Products of Values of Polynomials in Finite Fields

Xingyan(Summer) Zhou

Under the direction of

Rachana Madhukara and Alan Peng
MIT Mathematics

Research Science Institute
August 2, 2022

Abstract

In this paper we study products of quadratic and cubic polynomials in finite fields. We expand on the result of Sun in 2019 which determined $\prod_{1\leq i<j\leq \frac{p-1}{2}}(i^2+j^2)$ for prime $p \equiv 1 \pmod 4$, and generalize it to arbitrary finite fields of odd order. Then, we look at product of polynomials in the form of the sum of two cubics, and determine completely the product $\prod_{\substack{1\leq i<j\leq p-1,\\ i^3+j^3\neq 0}}(i^3+j^3)$.

We are also interested in a natural generalization of the original equation in quadratics to the cubics. For $p \geq 5$, we examine the nontrivial case when $p \equiv 1 \pmod 3$, and for $S = \{a^3 \mid a \in \mathbb{F}_p \text{ and } a \neq 0\}$ we evaluate the product $\prod_{\substack{i<j\in S\\ i+j\neq 0}}(i+j)$.

Summary

This paper continues the mathematical tradition of examining products of polynomials. We first generalize a result determining product of values of polynomials proven by Sun in 2019 to a less restricted range. And then, we consider two variations of the product of values of $i^3 + j^3$. The first traverse all ordered pairs of $\{i, j\}$ in modulo p with $i \neq j$, the second considers the sum of ordered pairs of distinct cubic.

1 Introduction

Fermat's little theorem (1640) evaluates $\prod_{1\le x\le p-1} a$, a product over the constant polynomial a (typically expressed as $a^{p-1} \pmod p$ for $a \neq 0$ in $\mathbb{F}_p$). Similarly, Wilson's theorem (1771), evaluates a product over the linear polynomial x, $\prod_{1\le x\le p-1} x$, more frequently expressed as $(p-1)! \pmod p$.

Extending this line of work, the Euler's criterion evaluates $\prod_{1\le i\le \frac{p-1}{2}}(a) \pmod p$. Gauss's lemma evaluates $\prod_{1\le i\le \frac{p-1}{2}}(ai) \pmod p$, underpinning many theorems of quadratic reciprocity. Continuing the trend, in 1961, Chowla and Mordell[1] computed the product $\prod_{1\le x\le \frac{p-1}{2}}(x) \pmod p$ for $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, respectively.

More recently, in 2019, Sun [2] demonstrated an elegant expression of the following product:

Theorem 1.1. *In the prime finite field $\mathbb{F}_p$,*

$$\prod_{1\le i<j\le \frac{p-1}{2}} (i^2+j^2) = \begin{cases} (-1)^{\lfloor \frac{p-5}{8} \rfloor} \text{ if } p \equiv 1 \pmod 4, \\ (-1)^{\lfloor \frac{p+1}{8} \rfloor} \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. For $p \equiv 1 \pmod 4$, see Sun's Theorem 1.2 in 2019 [2]. For $p \equiv 3 \pmod 4$, see Problem N.2 of [Sz, pp. 364-365] [3] . □

It is then natural to ask how results from prime finite fields can be extended to arbitrary finite fields. Theorem 1.2 provides an analogy of Theorem 1.1 for arbitrary finite fields.

Theorem 1.2. *Let $\mathbb{F}_q$ be a finite field for an odd q, with $q = p^r$ for a prime p. Then, for $S = \{a^2 \mid a \in \mathbb{F}_q \text{ and } a \neq 0\}$,*

$$\prod_{\substack{\{i,j\}\subseteq S,\\ i+j\neq 0}} (i+j) = (-1)^{r(\frac{p^2-1}{8})\cdot\frac{q+1}{2}+\lfloor\frac{q+1}{8}\rfloor+\frac{q+1}{2}}.$$

Besides expanding the polynomial from prime fields to arbitrary finite field, we also consider further results in another direction by replacing the quadratic terms in the product with cubic terms. We find a result for the product of sums of elements from 1 to $p-1$ raised to the cubic in Theorem 1.3.

