72-4917

KUBOTA, Robert Maruo, 1941-
WARING'S PROBLEM IN $F_q[x]$.

The University of Michigan, Ph.D., 1971
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED

WARING's PROBLEM IN $F_q[x]$

by

Robert Maruo Kubota

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1971

Doctoral Committee:

Professor D. J. Lewis, Chairman
Professor S. Baker
Professor R. C. Lyndon
Assistant Professor J. Milne
Instructor P. Weinberger

PLEASE NOTE:

Some Pages have indistinct print. Filmed as received.

UNIVERSITY MICROFILMS

Acknowledgements

Professor D. J. Lewis guided the research. The late Professor Harold Davenport also made suggestions. Dr. Peter Weinberger carefully read the manuscript and simplified the statement of the main theorem. I thank all three men.

TABLE OF CONTENTS

	Introduction	1
1.	Preliminaries	11
2.	The Farey Arcs	16
3.	The Contribution of the Major and Minor Arcs	18
4.	Weyl's Lemma	22
5.	The Singular Integral	34
6.	The Singular Series	40
7.	The Asymptotic Formula	54
8.	Estimates for g(k)	57

Introduction:

Waring's problem is to prove that for every integer $k \geq 2$ there is an integer $s = s(k)$ such that every positive integer N can be written as a sum

$$N = P_1^k + \cdots + P_s^k, \qquad (1)$$

where $P_i \geq 0$, $P_i \in \mathbb{Z}$, $i = 1, \cdots, s$.

In the last two centuries much work has been done on this problem. Essentially three different methods of proof have been given. The first by Hilbert, using identities, and the third by Linnik, using addition of sets, showed the existence of $s(k)$. The second by Hardy and Littlewood, and perfected by Vinogradov, uses analysis and p-adic methods and gives explicit bounds for $s(k)$.* In terms of subsequent research the most productive of these methods has been the second and, indeed here research has been so great that we well recognize the "Hardy-Littlewood-Vinogradov" method. As proofs using this method are necessarily long and detailed it is of interest to find, specifically, what properties of $\mathbb{Z}$ are essential and how they are used. One convenient way to do this is to look at Waring's problem not as a problem over $\mathbb{Z}$ but over other rings (especially where the result may have interest in itself). For rings of algebraic integers this was first done by Siegel [2, 3].

* The interested reader may see Ellison [1] for an introduction to the extensive literature on the subject.

Let F_q be the finite field of q elements. Let $F_q[x]$ be the ring of polynomials in one variable over F_q. It has long been known that one can do number theory over $F_q[x]$ and that $F_q[x]$ bears a close resemblance to $\mathbb{Z}$. Thus, for example, both $F_q[x]$ and $\mathbb{Z}$ are Euclidean domains, and modulo a prime ideal they are finite fields. The monic polynomials in $F_q[x]$ correspond to the positive integers and the monic irreducible polynomials correspond to the rational primes. The "absolute value" of a polynomial P is $|P| = q^n$ where $n = \deg P$. It is quite easy to prove the "prime number theorem" in $F_q[x]$, even with Riemann hypothesis sized error term, i.e., if $\pi(n)$ = number of monic irreducible polynomials of deg $\leq n$ then

$$\pi(n) = \frac{q^n}{n} + O(q^{n/2}).$$

Perhaps the first deep number-theoretic result for $F_q[x]$ was that of Artin [4] in 1924 showing that the number of primes in arithmetic progression was the correct size (though of course he did not show it with generalized Riemann hypothesis sized error). Later Hayes [5, 6] considered Goldbach's conjecture for $F_q[x]$ and the extension to $F_q[x]$ of Vinogradov's result on the sum of three primes. Thus it is a natural line of research to investigate Waring's problem in $F_q[x]$. The only previous research on this problem that has come to the knowledge of the present author is a short paper by R. Paley [7], in 1933, where he showed by means of identities that $\tilde{g}(k) = \tilde{g}(k, q)$ exists, where $\tilde{g}(k, q)$ is the least integer s such that every polynomial that is the sum of k^{th} powers of

polynomials is the sum of s k^{th} powers of polynomials, and found $\tilde{g}(k)$ in specific instances.

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 so also is

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

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

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

The principal theorem proven is the following (see Theorem 30):

Theorem: If $k < \text{char } F_q$ and $s \geq \max(3k+1,\ 2^k+1)$ and N is a polynomial of degree $< (k - 1 + \epsilon)m$ where $\frac{1}{2k} \leq \epsilon < 1$, then there exists $\delta > 0$ such that

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

where

$$1 << \frac{U(s, 0, q)}{q^{s-k} - 1} \gamma(N, s, k, q) << 1,$$

and $U(s, 0, q)$ is the number of s-tuples $c_1, \cdots, c_s$ such that

$$c_1^k + \cdots + c_s^k = 0 \text{ where } c_i \in F_q, \text{ and not all } c_i = 0. \qquad (4)$$

The value of the "singular integral" is $\frac{U(s, 0, q)}{q^{s-k}-1} q^{(s-k)m}$ and $\mathfrak{S}(N, s, k, q)$ is the "singular series".

The method of proof is as follows: Let K_∞ be the field of formal power series in x^{-1} over F_q, i.e., the set of all expressions (for all $m \in \mathbb{Z}$)

$$\alpha = \sum_{-\infty}^{m} a_i x^i, \quad a_i \in F_q, \quad a_m \neq 0$$

(together with 0) with the usual operations. We define $m = \operatorname{ord} \alpha$ (with $-\infty = \operatorname{ord} 0$). Then much as $\mathbb{Z}$ lies in $\mathbb{R}$ (the completion of $\mathbb{Q}$ with respect to $|\ |$), $F_q[x]$ lies in the completion K_∞ of the field of rational functions in one variable over F_q with respect to the valuation $|\alpha| = q^m$. We define an exponential function $e: K_\infty \to \mathbb{C}$ with the properties required for the Hardy-Littlewood method (Lemma 1). This may not be the only possible definition for e but it is a natural one in many ways. The Haar integral plays the role of the Riemann integral and $\{\alpha \mid \operatorname{ord} \alpha < 0\}$ plays the role of the unit interval. Thus (see Lemma 2) if $T(\alpha) = \sum_{\substack{\operatorname{ord} P < m \\ P \text{ a polynomial}}} e(\alpha P^k)$, then

$$r(N, m, s, k, q) = \int_{\operatorname{ord} \alpha < 0} T^s(\alpha)\, e(-N\alpha)\, d\alpha. \qquad (5)$$

As in the case of $\mathbb{Z}$, if α is "near" (under $|\ |$) to $\frac{A}{Q}$, A, Q polynomials, where Q has small (large) degree, we say that α is in a major (minor) arc about $\frac{A}{Q}$. The integral in (5) is split into an integral

over the minor arcs which is of the order of the error term (see § 4, especially Theorem 14) and an integral over the major arcs. The integral over the major arcs is replaced (Theorem 30) with acceptable error by a product of the singular integral (see § 5, especially Theorem 18) and the singular series (§ 6, especially Theorem 29). The work on the singular integral is different from the case of $\mathbb{Z}$ as they have different values but the work on the singular series is quite similar, the proofs being lifted almost verbatim from Davenport's lectures [8, Chapter 5, 6] (who follows Vinogradov [9, Chapter 2]).

We now turn to five remarks on the principal 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 $(k-1+\epsilon)m$ as stated. This is possible but a bit messy (see Lemma 17). The difficulty arises because now we must also consider the solutions of

$$c_1^k + \cdots + c_s^k = b$$

where b is the leading coefficient of N in the evaluation of the singular integral.

2) We must have $s \geq 3k+1$ in order to prove that the singular series converges absolutely (Lemma 23) and $s \geq k+1$ in order to show that the singular series is positive (Lemma 27). In the classical case, if $s \geq 2k$ (k odd) or $s \geq 4k$ (k even) the singular series is positive and if $s \geq 2k+1$, the singular series converges absolutely.

3) Since we have assumed $k < p$, every polynomial N is a sum

of k^{th} powers. In general, this is not true. For example, if $k = p^h - 1$, $q = p^h$, $h > 1$, p a prime, then the constant term of any polynomial P^k (over F_q) is either 0 or 1. Therefore no polynomial N whose constant term is in $F_q \setminus \mathbb{Z}_p$ is a sum of k^{th} powers. It is true (Theorem 37) that if $\text{char } F_q \nmid k$ then N is a sum of k^{th} powers if N is congruent to a sum of k^{th} powers, mod P, for all irreducible P such that $|P| \leq (k-1)^2$. (See Theorem 40 and Example 41 for further considerations.)

4) The principal defect in the theorem is the restriction $k < \text{char } F_q$. It seems likely that $\text{char } F_q \nmid k$ is the proper restriction. The difficulty arises in the proof of Weyl's Lemma (Proposition 12) which states that if $k < \text{char } F_q$, $\alpha \in$ minor arc and

$$S_k(f) = \sum_{\text{ord } P < m} e(f(P))$$

where

$$f(y) = \alpha y^k + \alpha_1 y^{k-1} + \cdots + \alpha_k, \quad \text{where } \alpha, \alpha_i \in K_\infty.$$

(here $k = \deg f$.) Then for every $\epsilon > 0$,

$$|S_k(f)| << q^{(1-\frac{1}{2^{k-1}} + \epsilon)m}. \tag{6}$$

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

$$S_1(\Delta_{y_{k-1}}(\cdots(\Delta_{y_1} f))\cdots) \quad \text{where } \Delta_{y_{k-1}}(\cdots(\Delta_{y_1} f(y))\cdots)$$

is linear in y, sums which we can estimate. Here

$$\Delta y_1 f(y) = f(y + y_1) - f(y),$$

and

$$\Delta y_{k-1} \cdots (\Delta y_1 f(y)) \cdots) = k!\, \alpha y + \text{terms independent of } y. \qquad (7)$$

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

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

$$\begin{array}{c} x_1 + \cdots + x_k \\ x_1^2 + \cdots + x_k^2 \\ \vdots \\ x_1^k + \cdots + x_k^k \end{array}$$

where $x_i \geq 0$, $x_i \in \mathbb{Z}$, $i = 1, \cdots k$

are independently distributed (in intervals of size proportional to the exponents j, $1 \leq j \leq k$, involved) when the x_i are in "well-separated"

intervals. This is false in $F_q[x]$ when $k \geq \text{char } F_q$ since then

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

Let $\tilde{g}(k) = \tilde{g}(k, q)$ be the least s such that every polynomial that is a sum of k^{th} powers is a sum of s k^{th} powers. Let $G(k) = G(k, q)$ be the least s such that every polynomial of sufficiently large degree that is a sum of k^{th} powers is a sum of s k^{th} powers. By the proof for $\mathbb{Z}$ given by Vinogradov [10], that $G(k) < c\, k \log k$, we show that in $F_q[x]$, $\tilde{g}(k) < c\, k \log k$ (see§ 8, Theorem 37). The improvement from $G(k)$ to $\tilde{g}(k)$ is due to a difference in structure. Consider, for $N \geq 0$

$$N = P_1^k + \cdots + P_s^k, \text{ where } P_i \geq 0,\ P_i \in \mathbb{Z},\ i = 1, \cdots, s.$$

The asymptotic formula gives the number of representations (if s is sufficiently large) as,

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

So for small N, the number of representations is fairly small. In $F_q[x]$, if $k < \text{char } F_q$, the number of representations (for s sufficiently large) is

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

when the P_i are restricted to $\text{ord } P_i < m$, $i = 1, \cdots, s$. So the number of representations of small N is about the same as the number of representations of large N. This behavior persists for $\text{char } F_q \nmid k$, and

naturally leads to a proof for $\tilde{g}(k)$ not $G(k)$.

