POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

[illegible]
[illegible]

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

KOMITET REDAKCYJNY

KAROL BORSUK redaktor

ANDRZEJ BIAŁYNICKI-BIRULA, BOGDAN BOJARSKI,
ZBIGNIEW CIESIELSKI, JERZY ŁOŚ, ANDRZEJ MOSTOWSKI,
ZBIGNIEW SEMADENI, MARCELI STARK, WANDA SZMIELEW

CXVII

R. M. KUBOTA

Waring's problem for $F_q[x]$

[illegible]

WARSZAWA 1974
PAŃSTWOWE WYDAWNICTWO NAUKOWE

6.7133

BIBLIOTEKA UNIWERSYTECKA W WARSZAWIE

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

CONTENTS

Introduction 5
1. Preliminaries 9
2. The Farey arcs 12
3. The contribution of the major and minor arcs 13
4. Weyl's Lemma 16
5. The singular integral 23
6. The singular series 28
7. The asymptotic formula 37
8. Estimates for $\tilde{g}(k)$ 40
Bibliography 55

INTRODUCTION

Let $F_q[x]$ be the ring of polynomials in one variable over the finite field of q elements. It is well known that these rings are closely analogous to $\boldsymbol{Z}$ and we may do analytic number theory over them as Artin [1] did, showing the number of primes (i.e., monic irreducible polynomials) was the right size or as Hayes ([4], [5]) who considered Goldbach's conjecture and the extension to $F_q[x]$ of Vinogradov's result on the sum of three primes.

In this paper we study Waring's problem, that is, whether given an integer $k \geqslant 2$ there is an integer s such that an arbitrary polynomial $N \in F_q[x]$ may be written as

$$N = P_1^k + \ldots + P_s^k, \quad \text{where} \quad P_i \in F_q[x]. \tag{1}$$

In additive problems in $F_q[x]$ it is not natural to restrict ourselves to monic polynomials (which in some respects are the analogues of the positive integers). This is because if P were a "positive" polynomial, then, presumably, so also is

$$\underbrace{P + \ldots + P}_{p-1 \text{ times},\ p = \operatorname{char} F_q} = -P.$$

Therefore, in this paper, we consider the number of representations, say $r(N, m, s, k, q)$, of a polynomial N as

$$N = P_1^k + \ldots + P_s^k, \quad \text{where} \quad P_i \in F_q[x],\ \deg P_i < m,\ i = 1, \ldots, s. \tag{2}$$

For the classical Waring's problem essentially three proofs are known, but only one, the Hardy–Littlewood method, gives sharp bounds for s and an asymptotic formula for the number of representations. Here we adapt the Hardy–Littlewood method to prove the asymptotic formula:

THEOREM 30. *If* (a) $0 < \varepsilon < 1$, (b) $\deg N < (k-1+\varepsilon)m$, (c) $s \geqslant 2^k+1$, (d) $3 \leqslant k < \operatorname{char} F_q$, *then there exists* $\delta > 0$ *such that*

$$r(N, m, s, k, q) = \frac{U(s, 0, q)}{q^{s-q}-1} \mathfrak{S}(N, s, k, q) q^{(s-k)m} + O(q^{(s-k-\delta)m}), \tag{3}$$

where

$$1 \ll \frac{U(s, 0, q)}{q^{s-k}-1} \mathfrak{S}(N, s, k, q) \ll 1. \tag{4}$$

Here $U(s, 0, q)$ is the number of s-tuples $c_1, \ldots, c_s \in F_q$ such that $c_1^k + \ldots + c_s^k = 0$, with not all $c_i = 0$. The value of the "singular integral" is $\dfrac{U(s, 0, q)}{q^{s-k}-1}$, and $\mathfrak{S}(N, s, k, q)$ is the analogue of the singular series. In particular, if the conditions (c) and (d) of the theorem are satisfied, letting $m \to \infty$ ensures that N is always represented in the form (2).

Many of the proofs for the singular series follow those for the Hardy–Littlewood method for $\boldsymbol{Z}$, see [2], [9]. The proofs for the singular integral are necessarily different.

We now turn to five remarks on the quality of the theorem:

(1) Since we are considering P_i of $\deg < m$, we would expect information on representations of N up to degree $= k(m-1)$ rather than $(k-1+\varepsilon)m$ as stated. This is possible but a bit messy (see Lemma 17). The difficulty arises because we must now also consider the solutions of

$$c_1^k + \ldots + c_s^k = b \tag{5}$$

where b is the leading coefficient of N. The value of the singular integral then varies according to b and $\deg N$.

(2) We must have $s \geqslant 3k+1$ in order to prove that the singular series converges absolutely (Lemma 23) and $s \geqslant k+1$ in order to show that the singular series is positive. In the classical case, if $s \geqslant 2k$ (k odd) or $s \geqslant 4k$ (k even), the singular series is positive and if $s \geqslant 2k+1$, the singular series converges absolutely. The stronger assumption that $s \geqslant 2^k+1$ comes from our reliance on a Weyl–Hua inequality.

(3) Since we have assumed $k < p = \operatorname{char} F_q$, every polynomial N is a sum of kth powers. In general this is not true. For example if $k = p^h - 1$ and $q = p^h$, $h > 1$, then the constant term of any polynomial P^k (over F_q) is either 0 or 1. Therefore no polynomial whose constant term is in $F_q \setminus \boldsymbol{Z}_p$ is a sum of kth powers. It is true (Theorem 37) that if $p \nmid k$, then N is a sum of kth powers if and only if N is congruent to a sum of kth powers $(\operatorname{mod} P)$, for all irreducible P such that $q^{\deg P} \leqslant (k-1)^2$. (See Theorem 40 and Example 41 for further considerations.)

(4) Let K_∞ be the field of formal power series in x^{-1} over F_q. Then K_∞ plays a role similar to $\boldsymbol{R}$ in the Hardy–Littlewood method, and the "interval" $\operatorname{ord} \alpha < 0$ plays the role of $[0, 1]$. This "interval" is divided into major and minor arcs and an exponential $e(f(P))$ is defined that satisfies conditions sufficient for the Hardy–Littlewood method. (See Lemma 1.)

The principal defect of the theorem is the restriction $k < p = \operatorname{char} F_q$. It seems likely that $p \nmid k$ is the proper restriction. The difficulty arises

in the proof of Weyl's Lemma (Proposition 12) which states that if $k < p$, $\alpha \in$ minor arc, and

$$S_k(f) = \sum_{\deg P < m} e\big(f(P)\big),$$

where

$$f(y) = ay^k + a_1 y^{k-1} + \ldots + a_k, \quad \text{with} \quad a \neq 0,\ a_i \in K_\infty,$$

then for every $\varepsilon > 0$,

$$|S_k(f)| \ll q^{\left(1-\frac{1}{2^{k-1}}+\varepsilon\right)m}. \tag{6}$$

The idea of the proof is essentially a recursion. We relate the sum $S_k(f)$ to several similar sums $S_{k-1}(\Delta_{y_1} f)$ where $\Delta_{y_1} f(y)$ has degree $k-1$ in y. Using this reduction $k-1$ times, we arrive at sums

$$S_1(\Delta_{y_{k-1}} \ldots \Delta_{y_1} f)$$

where $\Delta_{y_{k-1}} \ldots \Delta_{y_1} f(y)$ is linear in y. We must go this far since the only sums we can effectively estimate are linear in the variable.

Here $\Delta_{y_1} f(y) = f(y+y_1) - f(y)$ so that

$$\Delta_{y_{k-1}} \ldots \Delta_{y_1} f(y) = k!\,ay + \text{terms independent of } y. \tag{7}$$

When $k < \operatorname{char} F_q$, $k! \neq 0$ and (7) is linear in y but when $k \geqslant \operatorname{char} F_q$, $k! = 0$ and (7) is no longer linear in y, so the proof of Weyl's Lemma falls apart.

(5) The restriction $s \geqslant 2^k + 1$, in the case of $\boldsymbol{Z}$, is not the best known (for $k \geqslant 10$ or so). Indeed Vinogradov [9] has shown that $s \geqslant ck^2 \log k$, where c is a constant, suffices. In case $k < \operatorname{char} F_q$, although the work has not been carried out, the present author foresees no difficulty in proving a Vinogradov-type result. However when $k \geqslant \operatorname{char} F_q$, there is again a difficulty in principle. Vinogradov's proof is essentially an intricate reduction based on the fact that the sums

$$\begin{gathered} x_1 + \ldots + x_k, \\ x_1^2 + \ldots + x_k^2, \\ \cdots\cdots \\ x_1^k + \ldots + x_k^k, \end{gathered}$$

where

$$0 \leqslant x_i \in \boldsymbol{Z}, \quad i = 1, \ldots, k,$$

are independently distributed in intervals of size proportional to the exponents j on "well-separated" intervals. This is false in $F_q[x]$, if $k \geqslant \operatorname{char} F_q$, since

$$(x_1 + \ldots + x_k)^p = x_1^p + \ldots + x_k^p.$$

In addition to the principal Theorem 30 (the asymptotic formula) we prove a result of the following type: Let $\tilde{g}(k) = \tilde{g}(k, q)$ be the least s such that every polynomial that is a sum of (arbitrarily many) kth powers is a sum of s kth powers. Let $G(k)$ be the least s such that every sufficiently large rational integer is a sum of s kth powers of positive rational integers. Then Vinogradov [10] showed that $G(k) < c \cdot k \log k$. By an analogous proof, we show $\tilde{g}(k, q) < c \cdot k \log k$.

We get a result for g rather than a result only for polynomials of large degree because of the structure of $F_q[x]$. If s is sufficiently large, in $\boldsymbol{Z}$ the asymptotic formula gives

$$r(N) \sim c \cdot N^{s/k-1}$$

so for small N there are fairly few representations of N. In $F_q[x]$, for s sufficiently large

$$r(N) \sim c \cdot q^{(s-k)m}$$

when the P_i are restricted to $\deg P_i < m$, and so the number of representations of N of small degree and of large degree is about the same. This behavior persists when $\operatorname{char} F_q \nmid k$ and naturally leads to a proof for $\tilde{g}(k)$ and not $G(k)$. (See § 8, Theorem 37.)

In the case of $\boldsymbol{Z}$, $G(k) < c \cdot k \log k$ is very good since we know $G(k) \geqslant k+1$. However in case of $F_q[x]$, the result $\tilde{g}(k) < c \cdot k \log k$ is not nearly as profound. Let $\tilde{g}_1(k)$ be defined analogously to $\tilde{g}(k)$ except we now consider

$$N = \pm P_1^k \pm \ldots \pm P_s^k.$$

(the so-called easier Waring's problem). Paley [6], in the only previous research on Waring's problem in $F_q[x]$ of which the author is aware, showed that if $k = p^h+1$ then $\tilde{g}_1(k) \leqslant 6$. The essential point of the proof is that the various powers $k = p^h+1$ satisfy an identity based on

$$(A+B)^k = A^k + A^{k-1}B + AB^{k-1} + B^k,$$

and this leads to the uniform bound for $\tilde{g}_1(k)$. So, in this respect, the result $\tilde{g}(k) < c \cdot k \log k$ is not very satisfactory, but the present author does not know how to adequately exploit the difference.

This paper is my thesis submitted in partial fulfillment of the requirements for the Ph. D. to the Rackham School of Graduate Studies, University of Michigan. Professor D. J. Lewis guided the research. The late Professor Harold Davenport also made the suggestions. Dr. Peter Weinberger and an anonymous referee carefully read the manuscript and each made a suggestion that simplified the statement of the main theorem. I thank all four men.

1. PRELIMINARIES

Let F_q denote the finite field of $q = p^f$ elements. Elements of F_q, the constants will be denoted by $a, b, c, \ldots$; while $F_q[x]$ will denote the polynomials in one variable with coefficients in F_q. Elements of $F_q[x]$ will be denoted by $N, P, Q, A, B, \ldots$ The field of formal power series in x^{-1} over F_q, that is, the set of all expressions $\alpha = \sum_{-\infty}^{t} a_i x^i$, $a_t \neq 0$ (and $\alpha = 0$) with the usual operations will be denoted by K_∞. We define $\operatorname{ord}\alpha = t$ with $\operatorname{ord} 0 = -\infty$. Thus if α is a polynomial, $\operatorname{ord}\alpha = \deg\alpha$. The field K_∞ is a locally compact field under the valuation

$$|\alpha| = q^t = q^{\operatorname{ord}\alpha}. \tag{1}$$

We define $O_\infty = \{\alpha \mid \operatorname{ord}\alpha \leqslant 0\}$ and $x^{-n}O_\infty = \{\alpha \mid \operatorname{ord}\alpha \leqslant -n\}$. Then $x^{-1}O_\infty$ is a compact (additive) subgroup of K_∞, and so we may normalize the Haar measure on K_∞ by

$$\int_{\operatorname{ord}\alpha<0} 1\cdot d\alpha = 1. \tag{2}$$

This implies that for any fixed $\beta \in K_\infty$ and any $n \in \boldsymbol{Z}$,

$$\int_{\operatorname{ord}(\alpha-\beta)<-n} 1\cdot d\alpha = q^{-n}, \tag{3}$$

that is, the measure of the coset $\beta + x^{-n-1}O_\infty$ is q^{-n}. The polynomials form a discrete subring of K_∞.

For $a \in F_q$, we have the usual trace function which we denote by trace of $a = \operatorname{tr}_{F_q \to \boldsymbol{Z}_p} a = \operatorname{tr} a$. If, in the homomorphism $\boldsymbol{Z} \to \boldsymbol{Z}_p$, $u \to \operatorname{tr} a$ and $v \to \operatorname{tr} a$, then $e^{2\pi i u/p} = e^{2\pi i v/p}$. Therefore we may define $e_q\colon F_q \to \boldsymbol{C}$ by

$$e_q(a) = e^{2\pi i u/p}, \tag{4}$$

where u is any preimage in $\boldsymbol{Z}$ of $\operatorname{tr} a$.

For $\alpha = \sum_{-\infty}^{t} a_i x^i$, we define the residue of α as

$$\operatorname{res}\alpha = a_{-1}, \tag{5}$$

with $\operatorname{res} 0 = 0$. The exponential of α is defined as

$$e(\alpha) = e_q(\operatorname{res}\alpha) = e_q(a_{-1}). \tag{6}$$

LEMMA 1. (a) *If* $|\alpha - \beta| < q^{-1}$ *then* $e(\alpha) = e(\beta)$; *that is,* $e(\alpha)$ *is a locally constant function of* α.

(b) $e\colon K_\infty \to \boldsymbol{C}$ *is a continuous function.*

(c) e *is not identically* 1.

(d) $e(\alpha+\beta) = e(\alpha)e(\beta)$.

(e) $e(P) = 1$.

(f) $\int\limits_{\operatorname{ord} a < -n} e(Na)\,da = \begin{cases} q^{-n}, & \text{if } \operatorname{ord} N < n, \\ 0, & \text{otherwise.} \end{cases}$

(g) $\dfrac{1}{|Q|} \sum\limits_{\operatorname{ord} A < \operatorname{ord} Q} e\left(\dfrac{A}{Q} N\right) = \begin{cases} 1, & \text{if } Q \mid N, \\ 0, & \text{if } Q \nmid N. \end{cases}$

Proof. (We recall that A, P, Q, N automatically are restricted to be polynomials.) (a) Suppose $\alpha = \sum\limits_{-\infty}^{t} a_i x^i$ and $\beta = \sum\limits_{-\infty}^{t'} b_i x^i$. Then $|\alpha - \beta| < q^{-1}$, i.e. $\operatorname{ord}(\alpha - \beta) < -1$, says that

$$a_i = b_i, \quad \text{for} \quad i \geqslant -1.$$

So $e(\alpha) = e_q(a_{-1}) = e_q(b_{-1}) = e(\beta)$.

(b) is trivial since any locally constant function is continuous.

(c) follows since the trace is not identically 0.

(d) $e(\alpha)e(\beta) = e_q(a_{-1})e_q(b_{-1}) = e_q(a_{-1} + b_{-1}) = e(\alpha + \beta)$.

(e) If P is a polynomial, then $\operatorname{res} P = 0$ and $e(P) = e_q(0) = 1$.

(f) If $N = 0$, then $e(N\alpha) = 1$, and the formula (f) is our normalization convention (3). Now let $N = b_0 + b_1 x + \ldots + b_l x^l$, with $b_l \neq 0$. Since by assumption $\operatorname{ord} \alpha < -n$ we can write $\alpha = \sum\limits_{-\infty}^{-n-1} a_i x^i$. If $l < n$ then $\operatorname{res}(N\alpha) = 0$ and $e(N\alpha) = 1$ and so the conclusion (f) follows again from equation (3). If $l \geqslant n$ then

$$e(N\alpha) = e_q(a_{-n-1} b_n + a_{-n-2} b_{n+1} + \ldots + a_{-l-1} b_l).$$

Therefore,

$$\begin{aligned} &\int\limits_{\operatorname{ord} \alpha < -n} e(N\alpha)\,d\alpha \\ &= \sum_{a_{-n-1} \in F_q} \sum_{a_{-n-2} \in F_q} \cdots \sum_{a_{-l-1} \in F_q} \int\limits_{\gamma \in x^{-l-2} O_\infty} e_q(a_{-n-1} b_n + \ldots a_{-l-1} b_l)\,d\gamma \\ &= \sum_{a_{n-1} \in F_q} \cdots \sum_{a_{-l} \in F_q} e_q(a_{-n-1} b_n + \ldots + a_{-l} b_{+l-1}) \times \\ &\qquad\qquad \times \sum_{a_{-l-1} \in F_q} e_q(a_{-l-1} b_l) \int\limits_{\gamma \in x^{-l-2} O_\infty} 1 \cdot d\gamma. \end{aligned}$$

But $\int\limits_{\gamma \in x^{-l-2} O_\infty} 1 \cdot d\gamma = q^{-l-1}$ and since $b_l \neq 0$, this last sum is simply $q^{-l-1} \sum\limits_{a \in F_q} e_q(a) = q^{-l-1} \sum\limits_{a \in F_q} e^{\frac{2\pi i}{p} \operatorname{tr} a}$. Since the trace is not identically 0, the trace maps F_q *onto* Z_p and the number of times any particular pth root

of 1 is the image of some $a \in F_q$ is simply the cardinality of the kernel of the trace. Thus

$$\sum_{a \in F_q} e_q(a) = \Big(\sum_{j=0}^{p-1} e^{\frac{2\pi i}{p} j}\Big) \cdot \operatorname{card}\{\ker(\operatorname{tr})\} = 0.$$

Hence our integral has value 0 when $\operatorname{ord} N \geqslant n$.

