

Quadratic Forms over Global Fields

by

Yash Totani

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2025

© Yash Totani 2025

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner: Paul Pollack
Professor, Dept. of Mathematics, University of Georgia

Supervisors: Yu-Ru Liu
Professor, Dept. of Pure Mathematics, University of Waterloo

Wentang Kuo
Professor, Dept. of Pure Mathematics, University of Waterloo

Internal Members: David McKinnon
Professor, Dept. of Pure Mathematics, University of Waterloo

Jerry Xiaoheng Wang
Associate Professor, Dept. of Pure Mathematics,
University of Waterloo

Internal-External Member: David Jao
Professor, Dept. of Combinatorics and Optimization,
University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis is structured in two parts. The first part explores certain binary quadratic forms over the polynomial ring $\mathbb{F}_q[T]$. We derive explicit formulas for the number of representations of a polynomial and estimate their moments in two asymptotic scenarios: the large finite field limit, where the field size q grows with fixed polynomial degree n , and the large degree limit, where the degree n increases while q remains fixed. In the former, we employ a Dirichlet series framework to extract asymptotic behavior, while in the latter, we apply a refined partitioning of the space of polynomials of fixed degree to obtain sharp asymptotic estimates. The second part investigates the representation of integers as sums of an even number of triangular numbers. Using the Hardy–Littlewood circle method, we sum the associated singular series and establish its convergence to the Eisenstein component of the expressions obtained using the theory of modular forms, which are expressed in terms of generalized divisor functions.

Acknowledgements

I would like to express my deepest gratitude to my supervisors, Yu-Ru and Wentang, for their wisdom, guidance, and unwavering patience.

I am equally thankful to my friends and family for the endless philosophical conversations, for indulging my intellectual pursuits, for ensuring I was always well-fed, and for helping me maintain (relative) sanity throughout this journey.

Dedication

This work is dedicated to mathematics, my first true intellectual passion.

Table of Contents

Examining Committee Membership	ii
Author's Declaration	iii
Abstract	iv
Acknowledgements	v
Dedication	vi
1 Introduction	1
2 Characteristic 2	12
2.1 Characteristic 2 and the form $A^2 + TB^2$	12
2.2 Characteristic 2 and the form $A^2 + B^2$	13
3 Number of representations	15
3.1 Number of representations by the form $A^2 + TB^2$	15
3.2 Number of representations by the form $A^2 + B^2$	20
4 The method of Dirichlet series	25
4.1 Dirichlet series associated to the form $A^2 + TB^2$	25
4.2 First and second moments of r_1	31
4.3 Higher Moments of r_T in the large degree limit	35

5	A combinatorial approach	40
5.1	Higher Moments of r_T in the large finite field limit	40
5.2	Higher moments of r_1 in the large finite field limit	47
6	Sums of triangular numbers	52
6.1	Summing up the singular series	52
6.2	Number of representations by triangular numbers	58
	References	61

Chapter 1

Introduction

The problem of representing integers by quadratic forms has garnered extensive attention in mathematical research. Jacobi's theorem on sums of two squares provides a fundamental result in this domain, stating that the number of ways $r_2(n)$ to express a positive integer n as a sum of two squares is given by

$$r_2(n) = 4(d_1(n) - d_3(n)),$$

where $d_i(n)$ is the number of divisors of n congruent to i modulo 4 for $i = 1, 3$. Here, we count *all ordered pairs* $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = n$. That is, permutations and sign changes such as $(3, 4), (-3, 4), (4, 3), (-4, -3)$, etc., are each counted as distinct representations. Let the letters p, q represent primes congruent to $1, -1$ modulo 4 respectively. An equivalent formulation of Jacobi's theorem can be stated as follows. Let $n \in \mathbb{N} = \{1, 2, 3, \dots\}$ have the factorisation

$$n = 2^a \prod_{i=1}^k p_i^{b_i} \prod_{j=1}^l q_j^{c_j}$$

for positive integers b_i, c_j for $1 \leq i \leq k, 1 \leq j \leq l$. Then, as in [12, Theorem 278],

$$r_2(n) = \begin{cases} 4 \prod_{i=1}^k (b_i + 1) & \text{if } c_j \text{ is even for all } j \leq l, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\zeta(s)$ be the Riemann zeta function and $L_\chi(s)$ the L -function corresponding to the Kronecker symbol $\left(\frac{-4}{n}\right)$. In [12], Hardy and Littlewood present a formula for the Dirichlet

series corresponding to $r_2(n)$ in terms of $\zeta(s)$ and $L_{-4}(s)$. The formula states

$$\sum_{n=1}^{\infty} \frac{r_2(n)}{n^s} = 4\zeta(s)L_{-4}(s).$$

The Gauss circle problem, which seeks to determine the number of integer lattice points inside a circle of radius r centered at the origin, is linked to the study of the first moment of $r_2(n)$. Sierpinski's result [14, Satz 509] provides insight into the first moment of $r_2(n)$ indicating that

$$\sum_{n \leq x} r_2(n) = \pi x + O(x^{1/3}).$$

While it is conjectured that the exponent in the error term could be $(1/4+\epsilon)$, this conjecture remains elusive. For the second moment of $r_2(n)$, Borwein and Choi [5] derived the following asymptotic expression.

$$\sum_{n \leq x} r_2^2(n) = 4x \log x + 4\alpha x + O(x^{2/3}),$$

where $\alpha = 2.0166 \dots$. Their approach hinges on a Dirichlet series representation for $r_2^2(n)$:

$$\sum_{n=1}^{\infty} \frac{r_2^2(n)}{n^s} = \frac{(4\zeta(s)L_{-4}(s))^2}{(1 + 2^{-s}\zeta(2s))}.$$

Connors and Keating [9] explore higher moments of $r_2(n)$ to analyse accidental degeneracies in energy levels for square billiards, quantifying deviations from a Poisson distribution. In addition to its connections with the aforementioned issues, the exploration of moments in the representation theory of quadratic forms is inherently intriguing.

Denote the set of rational numbers by $\mathbb{Q}$ and the square root of -1 by i . The classical method to study sums of squares entails a study of the norms of the ring of integers of the quadratic extension $\mathbb{Q}(i)$ over $\mathbb{Q}$. More precisely, an integer can be expressed as a sum of two squares if and only if it is the norm of a Gaussian integer, meaning it is the norm of an element in the ring $\mathbb{Z}[i]$, where $\mathbb{Z}$ is the set of integers.

It is interesting to consider the analogous questions in the setting of polynomial rings $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is the finite field of q elements. Over $\mathbb{F}_q[T]$, let Q_M be the quadratic form given by

$$Q_M(A, B) = A^2 + MB^2.$$

and let

$$r_M(f) = \#\left\{(A, B) \mid A, B \in \mathbb{F}_q[T], f = Q_M(A, B)\right\}.$$

An approach to find formulas to r_M is to study norms of the extension ring $\mathbb{F}_q[T][\sqrt{-M}]$. Let $\mathcal{M}_{n,q}$ denote the set of monic polynomials of degree n with coefficients in $\mathbb{F}_q$. When $M = T$, for $f \in \mathcal{M}_{n,q}$, define

$$b_q(f) = \begin{cases} 1, & f = \alpha^2 + T\beta^2 \text{ for } \alpha, \beta \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

Consider the counting function

$$B_q(n) = \sum_{f \in \mathcal{M}_{n,q}} b_q(f),$$

which counts the total number of representations of monic polynomials of degree n over $\mathbb{F}_q$ which can be expressed by the form $A^2 + TB^2$. This function was studied by Bary-Soroker, Smilansky, and Wolf in [3], where they established *analogues of Landau's theorem* in the function field setting. In particular, they analyzed the asymptotic behaviour of $B_q(n)$ as either $n \rightarrow \infty$ with q fixed, or as $q \rightarrow \infty$ with n fixed.

In the first part of this thesis, we will investigate the function $r_M(f)$ and its moments for polynomial rings $\mathbb{F}_q[T]$, where q is a prime power for the following cases:

- $M = T$.
- $M = 1$.

Note: When -1 is a square in $\mathbb{F}_q$, i.e., $q \equiv 1 \pmod{4}$; there exists $i \in \mathbb{F}_q$ such that $i^2 = -1$. Then, for any polynomials $A, B \in \mathbb{F}_q[X]$, we have the identity

$$A^2 + B^2 = (A + iB)(A - iB),$$

Therefore, every polynomial in $\mathbb{F}_q[X]$ is a sum of two squares, with no restriction on the degrees of A and B . Thus, the study of the number of representations of a polynomial f reduces to a counting problem of the divisors of f . When degree restrictions are present, Mireille Car's article [6] gives an analogue of Landau's theorem in this setting.

In this thesis, we will be considering the problem when -1 is not a square. Whenever we talk about the quadratic form $A^2 + B^2$, we will assume that $q \equiv 3 \pmod{4}$.

A key focus will be comparing these results with the known results for the classical function $r_2(n)$. When $\mathbb{F}_q$ has characteristic 2, the *squaring map* $x \mapsto x^2$ defines an isomorphism of $\mathbb{F}_q$ as an additive group. We show that in this setting, every polynomial in $\mathcal{M}_{n,q}$ can be uniquely expressed in the form $\alpha^2 + T\beta^2$. This leads to the following result.

Theorem 1.1.1. *Let $\mathbb{F}_q$ be a field of characteristic 2 and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i -th moments of $r_T(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{n,q}} r_T(f)^i = q^n.$$

Representing a polynomial in the form $A^2 + B^2$ is somewhat more challenging. In this case, we can represent a polynomial as a sum of two squares in infinitely many ways if we do not place any degree restrictions. Hence, we will study the function

$$r_1(f) = \#\{(A, B) \mid A, B \in \mathbb{F}_q[T], f = Q_1(A, B) : \deg A, \deg B \leq d\}.$$

For this function, we have

Theorem 1.1.2. *Let $\mathbb{F}_q$ be a field of characteristic 2 and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i -th moments of $r_1(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{2n+1,q}} r_1^i(f) = 0$$

and

$$\sum_{f \in \mathcal{M}_{2n,q}} r_1^i(f) = q^{n+d+1}.$$

When $\mathbb{F}_q$ has odd characteristic, the formula for $r_M(f)$ is analogous to the one we get in the classical case. When $M = T$, we obtain

Theorem 1.1.3. *Let $\mathbb{F}_q$ be a field of odd characteristic and $f = T^a P_1^{c_1} P_2^{c_2} \dots P_k^{c_k} Q_1^{2d_1} \dots Q_l^{2d_l}$ be the prime factorisation of $f \in \mathcal{M}_{n,q}$ such that $\left(\frac{P_i}{T}\right) = 1$ and $\left(\frac{Q_j}{T}\right) = -1, \forall i, j$. Then*

$$r_T(f) = 2 \prod_{i=1}^k (c_i + 1).$$

Let the letters U and V denote monic irreducible polynomials in $\mathbb{F}_q[T]$ of even and odd degrees, respectively. When $M = 1$, we have the following result.

Theorem 1.1.4. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod{4}$ and $f = U_1^{a_1} U_2^{a_2} \dots U_k^{a_k} V_1^{2b_1} V_2^{2b_2} \dots V_j^{2b_j}$ be the prime factorisation of $f \in \mathbb{F}_q[T]$. Then*

$$r_1(f) = (q + 1) \prod_{i=1}^k (a_i + 1).$$

Now that we have explicit formulas for r_M , we proceed to analyse the asymptotic behaviour of its moments as q^n tends to infinity. This analysis is carried out in two distinct limiting regimes:

- Large degree limit: the size of the finite field $\mathbb{F}_q$ is fixed and the degree $n \rightarrow \infty$,
- Large finite field limit: the degree n is fixed and the field size $q \rightarrow \infty$.

Large degree limit:

Let $\mathcal{M}$ be the set of monic polynomials, $\zeta_q(s)$ the zeta function of $\mathbb{F}_q[T]$ and L_{χ_M} the L -series corresponding to the quadratic character $\chi_M(f) = \left(\frac{f}{M}\right)$. Analogous to the Dirichlet series in the classical case, we find in Theorem 4.1.1 that the Dirichlet series for r_M , when $M = T$ has the form

$$\sum_{f \in \mathcal{M}} \frac{r_T(f)}{|f|^s} = 2\zeta_q(s).$$

Similarly, we find in Theorem 4.1.2 that the Dirichlet series for the square of r_T is given by

$$\sum_{f \in \mathcal{M}} \frac{(r_M)^2(f)}{|f|^s} = \frac{4\zeta_q^2(s)}{\zeta_q(2s)(1 + |M|^{-s})}.$$

When $M = 1$, because of the nature of the quadratic character, the Dirichlet series for r_1 has the form

$$\sum_{f \in \mathcal{M}} \frac{r_1(f)}{|f|^s} = (q + 1)\zeta_{q^2}(s).$$

The Dirichlet series for the square of r_1 has the form

$$\sum_{f \in \mathcal{M}} \frac{(r_1)^2(f)}{|f|^s} = (q + 1)^2 \frac{\zeta_{q^2}^2(s)}{\zeta_q(2s)}.$$

Employing the Dirichlet series described above, we derive formulae for the first and second moments of r_M . When $M = T$, in the large degree limit, we have

Theorem 1.1.5. *Let $\mathbb{F}_q$ be a field of odd characteristic. The first and the second moments for $r_T(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{n,q}} r_T(f) = 2q^n,$$

and

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^2(f) = 4(n+1)q^n + 4 \sum_{k=1}^{n-1} (-1)^k (2n-2k+1)q^{n-k} + 4(-1)^n.$$

When $M = 1$, in the large degree limit, we have

Theorem 1.1.6. *Let $\mathbb{F}_q$ be a field of odd characteristic. The first and the second moments for $r_1(f)$ are given by*

$$\begin{aligned} \sum_{f \in \mathcal{M}_{2n,q}} r_1(f) &= (q+1)q^n, \\ \sum_{f \in \mathcal{M}_{2n,q}} r_1^2(f) &= (q+1)^2 ((n+1)q^{2n} - nq^{2n-1}), \end{aligned}$$

and

$$\sum_{f \in \mathcal{M}_{2n+1,q}} r_1(f) = \sum_{f \in \mathcal{M}_{2n+1,q}} r_1^2(f) = 0$$

While the Dirichlet series approach proves effective for the first and second moments, it encounters limitations with higher moments. Asymptotic formulae are obtained rather than exact formulae, as the Dirichlet series cannot be represented solely in terms of the zeta function $\zeta_q(s)$ and the L -function $L_\chi(s)$. Utilizing techniques similar to those in [9], we investigate the Dirichlet series for the i -th power of r_T , leading to the following results. Note that we only carry out this process for the case $M = T$ and later work out the other case with a more effective technique. In the large degree limit, we have

Theorem 1.1.7. *Let $\mathbb{F}_q$ be a field of odd characteristic. For a fixed q and $i \in \mathbb{N}$ with $i \geq 3$, the i -th moment for r_T is given by*

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^i(f) = -B_i(1)2^i \binom{n+2^{i-1}-1}{n} q^n + O(q^{n-1}),$$

where $B_i(1)$ is a fixed constant depending on i and q obtained from the Dirichlet series for $(r_T)^i$. The error term has a dependence on i and q .