In the case of $\mathbb{Z}$, Vinogradov's estimate $G(k) < ck \log k$ is thought to be a profound analysis since, among other things

$$G(k) \geq k + 1.$$

The known proofs for bounds on $G(k)$ depend on the size of k, and not that k may have a particular form.

In the case of $F_q[x]$, it is unlikely that a Vinogradov-style proof that $\tilde{g}(k) < c\, k \log k$ is anywhere near as profound. E.g., we show that (Theorem 39) for every q there exists q', $q \mid q'$ such that

$$\tilde{g}(k, q') \leq k.$$

Indeed, if $g_1(k)$ is defined analogously to $\tilde{g}(k)$ except that we consider representations

$$N = \pm P_1^k \pm \cdots \pm P_s^k,$$

(The so-called weak Waring's problem), Paley [op. cit.] has shown that if $k = p^h + 1$ then $g_1(k) \leq 6$. The essential point of the proof is that the various powers $k = p^h + 1$ satisfy an identity based on the identity

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

and this leads to the uniform bound for $g_1(k)$. So in this respect the result for $F_q[x]$ is not very satisfactory but the present author does not know how to adequately exploit the difference.

The rings $F_q[x]$ may be described as the ideal ones for the Hardy-Littlewood method. After the correct definitions are set up, the proofs generally follow quite closely to those for $\mathbb{Z}$ or are simplified. The results that follow from these proofs are naturally as good or better than for $\mathbb{Z}$. It is quite evident that the many variations of problems in $\mathbb{Z}$ susceptible to this method are also susceptible in $F_q[x]$ to the same method with minor alterations, except of course that Weyl's Lemma is shown only for $k < \text{char } F_q$.

1. Preliminaries: Let F_q denote the finite field of $q = p^f$ elements. Members of F_q, the constants will be denoted by $a, b, c, \cdots$. $F_q[x]$ will denote the polynomials in one variable with coefficients in F_q. Polynomials will be denoted by $N, P, Q, A, B, \cdots$. 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 $\mathcal{O}_\infty = \{\alpha \mid \operatorname{ord} \alpha \leq 0\}$ and $x^{-n}\mathcal{O}_\infty = \{\alpha \mid \operatorname{ord} \alpha \leq -n\}$. Then $x^{-1}\mathcal{O}_\infty$ 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 $\beta \in K_\infty$ and any $n \in \mathbb{Z}$,

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

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 $a = \operatorname{tr}_{F_q \to \mathbb{Z}_p} a = \operatorname{tr} a$. If, in the homomorphism $\mathbb{Z} \to \mathbb{Z}_p$, $u \to \operatorname{tr} a$ and $v \to \operatorname{tr} a$, then $e^{2\pi i u/p} = e^{2\pi i v/p}$. Therefore we may define $e_q : F_q \to \mathbb{C}$ by:

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

where u is any preimage in $\mathbb{Z}$ of 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 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) $e: K_\infty \to \mathbb{C}$ is a continuous function.

(c) e is not identically 1.

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

(e) $e(P) = 1$, if P is a polynomial.

(f) If N is a polynomial, $\int_{\operatorname{ord} \alpha < -n} e(N\alpha)\, d\alpha = \begin{cases} q^{-n}, & \text{if } \operatorname{ord} N < n, \\ 0, & \text{otherwise.} \end{cases}$

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

(We recall that A, Q, N automatically are restricted to polynomials.)

Proof: (a) Suppose $\alpha = \sum_{-\infty}^{t} a_i x^i$ and $\beta = \sum_{-\infty}^{t'} b_i x^i$. Then $|\alpha - \beta| < q^{-1}$, i.e. $\operatorname{ord}(\alpha - \beta) < -1$, says that

$$a_i = b_i, \qquad \text{for } i \geq -1.$$

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 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 $N = b_0 + b_1 x + \cdots + b_\ell x^\ell$, with $b_\ell \neq 0$. Since by assumption ord $\alpha < -n$ we can write $\alpha = \sum_{-\infty}^{-n-1} a_i x^i$. If $\ell < n$ then res$(N\alpha) = 0$ and $e(N\alpha) = 1$ and so the conclusion (f) follows again from equation (3). If $\ell \geq n$ then

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

Therefore,

$$\int_{\text{ord } \alpha < -n} e(N\alpha)\, d\alpha$$

$$= \sum_{a_{-n-1} \in F_q} \sum_{a_{-n-2} \in F_q} \cdots \sum_{a_{-\ell-1} \in F_q} \int_{\gamma \in x^{-\ell-2} \mathcal{O}_\infty} e_q(a_{-n-1} b_n + \cdots a_{-\ell-1} b_\ell)\, d\gamma$$

$$= \sum_{a_{n-1} \in F_q} \cdots \sum_{a_{-\ell} \in F_q} e_q(a_{-n-1} b_n + \cdots a_{-\ell} b_{+\ell-1}) \times$$

$$\times \sum_{a_{-\ell-1} \in F_q} e_q(a_{-\ell-1} b_\ell) \int_{\gamma \in x^{-\ell-2} \mathcal{O}_\infty} 1 \cdot d\gamma.$$

But $\int_{\gamma \in x^{-\ell-2} \mathcal{O}_\infty} 1\, d\gamma = q^{-\ell-1}$ and since $b_\ell \neq 0$, this last sum is simply $q^{-\ell-1} \sum_{a \in F_q} e_q(a) = q^{-\ell-1} \sum_{a \in F_q} e^{\frac{2\pi i}{p} \operatorname{tr} a}$. Since the trace is not identically 0,

the trace maps F_q onto $\mathbb{Z}_p$ and the number of times any particular p^{th} root of 1 is the image of some $a \in F_q$ is simply the cardinality of the kernel of the trace,

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

Hence our integral has value 0 when the polynomial N has ord not less than n.

(g) If $Q \mid N$ then $e(\frac{A}{Q} N) = e$ (polynomial) = 1, and

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

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 mod Q, AN_1 runs over $\frac{|Q|}{|Q_1|}$ complete sets of residues mod Q_1, so that

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

Suppose $Q_1 = q_0 + \cdots + q_n x^n$ where $n \geq 1$ and $q_n \neq 0$, and $R_1 = r_0 + \cdots + r_{n-1} x^{n-1}$. Then $\frac{R_1}{Q_1} = \frac{r_{n-1}}{q^n} x^{-1} + \sum_{-\infty}^{-2} a_i x^i$. This implies that

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

$$= 0,$$

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

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

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

Let

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

Then

$$r(N, m, s, k) = \int_{\alpha \in x^{-1}\mathscr{O}_\infty} (T(\alpha))^s e(-N\alpha)\, d\alpha. \tag{9}$$

Proof: $\int_{\alpha \in x^{-1}\mathscr{O}_\infty} T^s(\alpha)\, e(-N\alpha)\, d\alpha =$

$$= \sum_{\text{ord } P_1 < m} \cdots \sum_{\text{ord } P_s < m} \int_{\alpha \in x^{-1}\mathscr{O}_\infty} e((P_1^k + \cdots + P_s^k - N)\alpha)\, d\alpha.$$

By Lemma 1 (f) (with $n = 0$) the integral inside the summation is 1 or 0 depending on whether $P_1^k + \cdots + P_s^k = N$ 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 $\beta \in x^{-1}\mathcal{O}_\infty$ such that $\alpha = P + \beta$. We define $[\alpha] = P$ and $((\alpha)) = \beta$, the integral and fractional parts of α. $[\alpha]$ and $((\alpha))$ are F_q- linear functions of α.

Lemma 3: Let r be a positive integer. For every $\alpha \in x^{-1}\mathcal{O}_\infty$ there are unique polynomials A, Q such that

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

(b) Q is monic,

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

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

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

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 $\leq r$, so there are q^{r+1} power series $((R\alpha))$. These are distributed in q^r equivalence classes of $x^{-1}\mathcal{O}_\infty \pmod{x^{-r-1}\mathcal{O}_\infty}$. Consequently, there are R_1, R_2 such that $R_1 \neq R_2$ and

$$((R_1 \alpha)) \equiv ((R_2 \alpha)). \qquad \pmod{x^{-r-1}\mathcal{O}_\infty}.$$

Put $Q_1 = R_1 - R_2$ and $A_1 = [Q_1 \alpha]$. Then $Q_1 \neq 0$, $\operatorname{ord} Q_1 \leq r$ and if $A_1 \neq 0$ then $\operatorname{ord} A_1 \leq \operatorname{ord} Q_1 \alpha < \operatorname{ord} Q_1$. Also, $\operatorname{ord}(Q_1 \alpha - A_1) = \operatorname{ord}((Q_1 \alpha))$ $= \operatorname{ord}(((R_1 \alpha)) - ((R_2 \alpha))) < -r$, that is $\left| \alpha - \frac{A_1}{Q_1} \right| < q^{-r} \cdot \frac{1}{|Q_1|}$. 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

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

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 $k \geq 2$ and m be fixed positive integers. Let $r = (k - 1)\, m$, and consider all pairs A, Q satisfying (a) - (d) of the lemma. The Farey arc about $\frac{A}{Q}$ is the set

$$M(A, Q) = \left\{\alpha \epsilon x^{-1}\mathcal{O}_\infty \;\middle|\; \left|\alpha - \frac{A}{Q}\right| < \frac{1}{q^{(k-1)m}} \cdot \frac{1}{|Q|}\right\}.$$

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

3. The Contribution of the Major and Minor Arcs:

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

$$T(\alpha) = \frac{1}{|Q|} S(A, Q)\, T(\beta), \tag{10}$$

where

$$T(\alpha) = \sum_{\text{ord } P < m} e(\alpha P^k), \tag{11}$$

and

$$S(A,Q) = \sum_{Z (\text{mod } Q)} e(\frac{A}{Q} Z^k). \tag{12}$$

Proof: We may write P uniquely as

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

In (11) we have $\text{ord } P < m$, therefore $\text{ord } Y < m - \text{ord } Q$. Also,

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

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

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

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

Then

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

$$= \sum_{\text{ord } P < m} e(\frac{A}{Q} P^k)\ e(\beta P^k),$$

and by the preceding comment,

$$T(\alpha) = \sum_{\text{ord } Z < \text{ord } Q} \sum_{\text{ord } Y < m - \text{ord } Q} e(\frac{A}{Q} Z^k)\, e(\beta(QY + Z)^k)$$

$$= \sum_{\text{ord } Z < \text{ord } Q} e(\frac{A}{Q} Z^k) \sum_{\text{ord } Y < m - \text{ord } Q} e(\beta(QY + Z)^k). \tag{13}$$

To handle the inside sum, notice that since $\alpha = \frac{A}{Q} + \beta$ where

ord $\beta < -(k-1)m - \text{ord } Q$, we have

$$\text{ord}(\beta (QY + Z)^k - \beta(QY)^k) \leq \text{ord } \beta + \max_{1 \leq v \leq k} \text{ord}\binom{k}{v}(QY)^{k-v} Z^v$$

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

Since ord $Q \leq m$, we conclude that

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

and, therefore,

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

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

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

which is independent of Z. On the other hand, summing (14) over Y and the $|Q|$ residue classes $Z \pmod Q$,

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

$$= |Q| \sum_{\text{ord } Y < m - \text{ord } Q} e(\beta(QY)^k). \tag{16}$$

Substituting this back into (13), using (12), we get the proposition.