(g) If $Q|N$ then $e\left(\frac{A}{Q}N\right) = e(\text{polynomial}) = 1$, and

$$\frac{1}{|Q|} \sum_{\operatorname{ord} A < \operatorname{ord} Q} e\left(\frac{A}{Q}N\right) = \frac{1}{|Q|} \sum_{\operatorname{ord} A < \operatorname{ord} Q} 1 = 1.$$

If $Q \nmid N$ then we may reduce $\frac{N}{Q}$ to lowest terms $\frac{N_1}{Q_1}$, with $Q_1 \neq$ constant. As A runs over a complete set of residues $\bmod Q$, AN_1 runs over $\frac{|Q|}{|Q_1|}$ complete sets of residues $\bmod Q_1$, so that

$$\sum_{\operatorname{ord} A < \operatorname{ord} Q} e\left(\frac{A}{Q}N\right) = \frac{|Q|}{|Q_1|} \sum_{\operatorname{ord} R_1 < \operatorname{ord} Q_1} e\left(\frac{R_1}{Q_1}\right).$$

Suppose $Q_1 = q_0 + \ldots + q_n x^n$ where $n \geqslant 1$ and $q_n \neq 0$, and $R_1 = r_0 + \ldots + r_{n-1} x^{n-1}$. Then

$$\frac{R_1}{Q_1} = \frac{r_{n-1}}{q^n} x^{-1} + \sum_{-\infty}^{-2} a_i x^i.$$

This implies that

$$\sum_{\operatorname{ord} R_1 < \operatorname{ord} Q} e\left(\frac{R_1}{Q}\right) = \sum_{r_0 \in F_q} \cdots \sum_{r_{n-2} \in F_q} \Big[\sum_{r_{n-1} \in F_q} e_q\left(\frac{r_{n-1}}{q_n}\right)\Big] = 0,$$

since, as in part (f) the sum in brackets is zero.

LEMMA 2. *Let k be an integer, $k \geqslant 2$, m and s be integers, $m, s \geqslant 1$ and N a polynomial. Let $r(N, m, s, k)$ be the number of ordered s-tuples $(P_1, \ldots, P_s)$ where each P_i is a polynomial of degree $< m$ and*

$$P_1^k + \ldots + P_s^k = N. \tag{7}$$

Let

$$T(a) = T_m(a) = \sum_{\operatorname{ord} P < m} e(aP^k). \tag{8}$$

Then

$$r(N, m, s, k) = \int_{a \in x^{-1} O_\infty} (T(a))^s e(-Na)\, da. \tag{9}$$

Proof.

$$\int_{\alpha\in x^{-1}O_\infty} T^s(\alpha)e(-N\alpha)\,d\alpha$$
$$= \sum_{\operatorname{ord}P_1<m} \cdots \sum_{\operatorname{ord}P_s<m} \int_{\alpha\in x^{-1}O_\infty} e\big((P_1^k+\ldots+P_s^k-N)\alpha\big)\,d\alpha.$$

By Lemma 1(f) (with $n=0$) the integral inside the summation is 1 or 0 depending on whether $P_1^k+\ldots+P_s^k=N$ or not, and so the Lemma is proved.

2. THE FAREY ARCS

For $\alpha\in K_\infty$ there are a unique $P\in F_q[x]$ and a unique $\beta\in x^{-1}O_\infty$ such that $\alpha=P+\beta$. We define $[\alpha]=P$ and $((\alpha))=\beta$, the integral and fractional parts of α. Clearly $[\alpha]$ and $((\alpha))$ are F_q-linear functions of α.

LEMMA 3. *Let r be a positive integer. For every $\alpha\in x^{-1}O_\infty$ there are unique polynomials A, Q such that*

(a) $\operatorname{ord}Q\leqslant r$, $Q\neq 0$,

(b) *Q is monic,*

(c) $\operatorname{ord}A<\operatorname{ord}Q$,

(d) $(A,Q)=1$,

(e) $\left|\alpha-\dfrac{A}{Q}\right|<\dfrac{1}{q^r|Q|}$.

Proof. If $\alpha=0$, the result holds trivially with $A=0$. Now suppose $\alpha\neq 0$. There are q^{r+1} polynomials R of degree $\leqslant r$, so there are q^{r+1} power series $((R\alpha))$. These are distributed in q^r equivalence classes of $x^{-1}O_\infty$ $(\operatorname{mod} x^{-r-1}O_\infty)$. Consequently, there are R_1, R_2 such that $R_1\neq R_2$ and

$$((R_1\alpha))\equiv((R_2\alpha)) \quad (\operatorname{mod} x^{-r-1}O_\infty).$$

Put $Q_1=R_1-R_2$ and $A_1=[Q_1\alpha]$. Then $Q_1\neq 0$, $\operatorname{ord}Q_1\leqslant r$ and if $A_1\neq 0$ then $\operatorname{ord}A_1\leqslant\operatorname{ord}Q_1\alpha<\operatorname{ord}Q_1$. Also, $\operatorname{ord}(Q_1\alpha-A_1)=\operatorname{ord}((Q_1\alpha))$ $=\operatorname{ord}\big(((R_1\alpha))-((R_2\alpha))\big)<-r$, that is $\left|\alpha-\dfrac{A_1}{Q_1}\right|<q^{-r}\cdot\dfrac{1}{|Q_1|}$. Dividing Q_1 and A_1 by the leading coefficient of Q_1 and by their greatest common (monic) divisor, we get Q and A satisfying (a)–(e).

For uniqueness, suppose that A, Q and B, R are two pairs that satisfy the lemma. Then

$$\left|\frac{A}{Q}-\frac{B}{R}\right|\leqslant\max\left(\left|\alpha-\frac{A}{Q}\right|,\left|\alpha-\frac{B}{R}\right|\right)<\frac{1}{q^r}\max\left(\frac{1}{|Q|},\frac{1}{|R|}\right).$$

Therefore $|RA-QB|<1$ and since $RA-QB$ is a polynomial, we must

have $RA = QB$. Thus $\frac{A}{Q} = \frac{B}{R}$, but such a representation is unique when the denominator is monic and numerator and denominator are relatively prime.

For the next four sections, we let $k \geqslant 2$ and m be fixed positive integers. We fix r to be $r = (k-1)m$, and consider all pairs A, Q satisfying (a)–(d) of the lemma. The *Farey arc* about $\frac{A}{Q}$ is the set

$$M(A, Q) = \left\{ \alpha \in x^{-1} O_\infty \quad \text{where} \quad \left| \alpha - \frac{A}{Q} \right| < \frac{1}{q^{(k-1)m}} \cdot \frac{1}{|Q|} \right\}.$$

We shall say $M(A, Q)$ is a *major* (*minor*) *arc* if $\operatorname{ord} Q \leqslant m$ ($\operatorname{ord} Q > m$). From Lemma 3, it follows that the Farey arcs are pairwise disjoint and their union is $x^{-1} O_\infty$.

3. THE CONTRIBUTION OF THE MAJOR AND MINOR ARCS

Let

$$T(\alpha) = \sum_{\operatorname{ord} P < m} e(\alpha P^k) \tag{10}$$

and

$$S(A, Q) = \sum_{Z \,(\operatorname{mod} Q)} e\left(\frac{A}{Q} Z^k\right). \tag{11}$$

PROPOSITION 4. *If $M(A, Q)$ is a major arc and $\alpha = \frac{A}{Q} + \beta \in M(A, Q)$, then*

$$T(\alpha) = \frac{1}{|Q|} S(A, Q) T(\beta). \tag{12}$$

Proof. We may write P uniquely as

$$P = QY + Z, \quad \text{with} \quad \operatorname{ord} Z < \operatorname{ord} Q \leqslant m.$$

In (10) we have $\operatorname{ord} P < m$, therefore $\operatorname{ord} Y < m - \operatorname{ord} Q$. Also,

$$e\left(\frac{A}{Q} P^k\right) = e\left(\frac{A}{Q} (QY + Z)^k\right) = e\left(\frac{A}{Q}((QY + Z)^k - Z^k)\right) e\left(\frac{A}{Q} Z^k\right).$$

But the first factor being the exponential of a polynomial is equal to 1, and so

$$e\left(\frac{A}{Q} P^k\right) = e\left(\frac{A}{Q} Z^k\right).$$

Then

$$T(\alpha) = \sum_{\operatorname{ord} P<m} e\left(\left(\frac{A}{Q}+\beta\right)P^k\right) = \sum_{\operatorname{ord} P<m} e\left(\frac{A}{Q}P^k\right) e(\beta P^k),$$

and by the preceding comment,

$$T(\alpha) = \sum_{\operatorname{ord} Z<\operatorname{ord} Q} \sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\left(\frac{A}{Q}Z^k\right) e\big(\beta(QY+Z)^k\big) \tag{13}$$

$$= \sum_{\operatorname{ord} Z<\operatorname{ord} Q} e\left(\frac{A}{Q}Z^k\right) \sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\big(\beta(QY+Z)^k\big).$$

To handle the inside sum, notice that since $\alpha = \frac{A}{Q}+\beta$ where $\operatorname{ord}\beta < -(k-1)m-\operatorname{ord}Q$, we have

$$\operatorname{ord}\big(\beta(QY+Z)^k-\beta(QY)^k\big) \leqslant \operatorname{ord}\beta + \max_{1\leqslant v\leqslant k} \operatorname{ord}\binom{k}{v}(QY)^{k-v}Z^v$$

$$\leqslant -(k-1)m-1-\operatorname{ord}Q+\max_{1\leqslant v\leqslant k}\{(k-v)m+v(\operatorname{ord}Q-1)\}.$$

Since $\operatorname{ord}Q \leqslant m$, we conclude that

$$\operatorname{ord}\big(\beta(QY+Z)^k-\beta(QY)^k\big) < -1,$$

and, therefore,

$$e\big(\beta(QY+Z)^k\big) = e\big(\beta(QY)^k\big). \tag{14}$$

Summing over Y, we get the inside sum of (13) as

$$\sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\big(\beta(QY+Z)^k\big) = \sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\big(\beta(QY)^k\big), \tag{15}$$

which is independent of Z. On the other hand, there are $|Q|$ elements in $F_q[x]/QF_q(x)$ and hence summing (14) over Y and then over $|Q|$ residue classes $Z(\operatorname{mod}Q)$, we obtain

$$T(\beta) = \sum_{\operatorname{ord} Z<\operatorname{ord} Q} \sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\big(\beta(QY+Z)^k\big) \tag{16}$$

$$= |Q| \sum_{\operatorname{ord} Y<m-\operatorname{ord} Q} e\big(\beta(QY)^k\big).$$

Substituting this back into (13), using (11), we get the proposition.

PROPOSITION 5. *If $M(A,Q)$ is a minor arc and $\alpha\in M(A,Q)$ then*

$$T(\alpha) = T\left(\frac{A}{Q}\right). \tag{17}$$

Proof. Suppose $\alpha = \frac{A}{Q} + \beta$. Then

$$T(\alpha) = \sum_{\operatorname{ord} P < m} e\left(\frac{A}{Q} P^k\right) e(\beta P^k).$$

However, $\operatorname{ord} \beta P^k = \operatorname{ord} \beta + k \operatorname{ord} P < -(k-1)m - \operatorname{ord} Q + k(m-1)$. Since $M(A, Q)$ is a minor arc, $\operatorname{ord} Q \geqslant m+1$, so $\operatorname{ord} \beta P^k < -1$ and so

$$e(\beta P^k) = 1.$$

Hence (17) holds.

Definition. Let $\mathfrak{M}$ denote the set of major arcs. Let $\mathfrak{m}$ denote the set of minor arcs.

Lemma 6.

(a) *We have*

$$\int_{\mathfrak{M}} T^s(\alpha) e(-N\alpha)\, d\alpha = \sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q \leqslant m}} \sum_{\substack{\operatorname{ord} A < \operatorname{ord} Q \\ (A, Q) = 1}} \left(\frac{1}{|Q|} S(A, Q)\right)^s \times$$

$$\times\, e\left(-\frac{NA}{Q}\right) \int_{\operatorname{ord} \beta < -(k-1)m - \operatorname{ord} Q} T^s(\beta) e(-N\beta)\, d\beta.$$

(b) *If* $\operatorname{ord} N < km$, *then*

$$\int_{\mathfrak{m}} T^s(\alpha) e(-N\alpha)\, d\alpha$$

$$= q^{-(k-1)m} \sum_{\substack{Q \text{ monic} \\ m < \operatorname{ord} Q \leqslant (k-1)m}} \frac{1}{|Q|} \sum_{\substack{\operatorname{ord} A < \operatorname{ord} Q \\ (A, Q) = 1}} T^s\left(\frac{A}{Q}\right) e\left(-\frac{NA}{Q}\right).$$

Proof. (a) If $\alpha = \frac{A}{Q} + \beta$ then $e(-N\alpha) = e\left(-\frac{NA}{Q}\right) e(-N\beta)$. By Proposition 4, the integral over the major arcs $M(A, Q)$ gives the corresponding term on the right.

(b) If $\alpha = \frac{A}{Q} + \beta$, then $e(-N\alpha) = e\left(-\frac{NA}{Q}\right) e(-N\beta)$. If $\operatorname{ord} N < km$, then

$$\operatorname{ord}(-N\beta) < km - (k-1)m - \operatorname{ord} Q - 1 < -1.$$

Therefore $e(-N\beta) = 1$. By Proposition 5, the integral over the minor arcs $M(A, Q)$ gives the corresponding term on the right.

4. WEYL'S LEMMA

The purpose of this section is to show that $T(\alpha)$ is relatively small on the minor arcs provided $k < \operatorname{char} F_q$, and so the contribution of the minor arcs is negligible.

LEMMA 7.

$$\sum_{\operatorname{ord} P<m} e(\beta P) = \begin{cases} q^m, & \text{if} \quad \operatorname{ord}((\beta)) < -m, \\ 0, & \text{if} \quad \operatorname{ord}((\beta)) \geqslant -m. \end{cases} \tag{18}$$

Proof. If $\operatorname{ord}((\beta)) < -m$, then for each of the q^m polynomials P of $\deg < m$, we have $\operatorname{res}\beta P = 0$, and so $e(\beta P) = 1$. On the other hand, if $((\beta)) = \sum_{-\infty}^{-t-1} b_i x^i$ where $b_{-t-1} \neq 0$ and $0 > -t-1 \geqslant -m$ and $P = \sum_0^{m-1} p_i x^i$, then

$$\operatorname{res}\beta P = p_t b_{-t-1} + p_{t+1} b_{-t-2} + \ldots + p_{m-1} b_{-m}.$$

One now repeats the calculation used in Lemma 1(f) to obtain (18).

Again, in the sum (18), we are summing (perhaps several times) over all the pth roots of 1.

LEMMA 8. *Let $d(R)$ be the number of monic polynomials dividing R. If $R \neq 0$ then for every $\varepsilon > 0$,*

$$d(R) \ll |R|^{\varepsilon}, \tag{19}$$

that is $d(R) \leqslant C(\varepsilon)|R|^{\varepsilon}$, where $C(\varepsilon)$ is a constant depending only on ε (not on R).

Proof. If $P =$ constant, $d(P) = 1$ and the result is trivial, so we may assume $\operatorname{ord} P > 0$.

If P is an irreducible polynomial, then, for $n \geqslant 1$,

$$\frac{d(P^n)}{|P|^{n\varepsilon}} = \frac{n+1}{|P|^{n\varepsilon}} \leqslant \frac{n+1}{q^{n\varepsilon}} \leqslant \frac{n+1}{n\varepsilon \log q} \leqslant \frac{2}{\varepsilon \log q}.$$

Furthermore, if $\operatorname{ord} P \geqslant 1/\varepsilon$, that is, if $|P| \geqslant q^{1/\varepsilon}$ then

$$\frac{d(P^n)}{|P|^{n\varepsilon}} \leqslant \frac{n+1}{q^n} \leqslant 1.$$

For arbitrary $R \neq 0$,

$$\frac{d(R)}{|R|^{\varepsilon}} \leqslant \prod_{\substack{P|R \\ P \text{ irred}}} \frac{d(P^{n(P)})}{|P|^{n(P)\varepsilon}} \leqslant \prod_{\substack{P|R \\ \operatorname{ord} P<1/\varepsilon \\ P \text{ irred}}} \frac{2}{\varepsilon \log q} \leqslant \prod_{\substack{\operatorname{ord} P<1/\varepsilon \\ P \text{ irred}}} \frac{2}{\varepsilon \log q}.$$

This last term is a function only of ε and so the lemma follows.

LEMMA 9. *If* $\alpha = \frac{A}{Q} + \beta$ *where* $\operatorname{ord} Q \leqslant (k-1)m$, A, Q *are relatively prime*, $A \neq 0$, *and*

$$|\beta| < \frac{1}{|Q|^2}, \tag{20}$$

then the number D *of ordered* $(k-1)$*-tuples of polynomials* $P_1, \ldots, P_{k-1}$, *where* $\operatorname{ord} P_i < m$, $i = 1, \ldots, k-1$, *and*

$$\operatorname{ord}((\alpha P_1 \ldots P_{k-1})) < -m \tag{21}$$

is:

$$D \ll q^{\varepsilon m}\left(1 + \frac{|Q|}{q^m}\right)\left(1 + \frac{q^{(k-1)m}}{|Q|}\right). \tag{22}$$

Remark. Here and in all subsequent work the constant implied by $\ll$ will be independent of m, though it may depend on k, q, ε, etc.

Proof. Let us collect together those $(k-1)$-tuples with the same product, say, $U = P_1 \ldots P_{k-1}$. By Lemma 8, the number of such tuples is not more than

$$\big((q-1)\,d(U)\big)^{k-1} \ll q^{k-1}|U|^{(k-1)\varepsilon'} \ll q^{\varepsilon m}, \tag{23}$$

since $\operatorname{ord} U < (k-1)m$ and the factor q^{k-1} may be absorbed in $q^{\varepsilon m}$.

Now any such U may be written as

$$U = V + QW \tag{24}$$

where $\operatorname{ord} V < \operatorname{ord} Q$ and $\operatorname{ord} W < (k-1)m - \operatorname{ord} Q$.

