REPRESENTATION OF POLYNOMIALS AS THE SUM OF TWO 2-TH POWERS OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

CHENG-TSUNG SHEN

1. INTRODUCTION

In 1968, Rieger [2] used the results of Erdös to derive an asymptotic formula

$$E(x) = \frac{\pi x}{2\log^2 x}\left(1 + O\left(\left(\frac{\log\log x}{\log x}\right)^{2/3}\right)\right),$$

where $E(x)$ is the cardinality of the set

$$\left\{n \,\middle|\, n = p_1^2 + p_2^2 \le x,\ p_1 \text{ and } p_2 \text{ are primes}\right\}.$$

The purpose of this paper is to explore a polynomial analogue of the Rieger's formula for polynomial ring over finite field. Let $\mathbb{F}_q$ be a finite field with q elements of odd characteristic, let $\mathrm{A} = \mathbb{F}_q[T]$ denote its polynomial ring and let A_+ denote the set of monic polynomials in A. The degree of a polynomial f in A is denoted by $\deg f$, the absolute value of f is defined by $|f| = q^{\deg f}$ and the leading coeffcient of f is given by $\mathrm{sgn}(f)$.

Let $\mathfrak{ms}$ (resp. $\mathfrak{mi}$) denote the set of monic squarefree (resp. monic irreducible) polynomials in A. In Section 2, we establish a polynomial sieve. The main results are that for any $r_1, r_2 \in \mathbb{F}_q^\times$, we have

$$E(N) = \begin{cases} \frac{q^{2N}}{N^2}\left(1 + O\left(\frac{\log_q^4 \max\{q,N\}}{N}\right)\right), & \text{if } r_1 \neq r_2, \\ \frac{q^{2N}}{2N^2}\left(1 + O\left(\frac{\log_q^4 \max\{q,N\}}{N}\right)\right), & \text{if } r_1 = r_2, \end{cases}$$

where $E(N)$ is the cardinality of the set

$$\left\{f \,\middle|\, f = r_1P_1^2 + r_2P_2^2 \text{ with } P_1, P_2 \in \mathfrak{mi} \text{ and } \deg P_1 = \deg P_2 = N\right\}$$

and the implied constant does not depend on q. The polynomial prime number theorem provides us with the main terms in our asymptotic expansion and the polynomial sieve gives us an upper bound for the error terms.

Notation. We shall use the letter P, with or without subscripts, exclusively to denote monic irreducible polynomials and use the notation

$$\sum{}'$$

1991 *Mathematics Subject Classification.* 11T.
Key words and phrases. Selberg sieve method, Polynomial Ring .

to denote the sum over all monic polynomials in A.

2. APPLICATION OF A POLYNOMIAL SELBERG SIEVE

Let $\mathcal{A}$ be a finite sequence consisting of polynomials in A and let $\mathfrak{P}$ be a subset of $\mathfrak{mi}$. The sifting function $S(\mathcal{A};\mathfrak{P},z)$ is defined to be the number of elements in $\mathcal{A}$ which are not divisible by any $P\in\mathfrak{P}$ with $\deg P<z$. Given any real number z, we define

$$\mathfrak{P}(z)=\prod_{P\in\mathfrak{P},\deg P<z} P.$$

For any $d\in\mathfrak{ms}$, let $\mathcal{A}_d$ denote the subsequence of $a\in\mathcal{A}$ satisfying $d|a$ and let $|\mathcal{A}_d|$ denote the cardinality of the sequence $\mathcal{A}_d$.

Now we choose an approximation X to $|\mathcal{A}|$ and let $r_1=|\mathcal{A}|-X$. For each irreducible $P\in\mathfrak{P}$, we choose $\omega(P)\in\mathbb{R}$ so that $\frac{\omega(P)}{|P|}X$ is close to $|\mathcal{A}_P|$, and write for the remainder term

$$r_P=|\mathcal{A}_P|-\frac{\omega(P)}{|P|}X.$$

Given $d\in\mathfrak{ms}$, if $d|\mathfrak{P}(z)$ for some real number z, then we define

$$\omega(d)=\prod_{P\in\mathfrak{P},P|d}\omega(P);\quad r_d=|\mathcal{A}_d|-\frac{\omega(d)}{|d|}X.$$

Let $y\geq 1$ and let real numbers $\lambda_d(d\in\mathfrak{ms})$ satisfy

$$\lambda_1=1;\quad \lambda_d=0 \text{ for } \deg d\geq y. \tag{1}$$

Denote the polynomial möbius function by $\mu(d)$. Then we have

$$\begin{aligned}
S(\mathcal{A};\mathfrak{P},z)&=\sum_{a\in\mathcal{A},(a,\mathfrak{P}(z))=1}1\\
&=\sum_{a\in\mathcal{A}}\left(\sum_{d|(a,\mathfrak{P}(z))}{}'\mu(d)\right)^2\\
&\leq\sum_{a\in\mathcal{A}}\left(\sum_{d|(a,\mathfrak{P}(z))}{}'\lambda_d\right)^2\\
&=\sum_{d_1|\mathfrak{P}(z)}{}'\sum_{d_2|\mathfrak{P}(z)}{}'\lambda_{d_1}\lambda_{d_2}\sum_{a\in\mathcal{A},[d_1,d_2]|a}1\\
&=XS+R(y,z),
\end{aligned}\tag{2}$$

where

$$S = \sideset{}{'}\sum_{d_1|\mathfrak{P}(z)} \sideset{}{'}\sum_{d_2|\mathfrak{P}(z)} \lambda_{d_1}\lambda_{d_2}\frac{\omega([d_1,d_2])}{|[d_1,d_2]|}, \tag{3}$$

$$R(y,z) = \sum_{d_1|\mathfrak{P}(z)} \sum_{d_2|\mathfrak{P}(z)} \lambda_{d_1}\lambda_{d_2} r_{[d_1,d_2]}.$$