Proposition 5: If $M(A, Q)$ is a minor arc and $\alpha \in M(A, Q)$ then

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

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

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

However, $\text{ord } \beta P^k = \text{ord } \beta + k \text{ ord } P < -(k-1)m - \text{ord } Q + k(m-1)$. Since $M(A, Q)$ is a minor arc, $\text{ord } Q \geq m + 1$, so $\text{ord } \beta P^k < -1$ 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) $\int_{\mathfrak{M}} T^s(\alpha)\, e(-N\alpha)\, d\alpha =$

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

b) If $\text{ord } N < km$ then

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

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

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

(b) If $\alpha = \frac{A}{Q} + \beta$, then $e(-N\alpha) = e(-\frac{NA}{Q})\, e(-N\beta)$. If $\text{ord } N < km$, 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 $M(A, Q)$ 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 $k < \text{char } F_q$, and so the contribution of the minor arcs is negligible.

Lemma 7:
$$\sum_{\text{ord } P < m} e(\beta P) = \begin{cases} q^m, & \text{if ord } ((\beta)) < -m, \\ 0, & \text{if ord } ((\beta)) \geq -m. \end{cases} \tag{18}$$

Proof: If ord $((\beta)) < -m$, then for each of the q^m polynomials P of deg $< m$, we have 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 $0 > -t-1 \geq -m$ and

$P = \sum_{0}^{m-1} p_i x^i$, then

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

Again, in the sum (18), we are summing (perhaps several times) over all the p^{th} roots of 1.

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

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

that is $d(R) \leq C(\epsilon) |R|^{\epsilon}$, where $C(\epsilon)$ 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 ord $P > 0$.

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

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

Furthermore, if ord $P \geq \frac{1}{\epsilon}$, that is, if $|P| \geq q^{\frac{1}{\epsilon}}$ then

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

For arbitrary $R \neq 0$,

$$\frac{d(R)}{|R|^{\epsilon}} \leq \prod_{\substack{P|R \\ P \text{ irred}}} \frac{d(P^{nR})}{|P|^{nR\epsilon}} \leq \prod_{\substack{P|R \\ \text{ord } P < \frac{1}{\epsilon} \\ P \text{ irred}}} \frac{2}{\epsilon \log q} \leq \prod_{\substack{\text{ord } P < \frac{1}{\epsilon} \\ P \text{ irred}}} \frac{2}{\epsilon \log q} .$$

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

Lemma 9: If $\alpha = \frac{A}{Q} + \beta$ where ord $Q \leq (k-1)m$, 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 $P_1, \cdots, P_{k-1}$ where ord $P_i < m$, $i = 1, \cdots, k-1$, and

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

is:

$$D << q^{\epsilon m}(1 + \frac{|Q|}{q^m})(1 + \frac{q^{(k-1)m}}{|Q|}). \tag{22}$$

Here and in all subsequent work the constant implied by $<<$ 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, $U = P_1 \cdots P_{k-1}$. By Lemma 8, the number of such tuples is not more than

$$((q-1)\, d(U))^{k-1} << q^{k-1} |U|^{(k-1)\epsilon'} << q^{\epsilon m}, \tag{23}$$

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

Now any U may be written as

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

where ord $V <$ ord Q and ord $W <$ ord $(k-1)m -$ ord Q.

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

$$\text{ord } ((\alpha U)) < -m. \tag{25}$$

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

$$\text{ord}((\alpha(U - U_0))) = \text{ord}((\alpha(V - V_0))) < -m, \tag{26}$$

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

$$\text{ord}((\alpha(V - V_0))) = \text{ord}\{((\tfrac{A}{Q}(V - V_0))) + ((\beta(V - V_0)))\}. \tag{27}$$

Now ord $((\beta(V - V_0))) < -2$ ord $Q +$ ord $Q \leq -$ ord Q, and if $V \neq V_0$ then $A(V - V_0) \not\equiv 0 \pmod{Q}$, so that ord $((\frac{A}{Q}(V - V_0))) \geq -$ ord Q. Therefore, the ord of the sum on the right of (27) is simply the larger of the two

$$\text{ord}((\alpha(V - V_0))) = \text{ord}((\tfrac{A}{Q}(V - V_0))).$$

Since $(A, Q) = 1$, as V runs over a complete set of residues (mod Q) so does $A(V - V_0)$. There are precisely $\max(1, q^{-m}|Q|)$ residue classes Y such that $\operatorname{ord}((\frac{Y}{Q})) < -m$. (The max depends on whether $\operatorname{ord} Q \leq m$ or not.)

As there are at most $O(q^{\epsilon m})$ tuples leading to a particular value $U = V + QW$, and at most $\max(1, \frac{q^{(k-1)m}}{|Q|})$ choices of W, and for each W, at most $\max(1, \frac{|Q|}{q^m})$ choices of V, we have

$$D << q^{\epsilon m}(1 + \frac{|Q|}{q^m})(1 + \frac{q^{(k-1)m}}{|Q|}).$$

Lemma 10: Let $f(y) = \alpha y^k + \cdots + \alpha_k$ 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 $\Delta_z : K_\infty[y] \to K_\infty[y]$ 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 $z \mid \text{content } (\Delta_z f)$.

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

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

and the leading coefficient of $\Delta_z f$ is $k\alpha z$.

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

$$\Delta_{z_{k-1}}(\cdots(\Delta_{z_1} f)) = k!\, \alpha z_1 \cdots z_{k-1} y + \text{terms free of } y.$$

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

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

(e) follows from (d) by induction.

Lemma 11: If $f \in K_\infty[y]$ and $S(f) = \sum_{\text{ord } P < m} e(f(P))$ and $n \geq 1$, then

$$|S(f)|^{2^n} \leq q^{m(2^n-n-1)} \sum_{\text{ord } P_1 < m} \sum_{\text{ord } P_2 < m} \cdots \sum_{\text{ord } P_n < m} S(\Delta_{P_n}(\cdots \Delta_{P_1}(f))). \quad (29)$$

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

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

$$= \sum_{\text{ord } P < m} \sum_{\text{ord } Q < m} e(f(Q) - f(P)).$$

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

$$|S(f)|^2 = \sum_{\text{ord } P_1 < m} \sum_{\text{ord } P < m} e(f(P+P_1) - f(P)) \quad (30)$$

$$= \sum_{\text{ord } P_1 < m} S(\Delta_{P_1} f).$$

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

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

$$|S(f)|^{2^{n+1}} = (|S(f)|^{2^n})^2$$

$$\leq (q^{m(2^n-n-1)})^2 \{ \sum_{(P_1, \cdots, P_n)} S(\Delta_{P_n} \cdots \Delta_{P_1}(f)) \}^2 \quad (31)$$

$$\leq (q^m)^{2^{n+1}-(n+1)-1-n} \{ \sum_{(P_1, \cdots, P_n)} |S(\Delta_{P_n} \cdots \Delta_{P_1} f)| \}^2,$$

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

$$(\Sigma\, a_i\, b_i)^2 \le (\Sigma\, a_i^2)(\Sigma\, b_i^2),$$

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

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

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 $f(y) = \alpha y^k + \alpha_1 y^{k-1} + \cdots + \alpha_k$, $\alpha_i \in K_\infty$ and

(a) $2 \le k < \text{char } F_q$.

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

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

then, for every $\epsilon > 0$,

$$|S(f)| = \Big|\sum_{\text{ord } P < m} e(f(P))\Big| << q^{m(1+\epsilon)}\left(\frac{1}{q^m} + \frac{1}{|Q|} + \frac{|Q|}{q^{km}}\right)^{\frac{1}{2^{k-1}}}. \quad (34)$$

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

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

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

$$|S(f)|^{2^{k-1}} \le q^{m(2^{k-1}-k)} \sum_{\text{ord } P_{k-1} < m} \cdots \sum_{\text{ord } P_1 < m} S(\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f)). \quad (35)$$

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

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

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

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

Therefore (35) becomes

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

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

By Lemma 10 (e)

$$|S\,\Delta_{P_{k-1}} \cdots \Delta_{P_1}(f)| = \left| \sum_{\text{ord } P < m} e(k!\, \alpha P_1 \cdots P_{k-1} P) \right|.$$

By Lemma 7, the sum on the right is either 0 or q^m depending on whether ord $((k!\, \alpha P_1 \cdots P_{k-1})) \geq -m$ or not. Since $k < \text{char } F_q$, $k!$ is a non-zero

unit and,

$$\operatorname{ord}((k!\ \alpha P_1 \cdots P_{k-1})) = \operatorname{ord}((\alpha P_1 \cdots P_{k-1})).$$

By Lemma 9, the number of tuples $P_1 \cdots, P_{k-1}$ contributing to the sum is $O(q^{\epsilon m}(1 + \frac{|Q|}{q^m})(1 + \frac{q^{(k-1)m}}{|Q|}))$. Therefore (37) becomes

$$|S(f)|^{2^{k-1}} << q^{m(2^{k-1}-1)} + q^{m(2^{k-1}-k)}\, q^m\, q^{\epsilon m}(1 + \frac{|Q|}{q^m})(1 + \frac{q^{(k-1)m}}{|Q|})$$

$$<< q^{m(2^{k-1}+\epsilon)}(\frac{1}{q^m} + \frac{1}{|Q|} + \frac{|Q|}{q^{km}}).$$

Proposition 13 (Hua): If $S(\alpha G) = \sum_{\operatorname{ord} P < m} e(\alpha G(P))$ where $G(y) \in F_q[x][y]$ and if ν is an integer such that $\Delta_{y_\nu} \cdots \Delta_{y_1} G(y) \in F_q[x][y, y_1, \cdots, y_\nu]$ satisfies

$$\Delta_{y_\nu} \cdots \Delta_{y_1} G(y) \not\equiv 0. \tag{38}$$

Then, for every $\epsilon > 0$, $I_\nu = \int_{\alpha \in x^{-1}\mathcal{O}_\infty} |S(\alpha G)|^{2^\nu} d\alpha << q^{m(2^\nu - \nu + \epsilon)}$. (39)