Explicitly describing the constant $B_i(1)$ using the above methods is a non-trivial problem.

Large finite field limit:

Another approach, which is more combinatorial, can be used to determine the higher moments in the large finite field limit, i.e., when n is fixed and q goes to infinity. Inspired by the techniques in [3], we obtain the main results of this paper, which provide a second-order term for the higher moments. We make a note that in the integer setting, in the limit $n \rightarrow \infty$, formulas with an explicit second order term for the higher moments are not known. When $M = T$, in the large finite field limit, we get

Theorem 1.1.8. *Let $\mathbb{F}_q$ be a field of odd characteristic and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i^{th} moment for r_T for a fixed n is given by*

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^i(f) = 2^i \gamma_{i,n} q^n - \alpha_{i,n} q^{n-1} + O(q^{n-2}),$$

where

$$\alpha_{i,n} = (2^{2i-1} - 2^i) \gamma_{i,n-1} + (2^{2i-1} + 2^{3i-2} - 2^{i-1} - 2^{i-1} 3^i) \gamma_{i,n-2}$$

and $\gamma_{i,n}$ is the binomial coefficient

$$\gamma_{i,n} = \binom{n + 2^{(i-1)} - 1}{n}.$$

The error term has a dependence on i and n .

When $M = 1$, in the large finite field limit, we get

Theorem 1.1.9. *Let $\mathbb{F}_q$ be a field of odd characteristic. For $i \in \mathbb{N}$, the i^{th} moment for r_1 is given by*

$$\sum_{f \in \mathcal{M}_{2n+1,q}} (r_1)^i(f) = 0$$

and

$$\sum_{f \in \mathcal{M}_{2n,q}} (r_1)^i(f) = (q+1)^i (\gamma_{i,n} q^{2n} - (2^{i-1} - 1) \gamma_{i,n-1} q^{2n-1} + O(q^{2n-2})),$$

where $\gamma_{i,n}$ is the binomial coefficient

$$\gamma_{i,n} = \binom{n + 2^{(i-1)} - 1}{n}.$$

The error term has a dependence on i and n .

Even though this technique currently yields only the first two terms, in theory, it could be refined to generate additional terms as required. Note that for $i = 1, 2$, the first two terms of the result align with the first and second moments outlined earlier.

Up to this point, our analysis has centered on the function r_M and its associated moments in the setting of binary quadratic forms Q_M defined over the polynomial ring $\mathbb{F}_q[T]$. In this final chapter, we redirect our focus to a distinct but related theme: the study of a quadratic form in s variables over the ring of integers $\mathbb{Z}$, defined as

$$Q(y) = \frac{y_1(y_1 - 1)}{2} + \frac{y_2(y_2 - 1)}{2} + \cdots + \frac{y_s(y_s - 1)}{2},$$

where $y = (y_1, y_2, \dots, y_s) \in \mathbb{Z}^s$. Each summand on the right-hand side represents a triangular number, with the k th triangular number given by

$$T_k = \frac{k(k + 1)}{2}.$$

Representing a positive integer n by the quadratic form $Q(y)$ is thus equivalent to expressing n as a sum of s triangular numbers. This classical problem is intricately linked to the theory of representations of integers by squares. Specifically, the above expression admits the equivalent formulation,

$$(2y_1 - 1)^2 + (2y_2 - 1)^2 + \cdots + (2y_s - 1)^2 = 8Q(y) + s,$$

revealing a direct connection between triangular number representations and representations by the squares of odd integers.

Let $t_s(n)$ denote the number of representations of the integer n as a sum of s triangular numbers. The generating function associated to triangular numbers is given by the q -series,

$$\Psi(q) = \sum_{k=0}^{\infty} q^{T_k} = 1 + q + q^3 + q^6 + \cdots.$$

This series possesses notable modular properties. Building on foundational work by Ono, Robins, and Wahl [15], Atanasov et al. in [2] demonstrated that the function $q^k \Psi^{4k}(q^2)$ defines a modular form of weight $2k$ for the congruence subgroup $\Gamma_0(4)$. By leveraging the theory of modular forms, they derived an asymptotic formula for $t_{4k}(n)$.

To state this result, we introduce the generalised divisor function associated to Dirichlet characters ψ_1 and ψ_2 :

$$\sigma_{k, \psi_1, \psi_2}(n) = \sum_{\substack{d|n \\ d>0}} \psi_1(n/d) \psi_2(d) d^k.$$

Additionally, the generalised Bernoulli numbers $B_{n,\chi}$ are defined through the generating function

$$\sum_{a=1}^M \frac{\chi(a) t e^{at}}{e^{Mt} - 1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$$

With these definitions in place, the asymptotic formula established by Atanasov et al. takes the form:

$$t_{4k}(n) \sim \frac{-8k}{(-16)^k (4^k - 1) B_{2k,\chi_1}} \sigma_{2k-1,\chi_2,\chi_1}(2n+k). \quad (1.1)$$

In his master's thesis [18], the author establishes that the function $q^{2k+1} \Psi^{4k+2}(q^4)$ constitutes a modular form of weight $2k+1$ for the congruence subgroup $\Gamma_0(8)$. Employing the theory of modular forms, he derives the following asymptotic formula for $\delta_{4k+2}(n)$:

$$\delta_{4k+2}(n) \sim \frac{(2k+1)}{(-1)^{k+1} 2^{4k} B_{2k+1,\chi_{-4}}} \sigma_{2k,\chi_{-4},\chi_1}(4n+2k+1), \quad (1.2)$$

This result extends the framework developed for even-weight modular forms to the odd-weight setting. We make a note that these results are part of a more generalised work by Akbary and Aygin [1].

An alternative approach to deriving explicit formulas for $t_s(n)$ involves the use of the circle method, originally developed by Hardy and Littlewood. Bateman, Datskovsky, and Knopp present the following asymptotic formula for $t_s(n)$ in [4]:

$$t_s(n) = 2^{3-s} \frac{\pi^{s/2}}{\Gamma\left(\frac{s}{2}\right)} (8n+s)^{\frac{s}{2}-1} \sum_{\substack{k>0 \\ k \text{ odd}}} A_k^{(s)}(8n+s) + O\left((8n+s)^{\frac{s}{4}}\right), \quad (1.3)$$

where the exponential sum $A_k^{(s)}(m)$ is defined by

$$A_k^{(s)}(m) = \sum_{\substack{h \bmod k \\ (h,k)=1}} \left\{ \frac{G(h,k)}{k} \right\}^s e^{-2\pi i h m / k}, \quad (1.4)$$

and $G(h,k)$ denotes the classical Gauss sum:

$$G(h,k) = \sum_{j=1}^k e^{2\pi i h j^2 / k}.$$

The quantities $A_k^{(s)}(m)$ are multiplicative in k , and the total sum over all k gives rise to the so-called *singular series* $\mathcal{S}^{(s)}(n)$. More precisely,

$$\mathcal{S}^{(s)}(n) = \sum_{k>0} A_k^{(s)}(n) = \prod_p \chi_p^{(s)}(n),$$

where each local factor $\chi_p^{(s)}(n)$ is given by

$$\chi_p^{(s)}(n) = \sum_{j \geq 0} A_{p^j}^{(s)}(n). \quad (1.5)$$

In his seminal work on the representation of integers as sums of squares [11], Hardy introduced a technique for evaluating the singular series associated to $r_8(n)$, the number of representations of n as a sum of eight squares. Building upon Hardy's method, we extend the evaluation of singular series to all even values of s in the context of triangular number representations, thereby deriving asymptotic formulas for $t_s(n)$.

Let $L(s, \chi)$ denote the Dirichlet L -function associated with a character χ , defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Let χ_n denote the principal Dirichlet character modulo n and $\chi_{-4}(n)$ be the non-trivial character modulo 4 defined by

$$\chi_{-4}(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

We first establish the following result regarding the convergence of the singular series.

Theorem 1.1.10. *The singular series $\mathcal{S}^{(s)}(n)$ converges to*

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \sigma_{\frac{s}{2}-1}(\chi_2, \chi_1; n)}{L\left(\frac{s}{2}, \chi_2\right)} \quad \text{if } s \equiv 0 \pmod{4},$$

and

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \sigma_{\frac{s}{2}-1}(\chi_{-4}, \chi_1; n)}{L\left(\frac{s}{2}, \chi_{-4}\right)} \quad \text{if } s \equiv 2 \pmod{4},$$

where $\sigma_k(\chi_1, \chi_2; n)$ denotes the generalised divisor function.

With the singular series explicitly summed, we are able to derive asymptotic formulas for $t_s(n)$ that are consistent with those obtained via the theory of modular forms. Our main result is the following.

Theorem 1.1.11. *The number $t_s(n)$ of representations of n as a sum of s triangular numbers satisfies the asymptotic formulas*

$$t_{4k}(n) \sim \frac{(-1)^k \cdot 8k}{B_{2k, \chi_2}} \sigma_{2k-1}(\chi_2, \chi_1; 2n + k)$$

and

$$t_{4k+2}(n) \sim \frac{(-1)^{k+1}(8k+4)}{B_{2k+1, \chi_{-4}}} \sigma_{2k}(\chi_{-4}, \chi_1; 4n + 2k + 1),$$

where $B_{n, \chi}$ denotes the generalised Bernoulli number associated to the Dirichlet character χ .

Note that the k th triangular number $T_k = k(k+1)/2$ can also be obtained if we replace k by $-(k+1)$. Each triangular number is counted twice when working with the singular series and only once while using the technique of modular forms. This disparity is evident in the above theorem and the formulas (1.1), (1.2) obtained via the theory of modular forms.

There is another difference in formulas relating to the Bernoulli numbers, namely (1.1) has B_{2k, χ_1} and the above result has B_{2k, χ_2} . To see the relation between the two, note that

$$L(2k, \chi) = \left(1 - \frac{1}{2^{2k}}\right) \zeta(2k).$$

Substituting the formulas for $L(2k, \chi)$ and $\zeta(2k)$ shows that $B_{2k, \chi_2} = -(4^k - 1)B_{2k, \chi_1}$. Hence, the formulas obtained by the two methods agree.

In conclusion, this work highlights a central theme in number theory: the convergence of distinct analytic techniques, such as the circle method and the theory of modular forms, to reveal the same underlying arithmetic truths.

Chapter 2

Characteristic 2

In this chapter, we derive formulas for the number of representations $r_M(f)$ by the quadratic form $A^2 + MB^2$, where f is a monic polynomial in the ring $\mathbb{F}_q[T]$ and $\mathbb{F}_q$ has characteristic 2. We then analyse the moments of the function r_M . These computations are carried out for two distinct cases, each discussed in a separate section:

- $M = T$.
- $M = 1$.

2.1 Characteristic 2 and the form $A^2 + TB^2$

In this section, we will work with the assumption that $M = T$. We will prove the following result.

Theorem 1.1.1. *Let $\mathbb{F}_q$ be a field of characteristic 2 and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i -th moments of $r_T(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{n,q}} r_T(f)^i = q^n.$$

Proof. When $\mathbb{F}_q$ has characteristic 2, we claim that every $f \in \mathcal{M}_{n,q}$ can be written as $A^2 + TB^2$ in a single way. That is, $r_T(f) = 1$ for all $f \in \mathcal{M}_{n,q}$. To justify this claim, look at the squaring map

$$\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$$

given by $\phi(a) = a^2$. The map is an isomorphism as it has a trivial kernel. Let $f \in \mathcal{M}_{n,q}$. Then separating the even and odd degree terms of f , f can be written as $f = g + Th$, where

$$g = a_{2n}T^{2n} + \cdots + a_2T^2 + a_0$$

and

$$h = a_{2m+1}T^{2m} + \cdots + a_3T^2 + a_1.$$

Then f can be written as

$$f = (\phi^{-1}(a_{2n})T^n + \cdots + \phi^{-1}(a_0))^2 + T(\phi^{-1}(a_{2m+1})T^m + \cdots + \phi^{-1}(a_1))^2.$$

In fact, this is the only way to represent f in the form $A^2 + TB^2$ as there is a single way to separate f into its even and odd degree terms. Hence, the claim is justified. The study of moments becomes trivial and the i th moment is just given by

$$\sum_{f \in \mathcal{M}_{n,q}} r_T(f)^i = q^n.$$

This completes the proof of Theorem 1.1.1. □

2.2 Characteristic 2 and the form $A^2 + B^2$

In this section, we will work with the assumption that $M = 1$. We will prove the following result.