Theorem 1.3. *For a prime $p \geq 5$,*

$$\prod_{\substack{1 \leq i < j \leq p-1, \\ i^3 + j^3 \neq 0}} (i^3 + j^3) \equiv \left(\frac{3}{p}\right) \pmod{p}$$

Theorem 1.4 calculates the product of the sum of pairs of cubics in $\mathbb{F}_p$, which differs from Theorem 1.3 as different elements raised to the third might produce the same cubic.

Theorem 1.4. *For prime $p \geq 5$ and $p \equiv 1 \pmod 3$, let $S = \{a^3 \mid a \in \mathbb{F}_p \text{ and } a \neq 0\}$*

$$\prod_{\substack{i<j \subseteq S \\ i+j \neq 0}} (i+j) = \pm \left(\frac{1}{6}\right)^{\frac{p-1}{3}}.$$

In Section 2, we present the preliminary definitions and notations. In Section 3, we provide the proof of Theorem 1.2. In section 4, we provide the proof of Theorem 1.3. In Section 5, we provide the proof of Theorem 1.4.

2 Preliminaries

We first introduce the Legendre symbol $\left(\frac{a}{p}\right)$ is used to examine whether an integer is a quadratic residue modulo p.

Definition 2.1. For a prime p and $0 \leq a \leq p-1$, let

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 0 & \text{if } a \mid p, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Extending this to general finite fields, we define the symbol $\left(\frac{a}{\mathbb{F}_q}\right)$ as follows.

Definition 2.2.

$$\left(\frac{a}{\mathbb{F}_q}\right) \coloneqq \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \text{ is a quadratic residue in } \mathbb{F}_q, \\ -1 & \text{if } a \text{ is a quadratic nonresidue in } \mathbb{F}_q. \end{cases}$$

The lemma following this new notation is a standard result following the observation that the multiplicative group $\mathbb{F}_q^\times$ is cyclic.

Lemma 2.1. *If q is odd, then*

$$\left(\frac{a}{\mathbb{F}_q}\right) = a^{\frac{q-1}{2}}$$

.

in $\mathbb{F}_q$ for all $a \in \mathbb{F}_q$

3 Proof of Theorem 1.2

In this section, we fix an odd prime power $q = p^r$ for a prime p and consider the finite field $\mathbb{F}_q$. We begin by establishing an auxiliary lemma.

Lemma 3.1. *In $\mathbb{F}_q$, for all $a \in \mathbb{F}_p$,*

$$\left(\frac{a}{\mathbb{F}_q}\right) = \left(\frac{a}{p}\right)^r.$$

Proof. By Lemma 2.1,

$$\left(\frac{a}{\mathbb{F}_q}\right) = a^{\frac{q-1}{2}} = a^{\frac{p^r-1}{2}} = (a^{\frac{p-1}{2}})^{1+p+p^2+\cdots+p^{r-1}}.$$

Since $a \in \mathbb{F}_p$, we know that $a^{\frac{p-1}{2}} = \pm 1$, thus, the sign of the above only depends on the

parity of $1+p+p^2+\cdots+p^{r-1}$. Since p is odd, the parity of $1+p+p^2+\cdots+p^{r-1}$ matches that of r. Thus the above equals to

$$(a^{\frac{p-1}{2}})^r = \left(\frac{a}{p}\right)^r.$$

□

Lemma 3.2 (Berndt, Evans, Williams [4])**.** *In finite field* $\mathbb{F}_q$*,*

$$\sum_{x\in\mathbb{F}_q}\left(\frac{x^2+\alpha x+\beta}{\mathbb{F}_q}\right) = \begin{cases} -1 & \text{if } p \nmid \alpha^2-4\beta, \\ q-1 & \text{if } p \mid \alpha^2-4\beta. \end{cases}$$

Lemma 3.3. *For* $a,b,c\in\mathbb{F}_q$ *with* a *or* b *nonzero, we have that*

$$\sum_{x\in\mathbb{F}_q}\left(\frac{ax^2+bx+c}{\mathbb{F}_q}\right) = \begin{cases} -\left(\frac{a}{\mathbb{F}_q}\right) & \text{if} \quad b^2-4ac\neq 0, \\ (q-1)\left(\frac{a}{\mathbb{F}_q}\right) & \text{if} \quad b^2-4ac=0. \end{cases}$$

Proof. Here we prove a generalization of Lemma 3.2.