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

$$I_k << q^{m(2^k - k + \epsilon)} \tag{40}$$

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

$$\deg_y \Delta_{y_\mu} \cdots \Delta_{y_1} G \geq 1$$

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

$$I_1 = \int_{\alpha \in x^{-1}\mathcal{O}_\infty} \sum_{\operatorname{ord} P_1 < m} e(+\alpha G P_1)) \sum_{\operatorname{ord} P_1 < m} e(-\alpha G(P_2))\, d\alpha = \mathcal{H}$$

where $\mathcal{H}$ 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

$$I_1 \le k \cdot q^m << q^m << q^{m(2^1 - 1 + \epsilon)}.$$

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

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

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

$$I_{\nu+1} \le q^{m(2^\nu - \nu - 1)} \int_{\alpha \in x^{-1}\mathcal{O}_\infty} \sum_{P_\nu} \cdots \sum_{P_1} S(\Delta_{P_\nu} \cdots \Delta_{P_1}(\alpha G)) \cdot |S(\alpha G)|^{2^\nu} d\alpha.$$

$$\le q^{m(2^\nu - \nu - 1)} \cdot \mathcal{H}, \tag{41}$$

where $\mathcal{H}$ is the number of solutions (P, P_i, Q_j, R_ℓ) of

$$0 = \Delta_{P_\nu} \cdots \Delta_{P_1} G(P) + G(Q_1) + \cdots + G(Q_{2^\nu - 1}) - G(R_1) - G(R_{2^\nu - 1})$$

$$= \Delta_{P_\nu} \cdots \Delta_{P_1} G(P) + B(Q_1, \cdots, Q_{2^\nu - 1}, R_1, \cdots, R_{2^\nu - 1}), \tag{*}$$

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

We show by induction the following: If $H(y_1, \cdots, y_n) \not\equiv 0$ is an arbitrary polynomial of total degree $<< 1$ then there are $O(q^{m(n-1)})$ solutions $Y_1, \cdots, Y_n$ of $H(Y_1, \cdots, Y_n) = 0$, where each Y_i is a polynomial of degree $< n$. We may suppose H actually involves Y_n, thus

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

Given $Y_1, \cdots, Y_{n-1}$ not on the hypersurface $H_0 = H_1 = \cdots = H_t = 0$ there are at most $t = O(1)$ choices for Y_n, thus at most $O(q^{m(n-1)})$ choices not on the hypersurface. To be on this hypersurface, indeed to be on $H_n = 0$, the induction hypothesis says there are at most $O(q^{m(n-2)})$ choices for $Y_1, \cdots, Y_{n-1}$. As Y_n may then be chosen arbitrarily, 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 $<< q^{m\nu} I_\nu$ solutions of (*) with $B = 0$. For fixed $B \neq 0$, then outside the hypersurface where the coefficients of the powers of y disappear, given $P_1, \cdots, P_\nu$ there are $O(1)$ choices for P such that (*) holds. By Lemma 10 (c), $P_i \mid B$, $i = 1, \cdots, \nu$. Thus, by Lemma 8, there are at most $<< ((q-1)\, d(B))^\nu << q^k \cdot q^{k\epsilon' m} << q^{m\epsilon}$ choices for $P_1, \cdots, P_\nu$. Taking Q_i, R_j arbitrarily there are at most $O(q^{(2^\nu + \epsilon)m})$ 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 $P_1, \cdots, P_\nu$ 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

$$\mathcal{M}_1 = \int_{\alpha \in X^{-1}\mathcal{O}_\infty} |S(\alpha G)|^{2^\nu} e(-\alpha B)\, d\alpha \le I_\nu << q^{m(2^\nu - \nu + \epsilon)}.$$

There are, therefore,

$$<< q^m \cdot q^{m(\nu-1)}\, q^{m(2^\nu - \nu + \epsilon)}$$
$$<< q^{m(2^\nu + \epsilon)}$$

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

Therefore $\mathcal{M} << q^{m\nu} I_\nu + q^{m(2^\nu + \epsilon)}$. Together with (41) and the induction hypothesis,

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

Theorem 14: If $k < \text{char } F_q$ and $s \ge 2^k + 1$ then there is an $\epsilon > 0$ such that

$$\left| \int_{\mathfrak{m}} T^s(\alpha)\, e(-N\alpha)\, d\alpha \right| << q^{m(s-k-\epsilon)}. \tag{42}$$

Proof: Since $s \ge 2^k + 1$,

$$I = \left| \int_{\mathfrak{m}} T(\alpha)\, e(-N\alpha)\, d\alpha \right| \le \int_{\mathfrak{m}} |T(\alpha)|^s \, |e(-N\alpha)| d\alpha$$
$$\le \{ \max_{\alpha \in \mathfrak{m}} |T(\alpha)| \}^{s - 2^k} \int_{\mathfrak{m}} |T(\alpha)|^{2^k} d\alpha.$$

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

Thus:

$$I << q^{m(1 - \frac{1}{2^k - 1} + \delta)(s - 2^k)} \cdot q^{m(2^k - k + \delta')}$$
$$<< (q^m)^{(s-k) - \{(s-2^k)(\frac{1}{2^k-1} - \delta) - \delta'\}},$$

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

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

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 $m' \geq 0$, let $V(s, N, m')$ be the number of ordered tuples $P_1, \cdots, P_s$ such that $\operatorname{ord} P_i < m$, $i = 1, \cdots, s$ and

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

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

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

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

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

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

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

and such that

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

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

Proof: Let t be the least index such that $c_t \neq 0$. Let $P_t = c_t x^n + d_{n-1} x^{n-1} + \cdots + d_0$. 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 tuple $P_1, \cdots, P_s$ is to be counted iff $\text{ord}\, R' < m'$, that is, iff

$$r_i' = 0. \qquad i = kn,\ k\,n-1,\ \cdots,\ m'. \tag{48}$$

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

$$\begin{aligned}
0 = r'_{kn-1} &= k\,c_t^{k-1} d_{n-1} - r_{kn-1} \\
0 = r'_{kn-2} &= k\,c_t^{k-1} d_{n-2} + \binom{k}{2} c_t^{k-2} d_{n-1}^2 - r_{kn-2} \\
&\vdots \qquad\qquad \vdots \\
0 = r'_{m'} &= k\,c_t^{k-1} d_{m'-(k-1)n} + \left\{ \begin{array}{l} \text{terms involving } d_i, \\ m'-(k-1)n < i < n \end{array} \right\} - r_{m'}.
\end{aligned} \tag{49}$$

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

Thus any tuple $P_1, \cdots, P_s$ to be counted satisfies the set of equations (49). Conversely, since $k\,c_t^{k-1} \neq 0$, 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 $P_1, \cdots P_s$ 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, $(k-1)m \le m' \le km$. Let N be a polynomial of degree $\ell \le k \cdot (m-1)$ and leading coefficient b (where, for $N = 0$, we take $\ell = 0$, $b = 0$). Let $U(s, b)$ be the number of tuples $c_1, \cdots, c_s$ such that $c_i \in F_q$ $i = 1, \cdots, s$, not all $c_i = 0$, and

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

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

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

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

then

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

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

Case (a). If $k \nmid \ell$ and $m' \le \ell$ then

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

Case (b). If $k \mid \ell$ and $m' \le \ell$ then

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

Case (c). If $\ell < m'$ then

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

Proof: According to Lemma 15, $\int_{\text{ord}\,\beta < -m'} T^s(\beta)\, e(-N\beta)\, d\beta =$

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

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

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

$$= U(s, 0)\, q^{m' + (s-k)([\frac{\ell}{k}]+1)} \frac{q^{(s-k)m - [\frac{\ell}{k}] - 1} - 1}{q^{s-k} - 1}$$

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

Therefore, $C(s, N, m') = q^{-(s-k)m - m'} V(s, N, m')$

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

Since $s > k$ and $k \nmid \ell$ and $\ell \le k \cdot (m - 1)$,

$$(s - k)(m - 1 - [\tfrac{\ell}{k}]) \ge 1.$$

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

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

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

Arguing as in case (a) we obtain

$$C(s, N, m') = U(s, b)\, q^{-(s-k)(m-[\frac{\ell}{k}])} + \frac{U(s, 0)}{q^{s-k}-1}(1 - q^{-(s-k)(m-1-[\frac{\ell}{k}])}) \qquad (56)$$

Since $s > k$ and $\ell \leq k(m-1)$,

$$(s-k)\,(m - [\tfrac{\ell}{k}] - 1) \geq 0,$$

and

$$(s-k)\,(m - [\tfrac{\ell}{k}]) > 0.$$

Therefore

$$0 \leq U(s, b)\, q^{-(s-k)[m - \frac{\ell}{k}]} << 1,$$

$$0 \leq \frac{U(s, 0)}{q^{s-k}-1}\,(1 - q^{-(s-k)(m-1-[\frac{\ell}{k}])}) << 1.$$

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

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

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

Again, arguing as in case (a),

$$C(s, N, m') = q^{-(s-k)m - m'}\, V(s, N, m')$$

$$= q^{s([\frac{m'-1}{k}]+1)-(s-k)m-m'} + \frac{U(s, 0)}{q^{s-k}-1}(1 - q^{-(s-k)(m-1-[\frac{m'-1}{k}])}).$$

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

$$(s-k)(m-1-[\tfrac{m'-1}{k}]) \geq 0,$$

and

$$s([\frac{m'-1}{k}] + 1) - (s-k)m - m' = -(s-k)(m-1-[\frac{m'-1}{k}]) + k[\frac{m'-1}{k}] + k - m'$$
$$\leq k-1. \qquad (57)$$

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

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

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

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

$$m' = (k-1)m + \operatorname{ord} Q \leq (k-1+\epsilon)m,$$

and $\ell = \operatorname{ord} N \leq (k-1+\epsilon)m$. According to the hypothesis of Lemma 17, we must have $\ell \leq km - k$ instead of $\ell \leq km - (1-\epsilon)m$. Since we consider k fixed and m large, any discrepancy for small values of m may be absorbed in the error term. Then $(s-k)(m-1-[\frac{m'-1}{k}]) \geq \delta_1 m$, and $(s-k)(m-1-[\frac{\ell}{k}]) \geq \delta_1 m$, where $\delta_1 > 0$ is sufficiently small. According to formula (57),

$$s([\frac{m'-1}{k}] + 1) - (s-k)m - m' \leq -(s-k)(m-1-(1-\frac{1}{k}+\frac{\epsilon}{k})m) + k - 1$$
$$\leq -(s-k)(\frac{1-\epsilon}{k})m + s - 1 \leq -\delta_2 m.$$

The theorem follows.

6. The Singular Series: We have already defined

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

Let

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

Let

$$\mathfrak{N}(\epsilon \cdot m, N, s) = \mathfrak{N}(\epsilon \cdot m, N) = \sum_{\substack{Q \text{ monic} \\ \text{ord } Q < m}} \mathfrak{M}(Q). \tag{60}$$

$\mathfrak{N}(m, N)$ has already been seen in Lemma 6 (a). If $0 < \epsilon < 1$ is fixed, then $\mathfrak{N}(\epsilon m, N)$ (as $m \to \infty$) closely approximates $\mathfrak{N}(m, N)$. Let

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

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

$$P_1^k + \cdots + P_s^k \equiv N. \quad (\text{mod } Q).$$

Lemma 19: (a) If $(Q_1, Q_2) = 1$, $(A_1, Q_1) = 1$ and $(A_2, Q_2) = 1$, then

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

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

$$\mathfrak{M}(Q_1)\, \mathfrak{M}(Q_2) = \mathfrak{M}(Q_1 Q_2). \tag{63}$$

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

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

Since e(polynomial) = 1,

$$e\left(\frac{A_1}{Q_1}(Q_2 P_1)^k + \frac{A_2}{Q_2}(Q_1 P_2)^k\right) = e\left(\left(\frac{A_1}{Q_1} + \frac{A_2}{Q_2}\right)(Q_2 P_1 + Q_1 P_2)^k\right).$$

As P_1 and P_2 run independently over complete residue systems mod Q_1 and mod Q_2, respectively, $Q_2 P_1 + Q_1 P_2$ runs over a complete residue system mod $Q_1 Q_2$, and thus, the expression on the right of (64) is $S(A_1 Q_2 + A_2 Q_1, Q_1 Q_2)$.