Suppose a particular $U_0 = V_0 + QW_0$ satisfies the inequality

$$\operatorname{ord}((\alpha U_0)) < -m. \tag{25}$$

Then any other U of the form $U = V + QW_0$ satisfies (25) if and only if

$$\operatorname{ord}\big((\alpha(U - U_0))\big) = \operatorname{ord}\big((\alpha(V - V_0))\big) < -m. \tag{26}$$

Since $\alpha = \frac{A}{Q} + \beta$,

$$\operatorname{ord}\big((\alpha(V - V_0))\big) = \operatorname{ord}\left\{\left(\left(\frac{A}{Q}(V - V_0)\right)\right) + \big((\beta(V - V_0))\big)\right\}. \tag{27}$$

Now by (20), we have $\operatorname{ord}\big((\beta(V - V_0))\big) < -2\operatorname{ord} Q + \operatorname{ord} Q \leqslant -\operatorname{ord} Q$. Also, since $(A, Q) = 1$, if $V \neq V_0$ then $A(V - V_0) \not\equiv 0 \pmod{Q}$, so that $\operatorname{ord}\left(\left(\frac{A}{Q}(V - V_0)\right)\right) \geqslant -\operatorname{ord} Q$. Therefore, the ord of the sum on the right of (27) is simply the larger of the two, i.e.,

$$\operatorname{ord}\big((\alpha(V - V_0))\big) = \operatorname{ord}\left(\left(\frac{A}{Q}(V - V_0)\right)\right).$$

We further note that since $(A, Q) = 1$, as V runs over a complete set of residues $(\mathrm{mod}\, Q)$ so does $A(V-V_0)$. Also there are precisely $\max(1, q^{-m}|Q|)$ residue classes Y such that $\mathrm{ord}\left(\left(\frac{Y}{Q}\right)\right) < -m$. (The max depends on whether $\mathrm{ord}\, Q \leqslant m$ or not.)

Combining this facts, we see that as there are at most $O(q^{\varepsilon m})$ tuples leading to a particular value $U = V + QW$, and at most $\max\left(1, \frac{q^{(k-1)m}}{|Q|}\right)$ choices of W, and for each W, at most $\max\left(1, \frac{|Q|}{q^m}\right)$ choices of V. Thus we have

$$D \ll q^{\varepsilon m}\left(1+\frac{|Q|}{q^m}\right)\left(1+\frac{q^{(k-1)m}}{|Q|}\right).$$

LEMMA 10. *Let $f(y) = ay^k + \ldots + a_k$ be a polynomial in $K_\infty[y]$. For each $z \in F_q[x]$, we define*

$$\Delta_z(f) = f(y+z) - f(y). \tag{28}$$

Then Δ_z: $K_\infty[y] \to K_\infty[y]$ is a map such that

(a) *Δ_z is linear over K_∞.*

(b) *$\Delta_0 = 0$.*

(c) *If f has polynomial coefficients, that is $f \in F_q[x, y]$, then $\Delta_z(f)$ has polynomial coefficients and z divides the content $(\Delta_z f)$.*

(d) *If $\deg f = k < \mathrm{char}\, F_q$ and $z \neq 0$, then*

$$\deg \Delta_z f = k-1,$$

and the leading coefficient of $\Delta_z f$ is kaz.

(e) *If $\deg f = k < \mathrm{char}\, F_q$, and $z_1, \ldots, z_{k-1} \neq 0$, then*

$$\Delta_{z_{k-1}}(\ldots(\Delta_{z_1} f)) = k!az_1 \ldots z_{k-1} y + \textit{terms free of } y.$$

Proof. (a) and (b) are trivial. (c) and (d) follow from (a) and the fact that

$$\Delta_z(y^k) = kzy^{k-1} + \binom{k}{2} z^2 y^{k-2} + \ldots + z^k.$$

(e) follows from (d) by induction.

LEMMA 11. *If $f \in K_\infty[y]$ and $S(f) = \sum_{\mathrm{ord}\, P < m} e(f(P))$ and $n \geqslant 1$, then*

$$|S(f)|^{2^n} \leqslant q^{m(2^n-n-1)} \sum_{\mathrm{ord}\, P_1 < m} \sum_{\mathrm{ord}\, P_2 < m} \cdots \sum_{\mathrm{ord}\, P_n < m} S\big(\Delta_{P_n}(\ldots \Delta_{P_1}(f) \ldots)\big). \tag{29}$$

Proof. We proceed by induction. For $n = 1$,

$$|S(f)|^2 = S(f)\overline{S(f)} = \sum_{\operatorname{ord} Q<m} e\big(f(Q)\big) \sum_{\operatorname{ord} P<m} e\big(-f(P)\big)$$
$$= \sum_{\operatorname{ord} P<m} \sum_{\operatorname{ord} Q<m} e\big(f(Q)-f(P)\big).$$

Writing $Q = P+P_1$, and summing instead over P_1

$$(30) \qquad |S(f)|^2 = \sum_{\operatorname{ord} P_1<m} \sum_{\operatorname{ord} P<m} e\big(f(P+P_1)-f(P)\big) = \sum_{\operatorname{ord} P_1<m} S(\Delta_{P_1} f).$$

This is (29) for $n = 1$.

Now suppose we have shown (29) for n, where $n \geqslant 1$. Then

$$(31) \qquad |S(f)|^{2^{n+1}} = \big(|S(f)|^{2^n}\big)^2$$
$$\leqslant \big(q^{m(2^n-n-1)}\big)^2 \Big\{\sum_{(P_1,\ldots,P_n)} S\big(\Delta_{P_n}\cdots\Delta_{P_1}(f)\big)\Big\}^2$$
$$\leqslant (q^m)^{2^{n+1}-(n+1)-1-n} \Big\{\sum_{(P_1,\ldots,P_n)} |S(\Delta_{P_n}\cdots\Delta_{P_1} f)|\Big\}^2,$$

since $2(2^n-n-1) = 2^{n+1}-2(n+1) = 2^{n+1}-(n+1)-1-n$. Now we apply Cauchy's inequality

$$\Big(\sum a_i b_i\Big)^2 \leqslant \Big(\sum a_i^2\Big)\Big(\sum b_i^2\Big),$$

with $i = (P_1,\ldots,P_n)$, $a_i = 1$, $b_i = \big|S\big(\Delta_{P_n}\cdots\Delta_{P_1}(f)\big)\big|$, to get

$$(32) \qquad |S(f)|^{2^{n+1}} \leqslant q^{m(2^{n+1}-(n+1)-1)} \sum_{(P_1,\ldots,P_n)} \big|S\big(\Delta_{P_n}\cdots\Delta_{P_1}(f)\big)\big|^2.$$

To each of the terms of the sum on the right we may apply the first induction step (30) for $f = \Delta_{P_n}\cdots\Delta_{P_1}(f)$ to get the lemma for $n+1$.

PROPOSITION 12 (Weyl). *If* $f(y) = ay^k + a_1 y^{k-1} + \ldots + a_k$, $a_i \in K_\infty$, *and*

(a) $2 \leqslant k < \operatorname{char} F_q$,

(b) $\alpha = \dfrac{A}{Q} + \beta$ *where* A *and* Q *are relatively prime and*

$$(33) \qquad |\beta| < \frac{1}{|Q|^2},$$

then, for every $\varepsilon > 0$,

$$(34) \qquad |S(f)| \leqslant \Big|\sum_{\operatorname{ord} P<m} e\big(f(P)\big)\Big| \ll q^{m(1+\varepsilon)} \left(\frac{1}{q^m} + \frac{1}{|Q|} + \frac{|Q|}{q^{km}}\right)^{1/2^{k-1}}.$$

In particular, when $m < \operatorname{ord} Q \leqslant (k-1)m$,

$$|S(f)| \ll q^{m\left(1-\frac{1}{2^{k-1}}+s\right)}.$$

Proof. From Lemma 11, when $n = k-1$, we find that

$$(35) \qquad |S(f)|^{2^{k-1}} \leqslant q^{m(2^{k-1}-k)} \sum_{\operatorname{ord} P_{k-1}<m} \cdots \sum_{\operatorname{ord} P_1<m} S\big(\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f)\big).$$

In this sum, when any $P_i = 0$, it follows from Lemma 10 (a) and (b) that

$$\Delta_{P_{k-1}} \cdots \Delta_{P_1} f = 0,$$

so that, when some $P_i = 0$, we have

$$(36) \qquad S\big(\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f)\big) = \sum_{\operatorname{ord} P<m} e\big(\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f(P))\big) = q^m.$$

There are $q^{m(k-1)}$ choices of $P_1, \ldots, P_{k-1}$ and $(q^m-1)^{k-1}$ choices with each $P_i \neq 0$. Therefore the number of choices when some $P_i = 0$ is

$$\begin{aligned}
(q^m)^{k-1} - (q^m-1)^{k-1} &= (k-1)\,q^{m(k-2)} - \binom{k-1}{2} q^{m(k-3)} + \ldots \\
&\leqslant q^{m(k-2)} \sum_{1}^{k-1} \binom{k-1}{j} \left(\frac{1}{q^m}\right)^{j-1} \\
&\leqslant q^{m(k-2)} \left\{\left(1+\frac{1}{q^m}\right)^{k-1} - 1\right\} \\
&\leqslant \left(\frac{3}{2}\right)^{k-1} q^{m(k-2)} \qquad (\text{since } q^m \geqslant 2) \\
&\ll q^{m(k-2)}.
\end{aligned}$$

Therefore (35) becomes

$$(37) \qquad |S(f)|^{2^{k-1}} \ll (q^m)^{2^{k-1}-1} + (q^m)^{2^{k-1}-k} \sum_{P_{k-1}} \cdots \sum_{P_1}{}^{*} S(\Delta_{P_{k-1}} \cdots \Delta_{P_1} f),$$

where $*$ indicates the sum is over those $P_i \neq 0$.

By Lemma 10(e),

$$\big|S\big(\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f)\big)\big| = \Big|\sum_{\operatorname{ord} P<m} e(k!aP_1 \ldots P_{k-1}P)\Big|.$$

By Lemma 7, the sum on the right is either 0 or q^m depending on whether $\operatorname{ord}((k!aP_1 \ldots P_{k-1})) \geqslant -m$ or not. Since $k < \operatorname{char} F_q$, we see that $k!$ is a non-zero unit and,

$$\operatorname{ord}((k!aP_1 \ldots P_{k-1})) = \operatorname{ord}((aP_1 \ldots P_{k-1})).$$

By Lemma 9, the number of tuples $P_1, \ldots, P_{k-1}$ contributing to the sum is

$$O\left(q^{\varepsilon m}\left(1+\frac{|Q|}{q^m}\right)\left(1+\frac{q^{(k-1)m}}{|Q|}\right)\right).$$

Therefore (37) becomes

$$\begin{aligned}|S(f)|^{2^{k-1}} &\ll q^{m(2^{k-1}-1)}+q^{m(2^{k-1}-k)}q^m q^{\varepsilon m}\left(1+\frac{|Q|}{q^m}\right)\left(1+\frac{q^{(k-1)m}}{|Q|}\right)\\ &\ll q^{m(2^{k-1}+\varepsilon)}\left(\frac{1}{q^m}+\frac{1}{|Q|}+\frac{|Q|}{q^{km}}\right).\end{aligned}$$

PROPOSITION 13 (Hua). *Let* $S(aG) = \sum_{\operatorname{ord} P<m} e\big(aG(P)\big)$, *where* $G(y) \in F_q[x][y]$ *and let* ν *be an integer such that* $\Delta_{y_\nu} \ldots \Delta_{y_1} G(y) \in F_q[x]\,[y, y_1, \ldots, y_\nu]$ *satisfies*

$$\Delta_{y_\nu} \ldots \Delta_{y_1} G(y) \neq 0. \tag{38}$$

Then, for every $\varepsilon > 0$,

$$I_\nu = \int_{a \in x^{-1}O_\infty} |S(aG)|^{2^\nu} da \ll q^{m(2^\nu-\nu+\varepsilon)}. \tag{39}$$

In particular, if $k = \deg_y G(y) < \operatorname{char} F_q$, *then*

$$I_k \ll q^{m(2^k-k+\varepsilon)}. \tag{40}$$

Proof. The last remark is an instance of (39) since (38) is automatically satisfied if $k < \operatorname{char} F_q$. We proceed by induction noting that (38) for ν implies the stronger condition

$$\deg_y \Delta_{y_\mu} \ldots \Delta_{y_1} G \geqslant 1$$

for $\mu < \nu$. For $\nu = 1$, condition (38) says that $k = \deg_y G \geqslant 1$. Also,

$$I_1 = \int_{a \in x^{-1}O_\infty} \sum_{\operatorname{ord} P_1<m} e\big(+aG(P_1)\big) \sum_{\operatorname{ord} P_1<m} e\big(-aG(P_2)\big)\, da = \mathfrak{N}$$

where $\mathfrak{N}$ is the number of tuples (P_1, P_2) such that $\operatorname{ord} P_1 < m$, $\operatorname{ord} P_2 < m$ and

$$G(P_1) = G(P_2).$$

(See Lemma 1(f).) Picking P_1 arbitrarily, there are at most k solutions P_2 of $G(P_2) = G(P_1)$. Therefore

$$I_1 \leqslant k \cdot q^m \ll q^m \ll q^{m(2^1-1+\varepsilon)}.$$

Suppose we have proved the proposition for ν and that (38) holds also for $\nu+1$. Formula (29), Lemma 11, for $n=\nu$ and $f=\alpha G$, reads

$$|S(\alpha G)|^2 \leqslant q^{m(2^\nu-\nu-1)} \sum_{\operatorname{ord} P_\nu<m} \cdots \sum_{\operatorname{ord} P_1<m} S\big(\Delta_{P_\nu}\cdots\Delta_{P_1}(\alpha G)\big).$$

Multiplying this inequality by $|S(\alpha G)|^{2^\nu}$ and integrating we have

$$\begin{aligned}(41)\qquad I_{\nu+1} &\leqslant q^{m(2^\nu-\nu-1)} \int_{\alpha\in x^{-1}O_\infty} \sum_{P_\nu}\cdots\sum_{P_1} S\big(\Delta_{P_\nu}\cdots\Delta_{P_1}(\alpha G)\big)\cdot|S(\alpha G)|^{2^\nu}\,d\alpha\\ &\leqslant q^{m(2^\nu-\nu-1)}\cdot\mathfrak{N}',\end{aligned}$$

where $\mathfrak{N}'$ is the number of solutions (P, P_i, Q_j, R_l) of

$$\begin{aligned}(*)\quad 0 &= \Delta_{P_\nu}\cdots\Delta_{P_1}G(P)+G(Q_1)+\ldots+G(Q_{2^\nu-1})-G(R_1)-\ldots-G(R_{2^\nu-1})\\ &= \Delta_{P_\nu}\cdots\Delta_{P_1}G(P)+B(Q_1,\ldots,Q_{2^\nu-1},R_1,\ldots,R_{2^\nu-1}),\end{aligned}$$

where all variables run over polynomials of degree $<m$.

We show by induction the following: If $H(y_1,\ldots,y_n)\neq 0$ is an arbitrary polynomial of total degree $\ll 1$ then there are $O(q^{m(n-1)})$ solutions $Y_1,\ldots,Y_n$ of $H(Y_1,\ldots,Y_n)=0$, where each Y_i is a polynomial of degree $<n$. We may suppose H actually involves y_n, thus

$$H(y_1,\ldots,y_n)=H_t(y_1,\ldots,y_{n-1})y_n^t+\ldots+H_0(y_1,\ldots,y_{n-1}).$$

Given $Y_1,\ldots,Y_{n-1}$ not on the hypersurface $H_0=H_1=\ldots=H_t=0$ there are at most $t=O(1)$ zeros for Y_n, thus at most $O(q^{m(n-1)})$ choices Y not on the hypersurface. To be on this hypersurface, indeed to be on $H_t=0$, the induction hypothesis says there are at most $O(q^{m(n-2)})$ choices for $Y_1,\ldots,Y_{n-1}$, and Y_n may then be chosen arbitrarily. Thus there are $O(q^{m(n-1)})$ choices in all.

As there are exactly I_ν solutions Q_j, R_l of $B=0$, there are $\ll q^{m\nu}I_\nu$ solutions of $(*)$ with $B=0$. For fixed $B\neq 0$, then outside the hypersurface where the coefficients of the powers of y disappear, given $P_1,\ldots,P_\nu$ there are $O(1)$ choices for P such that $(*)$ holds. By Lemma 10 (c), $P_i|B$, $i=1,\ldots,\nu$. Thus, by Lemma 8, there are at most $\ll\big((q-1)d(B)\big)^\nu \ll q^k\cdot q^{ks'm}\ll q^{ms}$ choices for $P_1,\ldots,P_\nu$. Taking Q_i, R_j arbitrarily there are at most $O(q^{(2^\nu+s)m})$ solutions P, P_i, Q_j, R_l off the hypersurface.

On the hypersurface P may be picked arbitrarily. But to be on the hypersurface, there are $O(q^{m(\nu-1)})$ choices for $P_1,\ldots,P_\nu$ and so at most $O(q^{m(\nu-1)})$ choices for B. For any particular value of B, the number of Q_j, R_l giving B is

$$\mathfrak{N}_1=\int_{\alpha\in x^{-1}O_\infty}|S(\alpha G)|^{2^\nu}e(-\alpha B)\,d\alpha\leqslant I_\nu\ll q^{m(2^\nu-\nu+s)}.$$

There are, therefore,

$$\ll q^m \cdot q^{m(\nu-1)} q^{m(2^\nu-\nu+s)} \ll q^{m(2^\nu+s)}$$

solutions when $B \neq 0$ and on this hypersurface.