If $a=0$, then $b\neq 0$, then $\sum_{x\in\mathbb{F}_q}\left(\frac{bx+c}{\mathbb{F}_q}\right)$ is equivalent to $\sum_{x\in\mathbb{F}_q}\left(\frac{x}{\mathbb{F}_q}\right)$. It is a standard result that since there are $\frac{q-1}{2}$ quadratics and $\frac{q-1}{2}$ nonquadratics in $\mathbb{F}_q$, the sum of all Legendre symbols in $\mathbb{F}_q$ is 0 as sought.

For $a\neq 0$, we use Lemma 3.2 to arrive at

$$\sum_{x\in\mathbb{F}_q}\left(\frac{ax^2+bx+c}{\mathbb{F}_q}\right) = \left(\frac{a}{\mathbb{F}_q}\right)\sum_{x\in\mathbb{F}_q}\left(\frac{x^2+\frac{b}{a}ax+\frac{c}{a}}{\mathbb{F}_q}\right).$$

Thus, we multiply $\left(\frac{a}{\mathbb{F}_q}\right)$ into the results in Lemma 3.2 to arrive at Lemma 3.3.

□

Lemma 3.4. *For* $n\in\mathbb{F}_q$*, let* $S \coloneqq \{a^2 | a\in\mathbb{F}_q \text{ and } a\neq 0\}$

$$m(n) := |\{(j,k) \mid \{j,k\}\in\mathbb{F}_q, j\neq k \text{ and } j+k=n\}| \quad .$$

Then,

$$m(0) = \begin{cases} 0 & \text{if} \quad q \equiv 3 \pmod 4, \\ \frac{q-1}{4} & \text{if} \quad q \equiv 1 \pmod 4, \end{cases}$$

and for $n \neq 0$,

$$m(n) = \left\lfloor \frac{q+1}{8} \right\rfloor - \frac{1 + \left(\frac{2}{\mathbb{F}_q}\right)}{2} \frac{1 + \left(\frac{n}{\mathbb{F}_q}\right)}{2}.$$

The proof follows that of Sun's Lemma 2.3 in 2019, which proves the result for when q is prime [2], as illustrated below.

Proof. First consider the case when $n = 0$:

If $q \equiv 3 \pmod 4$, then $\left(\frac{-1}{\mathbb{F}_q}\right) = -1$ according to Lemma 2.1. Since $a^2 = -b^2$, $\left(\frac{a^2}{\mathbb{F}_q}\right) = \left(\frac{-1}{\mathbb{F}_q}\right)\left(\frac{b^2}{\mathbb{F}_q}\right)$ which means $\left(\frac{a}{\mathbb{F}_q}\right)^2 = -1$, contradiction. Thus, $m(0) = 0$.

If $q \equiv 1 \pmod 4$, then $\left(\frac{-1}{\mathbb{F}_q}\right) = 1$, which means $a^2 + b^2 = 0$ so let $a = jb$ for some j such that $j^2 = -1$. There are $2(q-1)$ ordered pairs (a, b); divided by 2 for the cases $a^2 = (-a)^2$, divided by 2 for the cases $b^2 = (-b)^2$, divided by 2 for the cases $\{a, b\} = \{b, a\}$, which gives us $\frac{q-1}{4}$ pairs. Note that there are no ordered pairs (a, b) with $a^2 + b^2 = 0$, $a, b \neq 0$, $a = b$.