For any $d \in \mathfrak{ms}$, define

$$\mathfrak{P}_d(z) = \prod_{P\in\mathfrak{P},\deg P<z,P\nmid d} P, \quad G_d(y,z) = \sideset{}{'}\sum_{\deg f<y, f|\mathfrak{P}_d(z)} g(f),$$

where $g(f)$ is given by

$$g(1)=1, \quad g(P)=\frac{\omega(P)}{|P|}\left(1-\frac{\omega(P)}{|P|}\right)^{-1}, \quad g(f)=\prod_{P\in\mathfrak{P},P|f} g(P). \tag{4}$$

Theorem 2.1. *Suppose* $0 < \omega(P)/|P| < 1$ *for all* $P \in \mathfrak{P}$ *and the real numbers* $\lambda_d (d \in \mathfrak{ms})$ *is given by*

$$\lambda_d = \frac{\mu(d)G_d(y-\deg d, z)}{G_1(y,z)} \prod_{P\in\mathfrak{P},P|d}\left(1-\frac{\omega(P)}{|P|}\right)^{-1}.$$

Then, if $y \geq 1$, *then we have*

$$S(\mathcal{A};\mathfrak{P},z) \leq \frac{X}{G_1(y,z)} + R(y,z).$$

Proof. Suppose that $d, d_1, d_2 \in \mathfrak{ms}$ satisfy $d|\mathfrak{P}(z), d_1|\mathfrak{P}(z)$ and $d_2|\mathfrak{P}(z)$. By (4), we have

$$\frac{|d|}{\omega(d)} = \prod_{P\in\mathfrak{P},P|d}\frac{|P|}{\omega(P)} = \prod_{P\in\mathfrak{P},P|d}\left(1+\frac{1}{g(P)}\right) = \sideset{}{'}\sum_{f|d}\frac{1}{g(f)}.$$

Since $\omega([d_1,d_2])\omega((d_1,d_2)) = \omega(d_1)\omega(d_2)$, we get

$$\frac{\omega([d_1,d_2])}{|[d_1,d_2]|} = \frac{\omega(d_1)\omega(d_2)}{|d_1||d_2|}\cdot\frac{|(d_1,d_2)|}{\omega((d_1\cdot d_2))} = \frac{\omega(d_1)\omega(d_2)}{|d_1||d_2|}\sideset{}{'}\sum_{f|(d_1,d_2)}\frac{1}{g(f)}.$$

Combining this with (3), we obtain

$$S = \sum_{d_1|\mathfrak{P}(z)}{}' \sum_{d_2|\mathfrak{P}(z)}{}' \lambda_{d_1}\lambda_{d_2}\frac{\omega([d_1,d_2])}{|[d_1,d_2]|}$$

$$\begin{aligned}
&= \sum_{d_1|\mathfrak{P}(z)}{}' \sum_{d_2|\mathfrak{P}(z)}{}' \lambda_{d_1}\lambda_{d_2}\left(\frac{\omega(d_1)\omega(d_2)}{|d_1||d_2|}\sum_{f|(d_1,d_2)}{}'\frac{1}{g(f)}\right) \\
&= \sum_{f|\mathfrak{P}(z)}{}'\frac{1}{g(f)}\left(\sum_{d_1|\mathfrak{P}(z),f|d_1}{}'\frac{\lambda_{d_1}\omega(d_1)}{|d_1|}\sum_{d_2|\mathfrak{P}(z),f|d_2}{}'\frac{\lambda_{d_2}\omega(d_2)}{|d_2|}\right) \\
&= \sum_{f|\mathfrak{P}(z)}{}'\frac{Y_f^2}{g(f)},
\end{aligned} \tag{5}$$

