *Monatsh. Math.* **62** (1958), 173–176.

[9] A. Sárközy, On difference sets of sequences of integers, I, *Acta. Math. Acad. Sci. Hungar.* **31** (1978), 125–149.