Now consider the case for $n \neq 0$:

$$\begin{aligned} &|\{(j,k) \mid j,k \in S \text{ and } j + k = n\}| \\ &\qquad = 2m(n) + |\{j \mid j \neq 0 \text{ and } j \in S \text{ and } 2j = n\}| \\ &\qquad = 2m(n) + \frac{1 + \left(\frac{\frac{n}{2}}{\mathbb{F}_q}\right)}{2}. \end{aligned} \tag{1}$$

Whether $\frac{n}{2}$ is a quadratic is equivalent to whether $2n$ is a quadratic since 4 is a quadratic. Thus, we have the above equals to

$$m(n) + \frac{1 + \left(\frac{2n}{\mathbb{F}_q}\right)}{2}.$$

Now we examine the first part of the equation. We rephrase equation 1 as follows.

$$|\{(j,k) \mid j,k \in S \text{ and } j+k=n\}| = |\{x \in \mathbb{F}_q \mid \left(\frac{x}{\mathbb{F}_q}\right) = 1 \text{ and } \left(\frac{n-x}{\mathbb{F}_q}\right) = 1\}|$$

Notice that when $\left(\frac{x}{\mathbb{F}_q}\right) = 1$, $\frac{1+\left(\frac{x}{\mathbb{F}_q}\right)}{2}$ is also one; when the Legendre symbol is -1, $\frac{1+\left(\frac{x}{\mathbb{F}_q}\right)}{2} = 0$, which gives us a way to add up all elements with $\left(\frac{x}{\mathbb{F}_q}\right) = 1$. With this, the above equation equals to

$$\begin{aligned}
&= \sum_{x \in \mathbb{F}_q^\times} \frac{1+\left(\frac{x}{\mathbb{F}_q}\right)}{2} \frac{1+\left(\frac{n-x}{\mathbb{F}_q}\right)}{2} - \frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{4} \\
&= \frac{q-1}{4} + \sum_{x \in \mathbb{F}_q^\times} \frac{\left(\frac{x}{\mathbb{F}_q}\right)}{4} + \sum_{x \in \mathbb{F}_q^\times} \frac{\left(\frac{n-x}{\mathbb{F}_q}\right)}{4} + \left(\sum_{x \in \mathbb{F}_q^\times} \frac{\left(\frac{nx-x^2}{\mathbb{F}_q}\right)}{4}\right) - \frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{4} \\
&= \frac{q-1}{4} + \sum_{x \in \mathbb{F}_q} \frac{\left(\frac{x}{\mathbb{F}_q}\right)}{4} + \left(\sum_{x \in \mathbb{F}_q^\times} \frac{\left(\frac{n-x}{\mathbb{F}_q}\right)}{4}\right) - \frac{\left(\frac{n}{\mathbb{F}_q}\right)}{4} + \left(\sum_{x \in \mathbb{F}_q^\times} \frac{\left(\frac{nx-x^2}{\mathbb{F}_q}\right)}{4}\right) - \frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{4}.
\end{aligned}$$

Now, by Lemma 3.3,

$$\sum_{x \in \mathbb{F}_q} \left(\frac{x}{\mathbb{F}_q}\right) = \sum_{x \in \mathbb{F}_q} \left(\frac{n-x}{\mathbb{F}_q}\right) = 0$$

and

$$\sum_{x \in \mathbb{F}_q} \left(\frac{nx-x^2}{\mathbb{F}_q}\right) = -\left(\frac{-1}{\mathbb{F}_q}\right).$$

Thus,

$$\begin{aligned}
|\{(j,k) \mid j,k \in S \text{ and } j+k=n\}| &= \frac{q-1}{4} - \frac{\left(\frac{n}{\mathbb{F}_q}\right)}{4} + \frac{-\left(\frac{-1}{\mathbb{F}_q}\right)}{4} - \frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{4} \\
&= \frac{q-\left(\frac{-1}{\mathbb{F}_q}\right)}{4} - \frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{2}.
\end{aligned}$$

We finally have

$$2m(n) = \frac{q - \left(\frac{-1}{\mathbb{F}_q}\right)}{4} - \frac{1 + \left(\frac{n}{\mathbb{F}_q}\right)}{2} - \frac{1 + \left(\frac{2n}{\mathbb{F}_q}\right)}{2},$$

$$\text{so} \quad m(n) = \frac{q - (-1)^{\frac{q-1}{2}}}{8} - \frac{1 + \left(\frac{n}{\mathbb{F}_q}\right)}{4} - \frac{1 + \left(\frac{2n}{\mathbb{F}_q}\right)}{4}$$

$$= \frac{q - (-1)^{\frac{q-1}{2}}}{8} - \frac{1 + \left(\frac{n}{\mathbb{F}_q}\right)}{4} - \frac{1 + \left(\frac{2n}{\mathbb{F}_q}\right)}{4}.$$

$$= \frac{q - (-1)^{\frac{q-1}{2}}}{8} + \frac{\left(\frac{2}{\mathbb{F}_q}\right) - 1}{4} - \frac{1 + \left(\frac{2}{\mathbb{F}_q}\right) + \left(\frac{n}{\mathbb{F}_q}\right) + \left(\frac{2n}{\mathbb{F}_q}\right)}{4}.$$