(b) Using part (a),

$$\sigma_1(Q_1)\sigma_1(Q_2) = \frac{1}{|Q_1 Q_2|^s} \sum_{\substack{A_1 \bmod Q_1 \\ (A_1, Q_1)=1}} \sum_{\substack{A_2 \bmod Q_2 \\ (A_2, Q_2)=1}} S^s(A_1 Q_2 + A_2 Q_1, Q_1 Q_2) \times e\left(-N\left(\frac{A_1}{Q_1} + \frac{A_2}{Q_2}\right)\right).$$

Since, by the Chinese remainder theorem, $A_1 Q_2 + A_2 Q_1$ runs over a reduced system of residues, mod $Q_1 Q_2$, the right hand side is $\sigma_1(Q_1 Q_2)$.

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

$$|S(A, P)| \leq (k' - 1)\, |P|^{\frac{1}{2}}. \tag{65}$$

Proof: The non-zero elements of $F_q[x]/(P)$ are a cyclic group of order $|P| - 1$, generated by a primitive $|P| - 1^{st}$ root of unity, (say) G. Then $Y^k (Y \not\equiv 0)$ runs over the subgroup generated by $G^{k'}$ k' times so that

$$S(A, P) = \sum_{Y \bmod P} e\left(\frac{A}{P} Y^k\right) = \sum_{Y \bmod P} e\left(\frac{A}{P} (Y^{k'})^{k/k'}\right)$$

$$= \sum_{Y \bmod P} e\left(\frac{A}{P} Y^{k'}\right) \tag{66}$$

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

where G is a primitive root. Since $e\left(\frac{A}{P} G^{k'y}\right)$ depends only on the equivalence class of $G^{k'y} \pmod P$, that is, only on the equivalence class of $k'y \pmod{|P| - 1}$,

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

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

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

$$= \left\{1 + \sum_{\substack{Y \bmod P \\ Y \not\equiv 0}} e\left(\frac{A}{P} Y\right)\right\} + \sum_{v=1}^{k'-1} \sum_{y=1}^{|P|-1} \exp\left(\frac{2\pi i}{k'} vy\right) e\left(\frac{A}{P} G^y\right).$$

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,

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

By Cauchy's inequality, $(\Sigma\, 1 \cdot a_i)^2 \le \{\#\text{ of terms}\} \cdot (\Sigma\, a_i^2)$, we have

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

Summing instead over $w = y - z$,

$$|S(A, P)|^2 \le (k'-1) \sum_{v=1}^{k'-1} \sum_{w (\mathrm{mod}\ |P|-1)} \exp(\tfrac{2\pi i}{k'} vw) \{ \sum_{z=1}^{|P|-1} e(\tfrac{A}{P}(G^w - 1)\, G^z) \}.$$

The sum in brackets is

$$\sum_{\substack{z \not\equiv 0 \\ z (\mathrm{mod}\ P)}} e(\tfrac{A}{P}(G^w - 1)z) = \begin{cases} |P| - 1 & \text{if } G^w - 1 \equiv 0 \pmod P \\ -1 & \text{if } G^w - 1 \not\equiv 0 \pmod P \end{cases}.$$

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

$$|S(A, P)|^2 \le (k'-1) \cdot \sum_{v=1}^{k'-1} \{ |P| - \sum_{w=1}^{|P|-1} \exp(\tfrac{2\pi i}{k'} vw) \}$$

$$\le (k'-1)^2 \cdot |P|,$$

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: If char $F_q \nmid k$, P is an irreducible polynomial and $A \not\equiv 0 \pmod P$, then

(a) If $1 < n \le k$ then

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

(b) if $n > k$

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

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

$$Y^k \equiv U^k + k\, U^{k-1}\, V\, P^{n-1} \pmod{P^n}.$$

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

$$S(A, P^n) = \sum_{Y \bmod P^n} e(\frac{A}{P^n} Y^k)$$

$$= \sum_{U \bmod P^{n-1}} e(\frac{A}{P^n} U^k) \sum_{V \bmod P} e(\frac{k A U^{k-1} V}{P}).$$

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

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

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

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

When $n > k$,

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

But $e(\frac{A}{P^{n-k}} U^k)$ 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 char $F_q \nmid k$ then

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

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

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

Proof: (a) We first prove (a) for the prime powers P^{μ}. Writing $\mu = k \cdot [\frac{\mu-1}{k}] + i$, where $0 < i \leq k$, we see that we may apply Lemma 21(b) $[\frac{\mu-1}{k}]$ times.

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

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

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

If $i = 1$, by Lemma 20,

$$\begin{aligned} |S(A, P^{\mu})| &\leq |P|^{(k-1)[\frac{\mu-1}{k}]} (k'-1) |P|^{\frac{1}{2}} \\ &\leq (k'-1) |P|^{\mu - [\frac{\mu-1}{k}] - \frac{1}{2}} \\ &\leq (k-1) |P|^{\mu - \frac{1}{k}\mu - (\frac{1}{2} - \frac{1}{k})} \end{aligned}$$

Thus when $k = 2$, $|S(A, P^{\mu})| \leq |P|^{\mu(1-\frac{1}{k})}$, (*)

and when $k \geq 3$, $|S(A, P^{\mu})| \leq \{(k-1) |P|^{-1/6}\} \cdot |P|^{\mu(1-\frac{1}{k})}$. (**)

The formula (70) for $k = 2$ now follows from Lemma 19 (a) and (*). For $k \geq 3$, write $Q = \prod P_j^{\mu_j}$. 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

$$|S(A, Q)| \le \prod_j |P_j|^{\mu_j(1 - \frac{1}{k})} \prod_j \max(1, (k-1)\,|P_j|^{-1/6})$$

$$\le |Q|^{1 - \frac{1}{k}} \cdot \prod_{\substack{P \text{ irreducible} \\ |P| < (k-1)^6}} |P|^{k-1}$$

$$\le (k-1)^{(k-1)^6} \cdot |Q|^{1 - \frac{1}{k}}.$$

(b) $$|\mathcal{M}(Q, N, s)| \le \left|\frac{1}{|Q|^s} \sum_{\substack{A \bmod Q \\ (A, Q)=1}} S^s(A, Q)\, e\left(-\frac{NA}{Q}\right)\right|$$

$$\ll \frac{1}{|Q|^s} \cdot |Q| \cdot |Q|^{(1 - \frac{1}{k})s} \ll |Q|^{1 - \frac{s}{k}}.$$

Lemma 23: For P irreducible, let

$$X(P, N, s) = 1 + \sum_{\mu=1}^{\infty} \mathcal{M}(P^\mu, N, s). \tag{72}$$

If char $F_q \nmid k$ and $s \ge 3k + 1$ then $\gamma(N, s) = \sum_{Q \text{ monic}} \mathcal{M}(Q, N, s)$ and $X(P, N, s)$ converge absolutely and

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

Also if $\gamma(\epsilon m, N, s) = \sum_{\substack{Q \text{ monic} \\ \text{ord } Q < \epsilon m}} \mathcal{M}(Q, N, s)$ then

$$|\gamma(N, s) - \gamma(\epsilon m, N, s)| \ll q^{-(1 + \frac{1}{k})\epsilon m}.$$

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

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

$$|\mathcal{O}(Q, N, s)| << |Q|^{1-\frac{s}{k}} << |Q|^{-2-\frac{1}{k}}.$$

It follows that

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

converges absolutely. Also

$$|\gamma(N, s)| \leq \sum_{\ell=0}^{\infty} \sum_{\substack{\text{ord } Q = \ell \\ Q \text{ monic}}} |\mathcal{O}(Q, N, s)| \leq \sum_{\ell=0}^{\infty} \sum_{\substack{\text{ord } Q = \ell \\ Q \text{ monic}}} (q^{\ell})^{-2-\frac{1}{k}},$$

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

$$|\gamma(N, s) - \gamma(\epsilon m, N, s)| \leq \sum_{\substack{Q \text{ monic} \\ \text{ord } Q \geq \epsilon m}} |\mathcal{O}(Q, N, s)|$$

$$\leq \sum_{\ell=[\epsilon m]}^{\infty} (q^{\ell})^{-1-\frac{1}{k}} \leq q^{-(1+\frac{1}{k})[\epsilon m]} \frac{1}{1 - q^{-1-\frac{1}{k}}} << q^{-(1+\frac{1}{k})(\epsilon m)}.$$

Finally,

$$\prod_{\substack{P \text{ monic, irreducible} \\ \text{ord } P < \ell}} X(P, N, s) = \sum_{\substack{Q \text{ monic} \\ \text{ord } Q < \ell}} \mathcal{O}(Q, N, s) + \sum{}' \mathcal{O}(Q, N, s)$$

where the second sum is over those Q which are monic, of degree $\geq \ell$ and all of whose irreducible factors has order $< \ell$. This sum tends to zero since $|\mathcal{O}(Q, N, s)| \leq |Q|^{-2-\frac{1}{k}}$. The first sum on the right tends to $\gamma(N, s)$, while the product tends to $\prod_{P \text{ monic, irreducible}} X(P, N, s)$.

Thus (73) is shown.

Lemma 24: Let $M(Q, N, s)$ be the number of distinct tuples $(P_1, \dots, P_s) \bmod Q$ such that

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

then

$$M(Q, N, s) = |Q|^{s-1} \sum_{\substack{Q_1 | Q \\ Q_1 \text{ monic}}} \sigma_1(Q_1, N, s). \tag{75}$$

Proof: By Lemma 1 (g),

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

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

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

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

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

$$= |Q|^{s-1} \sum_{\substack{Q_1 | Q \\ Q_1 \text{ monic}}} \sigma_1(Q_1, N, s).$$

Lemma 25: If 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

$$\begin{aligned} Y_1^k &\equiv B, \pmod{P^\mu} \\ Y_1 &\equiv Y_o. \pmod{P^\nu} \end{aligned} \tag{77}$$

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

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

Then $Y_1^k = Y_0^k + k\, Y_0^{k-1} RP^\nu + \sum_2^k \binom{k}{i} Y_0^{k-i} (RP)^{\nu i}$. But $\nu i \geq 2\nu \geq \nu + 1$ so that

$$Y_1^k \equiv Y_0^k + k\, Y_0^{k-1}\, RP^\nu \qquad (\mathrm{mod}\ P^{\nu+1}).$$

If $Y_0^k + HP^\nu = B$ then Y_1 satisfies the conclusion iff

$$H \equiv k\, Y_0^{k-1} R \qquad (\mathrm{mod}\ P).$$

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 $\nu+1, \cdots, \mu - 1$. Taking the solution Y_1 for $\mu - 1$