Theorem 1.1.2. *Let $\mathbb{F}_q$ be a field of characteristic 2 and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i -th moments of $r_1(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{2n+1,q}} r_1^i(f) = 0$$

and

$$\sum_{f \in \mathcal{M}_{2n,q}} r_1^i(f) = q^{n+d+1}.$$

Let $s(f)$ be the characteristic function of sums of squares, i.e.,

$$s(f) = \begin{cases} 1 & \text{if } f = A^2 + B^2; \ A, B \in \mathbb{F}_q[T], \\ 0 & \text{otherwise.} \end{cases}$$

Proof of Theorem 1.1.2. Assume $\text{char}(\mathbb{F}_q) = 2$. In this case, note that for any polynomials $A, B \in \mathbb{F}_q[T]$,

$$A^2 + B^2 = (A + B)^2.$$

Consequently, the polynomials that are perfect squares are exactly those polynomials whose terms have even degree, since

$$\psi : \mathbb{F}_q[T] \rightarrow \mathbb{F}_q[T], \quad \psi(f) = f^2,$$

is an $\mathbb{F}_q$ -linear isomorphism onto the subspace of polynomials with only even degree terms. The number of such monic polynomials of degree $2n$ is precisely q^n .

Now, if we impose the restriction $\deg(A), \deg(B) \leq d$, then for any choice of monic polynomial A , there exists a unique B such that

$$f = A^2 + B^2.$$

There are exactly q^{d+1} choices for A . This completes the proof. □

Chapter 3

Number of representations

In this chapter, we establish explicit formulas for the number of representations r_M associated with the quadratic form $Q_M = A^2 + MB^2$. We consider the following two cases, each explored in a separate section:

- $M = T$.
- $M = 1$.

3.1 Number of representations by the form $A^2 + TB^2$

We use the letters P and Q to denote irreducible polynomials that are, respectively, quadratic residues and non-residues modulo T . We will prove that

Theorem 1.1.3. *Let $\mathbb{F}_q$ be a field of odd characteristic and $f = T^a P_1^{c_1} P_2^{c_2} \dots P_k^{c_k} Q_1^{2d_1} \dots Q_l^{2d_l}$ be the prime factorisation of $f \in \mathcal{M}_{n,q}$ such that $\left(\frac{P_i}{T}\right) = 1$ and $\left(\frac{Q_j}{T}\right) = -1, \forall i, j$. Then*

$$r_T(f) = 2 \prod_{i=1}^k (c_i + 1).$$

We want to examine the quadratic field extension $L = \mathbb{F}_q(T, \sqrt{-T})$ over $K = \mathbb{F}_q(T)$. This extension is Galois and admits two automorphisms, defined by the mappings $\sqrt{-T} \mapsto \pm\sqrt{-T}$.

Let $\mathcal{T}$ and $\mathcal{N}$ denote the trace and norm maps associated with the quadratic extension L/K . The norm map

$$\mathcal{N} : L \rightarrow K$$

is given by

$$\mathcal{N}(A + B\sqrt{-T}) = (A + B\sqrt{-T})(A - B\sqrt{-T}) = A^2 + TB^2,$$

while the trace map

$$\mathcal{T} : L \rightarrow K$$

is given by

$$\mathcal{T}(A + B\sqrt{-T}) = 2A,$$

for $A, B \in K$.

We define the ring of integers of $K = \mathbb{F}_q(T)$ to be $\mathcal{A} = \mathbb{F}_q[T]$. A key step in our analysis is the construction of the ring of integers in the quadratic extension L , by which we mean the integral closure of $\mathcal{A}$ in L .

Proposition 3.1.1. *The ring of integers of L is given by $\mathcal{B} = \mathcal{A}[\sqrt{-T}]$.*

Proof. Every element of L is of the form $a + b\sqrt{-T}$ with $a, b \in K$. Let $x = a + b\sqrt{-T} \in O_L$, where O_L denotes the ring of integers of L . Using the fact that the trace and norm of x must belong to $\mathcal{A}$, we have $2a \in \mathcal{A}$ and $a^2 + Tb^2 \in \mathcal{A}$. Since the characteristic of $\mathbb{F}_q$ is odd, 2 is invertible and hence $a \in \mathcal{A}$. Using this information, we see that, $Tb^2 \in \mathcal{A}$ which can only occur when $b \in \mathcal{A}$. Hence, we have $x \in \mathcal{A}[\sqrt{-T}]$ and hence,

$$O_L \subseteq \mathcal{A}[\sqrt{-T}].$$

For the other side, let $x \in \mathcal{A}[\sqrt{-T}]$. Then $x = a + b\sqrt{-T}$, with $a, b \in \mathcal{A}$ has the minimal polynomial

$$X^2 + 2aX + (a^2 + Tb^2) \in \mathcal{A}[X].$$

Hence, the result follows. □

Next, we want to show that the extension $\mathcal{B}$ is a Euclidean domain and hence a unique factorization domain. We can in fact show that for any polynomial of degree 1, the extension $\mathcal{B}_M = \mathbb{F}_q[T][\sqrt{-M}]$ is a Euclidean domain.

Theorem 3.1.2. *let $M \in \mathcal{A}$ be a polynomial of degree 1. Then $\mathcal{B}_M = \mathbb{F}_q[T][\sqrt{-M}]$ is a Euclidean domain.*

Proof. Define the conjugate $\bar{\alpha}$ of $\alpha = A + \sqrt{-T}B \in \mathcal{A}$ as $\bar{\alpha} := A - \sqrt{-T}B$. We define the norm maps as follows: $\mathcal{N}_M : \mathcal{B}_M \rightarrow \mathcal{A}$ is given by $\alpha \mapsto \mathcal{N}_M(\alpha) := \alpha \cdot \bar{\alpha} = A^2 + MB^2$, and $N_M : \mathcal{B}_M \rightarrow \mathbb{R}$ by $\alpha \mapsto N_M(\alpha) := q^{\deg(\mathcal{N}_M(\alpha))}$ for $\alpha \neq 0$ with the convention that $\deg 0 = -\infty$. Note that $\mathcal{N}_M$ and N_M can be extended to the fraction fields of $\mathcal{B}_M$, by $\mathcal{N}_M(\alpha/\beta) := \mathcal{N}_M(\alpha)/\mathcal{N}_M(\beta)$, and $N_M(\alpha/\beta) := N_M(\alpha)/N_M(\beta)$, and be multiplicative. We would like to show there is a division algorithm on $\mathcal{B}_M$. Indeed, the standard division algorithm will work.

Let $\alpha = A + \sqrt{-M}B, 0 \neq \beta = C + \sqrt{-M}D \in \mathcal{B}_M$. We claim that there exists $\theta, \rho \in \mathcal{B}_M$, $N_M(\rho) < N_M(\beta)$, such that

$$\alpha = \theta \cdot \beta + \rho.$$

Consider

$$\alpha \cdot \bar{\beta} = E + \sqrt{-M}F.$$

Apply the division algorithm of $\mathcal{A}$ on E and F divided by $\mathcal{N}_M(\beta)$, we have

$$E = Q \cdot \mathcal{N}_M(\beta) + R, \quad F = Q' \cdot \mathcal{N}_M(\beta) + R',$$

where $\deg R, \deg R' \leq \deg \mathcal{N}_M(\beta) - 1$. Let

$$\theta = Q + \sqrt{-M}Q',$$

and then

$$\rho := \alpha - \theta \cdot \beta \in \mathcal{B}.$$

Note that

$$\begin{aligned} \rho &= \frac{\alpha \cdot \bar{\beta} - \theta \cdot \mathcal{N}_M(\beta)}{\bar{\beta}} \\ &= \frac{(E + \sqrt{-M}F) - (Q + \sqrt{-M}Q') \cdot \mathcal{N}_M(\beta)}{\bar{\beta}} \\ &= \frac{(E - Q \cdot \mathcal{N}_M(\beta)) + \sqrt{-M}(F - Q' \cdot \mathcal{N}_M(\beta))}{\bar{\beta}} \\ &= \frac{R + \sqrt{-M}R'}{\bar{\beta}}. \end{aligned}$$

Since N_M is multiplicative, we have

$$\begin{aligned}
N_M(\rho) &= N_M(R + \sqrt{-M}R')/N_M(\beta) \\
&= \frac{q^{\deg(\mathcal{N}_M(R + \sqrt{-M}R'))}}{N_M(\beta)} \\
&= \frac{q^{\deg(R^2 + MR'^2)}}{N_M(\beta)} \\
&\leq \frac{q^{\max(\deg(R^2), \deg(MR'^2))}}{q^{\deg \mathcal{N}_M(\beta)}} \\
&= \frac{q^{\max(2 \deg(R), 2 \deg R' + 1)}}{q^{\deg \mathcal{N}_M(\beta)}} \\
&\leq \frac{q^{2 \deg \mathcal{N}_M(\beta) - 1}}{q^{\deg \mathcal{N}_M(\beta)}} \\
&= q^{\deg \mathcal{N}_M(\beta) - 1} \\
&< q^{\deg \mathcal{N}_M(\beta)} = N_M(\beta).
\end{aligned}$$

It finishes the proof. □

Let Q_T be the quadratic form given by

$$Q_T(A, B) = A^2 + TB^2.$$

and let

$$r_T(f) = \# \left\{ (A, B) \mid A, B \in \mathbb{F}_q[T], f = Q_T(A, B) \right\}.$$

Let s_T be the characteristic function of the set of polynomials represented by Q_T , i.e.,

$$s_T(f) = \begin{cases} 1, & f = A^2 + TB^2 \text{ for some } A, B \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

The characteristic function s_T determines the irreducibility of primes of $\mathcal{A}$ in $\mathcal{B}$. We describe the elementary results from [3] here without proofs.

Lemma 3.1.3. [3, Lemma 2.1] *Let $P \in \mathcal{A}$ be a prime polynomial of degree n . Then P is reducible in $\mathcal{B}$ if and only if $s_T(P) = 1$. Moreover, if $P = A^2 + TB^2$ for some $A, B \in \mathcal{A}$, then $A \pm \sqrt{-T}B$ are irreducible in $\mathcal{B}$.*

Definition 3.1.4 (Legendre Symbol Modulo P). Let $\mathbb{F}_q$ be a finite field with odd characteristic and $P \in \mathbb{F}_q[T]$ be irreducible. For any polynomial $f \in \mathbb{F}_q[T]$ coprime to P , the Legendre symbol modulo P , denoted $\left(\frac{f}{P}\right)$, is the unique element of $\mathbb{F}_q^\times$ such that

$$\left(\frac{f}{P}\right) \equiv f^{\frac{|P|-1}{2}} \pmod{P}.$$

For any monic irreducible polynomial $P \in \mathbb{F}_q[T]$ coprime to T , the Legendre symbol $\left(\frac{P}{T}\right)$ is the unique element of $\{\pm 1\} \subset \mathbb{F}_q^\times$ satisfying

$$\left(\frac{P}{T}\right) \equiv P^{\frac{q-1}{2}} \pmod{T}.$$

Lemma 3.1.5. [3, Lemma 2.2, 2.3] Let $P \in \mathcal{A}$ be irreducible in $\mathcal{A}$. Then P is reducible in $\mathcal{B}$ if and only if $\left(\frac{P}{T}\right) = 1$.

We make a note that this method will be broken for $\deg M \geq 2$. In fact, for $\deg M \geq 2$, $\mathbb{F}_q[T][\sqrt{-M}]$ might not be a UFD. We have the following counterexample.

Let $q = 3$, $M = T^2 + 1$, $A = T$, and $B = 1$. Consider $A^2 + MB^2$,
 $(T + \sqrt{-M})(T - \sqrt{-M}) = A^2 + MB^2 = T^2 + (T^2 + 1) \cdot 1^2 = 2T^2 + 1 = 2(T^2 - 1) = 2(T - 1)(T + 1)$.

Clearly, $T + \sqrt{-M}$, $T - \sqrt{-M}$, $T - 1$, $T + 1$ are irreducible by the degree consideration. Therefore, $\mathbb{F}_3[T][\sqrt{-(T^2 + 1)}]$ is not a UFD.

Let $\mathcal{N}$ be the norm map from $\mathcal{B} \rightarrow \mathcal{A}$.

Proposition 3.1.6. [3, Proposition 2.4] Let $h(S) \in \mathcal{B}$ be a prime polynomial. Then exactly one of the following holds:

1. $\mathcal{N}(h) = \pm P$, where P is a prime of $\mathcal{A}$ with $\left(\frac{P}{T}\right) = 1$.
2. $h = \pm Q \in \mathcal{A}$ where Q is a prime in $\mathcal{A}$ with $\left(\frac{Q}{T}\right) = -1$. In particular $\mathcal{N}(h) = \pm Q^2$.
3. $\mathcal{N}(h) = -T$.

Proof of Theorem 1.1.3. Firstly, suppose $f, g \in \mathbb{F}_q[T]$ are coprime. Let $f_1 = A_1^2 + TB_1^2$ and $f_2 = A_2^2 + TB_2^2$. Then the product

$$f_1 f_2 = (A_1^2 + TB_1^2)(A_2^2 + TB_2^2)$$

can also be written in the form $A^2 + TB^2$, since

$$f_1 f_2 = (A_1 A_2 - T B_1 B_2)^2 + T(A_1 B_2 + A_2 B_1)^2.$$

We know that $s_M(f) = 1$ if and only if $f = N(h)$ for some $h \in \mathcal{B}$. So the question is how many elements in $\mathcal{B}$ have norm f . Let us see what happens when f is a prime power. For a prime Q , such that $\left(\frac{Q}{M}\right) = -1$, Q cannot be represented by Q_M . In fact, the only elements of norm Q^2 are $\pm Q$. We deduce that if $f = Q^{2b}$, then $\pm Q^b$ are the only elements in $\mathcal{B}$ with norm f .