Applying Lemma 3.1, the above equals

$$\frac{q - (-1)^{\frac{q-1}{2}} - 2 + 2\left(\frac{2}{p}\right)^r}{8} - \frac{1 + \left(\frac{n}{\mathbb{F}_q}\right)}{2}\frac{1 + \left(\frac{2}{\mathbb{F}_q}\right)}{2} \tag{2}$$

Simplifying the first term in 2, we can list out the first term's value for different values of $p \pmod 4$ and $r \pmod 2$:

	$r \equiv 0 \pmod 2$	$r \equiv 1 \pmod 2$
$p \equiv 1 \pmod 8$	$\frac{q-1}{8}$	$\frac{q-1}{8}$
$p \equiv 3 \pmod 8$	$\frac{q-1}{8}$	$\frac{q-3}{8}$
$p \equiv 5 \pmod 8$	$\frac{q-1}{8}$	$\frac{q-5}{8}$
$p \equiv 7 \pmod 8$	$\frac{q-1}{8}$	$\frac{q+1}{8}$

Considering all cases, we see that the value of the first term can be expressed as $\lfloor \frac{q+1}{8} \rfloor$. □

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. We rephrase the problem of finding the product of all $i + j$ to the product of n to the power of number of (i, j)'s such that $i + j = n$ for all possible sums n, which gives us

$$\prod_{\substack{\{i,j\} \in S, \\ i \neq j, \\ i+j \neq 0}} (i + j) = \prod_{n \in \mathbb{F}_q^\times} n^{m(n)}. \tag{3}$$

Then, applying Lemma 3.4, equation 3 equals to

$$\begin{aligned}&\prod_{n\in\mathbb{F}_q^\times} n^{\lfloor\frac{q+1}{8}\rfloor-\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}\frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{2}}\\&=\prod_{n\in\mathbb{F}_q^\times} n^{\lfloor\frac{q+1}{8}\rfloor}\prod_{n\in\mathbb{F}_q^\times} n^{-\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}\frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{2}}\end{aligned}\tag{4}$$

Notice that $\prod_{n\in\mathbb{F}_q^\times} n=-1$, which means equation 4 equals to

$$(-1)^{\lfloor\frac{q+1}{8}\rfloor}\prod_{n\in\mathbb{F}_q^\times} n^{-\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}\frac{1+\left(\frac{n}{\mathbb{F}_q}\right)}{2}}.\tag{5}$$

For the cases when $\left(\frac{n}{\mathbb{F}_q}\right)=-1$, the value of n to the power 0 is just 1, which means we only care about the cases when $\left(\frac{n}{\mathbb{F}_q}\right)=1$, which means equation 5 equals to

$$\begin{aligned}&(-1)^{\lfloor\frac{q+1}{8}\rfloor}\left(\prod_{n\in S} n^{\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}}\right)^{-1}\\&=(-1)^{\lfloor\frac{q+1}{8}\rfloor}\left(\prod_{n\in S} n^{\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}}\right)\end{aligned}\tag{6}$$

Every element in S has an inverse different from itself besides 1 or -1, which means $\prod_{n\in S}=-\left(\frac{-1}{\mathbb{F}_q}\right)=(-1)^{\frac{q+1}{2}}$ Thus, equation 6 equals

$$\begin{aligned}&=(-1)^{\lfloor\frac{q+1}{8}\rfloor}(-1)^{\frac{1+\left(\frac{2}{\mathbb{F}_q}\right)}{2}\cdot\frac{q+1}{2}}\\&=(-1)^{\lfloor\frac{q+1}{8}\rfloor}(-1)^{\frac{1+\left(\frac{2}{p}\right)^r}{2}\cdot\frac{q+1}{2}}\end{aligned}\tag{7}$$