Therefore $\mathfrak{N}' \ll q^{m\nu} I_\nu + q^{m(2^\nu+s)}$. Together with (41) and the induction hypothesis,

$$I_{\nu+1} \ll q^{m(2^\nu-\nu-1)} \{q^{m\nu} I_\nu + q^{m(2^\nu+s)}\} \ll q^{m(2^{\nu+1}-(\nu+1)+s)}.$$

THEOREM 14. *If* $k < \operatorname{char} F_q$ *and* $s \geqslant 2^k+1$, *then there is an* $\varepsilon > 0$ *such that*

$$\left| \int_{\mathfrak{m}} T^s(a) e(-Na)\, da \right| \ll q^{m(s-k-\varepsilon)}. \tag{42}$$

Proof. Since $s \geqslant 2^k+1$,

$$I = \left| \int_{\mathfrak{m}} T^s(a)\, e(-Na)\, da \right| \leqslant \int_{\mathfrak{m}} |T(a)|^s |e(-Na)|\, da$$

$$\leqslant \{\max_{a \in \mathfrak{m}} |T(a)|\}^{s-2^k} \int_{\mathfrak{m}} |T(a)|^{2^k} da.$$

The factor in braces may be estimated using Weyl's Lemma (Proposition 12) and the integral may be estimated using Proposition 13. Thus:

$$I \ll q^{m\left(1-\frac{1}{2^{k-1}}+\delta\right)(s-2^k)} \cdot q^{m(2^k-k+\delta')} \ll (q^m)^{(s-k)-\left\{(s-2^k)\left(\frac{1}{2^{k-1}}-\delta\right)-\delta'\right\}}.$$

Taking $\delta = \dfrac{1}{2^k}$, $\delta' = \dfrac{1}{2^{k+1}}$ we have

$$I \ll q^{m\left(s-k-\frac{1}{2^{k+1}}\right)}.$$

5. THE SINGULAR INTEGRAL

In this section we evaluate

$$\int_{\operatorname{ord}\beta < -(k-1)m - \operatorname{ord} Q} T^s(\beta)\, e(-N\beta)\, d\beta.$$

LEMMA 15. *For* $m' \geqslant 0$, *let* $V(s, N, m')$ *be the number of ordered tuples* $P_1, \ldots, P_s$ *such that* $\operatorname{ord} P_i \leqslant m$, $i = 1, \ldots, s$ *and*

$$\operatorname{ord}(P_1^k + \ldots + P_s^k - N) < m'. \tag{43}$$

Then

$$\int_{\operatorname{ord}\beta < -m'} T^s(\beta)\, e(-N\beta)\, d\beta = q^{-m'} V(s, N, m'). \tag{44}$$

Proof. The integral (44) is

$$\int_{\operatorname{ord}\beta<-m'} \sum_{\operatorname{ord}P_1<m} \cdots \sum_{\operatorname{ord}P_s<m} e\big((P_1^k+\ldots+P_s^k-N)\beta\big)\,d\beta.$$

According to Lemma 1(f), each s-tuple $P_1, \ldots, P_s$ contributes $q^{-m'}$ or 0 according to whether $\operatorname{ord}(P_1^k+\ldots+P_s^k-N) < m'$ or not.

LEMMA 16. *Let m', n be integers such that $0 \leqslant n < m$, and $(k-1)m \leqslant m' \leqslant kn$. Let N be a polynomial of degree $l \leqslant kn$ and leading coefficient b (where if $N = 0$, we take $l = 0$, $b = 0$). Suppose $c_1, \ldots, c_s$ are in F_q, not all zero, such that*

$$c_1^k+\ldots+c_s^k = \begin{cases} 0, & \text{if } l < kn, \\ b, & \text{if } l = kn. \end{cases} \tag{45}$$

If $p = \operatorname{char} F_q \nmid k$ then the number of tuples $P_1, \ldots, P_s$ such that

$$P_i = c_i x^n + P_i', \quad \operatorname{ord} P_i' < n, \quad i = 1, \ldots, s, \tag{46}$$

and such that

$$\operatorname{ord}(P_1^k+\ldots+P_s^k-N) < m', \tag{47}$$

is $q^{(s-k)n+m'}$.

Proof. In (45), let t be the least index such that $c_t \neq 0$. Let $P_t = c_t x^n + d_{n-1}x^{n-1}+\ldots+d_0$. Let $R = N - \sum_{i\neq t} P_i^k = \sum_0^{kn} r_i x^i$. Let $R' = \sum_{i=1}^s P_i^k - N = P_t^k - R = \sum_0^{kn} r_i' x^i$.

A particular s-tuple $P_1, \ldots, P_s$ is to be counted if and only if $\operatorname{ord} R' < m'$, that is, if and only if

$$r_i' = 0, \quad i = kn, kn-1, \ldots, m'. \tag{48}$$

Condition (45) of the hypothesis insures $r_{kn}' = 0$. For the remaining i,

$$\begin{aligned} 0 &= r_{kn-1}' = kc_t^{k-1} d_{n-1} - r_{kn-1}, \\ 0 &= r_{kn-2}' = kc_t^{k-1} d_{n-2} + \binom{k}{2} c_t^{k-2} d_{n-1}^2 - r_{kn-2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0 &= r_{m'}' = kc_t^{k-1} d_{m'-(k-1)n} - r_{m'} \text{ terms involving } d_i, \\ &\qquad\qquad\qquad\qquad \text{where } m'-(k-1)n < i < n. \end{aligned} \tag{49}$$

(Here $m'-(k-1)n > 0$ since $m' \geqslant (k-1)m > (k-1)n$.)

Thus any tuple $P_1, \ldots, P_s$ to be counted satisfies the set of equations (49). Conversely, since $kc_t^{k-1} \neq 0$, we may pick P_i', $i \neq t$, arbitrarily, and pick d_i, $i < m'-(k-1)n$, arbitrarily and determine the remaining

d_i's by (49). This gives us a tuple $P_1, \ldots, P_s$ to be counted. In all, the number of choices is

$$q^{(s-1)n+m'-(k-1)n} = q^{(s-k)n+m'}.$$

LEMMA 17. *Let m' be an integer, $(k-1)m \leqslant m' \leqslant km$. Let N be a polynomial of degree $l \leqslant k(m-1)$ and leading coefficient b (where, for $N = 0$, we take $l = 0$, $b = 0$). Let $U(s, b)$ be the number of tuples $c_1, \ldots, c_s$ such that $c_i \in F_q$ for $i = 1, \ldots, s$, with not all $c_i = 0$, and*

$$c_1^k + \ldots + c_s^k = b.$$

If $p = \operatorname{char} F_q \nmid k$ and $s > k$ and if

$$U(s, 0) > 0, \quad \text{if} \quad l < k(m-1), \tag{50}$$

$$U(s, b) > 0, \quad \text{if} \quad l = k(m-1), \tag{51}$$

then

$$\int_{\operatorname{ord}\beta < -m'} T^s(\beta) e(-N\beta)\, d\beta = C(s, N, m') q^{(s-k)m}, \tag{52}$$

where $0 < C(s, N, m') \ll 1$. The actual value of $C(s, N, m')$ is given according to the following formulae:

Case (a). *If $k \nmid l$ and $m' \leqslant l$ then*

$$C(s, N, m') = \frac{U(s, 0)}{q^{s-k}-1}\left(1 - q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right). \tag{53}$$

Case (b). *If $k | l$ and $m' \leqslant l$ then*

$$\begin{aligned} C(s, N, m') &= \frac{U(s, 0)}{q^{s-k}-1}\left(1 - q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right) + U(s, b) q^{-(s-k)\left(m-\left[\frac{l}{k}\right]\right)}. \end{aligned} \tag{54}$$

Case (c). *If $l < m'$ then*

$$\begin{aligned} C(s, N, m') &= \frac{U(s, 0)}{q^{s-k}-1}\left(1 - q^{-(s-k)\left(m-1-\left[\frac{m'-1}{k}\right]\right)}\right) + q^{s\left(\left[\frac{m'-1}{k}\right]+1\right)-(s-k)m-m'}. \end{aligned} \tag{55}$$

Proof. According to Lemma 15,

$$\int_{\operatorname{ord}\beta < -m'} T^s(\beta) e(-N\beta)\, d\beta = q^{-m'} V(s, N, m').$$

For any tuple of polynomials $P_1, \ldots, P_s$, let $n = \max_{1 \leqslant i \leqslant s} \operatorname{ord} P_i$. We propose to calculate $V(s, N, m')$ directly using Lemma 16, in each of the three cases.

Case (a). If $k \nmid l$ and $m' \leqslant l$, then for values of $n \leqslant \left[\frac{l}{k}\right]$ there are no tuples to be counted in $V(s, N, m')$. For the remaining values of n, we have $\left[\frac{l}{k}\right]+1 \leqslant n \leqslant m-1$. Hence, by Lemma 16,

$$\begin{aligned} V(s, N, m') &= \sum_{n=\left[\frac{l}{k}\right]+1}^{m-1} U(s, 0) q^{(s-k)n+m'} \\ &= U(s, 0) q^{m'+(s-k)\left(\left[\frac{l}{k}\right]+1\right)} \left(\frac{q^{(s-k)\left(m-\left[\frac{l}{k}\right]-1\right)}-1}{q^{s-k}-1} \right) \\ &= \frac{U(s, 0)}{q^{s-k}-1} \left(1-q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right) q^{(s-k)m+m'}. \end{aligned}$$

Therefore,

$$C(s, N, m') = q^{-(s-k)m-m'} V(s, N, m') = \frac{U(s, 0)}{q^{s-k}-1} \left(1-q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right).$$

Since $s > k$ and $k \nmid l$ and $l \leqslant k(m-1)$,

$$(s-k)\left(m-1-\left[\frac{l}{k}\right]\right) \geqslant 1.$$

Therefore $0 < C(s, N, m') \ll 1$.

Case (b). If $k|l$ and $m' \leqslant l$, then there are no tuples to be counted with $n < \left[\frac{l}{k}\right]$. Using Lemma 16

$$V(s, N, m') = U(s, b) q^{(s-k)\left[\frac{l}{k}\right]+m'} + \sum_{n=\left[\frac{l}{k}\right]+1}^{m-1} U(s, 0) q^{(s-k)n+m'}.$$

Arguing as in case (a) we obtain

(56) $$\begin{aligned} &C(s, N, m') \\ &\quad = U(s, b) q^{-(s-k)\left(m-\left[\frac{l}{k}\right]\right)} + \frac{U(s, 0)}{q^{s-k}-1} \left(1-q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right). \end{aligned}$$

Since $s > k$ and $l \leqslant k(m-1)$,

$$(s-k)\left(m-\left[\frac{l}{k}\right]-1\right) \geqslant 0,$$

and

$$(s-k)\left(m-\left[\frac{l}{k}\right]\right) > 0.$$

Therefore

$$0 \leqslant U(s, b) q^{-(s-k)\left[m-\frac{l}{k}\right]} \ll 1,$$

$$0 \leqslant \frac{U(s, 0)}{q^{s-k}-1} \left(1-q^{-(s-k)\left(m-1-\left[\frac{l}{k}\right]\right)}\right) \ll 1.$$

However conditions (50) and (51) of the hypothesis insure that at least one of these terms is strictly positive.

Case (c). If $m' > l$, then for $n \leqslant \left[\frac{m'-1}{k}\right]$; that is, for $\operatorname{ord} P_i^k < m'$, $i = 1, \ldots, s$; $P_1, \ldots, P_s$ may be picked arbitrarily. There are $q^{s\left(\left[\frac{m'-1}{k}\right]+1\right)}$ such choices. Using Lemma 16 for $\left[\frac{m'-1}{k}\right]+1 \leqslant n \leqslant m-1$,

$$V(s, N, m') = q^{s\left(\left[\frac{m'-1}{k}\right]+1\right)} + U(s, 0) \sum_{n=\left[\frac{m'-1}{k}\right]+1}^{m-1} q^{(s-k)n+m'}.$$

Again, arguing as in case (a),

$$\begin{aligned} C(s, N, m') &= q^{-(s-k)m-m'} V(s, N, m') \\ &= q^{s\left(\left[\frac{m'-1}{k}\right]+1\right)-(s-k)m-m'} + \frac{U(s, 0)}{q^{s-k}-1}\left(1 - q^{-(s-k)\left(m-1-\left[\frac{m'-1}{k}\right]\right)}\right). \end{aligned}$$

Since $m' \leqslant km$ and $s > k$ we have

$$(s-k)\left(m-1-\left[\frac{m'-1}{k}\right]\right) \geqslant 0,$$

and

$$\begin{aligned} (57) \qquad & s\left(\left[\frac{m'-1}{k}\right]+1\right)-(s-k)m-m' \\ &= -(s-k)\left(m-1-\left[\frac{m'-1}{k}\right]\right)+k\left[\frac{m'-1}{k}\right]+k-m' \leqslant k-1. \end{aligned}$$

Therefore

$$0 < C(s, N, m') \ll 1.$$

THEOREM 18. *Let ε be a real number, $0 < \varepsilon < 1$. Let Q be a polynomial such that* $\operatorname{ord} Q < \varepsilon m$. *Let N be a polynomial such that* $\operatorname{ord} N < (k-1+\varepsilon)m$. *If $p = \operatorname{char} F_q \nmid k$ and $s > 2k$ and $U(s, 0) > 0$, then for all sufficiently small $\delta > 0$,*

$$(57a) \qquad \int_{\operatorname{ord}\beta < -(k-1)m - \operatorname{ord} Q} T^s(\beta) e(-N\beta)\, d\beta = \frac{U(s, 0)}{q^{s-k}-1} q^{(s-k)m} + O(q^{(s-k-\delta)m}).$$

Proof. We use the three cases of the previous lemma with

$$m' = (k-1)m + \operatorname{ord} Q \leqslant (k-1+\varepsilon)m, \quad \text{and} \quad l = \operatorname{ord} N \leqslant (k-1+\varepsilon)m.$$

According to the hypothesis of Lemma 17, we must have $l \leqslant km-k$ instead of $l \leqslant km-(1-\varepsilon)m$. Since we consider k fixed and m large, any

discrepancy for small values of m may be absorbed in the error term. Then

$$(s-k)\left(m-1-\left[\frac{m'-1}{k}\right]\right) \geqslant \delta_1 m, \quad \text{and} \quad (s-k)\left(m-1-\left[\frac{l}{k}\right]\right) \geqslant \delta_1 m,$$

where $\delta_1 > 0$ is sufficiently small. According to formula (57),

$$s\left(\left[\frac{m'-1}{k}\right]+1\right)-(s-k)m-m' \leqslant -(s-k)\left(m-1-\left(1-\frac{1}{k}+\frac{\varepsilon}{k}\right)m\right)+k-1$$
$$\leqslant -(s-k)\left(\frac{1-\varepsilon}{k}\right)m+s-1 \leqslant -\delta_2 m.$$

The theorem follows.

6. THE SINGULAR SERIES

We have already defined

$$S(A, Q) = \sum_{P \,(\mathrm{mod}\, Q)} e\left(\frac{A}{Q}P^k\right). \tag{58}$$

Let

$$\mathfrak{A}(Q, N, s) = \mathfrak{A}(Q) = \sum_{\substack{A \,(\mathrm{mod}\, Q)\\ (A,Q)=1}} \left(\frac{1}{|Q|}S(A, Q)\right)^s e\left(-\frac{NA}{Q}\right). \tag{59}$$

Let

$$\mathfrak{S}(m, N, s) = \mathfrak{S}(m, N) = \sum_{\substack{Q \text{ monic}\\ \operatorname{ord} Q \leqslant m}} \mathfrak{A}(Q). \tag{60}$$

The function $\mathfrak{S}(m, N)$ has already appeared in Lemma 6 (a). If $0 < \varepsilon < 1$ is fixed, then as $m \to \infty$ the function $\mathfrak{S}(\varepsilon m, N)$ closely approximates $\mathfrak{S}(m, N)$, see Lemma 23. Let

$$\mathfrak{S}(N, s) = \mathfrak{S}(N) = \sum_{Q \text{ monic}} \mathfrak{A}(Q). \tag{61}$$

The purpose of this section is to show that $\mathfrak{S}(\varepsilon m, N)$ may be replaced by $\mathfrak{S}(N)$ with an acceptable error and to show the connection with the number of solutions to

$$P_1^k + \ldots + P_s^k \equiv N \,(\mathrm{mod}\, Q).$$

LEMMA 19. (a) *If* $(Q_1, Q_2) = 1$, $(A_1, Q_1) = 1$ *and* $(A_2, Q_2) = 1$, *then*

$$S(A_1, Q_1)S(A_2, Q_2) = S(A_1Q_2 + A_2Q_1, Q_1Q_2). \tag{62}$$

(b) *If* $(Q_1, Q_2) = 1$ *then*

$$\mathfrak{A}(Q_1)\mathfrak{A}(Q_2) = \mathfrak{A}(Q_1Q_2). \tag{63}$$

Proof. (a) Since Q_1 and Q_2 are relatively prime,

$$(64)\quad S(A_1, Q_1)S(A_2, Q_2) = \sum_{P_1 (\mathrm{mod}\, Q_1)} \sum_{P_2 (\mathrm{mod}\, Q_2)} e\left(\frac{A_1}{Q_1}(Q_2P_1)^k + \frac{A_2}{Q_2}(Q_1P_2)^k\right).$$

Since $e(\text{polynomial}) = 1$,

$$e\left(\frac{A_1}{Q_1}(Q_2P_1)^k + \frac{A_2}{Q_2}(Q_1P_2)^k\right) = e\left(\left(\frac{A_1}{Q_1} + \frac{A_2}{Q_2}\right)(Q_2P_1 + Q_1P_2)^k\right).$$

As P_1 and P_2 run independently over complete residue systems $\mathrm{mod}\, Q_1$ and $\mathrm{mod}\, Q_2$, respectively, $Q_2P_1 + Q_1P_2$ runs over a complete residue system $\mathrm{mod}\, Q_1Q_2$, and thus, the expression on the right of (64) is $S(A_1Q_2 + A_2Q_1, Q_1Q_2)$.

(b) Using part (a),

$$\mathfrak{A}(Q_1)\mathfrak{A}(Q_2)$$
$$= \frac{1}{|Q_1Q_2|^s} \sum_{\substack{A_1 \mathrm{mod}\, Q_1 \\ (A_1, Q_1)=1}} \sum_{\substack{A_2 \mathrm{mod}\, Q_2 \\ (A_2, Q_2)=1}} S^s(A_1Q_2 + A_2Q_1, Q_1Q_2)\, e\left(-N\left(\frac{A_1}{Q_1} + \frac{A_2}{Q_2}\right)\right).$$

Since, by the Chinese remainder theorem, $A_1Q_2 + A_2Q_1$ runs over a reduced system of residues $\mathrm{mod}\, Q_1Q_2$, the right hand side is $\mathfrak{A}(Q_1Q_2)$.