where

$$Y_f = \sum_{d|\mathfrak{P}(z),f|d}{}'\frac{\lambda_d\omega(d)}{|d|} \tag{6}$$

$$\begin{aligned}
&= \sum_{d|\mathfrak{P}(z),f|d}{}'\left(\frac{\mu(d)G_d(y-\deg d,z)}{G_1(y,z)}\prod_{P\in\mathfrak{P},P|d}\left(1-\frac{\omega(P)}{|P|}\right)^{-1}\right)\frac{\omega(d)}{|d|} \\
&= \frac{1}{G_1(y,z)}\sum_{d|\mathfrak{P}(z),f|d}{}'\frac{\omega(d)\mu(d)G_d(y-\deg d,z)}{|d|}\prod_{P\in\mathfrak{P},P|d}\left(1-\frac{\omega(P)}{|P|}\right)^{-1} \\
&= \frac{1}{G_1(y,z)}\sum_{d|\mathfrak{P}(z),f|d}{}'\mu(d)G_d(y-\deg d,z)g(d) \\
&= \frac{1}{G_1(y,z)}\sum_{d|\mathfrak{P}(z),f|d}{}'\mu(d)g(d)\sum_{k|\mathfrak{P}_d(z),\deg k<y-\deg d}{}'g(k) \\
&= \frac{1}{G_1(y,z)}\sum_{d|\mathfrak{P}(z),f|d}{}'\mu(d)\sum_{dk|\mathfrak{P}(z),\deg dk<y}{}'g(dk) \\
&= \frac{1}{G_1(y,z)}\sum_{k|\mathfrak{P}(z),\deg k<y}{}'g(k)\sum_{f|d,d|k}{}'\mu(d) \\
&= \frac{1}{G_1(y,z)}\sum_{f|k,k|\mathfrak{P}(z),\deg k<y}{}'g(k)\sum_{d|k/f}{}'\mu(f)\mu(d) \\
&= \begin{cases}\frac{\mu(f)g(f)}{G_1(y,z)}, & \text{if } \deg f<y \text{ and } f|\mathfrak{P}(z),\\ 0, & \textit{otherwise.}\end{cases}
\end{aligned}$$

Combining (5), (6) and the definition of $G_1(y,z)$, we obtain

$$S = \sum_{f|\mathfrak{P}(z)}{}' \frac{Y_f^2}{g(f)} = \sum_{f|\mathfrak{P}(z),\deg f<y}{}' \frac{g(f)}{G_1^2(y,z)} = \frac{1}{G_1(y,z)}.$$

Combining this with (2), we complete the proof. □

Lemma 2.1. *Let assumption be as in theorem* 2.1 *with* $y = z$. *If* $|r_d| \le \omega(d)$ *and* $\omega(d) \ge 1$ *for all* $d|\mathfrak{P}(z)$, *then we have*

$$G_1(z,z) = \sum_{f|\mathfrak{P}(z),\deg f<z}{}' \prod_{P\in\mathfrak{P},P|f} \left(\frac{\omega(P)}{|P|} + \frac{\omega^2(P)}{|P|^2} + \cdots\right),$$

$$|R(z,z)| \le q^{2z} \prod_{P|\mathfrak{P}(z)} \left(1 - \frac{\omega(P)}{|P|}\right)^{-2}.$$

Proof. By the definition of $G_1(y,z)$, we have

$$\begin{aligned} G_1(z,z) &= \sum_{f|\mathfrak{P}(z),\deg f<z}{}' g(f) \\ &= \sum_{f|\mathfrak{P}(z),\deg f<z}{}' \prod_{P\in\mathfrak{P},P|f} \left(\frac{\omega(P)}{|P|} + \frac{\omega^2(P)}{|P|^2} + \cdots\right). \end{aligned}$$

Suppose $d_1|\mathfrak{P}(z)$ and $d_2|\mathfrak{P}(z)$. By $|r_d| \le \omega(d)$ and $\omega(d) \ge 1$ for all $d|\mathfrak{P}(z)$, we have

$$|r_{[d_1,d_2]}| \le \omega([d_1,d_2]) = \frac{\omega(d_1)\omega(d_2)}{\omega((d_1,d_2))} \le \omega(d_1)\omega(d_2).$$

By the definitions of $R(y,z)$, λ_d and $0 < \omega(P)/|P| < 1$, we have

$$\begin{aligned}
|R(z,z)| &\leq \sum_{d_1|\mathfrak{P}(z)}{}' \sum_{d_2|\mathfrak{P}(z)}{}' |\lambda_{d_1}||\lambda_{d_2}||r_{[d_1,d_2]}| \\
&\leq \sum_{d_1|\mathfrak{P}(z)}{}' \sum_{d_2|\mathfrak{P}(z)}{}' |\lambda_{d_1}||\lambda_{d_2}|\omega(d_1)\omega(d_2) \\
&= \left(\sum_{d|\mathfrak{P}(z)}{}' |\lambda_d|\omega(d)\right)^2 \\
&\leq \left(\sum_{d|\mathfrak{P}(z),\deg d<z}{}' \omega(d) \prod_{P\in\mathfrak{P},P|d}\left(1-\frac{\omega(P)}{|P|}\right)^{-1}\right)^2 \\
&= \left(\sum_{d|\mathfrak{P}(z),\deg d<z}{}' |d| \prod_{P\in\mathfrak{P},P|d}\frac{\omega(P)}{|P|}\left(1-\frac{\omega(P)}{|P|}\right)^{-1}\right)^2 \\
&\leq \left(q^z \sum_{d|\mathfrak{P}(z),\deg d<z}{}' \prod_{P|\mathfrak{P},P|d}\left(\frac{\omega(P)}{|P|}+\frac{\omega^2(P)}{|P|^2}+\cdots\right)\right)^2 \\
&\leq \left(q^z \prod_{P|\mathfrak{P}(z)}\left(1+\frac{\omega(P)}{|P|}+\frac{\omega^2(P)}{|P|^2}+\cdots\right)\right)^2 \\
&= q^{2z}\prod_{P|\mathfrak{P}(z)}\left(1-\frac{\omega(P)}{|P|}\right)^{-2}.
\end{aligned}$$