Notice that $(-1)^{\frac{1+\left(\frac{2}{p}\right)^r}{2}}=-\left(\frac{2}{p}\right)^r$, so we can simplify equation 7 as

$$\begin{aligned}&(-1)^{\lfloor\frac{q+1}{8}\rfloor}\left(\frac{2}{p}\right)^{r\cdot\frac{q+1}{2}}\cdot(-1)^{\frac{q+1}{2}}\\&=(-1)^{\lfloor\frac{q+1}{8}\rfloor}(-1)^{r(\frac{p^2-1}{8})\cdot\frac{q+1}{2}}\cdot(-1)^{\frac{q+1}{2}}\\&=(-1)^{r(\frac{p^2-1}{8})\cdot\frac{q+1}{2}+\lfloor\frac{q+1}{8}\rfloor+\frac{q+1}{2}}.\end{aligned}$$

□

4 Proof of Theorem 1.3

In this section, instead of examining the value of $i^2 + j^2$, we extend our search to the cubic, looking at the values of $i^3 + j^3$ in finite fields. This section we prove Theorem 1.3.

Proof of Theorem 1.3. Notice that

$$\prod_{\substack{1\le i<j\le p-1\\ i^3+j^3\neq 0}} (i^3+j^3) = \prod_{\substack{1\le i<j\le p-1\\ i^3+j^3\neq 0}} (i+j) \prod_{\substack{1\le i<j\le p-1\\ i^3+j^3\neq 0}} (i^2-ij+j^2). \tag{8}$$

Now we consider each part separately.

$$\prod_{\substack{1\le i<j\le p-1,\\ i^3+j^3\neq 0}} (i+j) = \prod_{\substack{1\le i<j\le p-1,\\ i+j\neq 0,\\ i^2-ij+j^2\neq 0}} (i+j).$$

Fix a nonzero $n \in \mathbb{F}_p$. For the equation $i + j = n$, we know that there is one corresponding j for every i from 1 to p, constituting p pairs of (i, j). Out of these p pairs, there is one such that $i = j$, and there are two pairs with 0 involved, which are $(0, n)$ and $(n, 0)$. Excluding these three cases and dividing by 2 give us the total pairs of unordered (i, j) such that $i + j = n$ and $i, j \neq 0$ and $i < j$, which is $\frac{p-3}{2}$.

To exclude the cases $i + j = n$ and $i^2 - ij + j^2 = 0$, we suppose $i^2 - ij + j^2 = 0$. Then, substituting $j = n - i$ we have:

$$\begin{aligned} i^2 - (n-i)i + (n-i)^2 &= 0 \\ \implies 3i^2 + n^2 - 3ni &= 0 \\ \implies 3(i - \frac{n}{2})^2 + (\frac{1}{2}n)^2 &= 0 \\ \implies -3(i - \frac{n}{2})^2 &= (\frac{1}{2}n)^2. \end{aligned}$$

Note that both sides of the equation are nonzero in $\mathbb{F}_q$. If $\left(\frac{-3}{p}\right) = -1$, no i and j satisfy the equation. If $\left(\frac{-3}{p}\right) = 1$, then for every n, there are exactly two values of i that satisfy the final requirement. However, since these two possibilities of i add up to n, they account for only one pair of (i, j).

Thus, if $\left(\frac{-3}{p}\right) = -1$,

$$\prod_{\substack{1\le i<j\le p-1,\\ i^3+j^3\neq 0}} (i+j) = \prod_{n=1}^{p-1} n^{\frac{p-3}{2}} = (-1)^{\frac{p-3}{2}} = (-1)\left(\frac{-1}{p}\right).$$

If $\left(\frac{-3}{p}\right) = 1$,

$$\prod_{\substack{1\le i<j\le p-1,\\ i^3+j^3\neq 0}} (i+j) = \prod_{n=1}^{p-1} n^{\frac{p-5}{2}} = (-1)^{\frac{p-5}{2}} = \left(\frac{-1}{p}\right).$$