If $f = P^a$, where $\left(\frac{P}{M}\right) = 1$, then there are exactly $2(a+1)$ elements with norm f . To see this, if $N(A + B\sqrt{-M}) = P$, then $N(A - B\sqrt{-M}) = P$ as well. Hence,

$$N\left(\pm(A + B\sqrt{-M})^i (A - B\sqrt{-M})^{a-i}\right) = P^a$$

for all $0 \leq i \leq a$. The last thing we should check is the uniqueness of elements of norm P . That is provided to us by the unique factorization in $\mathcal{B}$. Hence, the result is evident. $\square$

3.2 Number of representations by the form $A^2 + B^2$

In the previous section, we considered M as an irreducible element of odd degree. Here, we replace M with a constant and explore how the same methodology can be applied to derive formulas for the number of representations by the quadratic form Q_M . We set $M = 1$, noting that other cases can be treated analogously.

To ensure that -1 is not a square modulo q , we restrict our attention to finite fields $\mathbb{F}_q$ where $q \equiv 3 \pmod{4}$. We introduce the letters U and V to represent irreducibles of even and odd degrees, respectively. We will prove the following result.

Theorem 1.1.4. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod{4}$ and $f = U_1^{a_1} U_2^{a_2} \dots U_k^{a_k} V_1^{2b_1} V_2^{2b_2} \dots V_j^{2b_j}$ be the prime factorisation of $f \in \mathbb{F}_q[T]$. Then*

$$r_1(f) = (q+1) \prod_{i=1}^k (a_i + 1).$$

Let $\mathcal{A}$ denote $\mathbb{F}_q[T]$ and define $\mathcal{B}$ as the ring of integers of the quadratic extension $L = \mathbb{F}_q(T)(\sqrt{-1})$, which is explicitly given by $\mathbb{F}_q[T][\sqrt{-1}]$. Every element $h \in \mathcal{B}$ can be expressed in the form

$$h = A + iB,$$

where $A, B \in \mathcal{A}$ and $i = \sqrt{-1}$.

We will work with the norm map

$$N : \mathcal{B} \rightarrow \mathcal{A},$$

defined as

$$N(h) = (A + iB)(A - iB) = A^2 + B^2.$$

Let s denote the characteristic function of the set of polynomials represented by the quadratic form $Q_1 = A^2 + B^2$, i.e.,

$$s(f) = \begin{cases} 1, & f = A^2 + B^2 \text{ for some } A, B \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3.2.1. *Let $P(T) \in \mathcal{A}$ be a monic irreducible of degree n . Then $P(T)$ is reducible in $\mathcal{B}$ if and only if $s(P) = 1$. Moreover, if $P = A^2 + B^2$, then $A \pm iB$ are irreducible in $\mathcal{B}$.*

Proof. First assume that $s(P) = 1$. Let

$$P = A^2 + B^2 = (A + iB)(A - iB).$$

We show that none of $A \pm iB$ are units. We claim that the units of $\mathcal{B}$ are precisely the polynomials f for which $\mathcal{N}(f)$ is a non-zero element of $\mathbb{F}_q$. To see this, let f be a unit of $\mathcal{B}$. Then there exists $g \in \mathcal{B}$ such that $f \times g = 1$. Taking norms we find

$$\mathcal{N}(f)\mathcal{N}(g) = 1,$$

meaning $\mathcal{N}(f)$ and $\mathcal{N}(g)$ are units in $\mathcal{A}$ and the only units in $\mathcal{A}$ are the non-zero elements of $\mathbb{F}_q$. Hence, the claim holds. Now if let's say without the loss of generality that $A + iB$ is a unit. Then $\mathcal{N}(A + iB) = A^2 + B^2$ would be a unit of $\mathcal{A}$ contradicting the fact that it is a prime in $\mathcal{A}$.

For the other direction, assume that P is reducible in $\mathcal{B}$. Then,

$$P = (A + iB)(C + iD),$$

where $A, B, C, D \in \mathcal{A}$. Applying the norm map, we get

$$P^2 = (A^2 + B^2)(C^2 + D^2).$$

We know that $\mathcal{A}$ has unique factorization. Hence,

$$P = c(A^2 + B^2)$$

for some $c \in \mathbb{F}_q$. Comparing the leading coefficients on both sides, we see that $1 = c(k_1^2 + k_2^2)$ for some $k_1, k_2 \in \mathbb{F}_q$. Hence, replacing $A + iB$ by $(A + iB)/(k_1 + ik_2)$, we get that

$$P = A^2 + B^2.$$

Hence $s(P) = 1$.

The last thing we want to show that if $P = A^2 + B^2$, $A \pm iB$ are irreducible in $\mathcal{B}$. Say $(C + iD)$ divides $(A + iB)$ in $\mathcal{B}$ and $C + iD$ is not a unit in $\mathcal{B}$. Then $C^2 + D^2$ is not a unit in $\mathcal{A}$. By taking norms,

$$(C^2 + D^2)|(A^2 + B^2) = P$$

in K . Since $C^2 + D^2$ is not a unit in $\mathcal{A}$, we must have $C^2 + D^2 = P = A^2 + B^2$. From unique factorisation in $\mathcal{B}$, we have $C + iD$ has to be equal to $A + iB$. Hence, we are done. $\square$

Lemma 3.2.2. *Let $P \in \mathcal{A}$ be irreducible in $\mathcal{A}$. P is reducible in $\mathcal{B}$ if and only if the Legendre symbol $\left(\frac{-1}{P}\right) = 1$, i.e., P has even degree in $\mathcal{A}$.*

Proof. First, assume that P is reducible in $\mathcal{B}$. Then, by the previous lemma, we have that $s(P) = 1$ and hence

$$P = A^2 + B^2$$

for some $A, B \in \mathcal{A}$. Note that A, B are coprime in $\mathcal{A}$. Hence, there exists $C, D \in \mathcal{A}$ such that $AD + BC = 1$. Hence

$$(A^2 + B^2)(C^2 + D^2) = (AC - BD)^2 + 1.$$

We have that $P|(X^2 + 1)$ for some $X \in \mathcal{A}$. Hence, -1 is a square modulo P . From the definition of the Legendre symbol (Definition 3.1.4), we have

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{q-1}{2} \deg P}.$$

Since $q \equiv 3 \pmod{4}$, $\deg(P)$ has to be even.

For the other direction, assume for the sake of a contradiction that P is irreducible in $\mathcal{B}$ and $\left(\frac{-1}{P}\right) = 1$, then there exists $X \in K$ such that

$$P|(X^2 + 1) = (X + i)(X - i).$$

Since we assumed P to be an irreducible in L , Without any loss of generality, say $P|(X+i)$. Complex conjugation gives $P|(X-i)$ and $P|2i$ which is a contradiction as a prime in $\mathcal{A}$ cannot have zero degree. So, we are done. $\square$

We are now ready to prove the main result of this section.

Proof of Theorem 1.1.4. Firstly, suppose $f_1, f_2 \in \mathcal{A}$ are coprime, and write their representations as norms from $\mathcal{B}$:

$$f_1 = N(A_1 + \omega B_1) = A_1^2 - gB_1^2, \quad f_2 = N(A_2 + \omega B_2) = A_2^2 - gB_2^2.$$

Then we have the generalized identity:

$$f_1 f_2 = N((A_1 + \omega B_1)(A_2 + \omega B_2)) = (A_1 A_2 + gB_1 B_2)^2 - g(A_1 B_2 + A_2 B_1)^2.$$

This demonstrates that the property of being a norm is multiplicative.

It is evident that $r_2^*(f) > 0$ if and only if $f = N(h)$ for some $h \in \mathcal{B}$. So the question is how many elements in $\mathcal{B}$ have norm f . Let us see what happens when f is a prime power.

Let $f = V^{2b}$, where V is a prime of odd degree, which means it is inert in $\mathcal{B}$. If an element $h \in \mathcal{B}$ has norm f , its factorization in $\mathcal{B}$ must be $h = c \cdot V^b$ for some unit $c \in \mathcal{B}$. Taking the norm, we have $N(h) = N(c)N(V^b) = N(c)V^{2b}$. For this to be equal to the monic polynomial $f = V^{2b}$, the norm of the unit must be one: $N(c) = 1$. The units of $\mathcal{B}$ are the non-zero elements of the field $\mathbb{F}_{q^2}$. The elements with norm 1 are precisely the kernel of the norm homomorphism $N : \mathbb{F}_{q^2}^* \rightarrow \mathbb{F}_q^*$, which is a group of size $q+1$. We deduce that if $f = V^{2b}$, then there are exactly $q+1$ elements in $\mathcal{B}$ with norm f .

Now, if $f = U^a$, where U is a prime of even degree, which means it splits in $\mathcal{B}$, then there are exactly $(q+1)(a+1)$ elements with norm f . To see this, we can write $U = N(\pi)$ for some irreducible $\pi = u + \omega v \in \mathcal{B}$. Then $N(\sigma(\pi)) = N(u - \omega v) = U$ as well. Hence, any element h with norm U^a must be of the form $h = c \cdot \pi^k \sigma(\pi)^{a-k}$ for all $0 \leq k \leq a$, where c is a unit in $\mathcal{B}$ whose norm must be 1. For each of the $a+1$ choices for the exponent k , there are $q+1$ choices for the unit c .

The last thing we should check is the uniqueness argument for these representations. If,

$$N(u + \omega v) = N(w + \omega x) = U$$

for $u, v, w, x \in \mathcal{A}$, then in $\mathcal{B}$ we have the factorization,

$$(u + \omega v)(u - \omega v) = (w + \omega x)(w - \omega x).$$

Each of the factors on both sides is an irreducible polynomial in $\mathcal{B}$. By unique factorization, we must have, without loss of generality, that

$$u + \omega v = c(w + \omega x)$$

for some unit $c \in \mathcal{B}$ (that is, $c \in \mathbb{F}_{q^2}^*$). Taking the norms and observing that U is monic, we get

$$N(u + \omega v) = N(c)N(w + \omega x) \implies U = N(c)U.$$

This means the norm of c has to be equal to 1. As established before, there are exactly $q + 1$ such units in $\mathbb{F}_{q^2}^*$ whose norm is 1. Hence, the result is evident. $\square$

Chapter 4

The method of Dirichlet series

Recall that r_M represents the number of representations by the quadratic form

$$A^2 + MB^2.$$

This chapter aims to achieve the following objectives, each of which is discussed in a separate section.

- Establish exact formulas for the Dirichlet series associated with r_T and its square, followed by results concerning the first and second moments of r_T .
- Obtain precise formulas for the Dirichlet series corresponding to r_1 and its square, and subsequently derive results for the first and second moments of r_1 .
- Investigate the higher moments of the function r_T .

4.1 Dirichlet series associated to the form $A^2 + TB^2$

In this section, we will study the Dirichlet series associated to r_T . Let $\delta_T = r_T/2$ and

$$L_{T,i}(s) = \sum_{f \in \mathcal{M}} \delta_T^i(f) |f|^{-s}.$$

We will prove that for $i = 1$, we obtain

Theorem 4.1.1. *We have*

$$L_{T,1}(s) = \zeta_q(s).$$

And for $i = 2$, we obtain

Theorem 4.1.2. *We have*

$$L_{T,2}(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1 + q^{-s})}.$$

For

$$f = T^c P_1^{a_1} P_2^{a_2} \dots P_k^{a_k} Q_1^{2c_1} Q_2^{2c_2} \dots Q_r^{2c_r}$$

with $\left(\frac{P_i}{T}\right) = 1$ and $\left(\frac{Q_j}{T}\right) = -1$ for all i, j , we have

$$r_T(f) = 2 \prod_{i=1}^k (a_i + 1).$$

Note that $\delta_T(f) = r_T(f)/2$ is a multiplicative function. Let $\mathcal{M}$ and $\mathcal{P}$ be the set of monic polynomials and the set of monic irreducibles in $\mathbb{F}_q[T]$ respectively. We want to study the Dirichlet series

$$L_{T,i}(s) = \sum_{f \in \mathcal{M}} \delta_T^i(f) |f|^{-s}$$

for $i = 1, 2$, where $|f| = q^{\deg(f)}$. Since $\delta_T(f)$ is multiplicative, we have a product of local factors

$$L_{T,i}(s) = \prod_{R \in \mathcal{P}} \left(\sum_{k=0}^{\infty} \delta_T^i(R^k) |R|^{-ks} \right),$$

where

$$\delta_T^i(R^k) = \begin{cases} (k+1)^i & \text{if } \left(\frac{R}{T}\right) = 1, \\ 1 & \text{if } R = T, \\ 1 & \text{if } \left(\frac{R}{T}\right) = -1 \text{ and } 2 \mid k, \\ 0 & \text{if } \left(\frac{R}{T}\right) = -1 \text{ and } 2 \nmid k. \end{cases}$$

Let χ_T be the quadratic character given by $\chi(f) = \left(\frac{f}{T}\right)$. The associated L series is

$$L_{\chi_T}(s) = \sum_{f \in \mathcal{M}} \chi(f) |f|^{-s} = \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 + |Q|^{-s})^{-1}. \quad (4.1)$$

Since χ_T is defined modulo a linear polynomial, $L_{\chi_T}(s) = 1$.