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

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

we find

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

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

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

Lemma 26: If char $F_q = p \nmid k$, P is an irreducible polynomial and

$$P_1^k + \cdots + P_s^k \equiv N, \pmod{P^\nu}$$

$$P \nmid P_i, \text{ for some } i,$$

then, for $\mu > \nu$, the number of tuples $(R_1, \cdots, R_s) \bmod P^\mu$ such that

$$R_1^k + \cdots + R_s^k \equiv N, \pmod{P^\mu}$$

$$R_i \equiv P_i, \pmod{P^\nu} \quad i = 1, \cdots, s$$

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

Proof: Suppose $P \nmid P_t$. For $i \neq t$, let $R_i = P_i + V_i P^\nu$, ord $V_i <$ $<$ ord $P^{\mu - \nu}$. Then $N - \sum_{i \neq t} R_i^k \equiv N - \sum_{i \neq t} P_i^k \equiv P_t^k \not\equiv 0. \pmod{P^\nu}$. By the previous lemma, there is $R_t \bmod P^\mu$ such that

$$R_t^k \equiv N - \sum_{i \neq t} R_i^k, \pmod{P^\mu}$$

$$R_t \equiv P_t. \pmod{P^\nu}$$

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

Lemma 27: If P is irreducible and $s \geq k + 1$ and N is congruent (mod P) to a sum of (arbitrarily many) k^{th} powers then $\exists$ $P_1, \cdots, P_s$ not all divisible by P such that

$$P_1^k + \cdots + P_s^k \equiv N. \pmod{P} \tag{78}$$

Proof: It suffices to show that when $P \nmid N$ the congruence (78) is solvable for some value of $s \leq k$ since in case $P \mid N$, we may solve (78)

instead for $N - 1^k$ and transpose. Let $t = t(N)$ be the least s for which (78) is solvable, say

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

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

$$(P_1')^k + \cdots + (P_s')^k \equiv R^k N \qquad \bmod P$$

with $s < t(N)$, we may divide R^k which is a unit (mod P). There are exactly $\frac{|P| - 1}{(k, |P|-1)}$ 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 $(k, |P| - 1) \leq k$ classes. Since $1 = 1^k$, $t(1) = 1$. Suppose we have shown that there are non-zero polynomials with $t(N) = 1, 2, \cdots, t'$. Either we have exhausted all the non-zero polynomials or there is an N' with $t(N') > t'$. Since N' exists, there is an N with $t(N) = t' + 1$. 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 N is congruent (mod P) to a sum of k^{th} powers. If $p = \text{char } F_q < k$, then N is congruent (mod P) to a sum of k^{th} powers for arbitrary irreducible P.

Proof: If ord $P = \ell$ then $F_q[x]/(P) \cong F_{q^\ell} = F_{p^{\ell'}}$. Let $\mathcal{R}(P, q, k) = \mathcal{R}$ be the set of those polynomials which are sums of k^{th} powers (mod P). Then $\mathcal{R}$ being closed under addition and multiplication and a subset of

a finite field is again a finite field, say $\mathcal{R} = F_{p^h}$. Suppose $\mathcal{R}$ is a proper subfield, i.e., $h < \ell'$. We must have $h \mid \ell'$ and also the order of the multiplicative subgroup $\mathcal{R}^x$ must divide the order of the whole group $F_{p^{\ell'}} \setminus \{0\}$:

$$\frac{p^{\ell'}-1}{p^h-1} = p^{\ell'-h} + p^{\ell'-2h} + \cdots + p^h + 1.$$

Let a be a primitive $p^{\ell'}-1^{st}$ root of 1. Then $a^k \in \mathcal{R}$ so that

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

It follows that $p^{\ell'}-1 \mid (p^h-1)k$. Therefore $p^{\ell'-h} + p^{\ell'-2h} + \cdots + p^h + 1 \mid k$. Therefore

$$p^{\ell'/2} + 1 \le p^{\ell'-h} + \cdots + p^h + 1 \le k,$$

or

$$|P| \le (k-1)^2.$$

To prove the second statement of the lemma we start from

$$p^{\ell'}-1 \mid (p^h-1)k.$$

Since $k < p$,

$$p^{\ell'}-1 \le (p^h-1)k \le p^{h+1}-p.$$

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

Theorem 29: If char $F_q \nmid k$, $s \ge 3k+1$, and either

(a) N is congruent to a sum of k^{th} powers mod P, for all irreducible P such that $|P| \le (k-1)^2$ or,

(b) $k < \text{char } F_q$ then

$$1 << \gamma(N, s) = \prod_{P \text{ irreducible, monic}} X(P, N, s) << 1.$$

Proof: We have only to show $\prod_P X(P, N, s) >> 1$ since Lemma 23 together with Lemma 22 (b) assert the remaining statements.

By Lemma 24, 26, 27, 28, for any $\mu \geq 1$, we have

$$\sum_{Q \mid P^\mu} \sigma(Q, N, s) = \frac{M(P^\mu, N, s)}{|P|^{\mu(s-1)}} \geq |P|^{(s-1)(\mu-1) - (s-1)\mu} \geq |P|^{-(s-1)}.$$

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

$$|X(P, N, s) - 1| = \sum_{\mu=1}^{\infty} |\sigma(P^\mu, N, s)| << \sum_{s=1}^{\infty} |P|^{\mu(-2 - \frac{1}{k})}$$
$$<< |P|^{-2 - \frac{1}{k}}.$$

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

7. The Asymptotic Formula.

Theorem 30: If $k < \text{char } F_q$ and $s \geq \max(3k+1, 2^k+1)$ and N is a polynomial of order $< (k-1+\epsilon)m$, $\frac{1}{2k} \leq \epsilon < 1$, then there exists $\delta > 0$ such that if $r(N, m, s, k)$ is the number of representations of N as a sum of s k^{th} powers of order $< m$ then

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

Furthermore $1 << \frac{U(s, 0)}{q^{s-k}-1} \gamma(N, s) << 1$.

Proof: The number of representations $r(N, m, s, k)$ is given by Lemma 2 as

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

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

where $\mathfrak{M}$ and $\mathfrak{m}$ are the set of major arcs and minor arcs, resp.

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

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

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

Let $0 < \epsilon < 1$. We split the sum over Q above into

$$\sum_{\substack{Q \text{ monic} \\ \text{ord } Q < \epsilon m}} + \sum_{\substack{Q \text{ monic} \\ \epsilon m < \text{ord } Q < m}} .$$

In the first sum the integral is given by Theorem 18 as:

$$\int_{\text{ord}\,\beta < -(k-1)m - \text{ord}\,Q} T^s(\beta)\, e(-N\beta)\, d\beta = \frac{U(s,0)}{q^{s-k}-1}\, q^{(s-k)m} + O(q^{(s-k-\epsilon_1)m}).$$

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

$$= \gamma(\epsilon m, N)\, \frac{U(s,0)}{q^{s-k}-1}\, q^{(s-k)m} + O(\gamma(\epsilon m, N)\, q^{(s-k-\epsilon_1)m}).$$

Lemma 23 and Theorem 29 gives this to be

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

Consider now the second sum:

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

$$= \sum_{\substack{Q \text{ monic} \\ \epsilon m < \text{ord}\,Q < m}} \mathcal{O}(Q,N,s) \int_{\text{ord}\,\beta < -(k-1)m - \text{ord}\,Q} T^s(\beta)\, e(-N\beta)\, d\beta \qquad (*)$$

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

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

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

According to Lemma 22 (b), $|\mathcal{O}(Q,N,s)| << |Q|^{1-s/k}$. Therefore the second sum is

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

Since $s \geq 3k+1$, the double sum is

$$\begin{aligned} |\Sigma\Sigma| &\ll q^{(s-k+1)m} \sum_{\substack{Q \text{ monic} \\ \epsilon m < \operatorname{ord} Q < m}} |Q|^{-s/k} \\ &\ll q^{(s-k+1)m} \sum_{[\epsilon m] < \ell < m} (q^{\ell})^{-2k-\frac{1}{k}} \\ &\ll q^{(s-k+1)m} \cdot q^{\epsilon m(-2k-\frac{1}{k})}. \end{aligned}$$

Taking $\frac{1}{2k} \leq \epsilon < 1$, the asymptotic formula follows. The singular series is not zero since $k < p$ (see Theorem 29). $\frac{U(s,0)}{q^{s-k-1}} >> 1$ since as usual, the constant in $>>$ may depend on q and s, k but is independent of m.

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 $g(k)$.

Theorem 31: Let $g(k, q)$ be the least number r such that every polynomial in $F_q[x]$ is the sum of at most r k^{th} powers. If $k < \text{char } F_q = p$ then

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

Proof: We consider first whether it is possible to write

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

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

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

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

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 3 & \cdots & k \\ 1^2 & 2^2 & \cdots & & \vdots \\ \vdots & \vdots & & & \\ 1^{k-1} & 2^{k-1} & \cdots & & k^{k-1} \end{vmatrix} = \prod_{i>j} (i-j) \neq 0. \tag{84}$$

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 $p-1$ k^{th} powers, it follows that $x + b$ can be written as a sum of not more than $k(p-1)$ k^{th} powers. To write an arbitrary polynomial, say $c_n x^n + \cdots + c_0$, as a sum of k^{th} powers, we may just substitute $C(x) = c_n x^n + \cdots + c_0 - b$ into the identity (83) in place of x:

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

This proves the theorem.

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

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

where: (a) ord $P_i < m$, $1 \leq i \leq 3k + 1$, $k \mid m$ and (87)

m is sufficiently large.

(b) U_1 and U_2 run through all the different monic polynomials of order km that are representable as a sum of ℓ k^{th} powers,

(c) ord $W = \frac{1}{k} m$, W monic,

---

* See p. 8.

(d) V_l runs through all the different monic polynomials of order $(k-l)m$ that are representable as a sum of ℓ' k^{th} powers.

The restriction $k|m$ is not essential but is taken to ensure $\frac{l}{k}m$ 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 k^{th} powers.

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

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

where (a) $\operatorname{ord} P_i < m, \quad 1 \le i \le s,$ (89)

(b) Z is a sum of k^{th} powers of some to be specified set $\mathfrak{Z}$.

Let $H(\alpha) = \sum_z e(\alpha Z)$, where the summation is over these Z in $\mathfrak{Z}$.

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

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

In the summation over Z there are $H(0)$ = number of Z terms, and for each of these terms, the integral is $>> q^{m(s-k)}$, provided $s \ge 3k+1$. Therefore, if $s \ge 3k+1$

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

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

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

Now we have

$$\begin{aligned} \mathfrak{J}_2 &= \int_{\mathfrak{m}} T^s(\alpha) H(\alpha)\, d\alpha \\ &\leq q^{sm} \int_{\mathfrak{m}} |H(\alpha)|\, d\alpha. \end{aligned} \tag{94}$$

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 $\mathfrak{Y}$ of polynomials of some special form. Let

$$L(\alpha) = \sum_{Y \in \mathfrak{Y}} e(\alpha Y), \tag{95}$$

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

$$|L(\alpha)| \leq L(0). \tag{96}$$

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

$$|L(\alpha)| \leq L(0)\, q^{-\epsilon m}. \tag{97}$$

Let Z be of the special form

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

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

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

and in particular,

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

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

$$\mathcal{I}_2 \leq q^{sm - t\epsilon m} H(0). \tag{101}$$

This is of the form (93) that we want, provided $t\epsilon \geq k + \delta$, 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

$$Y = P^k, \qquad \text{ord } P < m.$$

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

$$|L(\alpha)| << L(0)\, q^{-(\frac{1}{2k-1} - \epsilon')m}$$

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' k^{th} 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

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

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

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

In particular, $R(0) = \text{card}\, \mathcal{U}$. (104)

It follows that

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

The contribution of the minor arcs is

$$\mathfrak{J}_2 \leq q^{(s - t\epsilon)m}\, L^t(0) \int |R(\alpha)|^2 d\alpha. \tag{106}$$

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

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

it follows that

$$\int_{\text{ord } \alpha < 0} |R(\alpha)|^2 d\alpha \leq \sum_{U_1} \sum_{U_2} \int_{\text{ord } \alpha < 0} e(\alpha(U_1 - U_2)) d\alpha \qquad (107)$$

$$\leq R(0).$$

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

$$R(0) >> q^{\epsilon' m}, \qquad (108)$$

then

$$\begin{aligned} \mathcal{J}_2 &\leq q^{(s-t\epsilon)m} L^t(0) \int_{\mathcal{M}} |R(\alpha)|^2 d\alpha \\ &\leq q^{(s-t\epsilon)m} L^t(0) R(0) \qquad (109) \\ &<< q^{(s-t\epsilon-\epsilon')m} L^t(0) R^2(0). \end{aligned}$$

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

$$t\epsilon + \epsilon' \geq k + \delta.$$

Proving an estimate of the type (108) is done in Lemma 32 and gives rise to the 2ℓ k^{th} powers in the terms U_1 and U_2 in (86).