Thus, for all $p \geq 5$,

$$\prod_{\substack{1\le i<j\le p-1,\\ i^3+j^3\neq 0}} (i+j) = \left(\frac{-3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right).$$

Now we consider the second half of the right half of equation 8:

$$\prod_{\substack{1\le i<j\le p-1,\\ i^3+j^3\neq 0}} (i^2-ij+j^2) = \prod_{\substack{1\le i<j\le p-1,\\ i+j\neq 0,\\ i^2-ij+j^2\neq 0}} (i^2-ij+j^2)$$

From Theorem 1.2 of Sun in [5] we know that

$$\prod_{\substack{1\le i<j\le p-1,\\ i^2-ij+j^2\neq 0}} (i^2-ij+j^2) = -\left(\frac{-3}{p}\right).$$

Therefore,

$$\begin{aligned}
\prod_{\substack{1\le i<j\le p-1,\\ i+j\neq 0,\\ i^2-ij+j^2\neq 0}} (i^2-ij+j^2) &= -\frac{\left(\frac{-3}{p}\right)}{\prod_{\substack{1\le i<j\le p-1,\\ i+j=0}} i^2-ij+j^2} \\
&= -\frac{\left(\frac{-3}{p}\right)}{\prod_{1\le i\le \frac{p-1}{2}} 3i^2} \\
&= -\frac{\left(\frac{-3}{p}\right)}{3^{\frac{p-1}{2}}(-1)\left(\frac{-1}{p}\right)} \\
&= -\frac{\left(\frac{-3}{p}\right)}{\left(\frac{3}{p}\right)(-1)\left(\frac{-1}{p}\right)} \\
&= 1
\end{aligned} \tag{9}$$

Thus,

$$\prod_{\substack{1\le i<j\le p-1\\ i^3+j^3\neq 0}} (i^3+j^3) = \left(\frac{3}{p}\right)$$

□

5 Proof of Theorem 1.4

In this section, we prove Theorem 1.4.

Proof of Theorem 1.4. For $p \equiv 1 \pmod 3$ and $S = \{a^3 \mid a \in \mathbb{F}_p \text{ and } a \neq 0\}$, we know that all the product of monic linear polynomials with the cubics as the root would be

$$\prod_{a\in S}(x-a) = x^{\frac{p-1}{3}} - 1.$$

When $x = 1$, $a = 1$ would yield $x - a = 0$, so we first take out the case $a = 1$ and have:

$$\prod_{\substack{a\in S,\\ a\neq 1}}(x-a) = \frac{x^{\frac{p-1}{3}}-1}{x-1} = x^{\frac{p-1}{3}-1} + x^{\frac{p-1}{3}-2} + \cdots + 1.$$

Thus, plugging in $x = 1$,

$$\prod_{\substack{a\in S,\\ a\neq 1}} (1-a) = 1^{\frac{p-1}{3}-1} + 1^{\frac{p-1}{3}-2} + \cdots + 1 = \frac{p-1}{3}.$$

and since $-1 = (-1)^3$, we know $\prod_{b\in S} b = 1$, and

$$\prod_{b\in S} b^{\frac{p-4}{3}} \Big(\prod_{a\in S, a\neq 1} (1-a)\Big)^{\frac{p-1}{3}} = (-1)^{\frac{p-4}{3}} \left(\frac{p-1}{3}\right)^{\left(\frac{p-1}{3}\right)}$$

Moreover,

$$\begin{aligned}
\prod_{b\in S} b^{\frac{p-4}{3}} \Big(\prod_{\substack{a\in S,\\ a\neq 1}} (1-a)\Big)^{\frac{p-1}{3}} &= b^{\frac{p-4}{3}} \prod_{\substack{a\in S,\\ a\neq -1}} (1+a) \\
&= \prod_{\substack{a\in S,\\ b\in S,\\ a\neq -1}} b(1+a) \\
&= \prod_{\substack{a\in S,\\ b\in S,\\ a\neq -1}} (b+ab) \\
&= \prod_{\substack{x\in S,\\ y\in S,\\ x+y\neq 0}} (x+y)
\end{aligned} \tag{10}$$