Recall that r_T denotes the number of representations by the quadratic form $A^2 + TB^2$. In this section, we study the Dirichlet series to arrive at the first and second moments of r_T . We will prove that,

Theorem 1.1.5. *Let $\mathbb{F}_q$ be a field of odd characteristic. The first and the second moments for $r_T(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{n,q}} r_T(f) = 2q^n,$$

and

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^2(f) = 4(n+1)q^n + 4 \sum_{k=1}^{n-1} (-1)^k (2n-2k+1)q^{n-k} + 4(-1)^n.$$

Recall that for

$$f = T^c P_1^{a_1} P_2^{a_2} \dots P_k^{a_k} Q_1^{2c_1} Q_2^{2c_2} \dots Q_r^{2c_r}$$

with $(\frac{P_i}{T}) = 1$ and $(\frac{Q_j}{T}) = -1$ for all i, j , we have

$$r_T(f) = 2 \prod_{i=1}^k (a_i + 1).$$

Note that $\delta_T(f) = r_T(f)/2$ is a multiplicative function. Let $\mathcal{M}$ and $\mathcal{P}$ be the set of monic polynomials and the set of monic irreducibles in $\mathbb{F}_q[T]$ respectively. We want to study the Dirichlet series

$$L_{T,i}(s) = \sum_{f \in \mathcal{M}} \delta_T^i(f) |f|^{-s}$$

for $i = 1, 2$, where $|f| = q^{\deg(f)}$. Since $\delta_T(f)$ is multiplicative, we have a product of local factors

$$L_{T,i}(s) = \prod_{R \in \mathcal{P}} \left(\sum_{k=0}^{\infty} \delta_T^i(R^k) |R|^{-ks} \right),$$

where

$$\delta_T^i(R^k) = \begin{cases} (k+1)^i & \text{if } (\frac{R}{T}) = 1, \\ 1 & \text{if } R = T, \\ 1 & \text{if } (\frac{R}{T}) = -1 \text{ and } 2 \mid k, \\ 0 & \text{if } (\frac{R}{T}) = -1 \text{ and } 2 \nmid k. \end{cases}$$

Let χ_T be the quadratic character given by $\chi_T(f) = \left(\frac{f}{T}\right)$. The associated L series is

$$L_{\chi_T}(s) = \sum_{f \in \mathcal{M}} \chi(f) |f|^{-s} = \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 + |Q|^{-s})^{-1}. \quad (4.2)$$

Since χ_T is defined modulo a linear polynomial, $L_{\chi_T}(s) = 1$. The zeta function in $\mathbb{F}_q$ is given by

$$\begin{aligned} \zeta_q(s) &= \sum_{f \in \mathcal{M}} |f|^{-s} = (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-s})^{-1} \\ &= \frac{1}{1 - q^{1-s}}. \end{aligned} \quad (4.3)$$

Theorem 4.1.1. *We have*

$$L_{T,1}(s) = \zeta_q(s).$$

Proof. From the Euler product and the description of $\delta_2(P^k)$ provided above, we get

$$\begin{aligned} L_{T,1}(s) &= \left(\sum_{k=0}^{\infty} q^{-ks} \right) \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1) |P|^{-ks} \right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(\sum_{k=0}^{\infty} |Q|^{-2ks} \right) \\ &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-2} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1}. \end{aligned}$$

Comparing this with (4.1) and (4.3), we get

$$L_{T,1}(s) = \zeta_q(s).$$

□

Note that this also follows from the fact that $F_q[T][\sqrt{-T}] = F_q[\sqrt{-T}]$ is isomorphic to $F_q[U]$ for an indeterminate U . For the Dirichlet series associated to the square of r_T , we have

Theorem 4.1.2. *We have*

$$L_{T,2}(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1 + q^{-s})}.$$

Proof. From the Euler product and the description of $\delta_T(R^k)$ provided at the beginning of the section, we get

$$\begin{aligned}
L_{T,2}(s) &= \left(\sum_{k=0}^{\infty} q^{-ks} \right) \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^2 |P|^{-ks} \right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(\sum_{k=0}^{\infty} |Q|^{-2ks} \right) \\
&= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(2(1 - |P|^{-s})^{-3} - (1 - |P|^{-s})^{-2} \right) \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1} \\
&= \zeta_q(s) L_{\chi_T}(s) \left[\prod_{\left(\frac{P}{T}\right)=1} \left(2(1 - |P|^{-s})^{-1} - 1 \right) \right] \\
&= \zeta_q(s) L_{\chi_T}(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1 + |P|^{-s})}{(1 - |P|^{-s})} \\
&= \zeta_q(s) L_{\chi_T}(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1 - |P|^{-2s})}{(1 - |P|^{-s})^2}.
\end{aligned}$$

Here we used the fact that

$$\frac{2}{(1-x)^3} - \frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)^2 x^k.$$

We now multiply and divide the equation by $\prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})$. We get

$$L_{T,2}(s) = \zeta_q(s) L_{\chi_T}(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1 - |P|^{-2s})}{(1 - |P|^{-s})^2} \prod_{\left(\frac{Q}{T}\right)=-1} \frac{(1 - |Q|^{-2s})}{(1 + |Q|^{-s})(1 - |Q|^{-s})}.$$

Using the fact that

$$\zeta_q(2s) = (1 - q^{-2s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-2s})^{-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1},$$

we see that

$$L_{T,2}(s) = \frac{\zeta_q(s) L_{\chi_T}(s)}{\zeta_q(2s) (1 - q^{-2s})} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-2} \prod_{\left(\frac{Q}{T}\right)=-1} (1 + |Q|^{-s})^{-1} (1 - |Q|^{-s})^{-1}.$$

Further, using (4.1) and (4.3), we get

$$L_{T,2}(s) = \frac{\zeta_q^2(s) L_{\chi_T}^2(s) (1 - q^{-s})}{\zeta_q(2s) (1 - q^{-2s})}.$$

Using the fact that $L_{\chi_T}(s) = 1$, we have the result. □

Using the Dirichlet series $L_{T,i}(s)$ for $i = 1, 2$, we prove Theorem 1.1.5.

Proof of Theorem 1.1.5. For the first moment, we have from Theorem 4.1.1 that

$$L_{T,1}(s) = \zeta_q(s).$$

Expanding to retrieve the coefficient of q^{-ns} , we get

$$L_{T,1}(s) = \sum_{n=1}^{\infty} \frac{q^n}{q^{ns}}.$$

Hence we get that

$$\sum_{f \in \mathcal{M}_{n,q}} \delta_T(f) = q^n.$$

Now, since $r_T(f) = 2\delta_T(f)$, we have the first moment. For the second moment, we have from Theorem 4.1.2 that

$$L_{T,2}(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s) (1 + q^{-s})}.$$

We know that

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}} = \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}}.$$

Raising to the power of 2, we get

$$\zeta_q^2(s) = \left(\frac{1}{1 - q^{1-s}} \right)^2 = \sum_{n=0}^{\infty} \frac{(n+1)q^n}{q^{ns}}.$$

Lastly, we note that

$$\frac{1}{(1 + q^{-s})} = \sum_{n=0}^{\infty} \frac{(-1)^n}{q^{ns}}.$$

Combining all of the above, we get

$$L_{T,2}(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1+q^{-s})} = \left(\sum_{n=0}^{\infty} \frac{(n+1)q^n}{q^{ns}} \right) \left(\sum_{n=0}^{\infty} \frac{(-1)^n}{q^{ns}} \right) (1 - q^{1-2s}).$$

Extracting the coefficient of q^{-ns} from the right-hand side and using the fact that $r_T(f) = 2\delta_T(f)$, we have the second moment. $\square$

We note that the formulae obtained for the first and second moments in this section have no associated error and therefore work for all values of q and n .

4.2 First and second moments of r_1

Recall that r_1 denotes the number of representations by the quadratic form $A^2 + B^2$. In this section, we will analyse the first and second moments of r_1 . We will prove that,

Theorem 1.1.6. *Let $\mathbb{F}_q$ be a field of odd characteristic. The first and the second moments for $r_1(f)$ are given by*

$$\begin{aligned} \sum_{f \in \mathcal{M}_{2n,q}} r_1(f) &= (q+1)q^n, \\ \sum_{f \in \mathcal{M}_{2n,q}} r_1^2(f) &= (q+1)^2 ((n+1)q^{2n} - nq^{2n-1}), \end{aligned}$$

and

$$\sum_{f \in \mathcal{M}_{2n+1,q}} r_1(f) = \sum_{f \in \mathcal{M}_{2n+1,q}} r_1^2(f) = 0$$

Recall that $\mathcal{M}$ and $\mathcal{P}$ are the set of monic polynomials and the set of monic irreducibles in $\mathbb{F}_q[T]$ respectively. For $\delta_1(f) = r_1(f)/(q+1)$, define

$$M_i(s) := \sum_{f \in \mathcal{M}} \delta_1(f) |f|^{-s}$$

for $i = 1, 2$. Using multiplicativity, we have a product of local factors

$$M_i(s) = \prod_{P \in \mathcal{P}} \left(\sum_{k=0}^{\infty} \delta_1^i(P^k) |P|^{-ks} \right),$$

where

$$\delta_1^i(P^k) = \begin{cases} (k+1)^i & \text{if } \left(\frac{-1}{P}\right) = 1, \\ 1 & \text{if } \left(\frac{-1}{P}\right) = -1 \text{ and } 2 \mid k, \\ 0 & \text{if } \left(\frac{-1}{P}\right) = -1 \text{ and } 2 \nmid k. \end{cases}$$

Let ψ be the quadratic character given by $\psi(f) = \left(\frac{-1}{f}\right)$. The associated L series is

$$L_\psi(s) = \sum_{f \in \mathcal{M}} \psi(f) |f|^{-s} = \prod_{\left(\frac{-1}{U}\right)=1} (1 - |U|^{-s})^{-1} \prod_{\left(\frac{-1}{V}\right)=-1} (1 + |V|^{-s})^{-1}. \quad (4.4)$$

When $\deg(f)$ is even, $\psi(f) = 1$ and when $\deg(f)$ is odd, $\psi(f) = -1$. Hence, we have

$$L_\psi(f) = 1 - \frac{q}{q^s} + \frac{q^2}{q^{2s}} - \frac{q^3}{q^{3s}} + \cdots = \frac{1}{1 + q^{1-s}}. \quad (4.5)$$

Theorem 4.2.1. *We have*

$$M_1(s) = \zeta_{q^2}(s),$$

where, ζ_{q^2} is the zeta function in $\mathbb{F}_{q^2}[T]$.

Proof. From the Euler product and the description of $\delta_2(P^k)$ provided above, we get

$$\begin{aligned} M_1(s) &= \prod_{\left(\frac{-1}{U}\right)=1} \left(\sum_{k=0}^{\infty} (k+1) |U|^{-ks} \right) \prod_{\left(\frac{-1}{V}\right)=-1} \left(\sum_{k=0}^{\infty} |V|^{-2ks} \right) \\ &= \prod_{\left(\frac{-1}{U}\right)=1} (1 - |U|^{-s})^{-2} \prod_{\left(\frac{-1}{V}\right)=-1} (1 - |V|^{-2s})^{-1} \\ &= \prod_{\left(\frac{-1}{U}\right)=1} (1 - |U|^{-s})^{-2} \prod_{\left(\frac{-1}{V}\right)=-1} (1 - |V|^{-s})^{-1} (1 + |V|^{-s})^{-1}. \end{aligned}$$

We used the fact that

$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k.$$

Comparing this with (4.5), and (4.3), we get

$$M_1(s) = L_\psi(s) \zeta_q(s) = \frac{1}{(1 - q^{1-s})(1 + q^{1-s})} = \frac{1}{1 - q^{2-2s}} = \zeta_{q^2}(s).$$

□

Observe that the theorem can be understood more conceptually by noting that

$$\mathbb{F}_q[T][i] \cong \mathbb{F}_q[i][T] \cong \mathbb{F}_{q^2}[T].$$

Theorem 4.2.2. *We have*

$$M_2(s) = \frac{\zeta_{q^2}^2(s)}{\zeta_q(2s)}.$$

Proof. From the Euler product and the description of $\delta_2(P^k)$ provided at the beginning of the section, we get

$$\begin{aligned} M_2(s) &= \prod_{\left(\frac{-1}{U}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^2 |U|^{-ks} \right) \prod_{\left(\frac{-1}{V}\right)=-1} \left(\sum_{k=0}^{\infty} |V|^{-2ks} \right) \\ &= \prod_{\left(\frac{-1}{U}\right)=1} \left(2(1 - |U|^{-s})^{-3} - (1 - |U|^{-s})^{-2} \right) \prod_{\left(\frac{-1}{V}\right)=-1} (1 - |V|^{-2s})^{-1} \\ &= \zeta_q(s) L_\psi(s) \left[\prod_{\left(\frac{-1}{U}\right)=1} \left(2(1 - |U|^{-s})^{-1} - 1 \right) \right] \\ &= \zeta_q(s) L_\psi(s) \prod_{\left(\frac{-1}{U}\right)=1} \frac{(1 + |U|^{-s})}{(1 - |U|^{-s})} \\ &= \zeta_q(s) L_\psi(s) \prod_{\left(\frac{-1}{U}\right)=1} \frac{(1 - |U|^{-2s})}{(1 - |U|^{-s})^2}. \end{aligned}$$

Here we used the fact that

$$\frac{2}{(1-x)^3} - \frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)^2 x^k.$$

We now multiply and divide the equation by $\prod_{\left(\frac{-1}{V}\right)=-1} (1 - |V|^{-2s})$. We get

$$M_2(s) = \zeta_q(s) L_\psi(s) \prod_{\left(\frac{-1}{U}\right)=1} \frac{(1 - |U|^{-2s})}{(1 - |U|^{-s})^2} \prod_{\left(\frac{-1}{V}\right)=-1} \frac{(1 - |V|^{-2s})}{(1 + |V|^{-s})(1 - |V|^{-s})}.$$

Using the fact that

$$\zeta_q(2s) = \prod_{\left(\frac{-1}{U}\right)=1} (1 - |U|^{-2s})^{-1} \prod_{\left(\frac{-1}{V}\right)=-1} (1 - |V|^{-2s})^{-1},$$

we see that

$$\begin{aligned} M_2(s) &= \frac{\zeta_q(s)L_\psi(s)}{\zeta_q(2s)} \prod_{\left(\frac{-1}{U}\right)=1} (1 - |U|^{-s})^{-2} \prod_{\left(\frac{-1}{V}\right)=-1} (1 + |V|^{-s})^{-1}(1 - |V|^{-s})^{-1} \\ &= \frac{\zeta_q^2(s)L_\psi^2(s)}{\zeta_q(2s)} = \frac{\zeta_{q^2}^2(s)}{\zeta_q(2s)}. \end{aligned}$$

□

Using the Dirichlet series $M_i(s)$ for $i = 1, 2$, we compute the first and second moments for $r_1(f)$ as follows