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

Lemma 32: Let $U_\ell(m)$ denote the number of different monic polynomials of order km that are representable as a sum of ℓ k^{th} powers of

polynomials. If char $F_q \nmid k$ then

$$U_\ell(m) >> q^{km(1-\lambda^\ell)}, \tag{110}$$

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

Proof: We proceed by induction on ℓ. If $\ell = 1$, then there are q^m different monic polynomials P^k where ord $P = m$. Thus $U_1(m) >> q^m$. Consider those polynomials of the form $P^k + Q$, where ord $P = m$, P is monic and Q is a monic polynomial of order $k \cdot [\frac{1}{k}(k-1)m]$ which is the sum of $\ell - 1$ k^{th} 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 $P_1 = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$, and let $P_2 = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$. Since we have supposed P_1, P_2 monic, $a_0 = b_0 = 1$. Proceeding by induction, suppose we have proved $a_i = b_i$, $0 \le i < n \le m$. 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

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

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 $km - n \ge$ $\ge (k-1)m >$ ord $Q_i = k[\frac{1}{k}(k-1)m]$. Since $a_i = b_i$, $i < n$, and $a_0 = b_0 = 1$

and 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):

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

We again conclude $a_m = b_m$.

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

$$\begin{aligned} U_\ell(m) &\geq q^m\, U_{\ell-1}([\tfrac{1}{k}(k-1)m]) \\ &>> q^m\, q^{k[\frac{1}{k}(k-1)m](1-\lambda^{\ell-1})} \\ &>> q^{m + (k-1)m(1-\lambda^{\ell-1}) - k(1-\lambda^{\ell-1})} \\ &>> q^{m + (k-1)m(1-\lambda^{\ell-1})} \\ &\qquad (\text{since } q^{-k(1-\lambda^{\ell-1})} >> 1) \\ &>> q^{km(\frac{1}{k} + (1-\frac{1}{k})(1-(1-\frac{1}{k})^{\ell-1})} \\ &>> q^{km(1-\lambda^\ell)}. \end{aligned}$$

<u>Lemma 33</u>: Let $R(\alpha) = \sum_U e(\alpha U)$ where U runs through the different monic polynomials of order km that are sums of ℓ k^{th} powers. Then

$$\int_{\text{ord } \alpha < 0} |R(\alpha)|^2\, d\alpha = R(0) << q^{-km(1-\lambda^\ell)}\, R^2(0). \qquad (113)$$

Proof:

$$\int_{\text{ord } \alpha < 0} |R(\alpha)|^2 \, d\alpha = \sum_{U_1} \sum_{U_2} \int_{\text{ord } \alpha < 0} e(\alpha(U_1 - U_2)) \, d\alpha .$$

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

$$R(0) = U_\ell(m) >> q^{km(1-\lambda^\ell)}.$$

Lemma 34: Suppose $\mathcal{V}$ is a set of polynomials of the form:

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

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

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

Let
$$L(\alpha) = \sum_{V \in \mathcal{V}} \sum_{U \in \mathcal{U}} e(\alpha UV). \tag{116}$$

If (a) $$\alpha = \frac{A}{Q} + \beta, \tag{117}$$

(b) $$\text{ord } \beta \leq -1 - u - v,$$

(c) $$v < \text{ord } Q,$$

(d) $$u \geq \text{ord } Q,$$

(e) $$u_0 = \text{card } \mathcal{U}$$

(f) $$v_0 = \text{card } \mathcal{V}$$

then

$$|L(\alpha)|^2 \le u_0 v_0 q^u \tag{118}$$

Proof: Employing Cauchy's inequality in the form

$$|\Sigma a_i|^2 \le (\#\text{ of terms}) \ \Sigma |a_i|^2,$$

we conclude that

$$\begin{aligned} |L(\alpha)|^2 &= \Big|\sum_{V\in\mathcal{V}} \sum_{U\in\mathcal{U}} e(\alpha UV)\Big|^2 \\ &\le v_0 \sum_{V\in\mathcal{V}} \Big|\sum_{U\in\mathcal{U}} e(\alpha UV)\Big|^2 \\ &\le v_0 \sum_{\substack{\text{ord } V_1<v \\ V=x^v+V_1}} \Big|\sum_{U\in\mathcal{U}} e(\alpha UV)\Big|^2 \\ &\le v_0 \sum_{\substack{\text{ord } V_1<v \\ V=x^v+V_1}} \sum_{U\in\mathcal{U}} \sum_{U'\in\mathcal{U}} e(\alpha(U-U')V). \end{aligned} \tag{119}$$

where now the summation over V is over all polynomials of the form $V = x^v + V_1$, 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 $U = X^u + U_1$, $U' = X^u + U_1'$, ord U_1, $U_1' < u$ we conclude that ord $U'' < u$. It follows that

$$|L(\alpha)|^2 \le v_0 u_0 \sum_{\text{ord } U''<u} \Big|\sum_{\substack{\text{ord } V_1<v \\ V=x^v+V_1}} e(\alpha U''V)\Big|, \tag{120}$$

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

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

$$= \Big|\sum_{\text{ord } V_1 < v} e(\frac{A}{Q} U'' V_1)\Big|.$$

(Here $e(\frac{A}{Q} x^v)$ 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 ord $((\frac{A}{Q} U'')) \geq -v$ or not. Writing $U'' = Q U_2 + U_3$, ord $U_3 <$ ord Q,

$$|L(\alpha)|^2 \leq v_0 u_0 \sum_{\text{ord } U_2 < u - \text{ord } Q} \sum_{U_3 \bmod Q} \Big|\sum_{\text{ord } V_1 < v} e(\frac{A}{Q}(QU_2 + U_3) V_1)\Big|$$

$$\leq v_0 u_0 \frac{q^u}{|Q|} \sum_{U_3 (\text{mod } Q)} \Big|\sum_{\text{ord } V_1 < v} e(\frac{A}{Q} U_3 V_1)\Big|.$$

But as U_3 runs over a complete set of residues mod Q, so does $A U_3$. Out of this complete set of residues there are precisely $\frac{|Q|}{q^v}$ 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

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

$$\leq v_0 u_0 q^u.$$

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

$$|L(\alpha)| << L(0)\, q^{(-\frac{1}{2k} + \frac{1}{2}(1-\frac{1}{k})^{\ell'}(k-1))m}. \tag{122}$$

Proof: We use Lemma 34 with $V = W^k$ and $U = V_l$. Then $v = m$, $v_0 = q^{\frac{1}{k}m}$, $u = (k-1)m$ and $u_0 = U_{\ell'}(\frac{1}{k}(k-1)m)$. The hypotheses of Lemma 34 are easily seen to be valid so it follows that

$$|L(\alpha)|^2 \le u_0\, v_0\, q^u \le q^{(\frac{1}{k}+k-1)m}\, U_{\ell'}(\tfrac{1}{k}(k-1)m) \tag{123}$$

Also $L(0) = \#$ of terms in $L(\alpha)$

$$= U_{\ell'}(\tfrac{1}{k}(k-1)m) \cdot q^{\frac{1}{k}m}.$$

Therefore

$$|L(\alpha)|^2 \le |L(0)|^2\, U_{\ell'}^{-1}(\tfrac{1}{k}(k-1)m)\, q^{(-\frac{1}{k}+k-1)m}. \tag{124}$$

By Lemma 32, $U_{\ell'}(\frac{1}{k}(k-1)m) >> q^{(k-1)(1-\lambda^{\ell'})m}$. Therefore

$$|L(\alpha)| \le |L(0)|\, q^{(-\frac{1}{2k} + \frac{1}{2}(1-\frac{1}{k})^{\ell'}(k-1))m}.$$

Lemma 36: Let $\mathcal{M}$ denote the set of minor arcs. If $\ell = \ell' \ge k \log(3k^2 - k)$ then for some $\delta > 0$,

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

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

$$\int |T(\alpha)|^{3k+1} |R(\alpha)|^2 |L(\alpha)| \, d\alpha \ll$$

$$\ll q^{m(3k+1-\frac{1}{2k}+\frac{1}{2}(1-\frac{1}{k})^{\ell'}(k-1)-k+k(1-\frac{1}{k})^{\ell})} R^2(0) L(0)$$

$$\ll q^{m(2k+1-\frac{1}{2k}+\frac{1}{2}(1-\frac{1}{k})^{\ell}(3k-1)} R^2(0) L(0).$$

We want $$\frac{1}{2}(1-\frac{1}{k})^{\ell}(3k-1) < \frac{1}{2k},$$

or $$\ell \log(1-\frac{1}{k}) < -\log 2k - \log \frac{1}{2}(3k-1).$$

This is true if $$\ell \log(1-\frac{1}{k}) < -\frac{\ell}{k} \le -\log 2k - \log \frac{1}{2}(3k-1)$$

or $$\frac{\ell}{k} \ge \log \frac{1}{2}(3k-1) \cdot 2k,$$

that is if $$\ell \ge k \log(3k^2 - k).$$

Theorem 37: If char $F_q = p \nmid k$ then a polynomial N is a sum of k^{th} powers iff it is a sum of k^{th} powers mod P for all irreducible P such that $|P| \le (k-1)^2$. In that case, it is a sum of

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

k^{th} powers. If $p^{\nu} \| k$ then N is a sum of k^{th} powers iff 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 $p \mid k$ is obvious provided we show the case $p \nmid k$. Suppose $p \nmid k$. We consider representations of N in the form (86) with the provisions 87 (a) - (d). The number of such representations, say $r'(N)$ is

$$r'(N) = \int_{\text{ord}\,\alpha < 0} T(\alpha)^{3k+1} R^2(\alpha) L(\alpha)\, d\alpha.$$

The contribution of the major arcs is

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

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

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

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

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

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

$$\tilde{g}(k) \leq 3k + 1 + 3\ell$$
$$\leq 3k + 3k \log(3k^2 - k) + 4.$$

Corollary 38: There exists polynomials $B, B_1, \cdots, B_M$ such that a polynomial N is a sum of k^{th} powers iff $N \equiv B_i \pmod B$ for some i. If $p = \text{char } F_q \nmid k$ then B is a product of distinct irreducible polynomials P such that $|P| \leq (k-1)^2$. If $p^\nu \| k$ then B is a product of p^νth powers of distinct irreducible

polynomials P such that $|P| \leq (k-1)^2$. The B_i form a ring (mod B).