LEMMA 20. *Suppose P is an irreducible polynomial and $A \not\equiv 0 (\mathrm{mod}\, P)$. Let $k' = (k, |P|-1)$. Then,*

$$(65)\qquad |S(A, P)| \leqslant (k'-1)|P|^{1/2}.$$

Proof. The non-zero elements of $F_q[x]/(P)$ are a multiplicative cyclic group of order $|P|-1$ isomorphic to the $(|P|-1)$st roots of unity. Let G be a generator of this group. Then Y^k $(Y \neq 0)$ runs over the subgroup generated by $G^{k'}$ covering each element k' times, so that

$$(66)\qquad S(A, P) = \sum_{Y \mathrm{mod}\, P} e\left(\frac{A}{P} Y^k\right) = \sum_{Y \mathrm{mod}\, P} e\left(\frac{A}{P}(Y^{k'})^{k/k'}\right)$$
$$= \sum_{Y \mathrm{mod}\, P} e\left(\frac{A}{P} Y^{k'}\right) = 1 + \sum_{y=1}^{|P|-1} e\left(\frac{A}{P} G^{k'y}\right).$$

Since $e\left(\frac{A}{P} G^{k'y}\right)$ depends only on the equivalence class of $G^{k'y} (\mathrm{mod}\, P)$, that is, only on the equivalence class of $k'y \,\mathrm{mod}\, (|P|-1)$, we have

$$(67)\qquad S(A, P) = 1 + k' \sum_{y=1}^{(|P|-1)/k'} e\left(\frac{A}{P} G^{k'y}\right).$$

Also,

$$\sum_{v=0}^{k'-1} \exp\left(\frac{2\pi i}{k'} vy\right) = \begin{cases} k' & \text{if} \quad k' | y, \\ 0 & \text{if} \quad k' \nmid y. \end{cases}$$

Therefore,

$$S(A, P) = 1 + \sum_{y=1}^{|P|-1} \sum_{v=0}^{k'-1} \exp\left(\frac{2\pi i}{k'} vy\right) e\left(\frac{A}{P} G^y\right)$$

$$= \left\{1 + \sum_{\substack{Y \bmod P \\ Y \neq 0}} e\left(\frac{A}{P} Y\right)\right\} + \sum_{v=1}^{k'-1} \sum_{y=1}^{|P|-1} \exp\left(\frac{2\pi i}{k'} vy\right) e\left(\frac{A}{P} G^y\right).$$

The term in brackets is $\sum_{Y \bmod P} e\left(\frac{A}{P} Y\right) = 0$, as $A \not\equiv 0 \pmod{P}$. Therefore,

$$|S(A, P)|^2 \leqslant \left\{\sum_{v=1}^{k'-1} \left| \sum_{y=1}^{|P|-1} \exp\left(\frac{2\pi i}{k'} vy\right) e\left(\frac{A}{P} G^y\right) \right| \right\}^2.$$

By Cauchy's inequality, we have

$$|S(A, P)|^2 \leqslant (k'-1) \sum_{v=1}^{k'-1} \sum_{y=1}^{|P|-1} \sum_{z=1}^{|P|-1} \exp\left(\frac{2\pi i}{k'} v(y-z)\right) e\left(\frac{A}{P} (G^y - G^z)\right).$$

Summing instead over $w = y - z$,

$$|S(A, P)|^2 \leqslant (k'-1) \sum_{v=1}^{k'-1} \sum_{w (\bmod |P|-1)} \exp\left(\frac{2\pi i}{k'} vw\right) \left\{\sum_{z=1}^{|P|-1} e\left(\frac{A}{P} (G^w - 1) G^z\right)\right\}.$$

The sum in brackets is

$$\sum_{\substack{z \neq 0 \\ z (\bmod |P|)}} e\left(\frac{A}{P} (G^w - 1) G^z\right) = \begin{cases} |P| - 1 & \text{if} \quad G^w - 1 \equiv 0 \pmod{P}, \\ -1 & \text{if} \quad G^w - 1 \not\equiv 0 \pmod{P}. \end{cases}$$

But $G^w \equiv 1$ only when $w = |P| - 1$. So that

$$|S(A, P)|^2 \leqslant (k'-1) \sum_{v=1}^{k'-1} \left\{|P| - \sum_{w=1}^{|P|-1} \exp\left(\frac{2\pi i}{k'} vw\right)\right\} \leqslant (k'-1)^2 |P|,$$

since the sum over w is a (repeated) sum over all the k'th roots of 1, and thus is equal to zero. Taking square roots, the lemma follows.

LEMMA 21. *Suppose* char $F_q \nmid k$, *P is an irreducible polynomial and* $A \not\equiv 0 \pmod{P}$.

(a) *If* $1 < n \leqslant k$, *then*

$$S(A, P^n) = |P|^{n-1}. \tag{68}$$

(b) *If* $n > k$, *then*

$$S(A, P^n) = |P|^{k-1} S(A, P^{n-k}). \tag{69}$$

Proof. As U and V run over complete sets of residues $\bmod P^{n-1}$ and $\bmod P$, respectively, $Y = U + VP^{n-1}$ runs over a complete set of residues $\bmod P^n$. Also,

$$Y^k \equiv U^k + kU^{k-1} VP^{n-1} (\bmod P^n).$$

Therefore

$$e\left(\frac{A}{P^n} Y^k\right) = e\left(\frac{A}{P^n} U^k + \frac{kA U^{k-1} V}{P}\right),$$

and

$$S(A, P^n) = \sum_{Y \bmod P^n} e\left(\frac{A}{P^n} Y^k\right) = \sum_{U \bmod P^{n-1}} e\left(\frac{A}{P^n} U^k\right) \sum_{V \bmod P} e\left(\frac{kA U^{k-1} V}{P}\right).$$

The sum over V gives 0 unless $P | kA U^{k-1}$, i.e., unless $P | U$, in which case the sum is equal to $|P|$. Hence

$$S(A, P^n) = |P| \sum_{U \bmod P^{n-2}} e\left(\frac{A}{P^n} (PU)^k\right).$$

When $n \leqslant k$, $e\left(\frac{A}{P^n} (PU)^k\right) = 1$, and since there are $|P|^{n-2}$ terms we have

$$S(A, P^n) = |P|^{n-1}.$$

When $n > k$,

$$S(A, P^n) = |P| \sum_{U \bmod P^{n-2}} e\left(\frac{A}{P^{n-k}} U^k\right).$$

But $e\left(\frac{A}{P^{n-k}} U^k\right)$ is a function only of the residue class of $U (\bmod P^{n-k})$ and there are $|P|^{k-2}$ complete sets of residues $(\bmod P^{n-k})$ in a single complete set of residues $(\bmod P^{n-2})$. Therefore

$$S(A, P^n) = |P|^{k-1} S(A, P^{n-k}).$$

LEMMA 22. *If* $\operatorname{char} F_q \nmid k$ *then*

$$\text{(a)} \quad |S(A, Q)| \ll |Q|^{1-1/k}, \tag{70}$$

$$\text{(b)} \quad |\mathfrak{A}(Q, N, s)| \ll |Q|^{1-s/k}. \tag{71}$$

The constants implied by $\ll$ *may be taken independent of* q *and* N *and are pependent only on* k.

Proof. (a) We first prove (a) for the prime powers P^μ. Writing

$$\mu = k\left[\frac{\mu - 1}{k}\right] + i, \quad \text{where} \quad 0 < i \leqslant k,$$

we see that we may apply Lemma 21 (b) $\left[\frac{\mu-1}{k}\right]$ times, to obtain

$$S(A, P^\mu) = |P|^{(k-1)\left[\frac{\mu-1}{k}\right]} S(A, P^i).$$

If $i \neq 1$, by Lemma 21 (a)

$$S(A, P^\mu) = |P|^{(k-1)\left[\frac{\mu-1}{k}\right]} \cdot |P|^{i-1} \leqslant |P|^{\mu\left(1-\frac{1}{k}\right)}.$$

If $i = 1$, by Lemma 20,

$$|S(A, P^\mu)| \leqslant |P|^{(k-1)\left[\frac{\mu-1}{k}\right]}(k'-1)\,|P|^{1/2}$$
$$\leqslant (k'-1)\,|P|^{\mu-\left[\frac{\mu-1}{k}\right]-\frac{1}{2}} \leqslant (k-1)\,|P|^{\mu-\frac{1}{k}\mu-\left(\frac{1}{2}-\frac{1}{k}\right)}.$$

Thus when $k = 2$,

$$(*) \qquad |S(A, P^\mu)| \leqslant |P|^{\mu\left(1-\frac{1}{k}\right)},$$

and when $k \geqslant 3$,

$$(**) \qquad |S(A, P^\mu)| \leqslant \{(k-1)\,|P|^{-1/6}\} \cdot |P|^{\mu\left(1-\frac{1}{k}\right)}.$$

For $k = 2$, the formula (70) now follows from Lemma 19 (a) and (*). For $k \geqslant 3$, write $Q = \prod P_j^{\mu_j}$, where the P_j are irreducible. Let i_j be defined by

$$\mu_j = k\left[\frac{\mu_j-1}{k}\right] + i_j.$$

By Lemma 19 (a) and (**), we have

$$|S(A, Q)| \leqslant \prod_j |P_j|^{\mu_j\left(1-\frac{1}{k}\right)} \prod_j \max\left(1, (k-1)\,|P_j|^{-1/6}\right)$$
$$\leqslant |Q|^{1-\frac{1}{k}} \prod_{\substack{P_j \text{ irreducible} \\ P_j \mid Q, \\ |P_j| < (k-1)^6}} (k-1) \leqslant (k-1)^{(k-1)^6} |Q|^{1-1/k}.$$

$$\text{(b)} \qquad |\mathfrak{A}(Q, N, s)| \leqslant \left| \frac{1}{|Q|^s} \sum_{\substack{A \bmod Q \\ (A, Q)=1}} (S(A, Q))^s\, e\left(-\frac{NA}{Q}\right) \right|$$
$$\ll \frac{1}{|Q|^s} \cdot |Q| \cdot |Q|^{\left(1-\frac{1}{k}\right)s} \ll |Q|^{1-\frac{s}{k}}.$$

LEMMA 23. *For P irreducible, let*

$$(72) \qquad X(P, N, s) = 1 + \sum_{\mu=1}^{\infty} \mathfrak{A}(P^\mu, N, s).$$

If $\operatorname{char} F_q \nmid k$ *and* $s \geqslant 3k+1$, *then* $\mathfrak{S}(N, s) = \sum_{Q \text{ monic}} \mathfrak{A}(Q, N, s)$ *and* $X(P, N, s)$ *converge absolutely and*

$$\mathfrak{S}(N, s) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} X(P, N, s). \tag{73}$$

Also if $\mathfrak{S}(\varepsilon m, N, s) = \sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q < \varepsilon m}} \mathfrak{A}(Q, N, s)$, *then*

$$|\mathfrak{S}(N, s) - \mathfrak{S}(\varepsilon m, N, s)| \ll q^{-\left(1+\frac{1}{k}\right)\varepsilon m}.$$

(*Here the constans in* $\ll$ *may depend on* k, q *and* ε, *but not on* m.)

Proof. By Lemma 22 (b), since $s \geqslant 3k+1$,

$$|\mathfrak{A}(Q, N, s)| \ll |Q|^{1-\frac{s}{k}} \ll |Q|^{-2-\frac{1}{k}}.$$

It follows that

$$|X(P, N, s)| \leqslant 1 + \sum_{\mu=1}^{\infty} |P|^{\left(-2-\frac{1}{k}\right)\mu}$$

converges absolutely. Also

$$|\mathfrak{S}(N, s)| \leqslant \sum_{l=0}^{\infty} \sum_{\substack{\operatorname{ord} Q = l \\ Q \text{ monic}}} |\mathfrak{A}(Q, N, s)| \leqslant \sum_{l=0}^{\infty} \sum_{\substack{\operatorname{ord} Q = l \\ Q \text{ monic}}} (q^l)^{-2-\frac{1}{k}},$$

and since there are q^l monic polynomials of order l, the series converges absolutely. Also

$$|\mathfrak{S}(N, s) - \mathfrak{S}(\varepsilon m, N, s)| \leqslant \sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q \geqslant \varepsilon m}} |\mathfrak{A}(Q, N, s)|$$

$$\leqslant \sum_{l \geqslant \varepsilon m}^{\infty} (q^l)^{-1-\frac{1}{k}} \leqslant q^{-\left(1+\frac{1}{k}\right)(\varepsilon m)} \frac{1}{1 - q^{-1-\frac{1}{k}}} \ll q^{-\left(1+\frac{1}{k}\right)(\varepsilon m)}.$$

Finally,

$$\prod_{\substack{P \text{ monic} \\ \text{irreducible} \\ \operatorname{ord} P < l}} X(P, N, s) = \sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q < l}} \mathfrak{A}(Q, N, s) + \sum{}' \mathfrak{A}(Q, N, s)$$

where the second sum is over those Q which are monic, of degree $\geqslant l$ and all of whose irreducible factors has order $< l$. As $l \to \infty$, the second sum tends to zero since $|\mathfrak{A}(Q, N, s)| \leqslant |Q|^{-1-1/k}$. As $l \to \infty$, the first sum on the right tends to $\mathfrak{S}(N, s)$, while the product tends to $\prod_{\substack{P \text{ monic} \\ \text{irreducible}}} X(P, N, s)$. Thus (73) is shown.

LEMMA 24. *Let* $M(Q, N, s)$ *be the number of distinct tuples* $(P_1, \ldots, P_s) \bmod Q$ *such that*

$$P_1^k + \ldots + P_s^k \equiv N \pmod{Q}, \tag{74}$$

then

$$M(Q, N, s) = |Q|^{s-1} \sum_{\substack{Q_1|Q \\ Q_1 \text{ monic}}} \mathfrak{A}(Q_1, N, s). \tag{75}$$

Proof. By Lemma 1 (g),

$$M(Q, N, s) = \frac{1}{|Q|} \sum_{R \bmod Q} \sum_{P_1 \bmod Q} \cdots \sum_{P_s \bmod Q} e\left(\frac{R}{Q}(P_1^k + \ldots + P_s^k - N)\right).$$

Gathering together those R with the same value of (R, Q)

$$M(Q, N, s) = \frac{1}{|Q|} \sum_{\substack{Q_1|Q \\ Q_1 \text{ monic}}} \sum_{\substack{A_1 \bmod Q_1 \\ (A_1, Q_1)=1}} \sum_{P_1 \bmod Q} \cdots \sum_{P_s \bmod Q} e\left(\frac{A_1}{Q_1}(P_1^k + \ldots + P_s^k - N)\right).$$

But $e\left(\frac{A_1}{Q_1} P_i^k\right)$ is a function only of the congruence class of $P_i^k \bmod Q_1$ not $\bmod Q$. Thus

$$\sum_{P_i \bmod Q} e\left(\frac{A_1}{Q_1} P_i^k\right) = \frac{|Q|}{|Q_1|} \sum_{P_i \bmod Q_1} e\left(\frac{A_1}{Q_1} P_i^k\right) = \frac{|Q|}{|Q_1|} S(A_1, Q_1).$$

Therefore

$$M(Q, N, s) = \frac{1}{|Q|} \sum_{\substack{Q_1|Q \\ Q_1 \text{ monic}}} \sum_{\substack{A_1 \bmod Q_1 \\ (A_1, Q_1)=1}} \left(\frac{|Q|}{|Q_1|} S(A_1, Q_1)\right)^s e\left(-\frac{NA_1}{Q_1}\right)$$

$$= |Q|^{s-1} \sum_{\substack{Q_1|Q \\ Q_1 \text{ monic}}} \mathfrak{A}(Q_1, N, s).$$

LEMMA 25. *If* $\operatorname{char} F_q = p \nmid k$, P *is irreducible,* $P \nmid B$ *and*

$$Y_0^k \equiv B \pmod{P^\nu}, \tag{76}$$

then, for $\mu > \nu$, *there is a solution* Y_1 *of*

$$Y_1^k \equiv B \pmod{P^\mu} \quad \textit{with} \quad Y_1 \equiv Y_0 \pmod{P^\nu}. \tag{77}$$

Proof. We proceed by induction on μ. For $\mu = \nu + 1$, Y_1 must have the form

$$Y_1 = Y_0 + RP^\nu.$$

Then

$$Y_1^k = Y_0^k + kY_0^{k-1}RP^\nu + \sum_2^k \binom{k}{i} Y_0^{k-i}(RP)^{\nu i}.$$

But $\nu i \geqslant 2\nu \geqslant \nu + 1$ so that

$$Y_1^k \equiv Y_0^k + kY_0^{k-1}RP^\nu \pmod{P^{\nu+1}}.$$

If $Y_0^k+HP^\nu = B$, then Y_1 satisfies the conclusion if and only if

$$H \equiv kY_0^{k-1}R(\mathrm{mod}\,P).$$

Since $p\nmid k$ and $P\nmid Y_0$, we may solve for $R(\mathrm{mod}\,P)$ to find Y_1. Suppose now we have shown the lemma for $\nu+1,\ldots,\mu-1$. Taking the solution Y_1 for $\mu-1$

$$Y_1^k \equiv B(\mathrm{mod}\,P^{\mu-1}),$$

$$Y_1 \equiv Y_0(\mathrm{mod}\,P^\nu)$$

we find

$$Y_2^k \equiv B(\mathrm{mod}\,P^\mu),$$

$$Y_2 \equiv Y_1(\mathrm{mod}\,P^{\mu-1})$$

as in the first part of the proof. Then $Y_2 \equiv Y_1 \equiv Y_0(\mathrm{mod}\,P^\nu)$, so Y_2 satisfies the lemma for μ.

LEMMA 26. *If* $\mathrm{char}\,F_q = p\nmid k$, *$P$ is an irreducible polynomial and*

$$P_1^k+\ldots+P_s^k \equiv N(\mathrm{mod}\,P^\nu)$$

with $P\nmid P_i$, for some i, then, for $\mu>\nu$, the number of tuples $(R_1,\ldots,R_s)$ $(\mathrm{mod}\,P^\mu)$ such that

$$R_1^k+\ldots+R_s^k \equiv N(\mathrm{mod}\,P^\mu)$$

with $R_i \equiv P_i$ $(\mathrm{mod}\,P^\nu)$ for $i=1,\ldots,s$ is

$$\gg |P|^{(s-1)(\mu-\nu)}.$$

Proof. Suppose $P\nmid P_t$. For $i\neq t$, let $R_i = P_i+V_iP^\nu$, $\mathrm{ord}\,V_i < \mathrm{ord}\,P^{\mu-\nu}$. Then

$$N-\sum_{i\neq t} R_i^k \equiv N-\sum_{i\neq t} P_i^k \equiv P_t^k \not\equiv 0(\mathrm{mod}\,P^\nu).$$

By the previous lemma, there is $R_t(\mathrm{mod}\,P^\mu)$ such that

$$R_t^k \equiv N-\sum_{i\neq t} R_i^k(\mathrm{mod}\,P^\mu),$$

$$R_t \equiv P_t(\mathrm{mod}\,P^\nu).$$

In all, there are at least $|P|^{(s-1)(\mu-\nu)}$choices for $(R_1,\ldots,R_s)(\mathrm{mod}\,P^\mu)$.

LEMMA 27. *If P is irreducible and $s\geqslant k+1$ and N is congruent* $(\mathrm{mod}\,P)$ *to a sum of (arbitrarily many) k-th powers, then there exist $P_1,\ldots,P_s$ not all divisible by P such that*

$$P_1^k+\ldots+P_s^k \equiv N(\mathrm{mod}\,P). \tag{78}$$

Proof. It suffices to show that when $P\nmid N$ the congruence (78) is solvable for some value of $s\leqslant k$. For if that is so, when $P|N$ we can take P_{k-1} to be 1 and solve $P_1^k+\ldots+P_k^k \equiv N-1(\mathrm{mod}\,P)$.