□

Theorem 2.2. *Let integers $k, N \geq 1$, real number $\alpha \geq 0$ and let $a \in \mathbb{F}_q^\times, a_i, b_i \in \mathrm{A} (i = 1, 2, \cdots, k)$. Suppose $\deg a_i, \deg b_i \leq \alpha N$ and*

$$E = a_1 a_2 \cdots a_k \prod_{1\leq i<j\leq k}(a_i b_j - a_j b_i) \neq 0.$$

Let C be the number of $f \in \mathrm{A}$ such that $\deg f = N, \mathrm{sgn}(f) = a$ and $a_i f + b_i$ are irreducible polynomials for all i. Then we have

$$C = O\left(\frac{q^N \log_q^k \max\{q, N\}}{N^k}\right),$$

where the implied constant depends on α and k.

Proof. Let

$$\mathcal{A} = \{(a_1 f + b_1)(a_2 f + b_2) \cdots (a_k f + b_k) | f \in \mathrm{A}, \deg f = N, \mathrm{sgn}(f) = a\},$$
$$\mathfrak{P} = \{P \in \mathrm{mi} \,|\, P \nmid E, |P| > k\},$$
$$X = q^N,$$

and let $\omega(d)$ be the number of the solutions of $f \in \mathrm{A}$ satisfying

$$(a_1 f + b_1)(a_2 f + b_2) \cdots (a_k f + b_k) \equiv 0 \pmod{d}$$

with $\deg f < \deg d$. If $P \in \mathfrak{P}$, then $\omega(P) = k$ and $0 < \omega(P)/|P| < 1$. By chinese remainder theorem, we have

$$\omega(d) = \prod_{P \in \mathfrak{P}, P|d} \omega(P) \quad \text{and} \quad |r_d| \leq \omega(d)$$

for all $d | \mathfrak{P}(z)$. By theorem 2.1 and lemma 2.1, we have

$$\begin{aligned} C &\leq S(\mathcal{A}, \mathfrak{P}, z) + kq^{z+1} \\ &\leq \frac{q^N}{G_1(z,z)} + q^{2z} \prod_{P | \mathfrak{P}(z)} \left(1 - \frac{k}{|P|}\right)^{-2} + kq^{z+1}. \end{aligned} \tag{7}$$

To estimate $G_1(z,z)$: suppose $0 \neq f \in \mathrm{A}$. The polynomial divisor function $\tau_k(f)$ is defined to be the number of solutions of

$$f = \mathrm{sgn}(f) f_1 f_2 \cdots f_k$$

with $f_1, f_2, \cdots, f_k \in \mathrm{A}_+$. Let U be the set of $f \in \mathrm{A}_+$ such that $\deg f < z/k$ and $p \nmid f$ for all $P \notin \mathfrak{P}$. Taking $z = N/2 - 2k \log_q N$, by lemma 2.1, we

obtain

$$G_1(z,z) = \sum_{f|\mathfrak{P}(z),\deg f<z}{}' \prod_{P\in\mathfrak{P},P|f}\left(\frac{k}{|P|}+\frac{k^2}{|P|^2}+\cdots\right)$$

$$= \sum_{s\geq 1}\sum_{P_1\cdots P_s|\mathfrak{P}(z),\deg P_1\cdots P_s<z}\ \sum_{m_1,\cdots,m_s\geq 1}\frac{k^{m_1+\cdots+m_s}}{|P_1|^{m_1}\cdots|P_s|^{m_s}}$$

$$\geq \sum_{s\geq 1}\sum_{P_1\cdots P_s|\mathfrak{P}(z),\deg P_1\cdots P_s<z}\ \sum_{m_1,\cdots,m_s\geq 1}\frac{\tau_k(P_1^{m_1})\cdots\tau_k(P_s^{m_s})}{|P_1|^{m_1}\cdots|P_s|^{m_s}}$$

$$\geq \sum_{f_1\in U}\cdots\sum_{f_k\in U}\frac{1}{|f_1||f_2|\cdots|f_k|}$$

$$= \left(\sum_{f\in U}\frac{1}{|f|}\right)^k$$

by lemma 4.3, replacing d by z/k and $\mathfrak{P}$ by $\mathfrak{P}(z/k)$,

$$\gg \prod_{P|\mathfrak{P}(z/k)}\left(1-\frac{1}{|P|}\right)^{-k}$$

$$\geq \prod_{P|E}\left(1-\frac{1}{|P|}\right)^k \prod_{\deg P<z/k}\left(1-\frac{1}{|P|}\right)^{-k}\prod_{|P|\leq k}\left(1-\frac{1}{|P|}\right)^k$$

by (8)

$$\gg z^k\prod_{P|E}\left(1-\frac{1}{|P|}\right)^k$$

$$= z^k\left(\frac{\Phi(E)}{|E|}\right)^k$$

by $\deg a_i, \deg b_i \leq \alpha N$, lemma 4.1 with $Q=E$ and $\deg E \leq 3k^2\alpha N$

$$\gg \frac{N^k}{\log_q^k(\max\{q,N\})},$$

where the implied constant depends on α and k.