Proof of Theorem 1.1.6. For the first moment, we have from Theorem 4.2.1 that

$$M_1(s) = \zeta_{q^2}(s).$$

Expanding to retrieve the coefficient of q^{-ns} , we get

$$M_1(s) = \sum_{n=1}^{\infty} \frac{q^{2n}}{q^{2ns}}.$$

Hence we get that

$$\sum_{f \in \mathcal{M}_{n,q}} \delta_1(f) = \begin{cases} q^n & \text{if } n \in 2\mathbb{Z} \\ 0 & \text{if } n \notin 2\mathbb{Z} \end{cases}$$

Now, since $r_1(f) = (q+1)\delta_1(f)$, we have the first moment. For the second moment, we have from Theorem 4.2.2 that

$$M_2(s) = \frac{\zeta_{q^2}^2(s)}{\zeta_q(2s)}.$$

We know that

$$\zeta_{q^2}(s) = \frac{1}{1 - q^{2-2s}} = \sum_{n=0}^{\infty} \frac{q^{2n}}{q^{2ns}}.$$

Raising to the power of 2, we get

$$\zeta_{q^2}^2(s) = \left(\frac{1}{1 - q^{2-2s}} \right)^2 = \sum_{n=0}^{\infty} \frac{(n+1)q^{2n}}{q^{2ns}},$$

since

$$\frac{1}{(1-x)^2} = \sum_{n=0}^{\infty} (n+1)x^n.$$

Also,

$$\zeta_q^{-1}(2s) = 1 - q^{1-2s}.$$

Hence, we get that

$$\begin{aligned} M_2(s) &= \frac{\zeta_q^2(s)}{\zeta_q(2s)} = \left(\sum_{n=0}^{\infty} \frac{(n+1)q^{2n}}{q^{2ns}} \right) (1 - q^{1-2s}) \\ &= 1 + \sum_{n=1}^{\infty} \frac{(n+1)q^{2n} - nq^{2n-1}}{q^{2ns}}. \end{aligned}$$

Once again, using the fact that $r_1(f) = (q+1)\delta_1(f)$, we have the second moment. $\square$

4.3 Higher Moments of r_T in the large degree limit

Recall that r_T denotes the number of representations by the quadratic form $A^2 + TB^2$ and $\delta_T = r_T/2$. In this section, we will first compute the L -series corresponding to δ_T^i for $i \geq 3$. We then make some remarks about the higher moments of r_T from the aforementioned L functions. We use the approach taken by Connors and Keating in [9]. The L -series $L_{T,i}(s)$ for $\delta_T^i(f)$ is given by

$$\begin{aligned} L_{T,i}(s) &= \left(\sum_{k=0}^{\infty} |T|^{-ks} \right) \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks} \right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(\sum_{k=0}^{\infty} |Q|^{-2ks} \right) \\ &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks} \right) \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1}. \end{aligned}$$

To further simplify this, we want to simplify the expression

$$\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks}.$$

To this aim, we define

$$\gamma_i(x) := \sum_{k=0}^{\infty} (k+1)^i x^k. \tag{4.6}$$

Then, $\gamma_i(x)$ satisfies the recurrence

$$\frac{d}{dx} (x\gamma_{i-1}(x)) = \gamma_i(x). \quad (4.7)$$

We can write $\gamma_i(x)$ as

$$\gamma_i(x) = \frac{1 + a_i x + \tilde{i}(x)}{(1-x)^{i+1}}, \quad (4.8)$$

where a_i are integers and $\tilde{i}(x)$ is a polynomial in x with the least exponent term x^2 . One way to see why we can write $\gamma_i(x)$ in this manner is to multiply and divide the right-hand side of (4.6) by $(1-x)^{i+1}$ and notice that the constant term in the numerator will be 1. Before we move to estimate $L_{T,i}(s)$, we compute the leading coefficient, a_i as it will prove to be useful. Substituting the form of $\gamma_i(x)$ given in (4.8) in the recurrence relation (4.7), we get

$$\begin{aligned} \gamma_{i+1}(x) &= \frac{d}{dx} \left(\frac{x(1 + a_i x + \tilde{i}(x))}{(1-x)^{i+1}} \right) \\ &= \frac{(1-x)^{i+1}[1 + 2a_i x + x\tilde{i}'(x) + \tilde{i}(x)] + (1-x)^i(i+1)[x + a_i x^2 + x\tilde{i}(x)]}{(1-x)^{2i+2}}. \end{aligned}$$

The coefficient of x in the numerator is $(2a_i + i)$. Hence, a_i satisfies the recurrence $a_{i+1} = 2a_i + i$. Using induction, we see that

$$a_i = 2^i - i - 1.$$

Coming back to our estimation of $L_{T,i}(s)$, we have

$$\begin{aligned} L_{T,i}(s) &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks} \right) \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1} \\ &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 + a_i |P|^{-s} + b_i |P|^{-2s} + \dots) (1 - |P|^{-s})^{-(i+1)} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1}. \end{aligned}$$

The product

$$\prod_{\left(\frac{P}{T}\right)=1} (1 + a_i |P|^{-s} + b_i |P|^{-2s} + \dots)$$

does not converge near $s = 1$ when $a_i \neq 0$. Hence, we define

$$A_i(s) = \prod_{\left(\frac{P}{T}\right)=1} (1 + a_i |P|^{-s} + b_i |P|^{-2s} + \dots) (1 - |P|^{-s})^{a_i}.$$

Note that by construction,

$$A_i(s) = \prod_{\left(\frac{P}{T}\right)=1} (1 + c_i |P|^{-2s} + \dots)$$

for some c_i and hence $A_i(s)$ converges at $s = 1$ since it does not have any linear term. Therefore, we have

$$\begin{aligned} L_{T,i}(s) &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-(i+1+a_i)} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1} A_i(s) \\ &= (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-2i} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1} A_i(s). \end{aligned} \quad (4.9)$$

Now,

$$\zeta_q(s) = \zeta_q(s) L_\chi(s) = (1 - q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-2} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-1}.$$

Hence,

$$\zeta_q^{2^{i-1}}(s) = (1 - q^{-s})^{-2^{i-1}} \prod_{\left(\frac{P}{T}\right)=1} (1 - |P|^{-s})^{-2^i} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{-2^{i-1}}.$$

Using this in equation (4.9), we get

$$\begin{aligned} L_{T,i}(s) &= \zeta_q^{2^{i-1}}(s) (1 - q^{-s})^{2^{i-1}-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{2^{i-1}-1} A_i(s) \\ &= \zeta_q^{2^{i-1}}(s) B_i(s), \end{aligned} \quad (4.10)$$

where

$$B_i(s) = (1 - q^{-s})^{2^{i-1}-1} \prod_{\left(\frac{Q}{T}\right)=-1} (1 - |Q|^{-2s})^{2^{i-1}-1} A_i(s).$$

Note that $B_i(s)$ is non-singular for $\text{Re}(s) \geq 1$. Now, we will use the L -series $L_{T,i}(s)$ to prove higher moments for $r_T(f)$.

Proof of Theorem 1.1.7. We note from (4.10) that

$$\begin{aligned} L_{T,i}(s) &= \zeta_q^{2^{i-1}}(s) B_i(s) \\ &= \frac{B_i(s)}{(1 - qu)^{2^{i-1}}}, \end{aligned}$$

where $u = q^{-s}$. Abusing the use of notations, we will write $\mathcal{L}_i(u)$ and $\mathcal{B}_i(u)$ in place of $L_{T,i}(s)$ and $B_i(s)$. Now, by Perron's formula,

$$\sum_{f \in \mathcal{M}_{n,q}} \delta_T^i(f) = \frac{1}{2\pi i} \oint_{|u|=q^{-1-\epsilon}} \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}} u^{n+1}} du.$$

We have a pole of order 2^{i-1} at $u = q^{-1}$. Hence, we enlarge our contour to collect the residue at the pole. Hence,

$$\sum_{f \in \mathcal{M}_{n,q}} \delta_T^i(f) = \frac{1}{2\pi i} \oint_{|u|=q^{-\epsilon}} \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}} u^{n+1}} du - \text{Res} \left(\frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}} u^{n+1}}; u = q^{-1} \right). \quad (4.11)$$

We know that $\mathcal{B}_i$ converges absolutely when $|u| < q^{-1}$. Also

$$|qu - 1| > q^{1-\epsilon} - 1 \gg 1.$$

Hence,

$$\frac{1}{(1-qu)^{2^{i-1}}} \ll 1.$$

So we get

$$\frac{1}{2\pi i} \oint_{|u|=q^{-\epsilon}} \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}} u^{n+1}} du \ll \oint_{|u|=q^{-\epsilon}} \frac{1}{u^{n+1}} du \ll q^{n\epsilon}.$$

For the next step, we have to compute the residue in (4.11). To do just that, we make a note that for a meromorphic function $f(z)$ with a pole of order r at $z = z_0$, the residue is given by

$$\text{Res}(f(z), z_0) = \frac{1}{(r-1)!} \lim_{z \rightarrow z_0} \frac{d^{r-1}}{dz^{r-1}} ((z - z_0)^r f(z)).$$

Let

$$g(u) = \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}} u^{n+1}}.$$

Hence using the above formula for the residue, we get

$$\begin{aligned} \text{Res}(g(u), q^{-1}) &= \frac{1}{(2^{i-1} - 1)!} \lim_{u \rightarrow q^{-1}} \frac{d^{2^{i-1}-1}}{du^{2^{i-1}-1}} \left((u - q^{-1})^{2^{i-1}} g(u) \right) \\ &= \frac{1}{(2^{i-1} - 1)!} \frac{1}{q^{2^{i-1}}} \frac{d^{2^{i-1}-1}}{du^{2^{i-1}-1}} \left(\frac{\mathcal{B}_i(u)}{u^{n+1}} \right) \Bigg|_{u=q^{-1}} \\ &= \frac{1}{(2^{i-1} - 1)!} \sum_{j=0}^{2^{i-1}-1} \frac{1}{q^{2^{i-1}}} \frac{d^j}{du^j} \left(\frac{1}{u^{n+1}} \right) \frac{d^{2^{i-1}-1-j}}{du^{2^{i-1}-1-j}} \mathcal{B}_i(u) \Bigg|_{u=q^{-1}}. \end{aligned}$$

The vertical bar in the last two equations here means evaluate at. The last line follows by using the product rule. Noting that the $j = 0$ term corresponds to the leading order term of the residue, we get

$$\begin{aligned}\text{Res}(g(u), q^{-1}) &= \frac{1}{(2^{i-1} - 1)!} \frac{1}{q^{2^{i-1}}} \left(\mathcal{B}_i(q^{-1}) \frac{-(n + 2^{i-1} - 1)!}{n!} q^{n+2^{i-1}} + O(q^{n+2^{i-1}-1}) \right) \\ &= -\mathcal{B}_i(q^{-1}) \binom{n + 2^{i-1} - 1}{n} q^n + O(q^{n-1}),\end{aligned}$$

where $\binom{s}{t}$ is the binomial coefficient s choose t . Plugging it back into (4.11) and using the relation $r_T(f) = 2\delta_T(f)$ gives us the result. $\square$

Chapter 5

A combinatorial approach

Recall that r_M represents the number of representations by the quadratic form

$$A^2 + MB^2.$$

This chapter aims to achieve the following objectives, each of which is discussed in a separate section:

- Obtain explicit formulas for higher moments of r_T in the large finite field limit.
- Obtain explicit formulas for higher moments of r_1 in the large finite field limit.

5.1 Higher Moments of r_T in the large finite field limit

In this section, we use another approach to estimate the moments of r_T . We will prove that

Theorem 1.1.8. *Let $\mathbb{F}_q$ be a field of odd characteristic and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i^{th} moment for r_T for a fixed n is given by*

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^i(f) = 2^i \gamma_{i,n} q^n - \alpha_{i,n} q^{n-1} + O(q^{n-2}),$$

where

$$\alpha_{i,n} = (2^{2i-1} - 2^i) \gamma_{i,n-1} + (2^{2i-1} + 2^{3i-2} - 2^{i-1} - 2^{i-1} 3^i) \gamma_{i,n-2}$$

and $\gamma_{i,n}$ is the binomial coefficient

$$\gamma_{i,n} = \binom{n + 2^{(i-1)} - 1}{n}.$$

The error term has a dependence on i and n .

Notice that in the large finite field limit, we are able to get the two leading terms compared to Theorem 1.1.8 in the large degree limit. Even though we are not able to find the coefficient of the leading term explicitly in Theorem 1.1.8, based on the explicit computations of the first and second moments, it seems they should agree with the leading coefficients obtained here in the large finite field limit, but to have a certain answer seems to be out of reach with the methods employed in the thesis.

Define the set $\mathcal{F}_n \subset \mathcal{M}_{n,q}$ consisting of all $f \in \mathcal{M}_{n,q}$ such that $b_q(f) = 1$, where

$$b_q(f) = \begin{cases} 1, & f = \alpha^2 + T\beta^2 \text{ for } \alpha, \beta \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

By the definition of $\mathcal{F}_n$, it is clear that

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^i(f) = \sum_{f \in \mathcal{F}_n} (r_T)^i(f).$$

for each $i \in \mathbb{N}$.

Let the letters P and Q denote primes such that $\left(\frac{P_i}{M}\right) = 1$ and $\left(\frac{Q_j}{M}\right) = -1, \forall i, j$. Partitioning $\mathcal{F}_n$ as in [3], we define

$$\begin{aligned} \mathcal{F}_{1,n} &= \{f \in \mathcal{F}_n : f = P_1 P_2 \dots P_r, P_i \neq P_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{F}_{2,n} &= \{f \in \mathcal{F}_n : f = T P_1 P_2 \dots P_r, P_i \neq P_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{F}_{3,n} &= \{f \in \mathcal{F}_n : f = P_1 P_2 \dots P_r Q_1^2, \deg Q_1 = 1, P_i \neq P_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{F}_{4,n} &= \{f \in \mathcal{F}_n : f = P_1^2 P_2 \dots P_r, \deg P_1 = 1, P_i \neq P_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{F}_{5,n} &= \{f \in \mathcal{F}_n : f = T P_1 P_2 \dots P_r Q_1^2, \deg Q_1 = 1, P_i \neq P_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{F}_{6,n} &= \mathcal{F}_n \setminus \bigcup_{i=1}^5 \mathcal{F}_{i,n}. \end{aligned}$$

The motive behind the partitioning is that the major contribution to the moments of $r_T(f)$ comes from specific types of polynomials described in the partitions. To show this, we will estimate the sum for each of the subsets of $\mathcal{F}_n$. Before the estimation, we state the version of the Chebotarev density theorem we will be using.