Let $t = t(N)$ be the least s for which (78) is solvable, say

$$P_1^k + \ldots + P_{t(N)}^k \equiv N \pmod{P}. \tag{79}$$

We collect those polynomials with the same value of t into classes. If $R \not\equiv 0 \pmod{P}$, then $t(R^k N) = t(N)$ since we may multiply (79) by R^k, and on the other hand, if

$$(P_1')^k + \ldots + (P_s')^k \equiv R^k N \pmod{P}, \tag{80}$$

we may divide by R^k which is a unit $(\bmod P)$. There are exactly $\dfrac{|P|-1}{(k, |P|-1)}$ distinct values of $R^k (\bmod P)$ and therefore at least that many polynomials with the same value of t. Therefore there are at most $(k, |P|-1) \leqslant k$ classes. Since $1 = 1^k$, we have $t(1) = 1$. Suppose we have shown that there are non-zero polynomials with $t(N) = 1, 2, \ldots, t'$. Either we have exhausted all the non-zero polynomials or there is an N' with $t(N') > t'$, with $t(N')$ minimal. The existence of N' implies an N with $t(N) = t(N')-1$, hence $t(N') = t'+1$. Thus we have shown there are at most k values of t, and that they are consecutive, and so the lemma follows.

LEMMA 28. *If P is irreducible and $|P| > (k-1)^2$ then each N is congruent* $(\bmod P)$ *to a sum of k-th powers. If $p = \operatorname{char} F_q > k$, then each N is congruent* $(\bmod P)$ *to a sum of k-th powers for arbitrary irreducible P.*

Proof. If $\operatorname{ord} P = l$, then $F_q[x]/(P) \cong F_{q^l} = F_{p^{l'}}$. Let $\mathscr{R}(P, q, k) = \mathscr{R}$ be the set of those polynomials which are sums of kth powers $(\bmod P)$. We can think of $\mathscr{R}$ as a subset of $F_q[x]/(P)$. Then $\mathscr{R}$ being closed under addition and multiplication is a finite field, say $\mathscr{R} \cong F_{p^h}$. Suppose $\mathscr{R}$ is a proper subfield, i.e., $h < l'$. We must have $h|l'$ and also the order of the multiplicative subgroup $\mathscr{R}^\times$ must divide the order of the whole group $F_{p^{l'}} \setminus \{0\}$; thus

$$\frac{p^{l'}-1}{p^h-1} = p^{l'-h} + p^{l'-2h} + \ldots + p^h + 1.$$

Let a be a primitive $(p^{l'}-1)$st root of 1. Then $a^k \in \mathscr{R}$ so that

$$(a^k)^{p^h-1} = 1.$$

It follows that $(p^{l'}-1)|(p^h-1)k$. Therefore $p^{l'-h} + p^{l'-2h} + \ldots + p^h + 1 | k$. Hence

$$p^{l'/2} + 1 \leqslant p^{l'-h} + \ldots + p^h + 1 \leqslant k,$$

or

$$|P| \leqslant (k-1)^2,$$

contrary to our hypothesis. Thus $h = l'$ and each N is congruent $(\bmod P)$ to a sum of kth powers.

To prove the second statement of the lemma we start from

$$(p^{l'}-1)|(p^h-1)k.$$

Since $k < p$,

$$p^{l'} - 1 \leqslant (p^h - 1)k \leqslant p^{h+1} - p.$$

If $\mathscr{R}$ is a proper subfield, i.e., $h < l'$ or $h+1 \leqslant l'$, the inequality above is contradictory.

THEOREM 29. *If* $\operatorname{char} F_q \nmid k$, $s \geqslant 3k+1$, *and either*

(a) N *is congruent to a sum of* k*-th powers* $\bmod P$, *for all irreducible* P *such that* $|P| \leqslant (k-1)^2$, *or*,

(b) $k < \operatorname{char} F_q$,

then

$$1 \ll \mathfrak{S}(N, s) = \prod_{\substack{P \text{ irreducible} \\ \text{monic}}} X(P, N, s) \ll 1. \tag{81}$$

Proof. We have only to show $\prod_P X(P, N, s) \gg 1$ since Lemma 23 together with Lemma 22 (b) assert the remaining statements. By Lemmas 22, 24, 26, 27, 28, for any $\mu \geqslant 1$, we have

$$\sum_{\substack{Q \mid P^\mu \\ Q \text{ monic}}} \mathfrak{A}(Q, N, s) = \frac{M(P^\mu, N, s)}{|P|^{\mu(s-1)}} \geqslant |P|^{(s-1)(\mu-1)-(s-1)\mu} \geqslant |P|^{-(s-1)}.$$

Therefore, $|X(P, N, s)| \geqslant |P|^{-s-1}$. Also

$$|X(P, N, s) - 1| = \sum_{\mu=1}^{\infty} |\mathfrak{A}(P^\mu, N, s)| \ll \sum_{\mu=1}^{\infty} |P|^{\mu\left(-2-\frac{1}{k}\right)} \ll |P|^{-2-\frac{1}{k}}.$$

It follows that $\prod_{\substack{P \text{ monic} \\ \text{irreducible}}} X(P, N, s) \gg 1$.

7. THE ASYMPTOTIC FORMULA

THEOREM 30. *Let* N *be a polynomial and* $r(N, m, s, k)$ *be the number of representations of* N *as a sum of* s k*-th powers of polynomials each of order* $< m$. *If* (a) $3 \leqslant k < \operatorname{char} F_q$, (b) $s \geqslant 2^k + 1$, (c) $0 < \varepsilon < 1$, (d) $\operatorname{ord} N = \deg N < (k-1+\varepsilon)m$, *then there exists a* $\delta > 0$ *such that*

$$r(N, m, s, k) = \frac{U(s, 0)}{q^{s-k} - 1} \mathfrak{S}(N, s) q^{(s-k)m} + O(q^{(s-k-\delta)m}).$$

Furthermore

$$1 \ll \frac{U(s, 0)}{q^{s-k} - 1} \mathfrak{S}(N, s) \ll 1.$$

Proof. It is clear that if the theorem holds for $k/(k+1) \leqslant \varepsilon < 1$ then the theorem holds for all $0 < \varepsilon < 1$, so we may assume $\varepsilon \geqslant k/(k+1)$.

The number of representations is given by Lemma 2 as

$$r(N, m, s, k) = \int_{\operatorname{ord} \alpha < 0} T(\alpha)^s e(-N\alpha)\, d\alpha$$

$$= \int_{\mathfrak{M}} T(\alpha)^s e(-N\alpha)\, d\alpha + \int_{\mathfrak{m}} T(\alpha)^s e(-N\alpha)\, d\alpha,$$

where $\mathfrak{M}$ and $\mathfrak{m}$ are the set of major and minor arcs, respectively. Theorem 14 gives the contribution of the minor arcs as $O(q^{m(s-k-\delta)})$. Lemma 6 (a) gives the contribution of the major arcs as

$$\int_{\mathfrak{M}} T(\alpha)^s e(-N\alpha)\, d\alpha$$

$$= \sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q \leqslant m}} \sum_{\substack{\operatorname{ord} A < \operatorname{ord} Q \\ (A, Q) = 1}} \left(\frac{1}{|Q|} S(A, Q)\right)^s e\left(\frac{-NA}{Q}\right) \int_{\operatorname{ord} \beta < -(k-1)m - \operatorname{ord} Q} T(\beta)^s e(-N\beta)\, d\beta.$$

We split this sum over Q into

$$\sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q < \varepsilon m}} + \sum_{\substack{Q \text{ monic} \\ \varepsilon m \leqslant \operatorname{ord} Q \leqslant m}}.$$

The integrals in the first sum are given by Theorem 18 as:

$$\int_{\operatorname{ord} \beta < -(k-1)m - \operatorname{ord} Q} T(\beta)^s e(-N\beta)\, d\beta = \frac{U(s, 0)}{q^{s-k} - 1} q^{(s-k)m} + O(q^{(s-k-\varepsilon_1)m}).$$

Therefore this first sum is

$$\sum_{\substack{Q \text{ monic} \\ \operatorname{ord} Q < \varepsilon m}} \sum_{\substack{\operatorname{ord} A < \operatorname{ord} Q \\ (A, Q) = 1}} \left(\frac{1}{|Q|} S(A, Q)\right)^s e\left(\frac{-NA}{Q}\right) \int_{\operatorname{ord} \beta < -(k-1)m - \operatorname{ord} Q} T(\beta)^s e(-N\beta)\, d\beta$$

$$= \mathfrak{S}(\varepsilon m, N, s) \frac{U(s, 0)}{q^{s-k} - 1} q^{(s-k)m} + O\left(\mathfrak{S}(\varepsilon m, N, s) q^{(s-k-\varepsilon_1)m}\right).$$

Lemma 23 and Theorem 29 give this to be

$$= \mathfrak{S}(N, s) \frac{U(s, 0)}{q^{s-k} - 1} q^{(s-k)m} + O(q^{(s-k-\delta)m}).$$

Now consider the second sum:

$$(*)\qquad \sum_{\substack{Q \text{ monic}\\ \varepsilon m\leqslant \operatorname{ord} Q\leqslant m}} \sum_{\substack{\operatorname{ord} A\leqslant \operatorname{ord} Q\\ (A,Q)=1}} \left(\frac{1}{|Q|}S(A,Q)\right)^s \times$$

$$\times e\left(\frac{-NA}{Q}\right) \int_{\operatorname{ord}\beta\leqslant -(k-1)m-\operatorname{ord} Q} T(\beta)^s e(-N\beta)\,d\beta$$

$$= \sum_{\substack{Q \text{ monic}\\ \varepsilon m\leqslant \operatorname{ord} Q\leqslant m}} \mathfrak{A}(Q,N,s) \int_{\operatorname{ord}\beta\leqslant -(k-1)m-\operatorname{ord} Q} T(\beta)^s e(-N\beta)\,d\beta.$$

Using the trivial estimate $|T(\beta)|\leqslant q^m$, the integral is

$$\left|\int_{\operatorname{ord}\beta<(k-1)m-\operatorname{ord} Q} T(\beta)^s e(-N\beta)\,d\beta\right| \leqslant q^{sm} \int_{\operatorname{ord}\beta<-(k-1)m-\operatorname{ord} Q} 1\cdot d\beta$$

$$\leqslant q^{(s-k+1)m}\cdot\frac{1}{|Q|}.$$

According to Lemma 22 (b), $|\mathfrak{A}(Q,N,s)|\ll |Q|^{1-s/k}$, so that the second sum is

$$\ll \sum_{\substack{Q \text{ monic}\\ \varepsilon m<\operatorname{ord} Q<m}} |Q|^{1-(s/k)-1} q^{(s-k+1)m}.$$

Since $s\geqslant 3k+1$, this sum is:

$$\ll q^{(s-k+1)m} \sum_{\substack{Q \text{ monic}\\ \varepsilon m<\operatorname{ord} Q<m}} |Q|^{-s/k}$$

$$\ll q^{(s-k+1)m} \sum_{[\varepsilon m]<j<m} (q^j)^{(-3k-1)/k}$$

$$\ll q^{(s-k+1)m}\cdot q^{\varepsilon m(-3k-1/k)}.$$

Since $\varepsilon\geqslant k/(k+1)$, the asymptotic formula follows. The singular series is not zero (see Theorem 29), and $\dfrac{U(s,0)}{q^{s-k}-1}\gg 1$ since, as usual, the constant in $\gg$ may depend on q, s and k but is independent of m, and $U(s,0)\geqslant 0$ when $s\geqslant k+1$, by a theorem of Chevalley.

Note: We can in fact prove a much sharper result for $k=2$, since there are no minor arcs. But this requires some effort as we must sharpen all the estimates on the major arcs.

8. ESTIMATES FOR $\tilde{g}(k)$

Let $g(k, q)$ be the least number r such that every polynomial in $F_q[x]$ is the sum of r kth powers, where some summands may be zero.

THEOREM 31. *If* $k < \operatorname{char} F_q = p$ *then*

$$g(k, q) = g(k) \leqslant k(p-1). \tag{82}$$

Proof. We consider first whether it is possible to write

$$x+b = \sum_{i=1}^{k} a_i (x+i)^k, \qquad a_i \in \boldsymbol{Z}_p, \tag{83}$$

where $b \in \boldsymbol{Z}_p$ will be chosen later to suit our convenience. Solving for the coefficients of x^j, $0 \leqslant j \leqslant k$, in (83) we obtain:

$$\begin{aligned}
\sum a_i &= 0,\\
k\cdot \sum a_i \cdot i &= 0,\\
\binom{k}{2}\cdot \sum a_i \cdot i^2 &= 0,\\
\cdots\cdots\cdots\cdots\\
\binom{k}{k-2}\cdot \sum a_i \cdot i^{k-2} &= 0,\\
k\cdot \sum a_i \cdot i^{k-1} &= 1,\\
\sum a_i \cdot i^k &= b.
\end{aligned}$$

Since $k < p$, the binomial coefficients are non-zero and we may divide by them. Choosing $b = \sum a_i \cdot i^k$, the remaining equations are k linear equations in the k unknowns a_i with determinant:

$$\begin{vmatrix}
1 & 1 & 1 & \dots & 1\\
1 & 2 & 3 & \dots & k\\
1^2 & 2^2 & 3^2 & \dots & k^2\\
\dots & \dots & \dots & \dots & \dots\\
1^{k-1} & 2^{k-1} & 3^{k-1} & \dots & k^{k-1}
\end{vmatrix} = \prod_{i>j} (i-j) \not\equiv 0 \pmod p. \tag{84}$$

It follows that we can solve for the a_i. Since each $a_i = \sum_1^{a_i} 1^k$ is a sum of at most $p-1$ kth powers, it follows that $x+b$ can be written as a sum of not more than $k(p-1)$ kth powers. To write an arbitrary polynomial, say $c_n x^n + \ldots + c_0$, as a sum of kth powers, we may just substitute $C(x) = c_n x^n + \ldots + c_0 - b$ for x in the identity (83):

$$c_n x^n + \ldots + c_0 = \sum_1^k a_i \big(C(x)+i\big)^k. \tag{85}$$

This proves the theorem.

Let $\tilde{g}(k) = \tilde{g}(k, q)$ be the least s such that every polynomial that is the sum of kth powers is the sum of s kth powers.

Suppose $\operatorname{char} F_q \nmid k$. We shall show that $\tilde{g}(k)$ exists and in fact is less than $3k+1+2l+l'$ where eventually we choose $l = l' \leqslant [k\log(3k^2-k)]+1$. To do so, it suffices to show that every polynomial N that is a sum of kth powers may be written as

$$N = P_1^k + \ldots + P_{3k+1}^k + U_1 + U_2 + V_1 W^k, \tag{86}$$

where:

$$\begin{cases} \text{(a) } \operatorname{ord} P_i < m,\ 1 \leqslant i \leqslant 3k+1,\ k|m \text{ and } m \text{ is sufficiently large,} \\ \text{(b) } U_1 \text{ and } U_2 \text{ are monic polynomials of order } km \text{ that are representable as a sum of } l\ k\text{th powers,} \\ \text{(c) } \operatorname{ord} W = (1/k)m,\ W \text{ monic,} \\ \text{(d) } V_1 \text{ is a monic polynomial of order } (k-1)m \text{ that is representable as a sum of } l'\ k\text{th powers.} \end{cases} \tag{87}$$

Eventually we shall choose $l = l' \leqslant k\log(3k^2-k)+1$.

The restriction $k|m$ is not essential but is taken to ensure $(1/k)m$ is integral and to thereby avoid additional notational mess.

The choice of the variables is not arbitrary but related to three different ideas that combine to show that N is a sum of kth powers.

The first idea accounts for the contribution of the major arcs and gives rise to the first $3k+1$ kth powers P_i. It arises in the following way: Consider the number, say $r'(N)$ of representations of N as a sum of kth powers of the form

$$N = P_1^k + \ldots + P_s^k + Z, \tag{88}$$

where

$$\begin{cases} \text{(a) } \operatorname{ord} P_i < m,\ 1 \leqslant i \leqslant s, \\ \text{(b) } Z \text{ is a sum of } k\text{th powers of some to be specified set } \mathscr{Z}. \end{cases} \tag{89}$$

Let $H(\alpha) = \sum_{Z} e(\alpha Z)$, where the summation is over these Z in $\mathscr{Z}$. Let $T(\alpha) = \sum_{\operatorname{ord} P < m} e(\alpha P)$. Then

$$r'(N) = \int_{\operatorname{ord}\alpha < 0} T^s(\alpha) H(\alpha) e(-N\alpha)\, d\alpha. \tag{90}$$

The contribution of the major arcs is

$$\mathfrak{J}_1 = \sum_{Z} \int_{\mathfrak{M}} T^s(\alpha) e\big(-\alpha(N-Z)\big)\, d\alpha. \tag{91}$$

In the summation over Z there are $H(0)$ summands, and for each of these summands, the integral is $\gg q^{m(s-k)}$, provided $s \geqslant 3k+1$. Therefore, if $s \geqslant 3k+1$, we have

$$\mathfrak{J}_1 \gg q^{m(s-k)} H(0). \tag{92}$$

In order to prove $r'(N) > 0$ it would suffice to find some set $\mathscr{Z}$ of polynomials Z for which the contribution of the minor arcs to $r'(N)$, say $\mathfrak{J}_2$, is

$$\mathfrak{J}_2 \ll q^{m(s-k-\delta)} H(0). \tag{93}$$

Now we have

$$\mathfrak{J}_2 \leqslant \left| \int_{\mathfrak{m}} T^s(a) H(a)\, da \right| \leqslant q^{sm} \int_{\mathfrak{m}} |H(a)|\, da. \tag{94}$$

The second and third ideas arise when we try to find a set of Z for which we can give an estimate for the integral in (94) which is of the type needed in (93).