To estimate the second term of (7): by lemma 4.2, we have

$$q^{2z}\prod_{P|\mathfrak{P}(z)}\left(1-\frac{k}{|P|}\right)^{-2} \ll q^{2z}\prod_{\deg P<z}\left(1-\frac{1}{|P|}\right)^{-2k} = q^{2z}\left(\frac{|Q|}{\Phi(Q)}\right)^{2k},$$

where $Q = \prod_{\deg P<z} P$. By lemma 4.1 and (8), we have

$$\begin{aligned} q^{2z} \prod_{P|\mathfrak{P}(z)} \left(1 - \frac{k}{|P|}\right)^{-2} &\ll q^{2z} \log_q^{2k} (\max\{q, \deg Q\}) \\ &\ll q^{2z} z^{2k} \\ &\ll \frac{q^N}{N^{4k}} N^{2k} \\ &= \frac{q^N}{N^{2k}}, \end{aligned}$$

where the implied constant depends on k.

To estimate the third term of (7): since we take $z = N/2 - 2k \log_q N$, we have

$$kq^{z+1} = kq^{N/2-2k\log_q N+1} \ll q^{N/2+1}.$$

With these estimations at hand, the proof is complete. □

3. MAIN THEOREM

Let π_N denote the number of $P \in \mathrm{mi}$ with $\deg P = N$. The polynomial prime number theorem is given by

$$q^N/N - q^{N/2} < \pi_N \leq q^N/N. \tag{8}$$

Let $R_N(f)$ denote the number of $(P_1, P_2) \in \mathrm{mi}^2$ satisfying

$$f = r_1 P_1^2 + r_2 P_2^2$$

with $\deg P_1 = \deg P_2 = N$.

Lemma 3.1. *Suppose $r_1, r_2 \in \mathbb{F}_q^\times$. Then we have*

(a) *If $r_1 \neq r_2$, then*

$$\sum_{f\in \mathrm{A}, R_N(f)\neq 1} R_N(f) = O\left(\frac{q^{2N} \log_q^4 \max\{q, N\}}{N^3}\right).$$

(b) *If $r_1 = r_2$, then*

$$\sum_{f\in \mathrm{A}, R_N(f)\neq 2} R_N(f) = O\left(\frac{q^{2N} \log_q^4 \max\{q, N\}}{N^3}\right).$$

The implied constants do not depend on r_1, r_2 and q.

Proof. To prove (a), let $R'_N(f)$ denote the number of $(P_1, P_2) \in \mathrm{mi}^2$ satisfying

$$f = r_1 P_1^2 + r_2 P_2^2$$

with $\deg P_1 = \deg P_2 = N$ and $P_1 \neq P_2$. Then we have

$$\begin{aligned} \sum_{f\in \mathrm{A}, R_N(f)\geq 2} R_N(f) &\leq \sum_{f\in \mathrm{A}, R'_N(f)\geq 2} R'_N(f) + 2\pi_N \\ &\leq \sum_{f\in \mathrm{A}} \left(R'^2_N(f) - R'_N(f) \right) + 2\pi_N. \end{aligned} \tag{9}$$

Denote by D the number of $(P_1, P_2, P_3, P_4) \in \mathrm{mi}^4$ satisfying

$$r_1 P_1^2 + r_2 P_2^2 = r_1 P_3^2 + r_2 P_4^2$$

with $\deg P_i = N (i = 1, 2, 3, 4), P_1 \neq P_2, P_3 \neq P_4$ and $P_1 \neq P_3$ (hence $P_2 \neq P_4$). Then we get

$$\sum_{f\in \mathrm{A}} \left(R'^2_N(f) - R'_N(f) \right) = D. \tag{10}$$

To estimate D: suppose $(P_1, P_2, P_3, P_4) \in \mathrm{mi}^4$ satisfying

$$r_1 P_1^2 + r_2 P_2^2 = r_1 P_3^2 + r_2 P_4^2$$

with $\deg P_i = N (i = 1, 2, 3, 4), P_1 \neq P_2, P_3 \neq P_4$ and $P_1 \neq P_3$. Then $r_1(P_1^2 - P_3^2) = r_2(P_4^2 - P_2^2)$. Let $a = P_1 - P_3 \neq 0, b = P_4 - P_2 \neq 0, (a, b) = g$. We can write $a = a'g$ and $b = b'g$ for some $a', b' \in \mathrm{A}$ with $(a', b') = 1$. Then we have $r_1 a'(P_1 + P_3) = r_2 b'(P_2 + P_4)$ and $r_1 r_2^{-1}(P_1 + P_3)/b' = (P_2 + P_4)/a' \in \mathrm{A}$. Let $h = (P_2 + P_4)/a'$. Then we have $(P_1 + P_3) = r_1^{-1} r_2 b' h$ and $P_2 + P_4 = a'h$. Hence we get

$$\begin{aligned} 2P_1 &= a'g + r_1^{-1} r_2 b' h, \\ 2P_2 &= -b'g + a'h, \\ 2P_3 &= -a'g + r_1^{-1} r_2 b' h, \\ 2P_4 &= b'g + a'h, \end{aligned}$$

and since q is odd, we can easily check

$$\begin{aligned} &\mathrm{sgn}(a'h) = \mathrm{sgn}(r_1^{-1} r_2 b' h) = 2, \\ &\deg(a'h) = \deg(b'h) = N, \\ &a'b'gh \neq 0, \\ &\deg g < \deg h \leq N, \\ &a' \neq -b'. \end{aligned} \tag{11}$$