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

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

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

In particular, every $N \in F_q[x]$ is a sum of 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 $b_1, \cdots, b_k \in F_{q_1}$. Their Van der Monde determinant is

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

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

$$\sum_{1}^{k} a_i = 0$$

$$\sum a_i b_i = 0$$

$$\sum a_i b_i^2 = 0$$

$$\vdots$$

$$\sum a_i b_i^{k-2} = 0$$

$$\sum a_i b_i^{k-1} = \frac{1}{k}.$$

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 $c_i = a_i^{\frac{1}{k}}$, $1 \le i \le k$, 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 k^{th} powers by substituting $P - b$ for x in the identity (126b).

Theorem 40: Let $p = \text{char } F_q$, with say, $q = p^n$. The set of sums of k^{th} powers of constants from F_q is a field, say $F_{p^{n_1}}$. Let $\mathcal{R}(q, k)$ be the ring of polynomials over F_q which are sums of k^{th} powers. If $p \nmid k$ then

$$\dim_{\mathbb{Z}_p} F_q[x]/\mathcal{R}(q, k) \le \frac{k(k-1)}{2} n - (k-1) n_1. \tag{127}$$

Proof: Any subset of a finite field closed under addition and multiplication (and containing 1) is a field. Therefore the sums of k^{th} powers of constants

is indeed a field. Since $1 = 1^k \in \mathcal{R}(q, k)$, $\mathcal{R}(q, k)$ can be viewed as a vector space over $\mathbb{Z}_p$. For $A(x) \in F_q[x]$, $A^k(x) \in \mathcal{R}(q, k)$.

To prove the theorem it will suffice to show that an arbitrary polynomial P can be written as $P = P_1 + P_2$ where $P_1 \in \mathcal{R}(q, k)$ 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 $P_1 \in \mathcal{R}(q, k)$. If ord $P < (k-1)^2$ there is nothing to show. Now suppose $t = \text{ord } P \geq (k-1)^2$ and that we have proved the assertion for all polynomials Q of order $< t$. Write $t = (k-1)u + v$ where $0 \leq v < k-1$. Since $t \geq (k-1)^2$, $u \geq k-1 > v$. Suppose $P = b x^t + P'$ where ord $P' \leq t-1$. Let $a = \frac{1}{k} b$. Then

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

Therefore

$$\text{ord}(P + x^{ku} - (x^u + ax^v)^k)$$
$$\leq \max(\text{ord } P', (k-i)u + iv, 2 \leq i \leq k)$$
$$\leq \max(t-1, ku - \min_{2 \leq j \leq k} (u-v)j)$$
$$< t.$$

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

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

$$u = (k-2) \quad v = k-3,\ k-4,\ \cdots,\ 0$$

$$u = k-3 \quad v = k-4,\ k-5,\ \cdots,\ 0$$

$$\vdots$$

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

we may eliminate powers $x^t = x^{(k-1)u+v}$. In all there are

$1 + 2 + \cdots + (k-2) = \dfrac{(k-2)(k-1)}{2}$ less powers of x. We can also eliminate those powers of the form $(ax^w)^k$ of degree $< (k-1)^2$ hence with $0 \le w \le k-2$, to give $(k-1)n_1$ fewer dimensions. In all there are at most

$$\left\{(k-1)^2 - \frac{(k-2)(k-1)}{2}\right\} n - (k-1)n_1$$

$$= \frac{k^2-k}{2} n - (k-1)n_1$$

dimensions in $F_q[x]/\mathcal{Q}(q, k)$.

Example 41: $k = p^h+1$, $F_q = \mathbb{Z}_p$. In this case, $n = n_1 = 1$. In fact, equality holds in (127) of the previous theorem:

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

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 that the k^{th} power of an arbitrary n-nomial can be written as the sum of k^{th} powers of monomials and binomials. For $n = 1, 2$ there is nothing to prove. Suppose we have shown the assertion for arbitrary m-nomials, $m \le n-1$.

Any n-nomial can be written as $ax^t + bx^u + P$ where P is an $(n-2)$-nomial. Its k^{th} power is

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

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

Instead of using k^{th} 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 k^{th} power of an arbitrary binomial, with $k = 1 + p^h$, is the sum of k^{th} powers of monomials and a truncated binomial and conversely; for we have

$$\begin{aligned}(ax^u + bx^v)^k &= ((ax^u)^{p^h} + (bx^v)^{p^h})(ax^u + bx^v)\\ &= (ax^u)^k + ab(x^{p^h u + v} + x^{u + p^h v}) + (bx^v)^k.\end{aligned}$$

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

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

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

That is, those values of t for which

$$\begin{aligned} &u = 0, && v = 1, \cdots, k-2 \\ &u = 1 && v = 2, \cdots, k-2 \\ &u = 2 && v = 3, \cdots, k-2 \\ &\vdots \\ &u = k-3 && v = k-2. \end{aligned} \tag{130}$$

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

$$(u_0, v_0), (u_1, v_1), (u_2, v_2), \cdots (u_n, v_n) \tag{131}$$

such that

$$u_{i-1} + p^h v_{i-1} = u_i p^h + v_i, \quad 1 \le i \le n \tag{132}$$

and either

(a) $k \mid t_n = u_n p^h + v_n$

or

(b) $t_n = u_n p^h + v_n$ is 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 $k \nmid u_n p^h + v_n$ then also

$$p^h + 1 = k \mid u_{n-1} + p^h v_{n-1} = u_n p^h + v_n.$$

Therefore

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

and also

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

This contradicts the induction hypothesis since

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

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

$$p^h(u p^h + v) \equiv u + v p^h. \pmod{p^{2h} - 1}.$$

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

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

Therefore either (for n even)

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

or (for n odd)

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

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.,

$$r_0 = a_0 + a_1 p^h + a_2 p^{2h} + a_3 p^{3h} + \cdots$$

$$r_n = b_0 + b_1 p^h + \cdots$$

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

Then $r_0 \equiv r_n \mod p^{2h} - 1$ iff

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

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

$$\sum_{i \text{ even}} a_i = \sum_{i \text{ even}} b_i$$

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

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

$$u_0 = u_n$$

$$v_0 = v_n.$$

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 $P \in \mathcal{R}(q, k)$ is of the form

$$P = \sum_{1}^{\ell} a_i x^{t_i}, \tag{133}$$

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 k^{th} powers of monomial and truncated binomials:

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

We may assume $y_i \neq \gamma_i$, $1 \leq i \leq n$.

Let $\mathcal{T}$ be the following set of integers:

(a) $t_1 \in \mathcal{T}$,

(b) if $p^h y_i + \gamma_i \in \mathcal{T}$, $1 \leq i \leq n$, then $y_i + p^h \gamma_i \in \mathcal{T}$,

(c) if $y_i + p^h \gamma_i \in \mathcal{T}$, $1 \leq i \leq n$, then $p^h y_i + \gamma_i \in \mathcal{T}$.

(Here y_i, γ_i are those that appear in (134).) After renumbering we may assume that the first n_0 truncated binomials have their powers in $\mathcal{T}$.

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

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

Here $y_i \neq \gamma_i$, $1 \leq i \leq n_0$.

Now define the sets $\mathcal{T}_j$, $j \geq -1$ of powers of x:

(a) $\mathcal{T}_{-1} = \phi$,

(b) $\mathcal{T}_0 = \{t_1\}$,

(c) if $p^h y_i + z_i \in \mathcal{T}_j$, $1 \le i \le n_0$ and $y_i + p^h z_i \notin \mathcal{T}_{j-1}$
then $y_i + p^h z_i \in \mathcal{T}_{j+1}$,

(d) if $y_i + p^h z_i \in \mathcal{T}_j$, $1 \le i \le n_0$ and $p^h y_i + z_i \notin \mathcal{T}_{j-1}$,
then $p^h y_i + z_i \in \mathcal{T}_{j+1}$.

We show by induction on j the sets $\mathcal{T}_j$ are pairwise disjoint. Clearly $\mathcal{T}_{-1}, \mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2$ are pairwise disjoint. Suppose we have shown $\mathcal{T}_{-1}, \cdots, \mathcal{T}_j$, $j \ge 2$ are pairwise disjoint. Clearly $\mathcal{T}_{j+1} \cap \mathcal{T}_j =$ $= \mathcal{T}_{j+1} \cap \mathcal{T}_{j-1} = \mathcal{T}_{j+1} \cap \mathcal{T}_{-1} = \phi$. Suppose $\mathcal{T}_{j+1} \cap \mathcal{T}_\ell \neq \phi$, $-1 < \ell \le j-2$. Say $p^h y_i + z_i \in \mathcal{T}_{j+1} \cap \mathcal{T}_\ell$ where $y_i + p^h z_i \in \mathcal{T}_j$. Then either $y_i + p^h z_i \in \mathcal{T}_{\ell-1}$ or $y_i + p^h z_i \in \mathcal{T}_{\ell+1}$ contradicting the induction hypothesis. A similar argument holds when $y_i + p^h z_i \in \mathcal{T}_{j+1} \cap \mathcal{T}_\ell$.

In particular $t_1 \notin \mathcal{T}_j$, $j > 0$.

Let $\mathcal{L}_j = \{i \mid 1 \le i \le n_0,\ p^h y_i + z_i \in \mathcal{T}_j \text{ or } y_i + p^h z_i \in \mathcal{T}_j\}$.

In equation (135) the coefficient of x^{t_1} is

$$a_1 = \sum_{i \in \mathcal{L}_1} c_i.$$

The sum of the coefficients of x^u, $u \in \mathcal{T}_j$, $j \ge 1$ in equation (135) is:

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

Since $a_1 \neq 0$, it follows that

$$\sum_{i \in \Delta_j} c_i \neq 0, \quad j \geq 1.$$

This is a contradiction because the π_j (and so the Δ_j) are eventually empty.

Bibliography

1. W. J. Ellison, "Waring's Problem," Am. Math. Monthly 78 (1971): 10-36.

2. C. L. Siegel, "Additive Theorie der Zählkorper, II," Math. Ann. 88 (1923): 184-210.

3. C. L. Siegel, "Generalization of Waring's Problem to Algebraic Number Fields," Amer. J. Math. 66 (1944): 122-136.

4. E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenz, II," Math. Z. 19 (1924): 207-246.

5. D. Hayes, "A Polynomial Analogue of the Goldbach Conjecture," BAMS 69 (1963): 115-116.

6. D. Hayes, "The Expression of a Polynomial as a Sum of Three Irreducibles," Acta Arith. 11 (1966): 461-488.

7. R.E.A.C. Paley, "Theorems on Polynomials in a Galois Field," Quart. J. Math. (Oxford) 4 (1933): 52-63.

8. H. Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities, Ann Arbor Publishers, Ann Arbor (1962).

9. I. M. Vinogradov, The Method of Trigonometrical Sums in the Theory of Numbers, Interscience Publishers, Inc., N. Y. (1954).

10. I. M. Vinogradov, "On Waring's Problem," Ann. of Math. 36 (1935): 395-405.