Suppose Y runs through a set $\mathscr{Y}$ of polynomials of some special form. Let

$$L(a) = \sum_{Y \in \mathscr{Y}} e(aY), \tag{95}$$

where the summation is over these special Y. Since $|e(aY)| \leqslant 1 = e(0)$, we know (the trivial estimate)

$$|L(a)| \leqslant L(0). \tag{96}$$

But suppose we could prove that for $a \in \mathfrak{m}$, the union of the minor arcs, we have

$$|L(a)| \leqslant L(0) q^{-\varepsilon m}. \tag{97}$$

Let Z be of the special form

$$Z = Y_1 + \ldots + Y_t, \tag{98}$$

where each Y_i is in $\mathscr{Y}$. We would have

$$H(a) = L^t(a), \tag{99}$$

and in particular,

$$H(0) = L^t(0). \tag{100}$$

Using (100), (99) and (97) in (94) we have

$$\mathfrak{J}_2 \leqslant q^{sm - t\varepsilon m} H(0). \tag{101}$$

This is of the form (93) that we want, provided $t\varepsilon \geqslant k + \delta$, that is, provided t is taken large enough. The estimates of the form (97) are analogous to Weyl's Lemma, where we took the special form of Y to be simply

$$Y = P^k, \quad \operatorname{ord} P < m.$$

In that special case (see Proposition 12), we showed (if $k < \operatorname{char} F_q$)

$$|L(a)| \ll L(0) q^{-\left(\varepsilon' + \frac{1}{2^{k-1}}\right) m}$$

where ε' could be taken arbitrarily small. Here however we make a different choice for Y and prove an inequality of the type (97) in a different way. This is done in Lemmas 34 and 35 below and gives rise to the l' kth powers of the form $V_1 W^k$.

The estimate (101) may be thought of as analogous to what could be obtained by using Weyl's Lemma alone in proving the asymptotic formula. A much more efficient estimate was obtained by combining Weyl's Lemma with Hua's Lemma (Proposition 13). The third idea may be thought of as analogous to Hua's Lemma. It arises in the following way: Instead of taking Z in the form (98), we take

$$Z = Y_1 + \ldots + Y_t + U_1 + U_2, \tag{102}$$

where each Y_1 is from the set $\mathscr{Y}$ and each U_t is to be from a special set $\mathscr{U}$ of distinct polynomials to be specified later. Let

$$R(\alpha) = \sum_{U \in \mathscr{U}} e(\alpha U). \tag{103}$$

In particular,

$$R(0) = \operatorname{card} \mathscr{U}. \tag{104}$$

It follows that

$$H(\alpha) = L^t(\alpha) R^2(\alpha). \tag{105}$$

The contribution of the minor arcs is

$$\mathfrak{J}_2 \leqslant q^{(s-ts)m} L^t(0) \int_{\mathfrak{m}} |R(\alpha)|^2 d\alpha. \tag{106}$$

Since $|R(\alpha)|^2$ is non-negative we may extend the domain of integration in (106) to the whole interval $\operatorname{ord} \alpha < 0$. Since

$$\int_{\operatorname{ord}\alpha<0} e\big(\alpha(U_1 - U_2)\big) d\alpha = \begin{cases} 0 & \text{if} \quad U_1 \neq U_2, \\ 1 & \text{if} \quad U_1 = U_2, \end{cases}$$

it follows that

$$\int_{\operatorname{ord}\alpha<0} |R(\alpha)|^2 d\alpha \leqslant \sum_{U_1} \sum_{U_2} \int_{\operatorname{ord}\alpha<0} e\big(\alpha(U_1 - U_2)\big) d\alpha \leqslant R(0). \tag{107}$$

If we could pick the set $\mathscr{U}$ such that its cardinality, i.e., $R(0)$, is at least

$$R(0) \gg q^{\varepsilon' m}, \tag{108}$$

then

$$\begin{aligned} \mathfrak{J}_2 &\leqslant q^{(s-ts)m} L^t(0) \int_{\mathfrak{m}} |R(\alpha)|^2 d\alpha \\ &\leqslant q^{(s-ts)m} L^t(0) R(0) \ll q^{(s-ts-\varepsilon')m} L^t(0) R^2(0). \end{aligned} \tag{109}$$

This estimate is of the form (93), that we desire, provided

$$t\varepsilon+\varepsilon' \geqslant k+\delta.$$

Proving an estimate of the type (108) is done in Lemma 32 and gives rise to the $2l$ kth powers in the terms U_1 and U_2 in (86).

In the end, it will be convenient to take $t=1$, and $l=l'=$ smallest integer $r \geqslant k\log(3k^2-k)$. We now proceed to the proof of the lemmas.

LEMMA 32. *Let $U_l(m)$ denote the number of different monic polynomials of order km that are representable as a sum of l k-th powers of polynomials. If* $\operatorname{char} F_q \nmid k$, *then*

$$U_l(m) \gg q^{km(1-\lambda^l)}, \tag{110}$$

where $\lambda = 1-1/k$ and the constant implied by $\gg$ may depend on q, k and l but is independent of m.

Proof. We proceed by induction on l. If $l=1$, then there are q^m different monic polynomials P^k where $\operatorname{ord} P = m$. Thus $U_1(m) \gg q^m$. Consider those polynomials of the form P^k+Q, where $\operatorname{ord} P = m$, P is monic and Q is a monic polynomial of order $k\left[\frac{1}{k}(k-1)m\right]$ which is the sum of $l-1$ kth powers of polynomials. We assert that polynomials of this form are distinct for distinct choices of (P, Q). For suppose

$$P_1^k+Q_1 = P_2^k+Q_2. \tag{111}$$

Let $P_1 = a_0x^m+a_1x^{m-1}+\ldots+a_m$, and let $P_2 = b_0x^m+b_1x^{m-1}+\ldots+b_m$. Since we have supposed P_1, P_2 monic, $a_0=b_0=1$. Proceeding by induction, suppose we have proved $a_i=b_i$, $0 \leqslant i < n \leqslant m$. To show $a_n=b_n$, consider the coefficient of x^{km-n} on both sides of the equation (111). If $n<m$ or $k \nmid (k-1)m$ then this coefficient is

$$F(a_0, \ldots, a_{n-1})+ka_0^{k-1}a_n = F(b_0, \ldots, b_{n-1})+kb_0^{k-1}b_n. \tag{112}$$

Here the same form F involving only a_i, b_i for $i<n$ appears on both sides and the coefficients of Q_1 and Q_2 do not appear as $km-n \geqslant (k-1)m \geqslant \operatorname{ord} Q_i = k\left[\frac{1}{k}(k-1)m\right]$, with equality not holding everywhere. Since $a_i=b_i$, $i<n$, and $a_0=b_0=1$ and $\operatorname{char} F_q \nmid k$, we conclude that $a_n=b_n$.

If $n=m$ and $k \mid (k-1)m$, the leading coefficients of Q_1 and Q_2 (namely 1, since Q_1 and Q_2 are monic), appear in the coefficient of $x^{(k-1)m}$ on both sides of the equation (111):

$$F(a_0, \ldots, a_{m-1})+ka_0^{k-1}a_m+1 = F(b_0, \ldots, b_{m-1})+kb_0^{k-1}b_m+1.$$

We again conclude $a_m=b_m$.

It follows that $U_l(m)$ is at least the number of choices for P times the number of choices for Q.

$$U_l(m) \geqslant q^m U_{l-1}\left(\left[\frac{1}{k}(k-1)m\right]\right) \gg q^m q^{k\left[\frac{1}{k}(k-1)m\right](1-\lambda^{l-1})}$$

$$\gg q^{m+(k-1)m(1-\lambda^{l-1})-k(1-\lambda^{l-1})} \gg q^{m+(k-1)m(1-\lambda^{l-1})} \quad (\text{since } q^{-k(1-\lambda^{l-1})} \gg 1)$$

$$\gg q^{km\left(\frac{1}{k}+\left(1-\frac{1}{k}\right)\right)\left(1-\left(1-\frac{1}{k}\right)^{l-1}\right)} \gg q^{km(1-\lambda^l)}.$$

LEMMA 33. *Let $R(a) = \sum_U e(aU)$ where U runs through the different monic polynomials of order km that are sums of l k-th powers. Then*

$$\int_{\operatorname{ord} a<0} |R(a)|^2 da = R(0) \ll q^{-km(1-\lambda^l)} R^2(0). \tag{113}$$

Proof.

$$\int_{\operatorname{ord} a<0} |R(a)|^2 da = \sum_{U_1}\sum_{U_2} \int_{\operatorname{ord} a<0} e\big(a(U_1-U_2)\big) da.$$

The integral on the right is 0 unless $U_1 = U_2$ when it is 1. Therefore summing over U_1 and U_2 is the same as counting the number of U, which is also given by $R(0)$. Thus the first equality in (113) is established. The second inequality follows from the previous lemma, since the number of U is

$$R(0) = U_l(m) \gg q^{km(1-\lambda^l)}.$$

LEMMA 34. *Suppose $\mathscr{V}$ is a set of polynomials of the form:*

$$V = x^v + V_1, \quad \operatorname{ord} V_1 < v. \tag{114}$$

Also let $\mathscr{U}$ be a set of polynomials of the form:

$$U = x^u + U_1, \quad \operatorname{ord} U_1 < u. \tag{115}$$

Let

$$L(a) = \sum_{V\in\mathscr{V}}\sum_{U\in\mathscr{U}} e(aUV). \tag{116}$$

If

$$\left\{\begin{array}{l} \text{(a) } a = \dfrac{A}{Q} + \beta, \\ \text{(b) } \operatorname{ord}\beta \leqslant -1-u-v, \\ \text{(c) } v < \operatorname{ord} Q, \\ \text{(d) } u < \operatorname{ord} Q, \\ \text{(e) } u_0 = \operatorname{card}\mathscr{U}, \\ \text{(f) } v_0 = \operatorname{card}\mathscr{V}, \end{array}\right. \tag{117}$$

then

$$|L(a)|^2 \leqslant u_0 v_0 q^u. \tag{118}$$

Proof. Employing Cauchy's inequality in the form

$$\Big|\sum a_i\Big|^2 \leqslant (\# \text{ of terms}) \sum |a_i|^2,$$

we conclude that

$$(119) \qquad |L(a)|^2 = \Big|\sum_{V\in\mathscr{V}} \sum_{U\in\mathscr{U}} e(aUV)\Big|^2$$
$$\leqslant v_0 \sum_{V\in\mathscr{V}} \Big|\sum_{U\in\mathscr{U}} e(aUV)\Big|^2$$
$$\leqslant v_0 \sum_{\substack{\operatorname{ord} V_1<v\\ V=x^v+V_1}} \Big|\sum_{U\in\mathscr{U}} e(aUV)\Big|^2$$
$$\leqslant v_0 \sum_{\substack{\operatorname{ord} V_1<v\\ V=x^v+V_1}} \sum_{U\in\mathscr{U}} \sum_{U'\in\mathscr{U}} e\big(a(U-U')V\big),$$

where now the summation over V is over all polynomials of the form $V = x^v + V_1$, $\operatorname{ord} V_1 < v$. In the summation over U and U' in (119), there are at most u_0 pairs (U, U') giving any particular value of $U'' = U - U'$. Also since $U = X^u + U_1$, $U' = X^u + U_1'$, $\operatorname{ord} U_1 < u$, $\operatorname{ord} U_2 < u$, we conclude that $\operatorname{ord} U'' < u$. It follows that

$$(120) \qquad |L(a)|^2 \leqslant v_0 u_0 \sum_{\operatorname{ord} U''<u} \Big|\sum_{\substack{\operatorname{ord} V_1<v\\ V=x^v+V_1}} e(aU''V)\Big|,$$

where U'' now ranges over all the polynomials of order $< u$. It follows from (b) of the hypothesis that $\operatorname{ord} \beta U'' V < -1$. Therefore

$$\Big|\sum_{\substack{\operatorname{ord} V_1<v\\ V=x^v+V_1}} e(aU''V)\Big| = \Big|\sum_{\substack{\operatorname{ord} V_1<v\\ V=x^v+V_1}} e\Big(\frac{A}{Q}U''V\Big)\Big| = \Big|\sum_{\operatorname{ord} V_1<v} e\Big(\frac{A}{Q}U''V_1\Big)\Big|.$$

(Here $e\Big(\frac{A}{Q}x^v\Big)$ is a uniform constant factor and so may be omitted in the sum.) Summation over V_1 gives 0 or q^v depending on whether $\operatorname{ord}\Big(\Big(\frac{A}{Q}U''\Big)\Big) \geqslant -v$ or not. Writing $U'' = QU_2 + U_3$, $\operatorname{ord} U_3 < \operatorname{ord} Q$,

$$|L(a)|^2 \leqslant v_0 u_0 \sum_{\operatorname{ord} U_2<n-\operatorname{ord} Q} \sum_{U_3 \bmod Q} \Big|\sum_{\operatorname{ord} V_1<v} e\Big(\frac{A}{Q}(QU_2+U_3)V_1\Big)\Big|$$
$$\leqslant v_0 u_0 \frac{q^u}{|Q|} \sum_{U_3 (\bmod Q)} \Big|\sum_{\operatorname{ord} V_1<v} e\Big(\frac{A}{Q}U_3V_1\Big)\Big|.$$

But as U_3 runs over a complete set of residues $\bmod Q$, so does AU_3. Out of this complete set of residues there are precisely $|Q|/q^v$ residue classes

whose fractional parts have order less than $-v$. For each such residue the inner sum has value q^v and for the remaining classes the inner sum is zero. Thus

$$|L(\alpha)|^2 \leqslant v_0 u_0 \frac{q^u}{|Q|} \cdot \frac{|Q|}{q^v} q^v \leqslant v_0 u_0 q^u. \tag{121}$$

LEMMA 35. *Suppose $k|m$. Let W run through all the monic polynomials of order $\frac{1}{k}m$. Let V_1 run through all the monic polynomials of order $(k-1)m$ which are the sums of l' k-th powers. Let $L(\alpha) = \sum_{V_1}\sum_{W} e(\alpha V_1 W^k)$. Suppose $\alpha \in$ minor arc $M(A, Q)$. Then*

$$|L(\alpha)| \ll L(0) q^{\left(-\frac{1}{2k}+\frac{1}{2}\left(1-\frac{1}{k}\right)^{l'}(k-1)\right)m}. \tag{122}$$

Proof. We use Lemma 34 with $V = W^k$ and $U = V_1$. Then $v = m$, $v_0 = q^{\frac{1}{k}m}$, $u = (k-1)m$ and $u_0 = U_{l'}\left(\frac{1}{k}(k-1)m\right)$. Since α is on a minor arc, $\alpha = \frac{A}{Q} + \beta$ with $\operatorname{ord} Q < m$ and $\operatorname{ord}\beta < -\operatorname{ord} Q - (k-1)m$. The hypotheses of Lemma 34 are easily seen to be valid, so it follows that

$$|L(\alpha)|^2 \leqslant u_0 v_0 q^u \leqslant q^{\left(\frac{1}{k}+k-1\right)m} U_{l'}\left(\frac{1}{k}(k-1)m\right). \tag{123}$$

Also $L(0) = \#$ of terms in $L(\alpha) = u_0 v_0 = U_{l'}\left(\frac{1}{k}(k-1)m\right) \cdot q^{\frac{1}{k}m}$. Therefore

$$|L(\alpha)|^2 \leqslant |L(0)|^2 U_{l'}^{-1}\left(\frac{1}{k}(k-1)m\right) q^{\left(-\frac{1}{k}+k-1\right)m}. \tag{124}$$

By Lemma 32, $U_{l'}\left(\frac{1}{k}(k-1)m\right) \gg q^{(k-1)(1-\lambda^{l'})m}$. Therefore

$$|L(\alpha)| \leqslant |L(0)| q^{\left(-\frac{1}{2k}+\frac{1}{2}\left(1-\frac{1}{k}\right)^{l'}(k-1)\right)m}.$$

LEMMA 36. *Let $\mathfrak{m}$ denote the set of minor arcs. If $l = l' \geqslant k\log(3k^2-k)$ then for some $\delta > 0$,*

$$\int_{\mathfrak{m}} |T(\alpha)|^{3k+1} |R(\alpha)|^2 |L(\alpha)|\, d\alpha \ll q^{m(2k+1-\delta)} R^2(0) L(0). \tag{125}$$

Proof. We use the trivial estimate $|T(\alpha)| \leqslant q^m$, Lemma 33 and Lemma 35. We conclude that

$$\begin{aligned}\int_{\mathfrak{m}} |T(\alpha)|^{3k+1} |R(\alpha)|^2 |L(\alpha)|\, d\alpha \\ &\ll q^{m\left(3k+1-\frac{1}{2k}+\frac{1}{2}\left(1-\frac{1}{k}\right)^{l'}(k-1)-k+k\left(1-\frac{1}{k}\right)^{l}\right)} R^2(0) L(0) \\ &\ll q^{m\left(2k+1-\frac{1}{2k}+\frac{1}{2}\left(1-\frac{1}{k}\right)^{l}(3k-1)\right)} R^2(0) L(0).\end{aligned}$$

We want

$$\frac{1}{2}\left(1-\frac{1}{k}\right)^l(3k-1) < \frac{1}{2k},$$

or

$$l\log\left(1-\frac{1}{k}\right) < -\log 2k - \log\frac{1}{2}(3k-1).$$

This is true if

$$l\log\left(1-\frac{1}{k}\right) < -\frac{l}{k} \leqslant -\log 2k - \log\frac{1}{2}(3k-1)$$

or

$$\frac{l}{k} \geqslant \log\frac{1}{2}(3k-1)\cdot 2k,$$

that is if

$$l \geqslant k\log(3k^2-k).$$

THEOREM 37. *If* $\operatorname{char} F_q = p \nmid k$ *then a polynomial* N *is a sum of* k*-th powers if and only if it is a sum of* k*-th powers* $\bmod P$ *for all irreducible* P *such that* $|P| \leqslant (k-1)^2$. *In that case, it is expressible as a sum of*

$$\tilde{g}(k) < 3k + 3[k\log(3k^2-4)] + 4 \tag{126}$$

k*-th powers. If* $p^\nu \| k$ *then* N *is a sum of* k*-th powers if and only if* N *is a* p^ν*-th power of a polynomial* N_1 *where* N_1 *satisfies a similar condition for* $k_1 = k/p^\nu$. *In this case* $\tilde{g}(k) = \tilde{g}(k_1)$ *satisfies a condition similar to* (126) *with* k_1 *in place of* k.