Denote now by C the set of $(a', b', g, h) \in \mathrm{A}^4$ satisfying (11) and polynomials

$$a'g + r_1^{-1} r_2 b' h, \quad -b'g + a'h, \quad -a'g + r_1^{-1} r_2 b' h, \quad b'g + a'h$$

are irreducible polynomials. Then we have

$$D \le |C| \tag{12}$$

Set $C' = \{(a', b', g, h) \in C | \deg g \le N/2)\}$ and $C'' = \{(a', b', g, h) \in C | N/2 < \deg g < N)\}$. We have $C = C' \cup C''$.

To estimate $|C'|$. Given $b', g, h \in \mathrm{A}$, we set

$$C'_{b',g,h} = \{a' \in \mathrm{A} \,|\, (a', b', g, h) \in C'\}.$$

Then we have

$$|C'| = \sum_{\substack{0 \ne g \in \mathrm{A} \\ \deg g \le N/2}} \sum_{\substack{0 \ne h \in \mathrm{A} \\ \deg g < \deg h \le N}} \sum_{\substack{0 \ne b' \in \mathrm{A} \\ \deg b' = N - \deg h \\ \mathrm{sgn}(b') = 2 r_1 r_2^{-1} \mathrm{sgn}^{-1}(h)}} |C'_{b',g,h}|. \tag{13}$$

In order to estimate $|C'_{b',g,h}|$, we consider the following two cases:

(1) Suppose $\deg g < \deg h \le 3N/4$. By theorem 2.2 with $k = 4, \alpha = 4, a = 2\,\mathrm{sgn}^{-1}(h), a_1 = -a_3 = g, a_2 = a_4 = h, b_1 = b_3 = r_1^{-1} r_2 b' h, -b_2 = b_4 = b' g$ and replacing N by $N - \deg h$, it is easy to check that $E \ne 0$ (because q is odd and $\deg g < \deg h$) and since $\deg g < \deg h \le 3N/4$, $\deg a_i, \deg b_i \le N \le 4(N - \deg h) = \alpha(N - \deg h)$. Thus we have

$$\begin{aligned} |C'_{b',g,h}| &\ll \frac{q^{N - \deg h} \log_q^4(\max\{q, N - \deg h\})}{(N - \deg h)^4} \\ &\ll \frac{q^N \log_q^4 \max\{q, N\}}{|h| N^4}. \end{aligned}$$

(2) Suppose $3N/4 < \deg h \le N$. The trivial estimation have

$$|C'_{b',g,h}| \le q^N / |h|.$$

Combining these two cases with (13), we obtain

$$\begin{aligned} |C'| &\ll \sum_{\substack{0 \ne g \in \mathrm{A} \\ \deg g \le N/2}} \sum_{\substack{0 \ne h \in \mathrm{A} \\ \deg g < \deg h \le \frac{3N}{4}}} \frac{q^{2N} \log_q^4(\max\{q, N\})}{|h|^2 N^4} \\ &\quad + \sum_{\substack{0 \ne g \in \mathrm{A} \\ \deg g \le N/2}} \sum_{\substack{0 \ne h \in \mathrm{A} \\ \frac{3N}{4} < \deg h \le N}} \frac{q^{2N}}{|h|^2} \qquad (14) \\ &\le \sum_{\substack{0 \ne g \in \mathrm{A} \\ \deg g \le N/2}} \left(\frac{q^{2N} \log_q^4(\max\{q, N\})}{|g| N^4} + q^{\frac{5N}{4}} \right) \\ &\ll \frac{q^{2N} \log_q^4(\max\{q, N\})}{N^3}, \end{aligned}$$

where the implied constant does not depend on r_1, r_2 and q.

To estimate $|C'''|$. Given $a', b', g \in \mathrm{A}$, we set

$$C'''_{a',b',g} = \{h \in \mathrm{A} \,|\, (a', b', g, h) \in C'''\}.$$

Then we have

$$|C'''| = \sum_{\substack{0 \neq g \in \mathrm{A} \\ N/2 < \deg g < N}} \sum_{\substack{0 \neq a' \in \mathrm{A} \\ \deg a' < N - \deg g}} \sum_{\substack{0 \neq b' \in \mathrm{A} \\ \deg b' = \deg a' \\ \mathrm{sgn}(b') = r_1 r_2^{-1} \mathrm{sgn}(a') \\ b' \neq -a'}} |C'_{a',b',g}|. \tag{15}$$