Lemma 5.1.1. [[3](#), Lemma 3.2] Let

$$\pi_{q;\alpha}(n) := \# \left\{ R \in \mathcal{M}_{n,q} : \left(\frac{R}{T} \right) = \alpha, \alpha = \pm 1, R \text{ irreducible} \right\}.$$

Then, we have

$$\begin{aligned} \pi_{q;\alpha}(1) &= \frac{q-1}{2}, \\ \pi_{q;\alpha}(2) &= \frac{1}{4}q^2 - \frac{1+\alpha}{4}q + \frac{\alpha}{4}, \text{ and} \\ \pi_{q;\alpha}(n) &= \frac{q^n}{2n} + O(q^{n-2}), \quad n \geq 3. \end{aligned}$$

Let us introduce some notations before we proceed. Let $\lambda \vdash n$ denote a partition $(\lambda_1, \lambda_2, \dots, \lambda_n)$ of n such that $\sum_{j=1}^n j\lambda_j = n$, i.e., λ_j is the number of times j appears in the partition. In the next few results, certain coefficients show up often. We define

$$\gamma_{i,n} = \sum_{\lambda \vdash n} \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!}.$$

Proposition 5.1.2. We have

$$\sum_{f \in \mathcal{F}_{1,n}} (r_T)^i(f) = 2^i \gamma_{i,n} q^n - 2^i (2^{(i-1)} \gamma_{i,n-1} + (2^{(i-1)} + 2^{2(i-1)}) \gamma_{i,n-2}) q^{n-1} + O(q^{n-2}).$$

Proof. Say $f \in \mathcal{F}_{1,n}$. We have $f = P_1 P_2 \dots P_k$ for primes P_j , $j \leq k$. The degrees of P_i form a partition of n say $(\lambda_1, \lambda_2, \dots, \lambda_n)$, where λ_j is the number of primes in the factorisation with degree j . Since every prime in the factorisation has exponent 1, Theorem [1.1.3](#) gives

$$r_T(f) = 2 \cdot 2^{\lambda_1 + \lambda_2 + \dots + \lambda_n}.$$

Hence, we have

$$\sum_{f \in \mathcal{F}_{1,n}} (r_T)^i(f) = 2^i \sum_{\lambda \vdash n} \prod_{j=1}^n \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

Note that the term $\binom{\pi_{q;1}(j)}{\lambda_j}$ denotes the number of ways to choose λ_j primes of degree j . From Lemma [5.1.1](#), we have

$$\begin{aligned}
\binom{\pi_{q;1}(1)}{\lambda_1} 2^{i\lambda_1} &= \frac{2^{(i-1)\lambda_1}}{\lambda_1!} q^{\lambda_1} - \frac{2^{(i-1)\lambda_1} \lambda_1^2}{\lambda_1!} q^{\lambda_1-1} + O(q^{\lambda_1-2}), \\
\binom{\pi_{q;1}(2)}{\lambda_2} 2^{i\lambda_2} &= \frac{2^{(i-1)\lambda_2}}{2^{\lambda_2} \lambda_2!} q^{2\lambda_2} - \frac{2^{(i-1)\lambda_2} 2\lambda_2}{2^{\lambda_2} \lambda_2!} q^{2\lambda_2-1} + O(q^{2\lambda_2-2}), \text{ and} \\
\binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j} &= \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} q^{j\lambda_j} + O(q^{j\lambda_j-2}).
\end{aligned}$$

Hence, we get

$$\prod_{j=1}^n \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j} = \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} q^n - \left(\lambda_1^2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} + 2\lambda_2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right) q^{n-1} + O(q^{n-2}).$$

Hence

$$\sum_{\lambda \vdash n} \prod_{j=1}^n \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j} = \gamma_{i,n} q^n - \sum_{\lambda \vdash n} \left(\lambda_1^2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} + 2\lambda_2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right) q^{n-1} + O(q^{n-2}). \quad (5.1)$$

Define C_λ and, D_λ as

$$C_\lambda = \left(\lambda_1^2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right), \quad D_\lambda = \left(2\lambda_2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right).$$

Also, define the partitions μ and ν as follows: μ is a partition of $n-1$ given by $(\lambda_1 - 1, \lambda_2, \dots, \lambda_{n-1})$ and ν is a partition of $n-2$ given by $(\lambda_1 - 2, \lambda_2, \dots, \lambda_{n-2})$. If $\lambda_1 = 0$, then, $C_\lambda = 0$ and hence such partitions do not contribute to our sum. If $\lambda_1 = 1$, then $\lambda_n = 0$ and

$$C_\lambda = 2^{(i-1)} \left(\prod_{j=1}^{n-1} \frac{2^{(i-1)\mu_j}}{j^{\mu_j} \mu_j!} \right),$$

where μ is a partition of $n-1$. So, when λ runs through all the partitions of n with $\lambda_1 = 1$, μ runs through all partitions of $n-1$ with $\mu_1 = 0$. If $\lambda_1 \geq 2$, $\lambda_{n-1} = \lambda_n = 0$ and

$$C_\lambda = \left(\lambda_1^2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right) = \left(\lambda_1 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right) + \left(\lambda_1(\lambda_1 - 1) \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right).$$

Hence

$$C_\lambda = 2^{(i-1)} \left(\prod_{j=1}^{n-1} \frac{2^{(i-1)\mu_j}}{j^{\mu_j} \mu_j!} \right) + 2^{2(i-1)} \left(\prod_{j=1}^{n-2} \frac{2^{(i-1)\nu_j}}{j^{\nu_j} \nu_j!} \right),$$

where μ is a partition of $n - 1$ and ν is a partition of $n - 2$. In this case, when λ runs through all partitions of n with $\lambda_1 \geq 2$, μ runs through all partitions of $n - 1$ with $\mu_1 \geq 1$ and ν runs through all partitions of $n - 2$. So overall, as λ runs through all partitions of n , μ and ν runs through all the partitions of $n - 1$ and $n - 2$. Hence

$$\begin{aligned} \sum_{\lambda \vdash n} C_\lambda &= 2^{(i-1)} \sum_{\mu \vdash (n-1)} \left(\prod_{j=1}^{m-1} \frac{2^{(i-1)\mu_j}}{j^{\mu_j} \mu_j!} \right) + 2^{2(i-1)} \sum_{\nu \vdash (n-2)} \left(\prod_{j=1}^{n-2} \frac{2^{(i-1)\nu_j}}{j^{\nu_j} \nu_j!} \right) \\ &= 2^{(i-1)} \gamma_{i,n-1} + 2^{2(i-1)} \gamma_{i,n-2}. \end{aligned} \quad (5.2)$$

If $\lambda_2 = 0$, then $D_\lambda = 0$ and hence such partitions do not contribute to the sums. If $\lambda_2 \geq 1$, $\lambda_{n-1} = \lambda_n = 0$. Hence

$$D_\lambda = \left(2\lambda_2 \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} \right) = 2^{(i-1)} \prod_{j=1}^{n-2} \frac{2^{(i-1)\xi_j}}{j^{\xi_j} \xi_j!},$$

where ξ is a partition of $n - 2$ given by $(\lambda_1, \lambda_2 - 1, \dots, \lambda_{n-2})$. We see that as λ runs through all partitions of n , ξ runs through all partitions of $n - 2$. Hence,

$$\sum_{\lambda \vdash n} D_\lambda = 2^{(i-1)} \sum_{\xi \vdash (n-2)} \left(\prod_{j=1}^{n-2} \frac{2^{(i-1)\xi_j}}{j^{\xi_j} \xi_j!} \right) = 2^{(i-1)} \gamma_{i,n-2}. \quad (5.3)$$

Finally using (5.2) and (5.3) in (5.1), we have our result. $\square$

Proposition 5.1.3. *We have,*

$$\sum_{f \in \mathcal{F}_{2,n}} (r_T)^i(f) = 2^i \gamma_{i,n-1} q^{n-1} + O(q^{n-2}),$$

Proof. We exploit the one to one correspondence between $\mathcal{F}_{2,n}$ and $\mathcal{F}_{1,n-1}$. For $f \in \mathcal{F}_{2,n}$, the degrees of P_i form a partition of $n - 1$ and so we have

$$\sum_{f \in \mathcal{F}_{2,n}} (r_T)^i(f) = 2^i \sum_{\lambda \vdash n-1} \prod_{j=1}^{n-1} \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

Using (5.1), we have the result. $\square$

Proposition 5.1.4. *We have*

$$\sum_{f \in \mathcal{F}_{3,n}} (r_T)^i(f) = 2^{(i-1)} \gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

Proof. Say $f = P_1 P_2 \dots P_r Q_1^2 \in \mathcal{F}_{3,n}$ with degree of Q_1 being 1. Let Q be fixed. Then the degrees of P_i form a partition of $n-2$ and for a fixed Q , we have a correspondence between $\mathcal{F}_{3,n}$ and $\mathcal{F}_{1,n-2}$. So we have

$$\sum_{f \in \mathcal{F}_{3,n}, Q \text{ fixed}} (r_T)^i(f) = 2^i \gamma_{i,n-2} q^{n-2} + O(q^{n-3}).$$

Note that the choice of Q does not influence the function $r_T(f)$. We have $\frac{q-1}{2}$ choices for Q . Hence,

$$\sum_{f \in \mathcal{F}_{3,n}} (r_T)^i(f) = \frac{q-1}{2} (2^i \gamma_{i,n-2} q^{n-2} + O(q^{n-3})) = 2^{(i-1)} \gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

□

Proposition 5.1.5. *We have*

$$\sum_{f \in \mathcal{F}_{4,n}} (r_T)^i(f) = \frac{6^i}{2} \gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

Proof. For $f \in \mathcal{F}_{4,n}$, say $f = P_1^2 P_2 \dots P_r$ with degree of P_1 being 1, the degrees of $P_2, P_3, \dots, P_r$ form a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_{n-2})$ of $n-2$ where λ_1 is the number of linear terms in the factorisation excluding P_1 . Also,

$$r_T(f) = 6 \cdot 2^{\lambda_1 + \lambda_2 + \dots + \lambda_{n-2}}.$$

Hence

$$\sum_{f \in \mathcal{F}_{4,n}} (r_T)^i(f) = \left(\frac{q-1}{2}\right) 6^i \sum_{\lambda \vdash n-2} \binom{\pi_{q;1}(1) - 1}{\lambda_1} 2^{i\lambda_1} \prod_{j=2}^{n-2} \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

Similar analysis gives the result. □

Proposition 5.1.6. *We have*

$$\sum_{f \in \mathcal{F}_{5,n} \cup \mathcal{F}_{6,n}} (r_T)^i(f) = O(q^{n-2}).$$

Proof. Exploiting the one to one correspondence between $\mathcal{F}_{5,n}$ and $\mathcal{F}_{3,n-1}$, we have from Proposition 5.1.4 that

$$\sum_{f \in \mathcal{F}_{5,n}} (r_T)^i(f) = O(q^{n-2}).$$

Let us first estimate the size of $\mathcal{F}_{6,n}$. Note that,

$$\# \{f \in \mathcal{F}_n : T^2 \mid f\} \leq \# \{f \in \mathcal{M}_{n,q} : T^2 \mid f\} = q^{n-2}.$$

Similarly, since there are q^d monic polynomials h of degree d , and for each h , there are at most q^{n-2d} possibilities for f/h^2 , it follows that

$$\# \{f \in \mathcal{F}_n : \exists h, \deg h > 1, h^2 \mid f\} \leq \sum_{2 \leq d \leq n/2} q^d \cdot q^{n-2d} = q^n \sum_{2 \leq d \leq n/2} q^{-d} \quad (5.4)$$

$$\leq q^n \cdot \frac{q^{-2}}{1 - q^{-1}} = \frac{q^{n-2}}{1 - q^{-1}} \leq \frac{4}{3} q^{n-2}, \quad (5.5)$$

where the last inequality uses $q \geq 2$.

Now, if $f \in \mathcal{F}_{6,n}$, then either $T^2 \mid f$, or f has a square factor h^2 with $\deg h > 1$. Therefore,

$$\#\mathcal{F}_{6,n} \leq q^{n-2} + \frac{4}{3} q^{n-2} = \frac{7}{3} q^{n-2}.$$

Lastly if $f = T^a P_1^{c_1} P_2^{c_2} \dots P_k^{c_k} Q_1^{2d_1} \dots Q_l^{2d_l} \in \mathcal{F}_{6,n}$, we have

$$r_T(f) = 2 \prod_{i=1}^k (c_i + 1).$$

The c_i are bounded above trivially by the degree of f , implying that $r_T(f)$ is bounded above trivially by $(n+1)^k$. We can of course offer sharper estimates, but this will do for now. Hence, the result follows, noting that the error term in the theorem depends of n . $\square$

The coefficients $\gamma_{i,n}$ also arise naturally in the study of Ewens sampling formula, which describes the probabilities associated with the number of different alleles observed in a sample. Using the sampling formula, we get that,

$$\gamma_{i,n} = \sum_{\lambda \vdash n} \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j} \lambda_j!} = \frac{(n + 2^{(i-1)} - 1)!}{n! (2^{(i-1)} - 1)!} = \binom{n + 2^{(i-1)} - 1}{n}.$$

Refer to [13] for more details.