Proof. The case where $p|k$ is obvious provided we show the case where $p \nmid k$. Suppose $p \nmid k$. Then the first statement follows from Lemma 29. We consider representations of N in the form (86) with the provisions (87) (a)—(d). The number of such representations, say $r'(N)$ is

$$r'(N) = \int_{\operatorname{ord} a<0} T(a)^{3k+1} R^2(a) L(a) e(-Na)\, da.$$

The contribution of the major arcs is

$$\mathfrak{J}_1 = \sum_{U_1}\sum_{U_2}\sum_{V}\sum_{W}\int_{\mathfrak{M}} T^{3k+1}(a) e\big(a(-N+U_1+U_2+VW^k)\big)\, da.$$

There are $R^2(0)L(0)$ such terms, and for each, the contribution of the integral is $\gg q^{m(k+1)}$. (See Lemma 29 and Theorem 30.) In all, the major arcs give

$$\mathfrak{J}_1 \gg R^2(0)L(0)q^{m(2k+1)}.$$

According to Lemma 36, the contribution of the minor arcs is

$$\ll q^{m(2k+1-\delta)} R^2(0)L(0).$$

Thus $r'(N)\to\infty$ as $m\to\infty$ through values divisible by k. It follows that

$$\tilde{g}(k)\leqslant 3k+1+3l<2k+3[k\log(3k^2-k)]+4.$$

COROLLARY 38. *There exist polynomials B, $B_1,\ldots,B_M$ such that a polynomial N is a sum of k-th powers if and only if $N\equiv B_i(\operatorname{mod}B)$ for some i. If $p=\operatorname{char}F_q\nmid k$ then B is the product of distinct irreducible polynomials P such that $|P|\leqslant(k-1)^2$. If $p^\nu\|k$ then B is the product of p^ν-th powers of distinct irreducible polynomials P such that $|P|\leqslant(k-1)^2$. Modulo B, the B_i form a ring.*

Proof. This follows from Theorem 37. The B_i form a ring $(\operatorname{mod}B)$ since the polynomials that are sums of kth powers are closed under subtraction and multiplication since $-1=\underbrace{1^k+\ldots+1^k}_{p-1\text{ times}}$.

THEOREM 39. *Given k and F_q. If $\operatorname{char}F_q\nmid k$ there is an extension $F_{q'}$ of F_q such that*

$$g(k,q')\leqslant k.$$

In particular, every $N\in F_q[x]$ is a sum of at most k k-th powers of polynomials in $F_{q'}[x]$.

Proof. The proof is similar to the proof of Theorem 31. Let F_{q_1} be an extension of F_q with at least k different elements $b_1,\ldots,b_k\in F_{q_1}$. Their Vandermonde determinant is

$$\begin{vmatrix} 1 & 1 & \ldots & 1\\ b_1 & b_2 & \ldots & b_k\\ b_1^2 & b_2^2 & \ldots & b_k^2\\ \ldots & \ldots & \ldots & \ldots\\ b_1^{k-1} & b_2^{k-1} & \ldots & b_k^{k-1}\end{vmatrix}=\prod_{i>j}(b_i-b_j)\neq 0.$$

It follows that there is a solution $a_1,\ldots,a_k\in F_{q_1}$ of the equations

$$\begin{gathered}\sum_1^k a_i=0,\\ \sum a_ib_i=0,\\ \sum a_ib_i^2=0,\\ \ldots\ldots\ldots\ldots\\ \sum a_ib_i^{k-2}=0,\\ \sum a_ib_i^{k-1}=\frac{1}{k}.\end{gathered}$$

Thus with $b = \sum_1^k a_i b_i^k$, we have

$$x+b = \sum_1^k a_i (x+b_i)^k. \tag{126a}$$

Let $F_{q'}$ be the extension of F_{q_1} with $c_i = a_i^{1/k}$, $1 \leqslant i \leqslant k$, adjoined. We find

$$x+b = \sum_1^k (c_i x + c_i b_i)^k. \tag{126b}$$

An arbitrary polynomial $P \in F_{q'}[x]$ may be written as a sum of k kth powers by substituting $P-b$ for x in the identity (126b).

THEOREM 40. *Let $p = \operatorname{char} F_q$, with say, $q = p^n$. The set of sums of k-th powers of elements from F_q is a field, say F_{p^m}. Let $\mathscr{R}(q, k)$ be the ring of polynomials over F_q which are sums of k-th powers. If $p \nmid k$ then*

$$\dim_{Z_p} F_q[x]/\mathscr{R}(q, k) \leqslant \frac{k(k-1)}{2} n - (k-1)m. \tag{127}$$

Proof. Any subset of a finite field closed under addition and multiplication (and containing 1) is a field. Therefore the sums of kth powers of F_q is indeed a field. Since $1 = 1^k \in \mathscr{R}(q, k)$, $\mathscr{R}(q, k)$ can be viewed as a vector space over $\boldsymbol{Z}_p$. For $A(x) \in F_q[x]$, $A^k(x) \in \mathscr{R}(q, k)$.

To prove the theorem it will suffice to show that an arbitrary polynomial P can be written as $P = P_1 + P_2$ where $P_1 \in \mathscr{R}(q, k)$ and P_2 is in a vector space of the indicated dimension. We first show by induction that we can reduce P to a polynomial of order $< (k-1)^2$ by adding a polynomial $P_1 \in \mathscr{R}(q, k)$. If $\operatorname{ord} P < (k-1)^2$ there is nothing to show. Now suppose $t = \operatorname{ord} P \geqslant (k-1)^2$ and that we have proved the assertion for all polynomials Q of order $< t$. Write $t = (k-1)u + v$ where $0 \leqslant v < k-1$. Since $t \geqslant (k-1)^2$, $u \geqslant k-1 > v$. Suppose $P = bx^t + P'$ where $\operatorname{ord} P' \leqslant t-1$. Let $a = \frac{1}{k} b$. Then

$$\begin{aligned} P + x^{ku} - (x^u + ax^v)^k \\ = bx^t + P' + x^{ku} - \Big(x^{ku} + bx^{(k-1)u+v} + \sum_{i=2}^k \binom{k}{i} a^i x^{(k-i)u+iv}\Big). \end{aligned}$$

Therefore

$$\begin{aligned} \operatorname{ord}\big(P + x^{ku} - (x^u + ax^v)^k\big) &\leqslant \max_{2 \leqslant i \leqslant k}\big(\operatorname{ord} P', (k-i)u + iv\big) \\ &\leqslant \max\big(t-1, ku - \min_{2 \leqslant j \leqslant k}\{(u-v)j\}\big) < t. \end{aligned}$$

(Here $u > v$, so $ku - \min_{2 \leqslant j \leqslant k} (u-v)j = ku - 2(u-v) < (k-1)u + v = t$.)

Now the induction hypothesis gives the assertion.

Next we note that we can still use the same trick to eliminate the powers x^t, for $t < (k-1)^2$, provided $u > v$. Starting from

$$u = k-2,\ v = k-3,\ k-4,\ \ldots,\ 0,$$
$$u = k-3,\ v = k-4,\ k-5,\ \ldots,\ 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

to

$$u = 1, \qquad v = 0,$$

we may eliminate powers $x^t = x^{(k-1)u+v}$. In all there are $1+2+\ldots+$ $+(k-2) = \dfrac{(k-2)(k-1)}{2}$ less powers of x. We can also eliminate those powers of the form $(ax^w)^k$ of degree $< (k-1)^2$ hence with $0 \leqslant w \leqslant k-2$, to give $(k-1)m$ fewer dimensions. In all the dimension of $F_q[x]/\mathscr{R}(q, k)$ is at most

$$\left\{(k-1)^2 - \frac{(k-2)(k-1)}{2}\right\} n - (k-1)m = \frac{k^2-k}{2} n - (k-1)m.$$

EXAMPLE 41. $k = p^h+1$, $F_q = \boldsymbol{Z}_p$. In this case, $n = m = 1$. In fact, equality holds in (127) of the previous theorem:

$$\dim_{\boldsymbol{Z}_p} \boldsymbol{Z}_p[x]/\mathscr{R}(p, p^h+1) = \frac{k^2-3k+2}{2}.$$

Proof. We define an n-nomial as a polynomial in which n distinct powers of x appear. Thus there are monomials, binomials and so forth.

We show by induction, for $k = p^h+1$ the kth power of an arbitrary n-nomial can be written as the sum of kth powers of monomials and binomials. For $n = 1, 2$ there is nothing to prove. Suppose we have shown the assertion for arbitrary m-nomials, $m \leqslant n-1$.

Any n-nomial can be written as ax^t+bx^u+P where P is an $(n-2)$-nomial of degree less than u. Its kth power is

$$\begin{aligned}(ax^t+bx^u+P)^k &= (ax^t+bx^u+P)^{p^h}(ax^t+bx^u+P)\\ &= \{(ax^t)^{p^h}+(bx^u)^{p^h}+P^{p^h}\}(ax^t+bx^u+P)\\ &= (ax^t+bx^u)^k+(ax^t+P)^k+(bx^u+P)^k-(ax^t)^k-(bx^u)^k-P^k.\end{aligned}$$

The induction hypothesis now shows that $(ax^t+bx^u+P)^k$ is a sum of kth powers of monomials and binomials.

Instead of using kth powers of binomials $(ax^u+bx^v)^k$ it will be convenient to use truncated binomials of the form

$$a(x^{p^h u+v}+x^{u+p^h v}).$$

No generality is lost since the kth power of an arbitrary binomial, with $k = 1+p^h$, is the sum of kth powers of monomials and a truncated binomial and conversely; for we have

$$(128)\qquad (ax^u+bx^v)^k = \left((ax^u)^{p^h}+(bx^v)^{p^h}\right)(ax^u+bx^v)$$
$$= (ax^u)^k+ab\left(x^{p^h u+v}+x^{u+p^h v}\right)+(bx^v)^k.$$

We will assume $u \neq v$ when we write a truncated binomial. The reduction process in Theorem 40 left the powers

$$(129)\qquad x^t = x^{(k-1)u+v} = x^{p^h u+v}$$

where

$$t < (k-1)^2, \qquad 0 \leqslant u < v < k-1.$$

That is, those values of t for which

$$(130)\qquad \begin{array}{ll} u = 0, & v = 1, \ldots, k-2, \\ u = 1, & v = 2, \ldots, k-2, \\ u = 2, & v = 3, \ldots, k-2, \\ \multicolumn{2}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ u = k-3, & v = k-2. \end{array}$$

Let $t_0 = p^h u_0+v_0$ be one of the special exponents of the form (129). We show by induction on n that there is no chain

$$(131)\qquad (u_0, v_0),\ (u_1, v_1),\ (u_2, v_2), \ldots, (u_n, v_n)$$

such that

$$(132)\qquad u_{i-1}+p^h v_{i-1} = u_i p^h+v_i, \qquad 1 \leqslant i \leqslant n$$

and either

(a) $t_n = u_n p^h+v_n$ is divisible by k,

or

(b) $t_n = u_n p^h+v_n$ is one of the special exponents of the form (129) different from $t_0 = p^h u_0+v_0$. In case $n = 0$ there is nothing to prove. Suppose there are no such chains of length $n-1$ but there is such a chain of length n.

If $k|(u_n p^h+v_n)$, then $p^h+1 = k$ also divides $u_{n-1}+p^h v_{n-1} = u_n p^h+v_n$. Therefore

$$k \text{ divides } u_{n-1}-v_{n-1} = u_{n-1}+v_{n-1}p^h-kv_{n-1},$$

and also

$$k \text{ divides } u_{n-1}+v_{n-1}p^h+(p^h-1)(u_{n-1}-v_{n-1}) = u_{n-1}p^h+v_n.$$

This contradicts the induction hypothesis since

$$(u_0, v_0), \ldots, (u_{n-1}, v_{n-1})$$

would be a chain of length $n-1$.

Therefore it must be that $t_n = u_n p^h + v_n$ is one of the special powers different from t_0. But

$$p^h(up^h+v) \equiv u+vp^h (\operatorname{mod} p^{2h}-1).$$

Using this relation repeatedly with (132), we conclude that

$$p^{hn}(p^h u_0+v_0) \equiv p^{h(n-1)}(u_1 p^h+v_1) \equiv \ldots \equiv p^h u_n+v_n (\operatorname{mod} p^{2h}-1).$$

Therefore either (for n even)

$$(*) \qquad p^h u_0+v_0 \equiv p^h u_n+v_n (\operatorname{mod} p^{2h}-1)$$

or (for n odd)

$$(**) \qquad p^h v_0+u_0 \equiv p^h u_n+v_n (\operatorname{mod} p^{2h}-1).$$

Neither of these two congruences $(*)$ or $(**)$ is possible for two values $(u_0, v_0) \neq (u_n, v_n)$ from table (130) as can be seen by the following argument: Suppose two integers, say r_0, r_n, are given in base p^h, i.e.,

$$r_0 = a_0+a_1 p^h+a_2 p^{2h}+a_3 p^{3h}+\ldots,$$
$$r_n = b_0+b_1 p^h+\ldots$$

where $0 \leqslant a_i, b_i < p^h-1$.

Then $r_0 \equiv r_n \operatorname{mod} p^{2h}-1$ if and only if

$$\sum_{i \text{ even}} a_i+p^h \sum_{i \text{ odd}} a_i \equiv \sum_{i \text{ even}} b_i+p^h \sum_{i \text{ odd}} b_i (\operatorname{mod} p^{2h}-1).$$

If, in addition, each of the four summations in this congruence are less than p^h, then

$$\sum_{i \text{ even}} a_i = \sum_{i \text{ even}} b_i, \qquad \sum_{i \text{ odd}} a_i = \sum_{i \text{ odd}} b_i.$$

Therefore taking $r_0 = v_0+u_0 p^h$, and $r_n = v_n+u_n p^h$ and assuming $(*)$ we see that

$$u_0 = u_n, \qquad v_0 = v_n.$$

A similar argument holds for $r_0 = u_0+v_0 p^h$, $r_n = v_n+u_n p^h$ and $(**)$.

Suppose that inequality holds in (127). It must be that some polynomial $P \in \mathscr{R}(q, k)$ is of the form

$$(133) \qquad P = \sum_1^l a_i x^{t_i},$$

where

(a) each t_i is of the form t in (129),
(b) the t_i are distinct,
(c) the $a_i \neq 0$.

It follows that P is the sum of kth powers of monomial and truncated binomials:

$$\sum_{i=1}^{l} a_i x^{t_i} = \sum_{1}^{m} (b_i x^{\omega_i})^k + \sum_{1}^{n} c_i (x^{p^h y_i + \zeta_i} + x^{y_i + p^h \zeta_i}). \tag{134}$$

We may assume $y_i \neq \zeta_i$, $1 \leqslant i \leqslant n$.

Let Π be the following set of integers:

(a) $t_1 \in \Pi$,

(b) if $p^h y_i + \zeta_i \in \Pi$, $1 \leqslant i \leqslant n$, then $y_i + p^h \zeta_i \in \Pi$,

(c) if $y_i + p^h \zeta_i \in \Pi$, $1 \leqslant i \leqslant n$, then $p^h y_i + \zeta_i \in \Pi$.

(Here y_i, ζ_i are those that appear in (134).) After renumbering we may assume that the first n_0 truncated binomials have their powers in Π.

Since there is no chain of the form (131)–(132) we may conclude that:

$$a_1 x^{t_1} = \sum_{1}^{n_0} c_i (x^{p^h y_i + \zeta_i} + x^{y_i + p^h \zeta_i}). \tag{135}$$

Here $y_i \neq \zeta_i$, $1 \leqslant i \leqslant n_0$.

Now define the sets Π_j, $j \geqslant -1$ of powers of x:

(a) $\Pi_{-1} = \emptyset$,

(b) $\Pi_0 = \{t_1\}$,

(c) if $p^h y_i + \zeta_i \in \Pi_j$, $1 \leqslant i \leqslant n_0$ and $y_i + p^h \zeta_i \notin \Pi_{j-1}$, then $y_i + p^h \zeta_i \in \Pi_{j+1}$,

(d) if $y_i + p^h \zeta_i \in \Pi_j$, $1 \leqslant i \leqslant n_0$ and $p^h y_i + \zeta_i \notin \Pi_{j-1}$, then $p^h y_i + \zeta_i \in \Pi_{j+1}$.

We show by induction on j the sets Π_j are pairwise disjoint. Clearly $\Pi_{-1}, \Pi_0, \Pi_1, \Pi_2$ are pairwise disjoint. Suppose we have shown $\Pi_{-1}, \ldots, \Pi_j$, $j \geqslant 2$ are pairwise disjoint. Clearly $\Pi_{j+1} \cap \Pi_j = \Pi_{j+1} \cap \Pi_{j-1} = \Pi_{j+1} \cap \Pi_{-1} = \emptyset$. Suppose $\Pi_{j+1} \cap \Pi_l \neq \emptyset$, $-1 < l \leqslant j-2$. Say $p^h y_i + \zeta_i \in \Pi_{j+1} \cap \Pi_l$ where $y_i + p^h \zeta_i \in \Pi_j$. Then either $y_i + p^h \zeta_i \in \Pi_{l-1}$ or $y_i + p^h \zeta_i \in \Pi_{l+1}$ contradicting the induction hypothesis. A similar argument holds when $y_i + p^h \zeta_i \in \Pi_{j+1} \cap \Pi_l$.

In particular $t_1 \notin \Pi_j$, $j > 0$.

Let $\mathscr{I}_j = \{i \mid 1 \leqslant i \leqslant n_0,\ p^h y_i + \zeta_i \in \Pi_j \text{ or } y_i + p^h \zeta_i \in \Pi_j\}$. In equation (135) the coefficient of x^{t_1} is

$$a_1 = \sum_{i \in \mathscr{I}_1} c_i.$$

The sum of the coefficients of x^u, $u \in \Pi_j$, $j \geqslant 1$ in equation (135) is:

$$0 = \sum_{i \in \mathscr{I}_{j-1}} c_i + \sum_{i \in \mathscr{I}_j} c_i.$$

Since $a_1 \neq 0$, it follows that

$$\sum_{i \in \mathscr{I}_j} c_i \neq 0, \quad j \geqslant 1.$$

This is a contradiction because the Π_j (and so the $\mathscr{I}_j$) are eventually empty.

BIBLIOGRAPHY

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenz, II*, Math. Zeitschr. 19 (1924), pp. 207–246.

[2] H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Ann Arbor 1962.

[3] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly 78 (1971), pp. 10–36.

[4] D. Hayes, *A polynomial analogue of the Goldbach conjecture*, BAMS 69 (1963), pp. 115–116.

[5] — *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11 (1966), pp. 461–488.

[6] R. E. A. C. Paley, *Theorems on polynomials in a Galois Field*, Quart. J. Math. (Oxford) 4 (1933), pp. 52–63.

[7] C. L. Siegel, *Additive Theorie der Zählkorper, II*, Math. Ann. 88 (1923), pp. 184–210.

[8] — *Generalization of Waring's problem to Algebraic Number Fields*, Amer. J. Math. 66 (1944), pp. 122–136.

[9] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, New York 1954.

[10] — *On Waring's problem*, Ann. of Math. 36 (1935), pp. 395–405.