Let $a', b', g \in \mathrm{A}$ satisfying $a'b'g \neq 0, N/2 < \deg g < N, \deg a' < N - \deg g, \deg b' = \deg a', \mathrm{sgn}(b') = r_1 r_2^{-1} \mathrm{sgn}(a')$ and $b' \neq -a'$. By theorem 2.2 with $k = 4, \alpha = 2, a = 2\,\mathrm{sgn}(a')^{-1}, a_1 = a_3 = r_1^{-1} r_2 b', a_2 = a_4 = a', b_1 = -b_3 = a'g, -b_2 = b_4 = b'g$ and replacing N by $N - \deg a'$, it is easy to check that $E \neq 0$ (because q is odd, $r_1 \neq r_1$ and $\mathrm{sgn}(b') = r_1 r_2^{-1} \mathrm{sgn}(a')$) and $\deg a_i, \deg b_i \leq \deg a' + \deg g < N < 2(N - \deg a') = \alpha(N - \deg a')$ (because $\deg a' < N - \deg g$ and $N/2 < \deg g$). Thus we obtain

$$|C'''_{a',b',g}| \ll \frac{q^{N - \deg a'} \log_q^4 \max\{q, N - \deg a'\}}{(N - \deg a')^4} \ll \frac{q^N \log_q^4 \max\{q, N\}}{|a'| N^4}.$$

Therefore, we obtain

$$\begin{aligned} |C'''| &\ll \sum_{\substack{0 \neq g \in \mathrm{A} \\ N/2 < \deg g < N}} \sum_{\substack{0 \neq a' \in \mathrm{A} \\ \deg a' < N - \deg g}} \frac{q^N \log_q^4 \max\{q, N\}}{N^4} \\ &\leq \sum_{\substack{0 \neq g \in \mathrm{A} \\ N/2 < \deg g < N}} \frac{q^{2N} \log_q^4 \max\{q, N\}}{|g| N^4} \\ &\leq \frac{q^{2N} \log_q^4 \max\{q, N\}}{N^3}, \end{aligned} \tag{16}$$

where the implied constant does not depend on r_1, r_2 and q. Combining (9), (10), (12), (14), (16) and the polynomial prime number theorem (8), the proof of lemma 3.1 (a) is complete.

To prove (b), we have

$$\sum_{f \in \mathrm{A}, R_N(f) > 2} R_N(f) \leq \sum_{f \in \mathrm{A}} \left(R_N^2(f) - 2R_N(f)\right) + \pi_N.$$

Hence

$$\sum_{f \in \mathrm{A}, R_N(f) \neq 2} R_N(f) \leq \sum_{f \in \mathrm{A}} \left(R_N^2(f) - 2R_N(f)\right) + 2\pi_N.$$

Denote by D the number of $(P_1, P_2, P_3, P_4) \in \mathrm{mi}^4$ satisfying

$$P_1^2 + P_2^2 = P_3^2 + P_4^2$$

with $\deg P_i = N (i = 1, 2, 3, 4)$, $P_1 \neq P_3$ and $P_1 \neq P_4$ (hence $P_2 \neq P_3$). Then we have

$$\sum_{f \in \mathrm{A}} \left(R_N^2(f) - 2R_N(f) \right) + \pi_N = D$$

Therefore

$$\sum_{f \in \mathrm{A}, R_N(f) \neq 2} R_N(f) \leq D + \pi_N.$$

The proof of the remainder of lemma 3.1 (b) is similar to the proof of part (a). □

Theorem 3.1. *Let $r_1, r_2 \in \mathbb{F}_q^\times$ satisfy $r_1 \neq r_2$. Then we have*

$$E(N) = \frac{q^{2N}}{N^2} \left(1 + O\left(\frac{\log_q^4 \max\{q, N\}}{N} \right) \right),$$

where the implied constant does not depend on r_1, r_2 and q.

Proof. By (8), we have

$$E(N) = \sum_{f \in \mathrm{A}, R_N(f) > 0} 1 \leq \sum_{f \in \mathrm{A}} R_N(f) = \pi_N^2 \leq q^{2N}/N^2.$$

On the other hand, by lemma 3.1 (a) and (8), we have

$$\begin{aligned} E(N) &\geq \sum_{f \in \mathrm{A}, R_N(f) = 1} 1 \\ &= \sum_{f \in \mathrm{A}} R_N(f) - \sum_{f \in \mathrm{A}, R_N(f) \geq 2} R_N(f) \\ &\geq \pi_N^2 + O\left(\frac{q^{2N} \log_q^4 \max\{q, N\}}{N^3} \right) \\ &\geq \frac{q^{2N}}{N^2} \left(1 + O\left(\frac{\log_q^4 \max\{q, N\}}{N} \right) \right), \end{aligned}$$

where the implied constant does not depend on r_1, r_2 and q. The proof of the theorem 3.1 is complete. □

Theorem 3.2. *Let $r_1, r_2 \in \mathbb{F}_q^\times$ satisfy $r_1 = r_2$. Then we have*

$$E(N) = \frac{q^{2N}}{2N^2} \left(1 + O\left(\frac{\log_q^4 \max\{q, N\}}{N} \right) \right),$$

where the implied constant does not depend on r_1, r_2 and q.