Now we take out the cases when $x = y$:

$$\begin{aligned}
\prod_{\substack{x\in S, y\in S,\\ x\neq y,\\ x+y\neq 0}} (x+y) &= \frac{\prod_{\substack{x\in S,\\ y\in S,\\ x+y\neq 0}} x+y}{\prod_{x\in S, x\neq 0} 2x} \\
&= \frac{\prod_{\substack{x\in S,\\ y\in S,\\ x+y\neq 0}} x+y}{2^{\frac{p-4}{3}} \cdot (-1)} \\
&= \frac{(-1)^{\frac{p-1}{3}} \cdot \left(\frac{p-1}{3}\right)^{\frac{p-1}{3}}}{2^{\frac{p-4}{3}}} \\
&= \left(\frac{1}{6}\right)^{\frac{p-1}{3}}
\end{aligned} \tag{11}$$

This is the product of all unordered pairs, which means it is the square of the product of all ordered pairs. Since $p \geq 5, p \equiv 1 \pmod 2$ and $p \equiv 1 \pmod 3$, we know that $p \equiv 1 \pmod 6$, and thus $\frac{p-1}{6}$ is an integer. Taking the square root of the above we have

$$\prod_{i<j\in S}(i+j) = \pm\left(\frac{1}{6}\right)^{\frac{p-1}{3}}.$$

□

6 Future Work

We are unable to determine the correct sign in Theorem 1.4 because we only compute the square of $\prod_{i<j\in S}(i+j)$. However, if we can compute its cube, we can easily eliminate the $\pm$ sign and determine the exact value of the product. We have the following conjecture for the cube of the expression:

Conjecture 6.1. *For prime p,*

$$\left(\prod_{i<j\in S}(i+j)\right)^3 = -\left(\frac{-1}{p}\right).$$

7 Conclusion

In this paper we generalized the result from Sun 2019 [2], which concerns the product $\prod_{1\leq i<j\leq\frac{p-1}{2}}(i^2+j^2)$, from prime finite fields to arbitrary finite fields. We also examined product of polynomials in the form of sum of two cubics, providing two results for different restrictions on the pair (i, j). Theorem 1.2 is a natural extension of Sun 2019 [2] from prime finite fields to arbitrary finite fields, while Theorem 1.4 is a natural extension of Sun 2019 [2] from quadratic polynomials to cubic polynomials.

8 Practical Takeaway

It is a tradition to examine product of polynomials in elegant forms, and further investigation on this topic is mathematically meaningful in the field of number theory. The mathematical tools used in this paper is foundational for further investigation in raising the polynomials to higher powers, potentially finding a general expression for $\prod(i^n + j^n)$ in finite fields. What's more, polynomials with simple symmetries is also of interest in the field of combinatorics, and tools like Legendre symbol are crucial for cryptography.

9 Acknowledgments

First I would like to thank my mentor Rachana Madhukara and Alan Peng for their guidance. I want to thank my tutor Dr. John Rickert for his suggestions for my paper, and Dr. Tanya Khovanova, Prof. David Jerison, Prof. Ankur Moitra from MIT Mathematics for their advice. I want to thank Prof. Bjorn Poonen for suggesting the problem. I would also want to thank my counselor, Jessica Lee, for her support throughout my time at RSI. Finally, I am very thankful to the MIT Mathematics Department, RSI, CEE, and its sponsors for providing me this opportunity.

References

[1] S. Chowla. On the class number of real quadratic fields. *Proceedings of the National Academy of Sciences*, 47(6):878–878, 1961.

[2] Z.-W. Sun. Quadratic residues and related permutations and identities. *Finite Fields and Their Applications*, 59:246–283, 2019.

[3] G. J. Székely. *Contests in higher mathematics: Miklós Schweitzer Competitions 1962–1991*. Springer Science & Business Media, 2012.

[4] K. S. W. Bruce C. Berndt, Ronald J. Evans. Gauss and jacobi sums. page 58, 1998.

[5] Z.-W. Sun. Quadratic residues and quartic residues modulo primes. *International Journal of Number Theory*, 16(08):1833–1858, 2020.