Proof. By (8), we have

$$\begin{aligned} E(N) &= \sum_{f\in \mathrm{A}, R_N(f)\geq 2} 1 + \sum_{f\in \mathrm{A}, R_N(f)=1} 1 \\ &\leq \frac{1}{2}\sum_{f\in \mathrm{A}} R_N(f) + \pi_N \\ &= \frac{\pi_N^2}{2} + \pi_N \\ &\leq \frac{q^{2N}}{2N^2}\left(1 + O\left(\frac{\log_q^4 \max\{q, N\}}{N}\right)\right), \end{aligned}$$

where the implied constant does not depend on r_1, r_2 and q.

On the other hand, by lemma 3.1(b) and (8), we have

$$\begin{aligned} E(N) &\geq \sum_{f\in \mathrm{A}, R_N(f)=2} 1 \\ &= \frac{1}{2}\left(\sum_{f\in \mathrm{A}} R_N(f) - \sum_{f\in \mathrm{A}, R_N(f)\neq 2} R_N(f)\right) \\ &\geq \frac{1}{2}\left(\pi_N^2 + O\left(\frac{q^{2N}\log_q^4 \max\{q, N\}}{N^3}\right)\right) \\ &\geq \frac{q^{2N}}{2N^2}\left(1 + O\left(\frac{\log_q^4 \max\{q, N\}}{N}\right)\right), \end{aligned}$$

where the implied constant does not depend on r_1, r_2 and q. The proof of theorem 3.2 is complete. □

4. Auxiliary Lemmas

Let $Q \in \mathrm{A}_+$. The polynomial Euler phi function $\Phi(Q)$ is defined to be the order of $(\mathrm{A}/Q\,\mathrm{A})^\times$. In fact, we have

$$\Phi(Q) = |Q| \prod_{P|Q}\left(1 - \frac{1}{|P|}\right).$$

Lemma 4.1. *We have*

$$\frac{|Q|}{\Phi(Q)} < 32 \log_q \max\{q, \deg Q\}.$$

Proof. Let $d = \deg Q$. If $d \leq q$, then we have

$$\ln \frac{|Q|}{\Phi(Q)} = -\sum_{P|Q} \ln\left(1 - \frac{1}{|P|}\right) \leq \sum_{P|Q}\left(\frac{1}{|P|} + \frac{1}{|P|^2}\right) \leq 1 + \frac{1}{q} \leq \frac{3}{2}.$$

Thus we have

$$\frac{|Q|}{\Phi(Q)} \leq e^{\frac{3}{2}} < 32.$$

If $d > q$, then let N be the integer satisfying

$$1 \cdot \pi_1 + 2 \cdot \pi_2 + \cdots + (N-1) \cdot \pi_{N-1} < d \leq 1 \cdot \pi_1 + 2 \cdot \pi_2 + \cdots + N \cdot \pi_N.$$

By the second inequality of (8), we have

$$\ln \frac{|Q|}{\Phi(Q)} \leq \sum_{i=1}^{N} \frac{q^i}{i} \left(\frac{1}{q^i} + \frac{1}{q^{2i}} \right) \leq \sum_{i=1}^{N} \left(\frac{1}{i} + \frac{1}{q^i} \right) \leq \ln N + 2.$$

When $N > 6$, using the first inequality of (8), we have $N < 3 \log_q d$ and

$$\frac{|Q|}{\Phi(Q)} < 3e^2 \log_q d < 32 \log_q \deg Q.$$

When $N \leq 6$, we have

$$\ln \frac{|Q|}{\Phi(Q)} \leq \sum_{i=1}^{6} \left(\frac{1}{i} + \frac{1}{q^i} \right) \leq 3.44.$$

Thus, by $\deg Q = d > q$, we get

$$\frac{|Q|}{\Phi(Q)} \leq e^{3.44} < 32 \log_q \deg Q = 32 \log_q \max\{q, \deg Q\}.$$

□

Lemma 4.2. *Suppose that $\mathfrak{P} \subset \mathrm{mi}$ and k is a positive integer. Then we have*

$$\prod_{P \in \mathfrak{P}, |P| > k} \left(1 - \frac{k}{|P|}\right)^{-1} = O\left(\prod_{P \in \mathfrak{P}, |P| > k} \left(1 - \frac{1}{|P|}\right)^{-k} \right),$$

where the implied constant depend only on k.

Proof. We have

$$\left(1 - \frac{1}{|P|}\right)^k = 1 - \frac{k}{|P|} + \frac{\delta(k, P)}{|P|^2},$$

where

$$\delta(k, P) = \binom{k}{2} - \frac{1}{|P|}\binom{k}{3} + \cdots + \frac{(-1)^k}{|P|^{k-2}}\binom{k}{k}.$$

If $|P| \geq k + 1$, then we have

$$\begin{aligned} |\delta(k, P)| &= \left| \binom{k}{2} - \frac{1}{|P|}\binom{k}{3} + \cdots \right| \\ &\leq k^2 \left(1 + \frac{k}{|P|} + \frac{k^2}{|P|^2} + \cdots \right) \\ &= O(1), \end{aligned}$$