Proof of Theorem 1.1.8. From the definition of $\mathcal{F}_n$,

$$\sum_{f \in \mathcal{M}_{n,q}} (r_T)^i(f) = \sum_{f \in \mathcal{F}_n} (r_T)^i(f).$$

Splitting the sum over partitions of $\mathcal{F}_n$ and using the estimates obtained in Proposition 5.1.2 to Proposition 5.1.6, we get the result. $\square$

5.2 Higher moments of r_1 in the large finite field limit

In this section, we will use the same approach used in the last section to estimate the moments of r_1 . We will prove that

Theorem 1.1.9. *Let $\mathbb{F}_q$ be a field of odd characteristic. For $i \in \mathbb{N}$, the i^{th} moment for r_1 is given by*

$$\sum_{f \in \mathcal{M}_{2n+1,q}} (r_1)^i(f) = 0$$

and

$$\sum_{f \in \mathcal{M}_{2n,q}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n} q^{2n} - (2^{i-1} - 1) \gamma_{i,n-1} q^{2n-1} + O(q^{2n-2}) \right),$$

where $\gamma_{i,n}$ is the binomial coefficient

$$\gamma_{i,n} = \binom{n + 2^{(i-1)} - 1}{n}.$$

The error term has a dependence on i and n .

Define the set $\mathcal{G}_n \subset \mathcal{M}_{n,q}$ consisting of all $f \in \mathcal{G}_{n,q}$ such that $s(f) = 1$, where

$$s(f) = \begin{cases} 1, & f = \alpha^2 + \beta^2 \text{ for } \alpha, \beta \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

Hence, we have that

$$\sum_{f \in \mathcal{M}_{n,q}} r_1(f) = \sum_{f \in \mathcal{G}_n} r_1(f).$$

We partition our set $\mathcal{G}_n$ as follows

$$\begin{aligned}\mathcal{G}_{1,n} &= \{f \in \mathcal{G}_n : f = U_1 U_2 \dots U_r, U_i \neq U_j \ \forall i \neq j, r \geq 0\}, \\ \mathcal{G}_{2,n} &= \{f \in \mathcal{G}_n : f = U_1 U_2 \dots U_r V_1^2, U_i \neq U_j \ \forall i \neq j, r \geq 0, \deg(V_1) = 1\}, \\ \mathcal{G}_{3,n} &= \mathcal{G}_n \setminus \bigcup_{i=1}^2 \mathcal{G}_{i,n}.\end{aligned}$$

Proposition 5.2.1. *We have*

$$\sum_{f \in \mathcal{G}_{1,2n+1}} (r_1)^i(f) = 0$$

and

$$\sum_{f \in \mathcal{G}_{1,2n}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n} q^{2n} - 2^{i-1} \gamma_{i,n-1} q^{2n-1} + O(q^{2n-2}) \right).$$

Proof. Say $f \in \mathcal{G}_{1,2n+1}$. Then $r_1(f) = 0$ and hence the moments are trivially zero. Say $f \in \mathcal{G}_{1,2n}$. We have

$$f = U_1 U_2 \dots U_r$$

for primes U_i for all $i \leq r$. We have

$$\deg(U_1) + \deg(U_2) + \dots + \deg(U_r) = 2n$$

where each of the terms $\deg(U_i)$ is even. Therefore, $\deg(U_i)/2$ form a partition of n say $(\lambda_1, \lambda_2, \dots)$ where λ_i is the number of primes of degree $2i$. For this choice of f , we have

$$r_1(f) = (q+1) \cdot 2^{\lambda_1 + \lambda_2 + \dots + \lambda_n}.$$

Hence, for the first moment,

$$\sum_{f \in \mathcal{G}_{1,2n}} (r_1)^i(f) = (q+1)^i \sum_{\lambda \vdash n} \prod_{j=1}^n \binom{\pi_q(2j)}{\lambda_j} 2^{i\lambda_j}, \quad (5.6)$$

where $\pi_q(2j)$ is the number of monic irreducibles of degree $2j$ in $\mathbb{F}_q[T]$. From Lemma 5.1.1,

$$\begin{aligned}\pi_q(2) &= \frac{q(q-1)}{2} \text{ and} \\ \pi_q(2j) &= \frac{q^{2j}}{2j} + O(q^{2j-2}) \text{ for } j \geq 2.\end{aligned}$$

Hence, we have that

$$\begin{aligned}
\binom{\pi_q(2)}{\lambda_1} &= \binom{q(q-1)/2}{\lambda_1} \\
&= \frac{1}{\lambda_1!} \left(\frac{q(q-1)}{2} \right)^{\lambda_1} - \frac{\lambda_1(\lambda_1-1)}{2\lambda_1!} \left(\frac{q(q-1)}{2} \right)^{\lambda_1-1} + O(q^{2\lambda_1-2}) \\
&= \frac{q^{2\lambda_1}}{2^{\lambda_1}\lambda_1!} - \frac{\lambda_1 q^{2\lambda_1-1}}{2^{\lambda_1}\lambda_1!} + O(q^{2\lambda_1-2}), \quad \text{and for } j \geq 2, \\
\binom{\pi_q(2j)}{\lambda_j} &= \binom{q^{2j}/2j + O(q^{2j-2})}{\lambda_j} = \frac{q^{2j\lambda_j}}{(2j)^{\lambda_j}\lambda_j!} + O(q^{2j\lambda_j-2}).
\end{aligned}$$

Substituting these into (5.6), we get

$$\begin{aligned}
\sum_{f \in \mathcal{G}_{1,2n}} (r_1)^i(f) &= (q+1)^i \sum_{\lambda \vdash n} \left(\frac{q^{2\lambda_1}}{2^{\lambda_1}\lambda_1!} - \frac{\lambda_1 q^{2\lambda_1-1}}{2^{\lambda_1}\lambda_1!} \right) 2^{i\lambda_1} \prod_{j \geq 2} \left(\frac{q^{2j\lambda_j}}{(2j)^{\lambda_j}\lambda_j!} 2^{i\lambda_j} \right) + O(q^{2n-2}) \\
&= (q+1)^i \sum_{\lambda \vdash n} \left[q^{2n} \prod_{j \geq 1} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} - q^{2n-1} \lambda_1 \prod_{j \geq 1} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} + O(q^{2n-2}) \right].
\end{aligned} \tag{5.7}$$

Recall that

$$\gamma_{i,n} = \sum_{\lambda \vdash n} \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}.$$

Using the sampling formula, we get that,

$$\gamma_{i,n} = \sum_{\lambda \vdash n} \prod_{j=1}^n \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} = \frac{(n + 2^{(i-1)} - 1)!}{n!(2^{(i-1)} - 1)!} = \binom{n + 2^{(i-1)} - 1}{n}.$$

Refer to [13] for more details. Let

$$U_\lambda = \lambda_1 \prod_{j \geq 1} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}.$$

Define a partition μ of $n-1$ as $(\lambda_1-1, \dots, \lambda_{n-1})$. If $\lambda_1 = 0$, $U_\lambda = 0$. If $\lambda_1 > 0$, $\lambda_n = 0$ and

$$U_\lambda = 2^{i-1} \prod_{j \geq 1} \frac{2^{(i-1)\lambda_j}}{j^{\mu_j}\mu_j!}.$$

So when λ runs through all partitions of n with $\lambda_1 \geq 1$, μ runs through all partitions of $n - 1$. Hence, we have

$$\sum_{\lambda \vdash n} U_\lambda = \sum_{\mu \vdash (n-1)} 2^{i-1} \prod_{j \geq 1} \frac{2^{(i-1)\mu_j}}{j^{\mu_j} \mu_j!} = 2^{i-1} \gamma_{i,n-1}.$$

Substituting this back into (5.7), we get

$$\sum_{f \in \mathcal{G}_{1,2n}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n} q^{2n} - 2^{i-1} \gamma_{i,n-1} q^{2n-1} + O(q^{2n-2}) \right).$$

□

Proposition 5.2.2. *We have*

$$\sum_{f \in \mathcal{G}_{2,2n+1}} (r_1)^i(f) = 0$$

and

$$\sum_{f \in \mathcal{G}_{2,2n}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n-1} q^{2n-1} + O(q^{2n-2}) \right).$$

Proof. If $f \in \mathcal{G}_{2,2n+1}$, $r_1(f) = 0$ and the first and second moments are trivially zero as we saw earlier working with the set $\mathcal{G}_{1,2n+1}$. Say $f \in \mathcal{G}_{2,2n}$. Then

$$f = U_1 U_2 \cdots U_r V_1^2$$

with $\deg V_1 = 1$. For a fixed choice of V_1 , the choices for f/V_1^2 are in one to one correspondence with the set $\mathcal{G}_{1,2n-2}$. Note that the factor of V_1^2 does not contribute to $r_1(f)$. Hence, exploiting the correspondence and using the previous proposition gives

$$\sum_{f \in \mathcal{G}_{2,2n}, V_1 \text{ fixed}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n-1} q^{2n-2} + O(q^{2n-3}) \right).$$

Now, noting that we have q choices of V_1 since there are q primes of degree 1 in $\mathbb{F}_q[T]$, we get

$$\sum_{f \in \mathcal{G}_{2,2n}} (r_1)^i(f) = (q+1)^i \left(\gamma_{i,n-1} q^{2n-1} + O(q^{2n-2}) \right).$$

□

At last, we note that the contribution to the first and second moments from the remaining polynomials has low order. To be more precise, we have

Proposition 5.2.3. *We have*

$$\sum_{f \in \mathcal{G}_{3,2n+1}} (r_2^*)^i(f) = 0$$

and

$$\sum_{f \in \mathcal{G}_{3,2n}} (r_2^*)^i(f) = O((q+1)^i q^{2n-2}) = O(q^{i+2n-2}).$$

Proof. If $f \in \mathcal{G}_{3,2n+1}$, $r_1(f) = 0$ and the moments are trivial, as in the proofs of the last propositions. We claim that the size of the set $\mathcal{G}_{3,2n}$ is $O(q^{2n-2})$. To see that, let $f \in \mathcal{G}_{3,2n}$. Then, there exists a polynomial h of degree $d \geq 2$ such that $h^2|f$. Hence,

$$\begin{aligned} |\mathcal{G}_{3,2n}| &\leq \#\{f \in \mathcal{M}_{2n,q}, h^2|f, \deg(h) \geq 2\} \\ &= \sum_{d=2}^n q^d \cdot q^{2n-2d} \\ &\leq q^{2n} \sum_{d=2}^{\infty} q^{-d} = O(q^{2n-2}). \end{aligned}$$

We used the fact that for a degree d polynomial h , we have q^d choices whereas, for f/h^2 , we have q^{2n-2} choices. We just summed it over all values of d from 2 to n . Given the size of the set $\mathcal{G}_{3,2n}$, the result follows. $\square$

All the estimates in this section collectively prove Theorem [1.1.9](#).

Chapter 6

Sums of triangular numbers

Recall that $t_s(n)$ denotes the number of representations of an integer n as a sum of s triangular numbers. In this chapter, we will study the singular series

$$\mathcal{S}^{(s)}(n) = \sum_{k \geq 0} A_k^{(s)}(n) = \prod_p \chi_p^{(s)}(n),$$

where the exponential sums $A_k^{(s)}$ and the local factors $\chi_p^{(s)}(n)$ are defined in (1.4) and (1.5) respectively. Studying the singular series will allow us to find asymptotic formulas for $t_s(n)$.

6.1 Summing up the singular series

We will be using the technique introduced by Hardy to evaluate the singular series. A more comprehensive treatment of these concepts can be found in Dickson's book [10], which we shall adopt as our primary reference. Recall that

$$t_s(n) = 2^{3-s} \frac{\pi^{\frac{s}{2}}}{\Gamma(\frac{s}{2})} (8n+s)^{\frac{s}{2}-1} \sum_{k \text{ odd} \geq 0} A_k^{(s)}(8n+s) + O((8n+s)^{\frac{s}{4}}). \quad (6.1)$$

and the singular series

$$\mathcal{S}^{(s)}(n) = \sum_{k \text{ odd} \geq 0} A_k^{(s)}(n) = \prod_{p \neq 2} \chi_p^{(s)}(n)$$

with

$$\chi_p^{(s)}(n) = \sum_{j \geq 0} A_{p^j}^{(s)}(n).$$

We begin by presenting several results from [10] that characterize the functions $A_k^{(s)}(n)$.

Lemma 6.1.1. ([10, Chapter 13, Lemma 15]) *Let p be an odd prime. If p is not a divisor of n ,*

$$\begin{aligned} A_p^{(s)}(n) &= -p^{\frac{-s}{2}}, \quad s \equiv 0 \pmod{4}, \quad \text{and} \\ A_p^{(s)}(n) &= -(-1)^{\frac{1}{2}(p-1)} p^{\frac{-s}{2}}, \quad s \equiv 2 \pmod{4}. \end{aligned}$$

If p divides n , we have

$$\begin{aligned} A_p^{(s)}(n) &= (p-1)p^{\frac{-s}{2}}, \quad s \equiv 0 \pmod{4}, \quad \text{and} \\ A_p^{(s)}(n) &= (-1)^{\frac{1}{2}(p-1)}(p-1)p^{\frac{-s}{2}}, \quad s \equiv 2 \pmod{4}. \end{aligned}$$

The behavior of $A_{p^u}^{(s)}(n)$ is determined by the parity of u . When u is odd, we have the following result.

Lemma 6.1.2. ([10, Chapter 13, Lemma 16]) *Assume that u is odd and > 1 . Then $A_{p^u}^{(s)}(n) = 0$ unless p^{u-1} divides n . If p^{u-1} strictly divides n ,*

$$A_{p^u}^{(s)}(n) = p^{-(\frac{s}{2}-1)(u-1)} A_p^{(s)}(\nu) \quad \text{if } n = p^{u-1}\nu, \quad \nu \not\equiv 0 \pmod{p}.$$

If p^u divides n ,

$$A_{p^u}^{(s)}(n) = \begin{cases} (p-1)p^{u-1-\frac{su}{2}}, & s \equiv 0 \pmod{4}, \\ (-1)^{\frac{1}{2}(p-1)}(p-1)p^{u-1-\frac{su}{2}}, & s \equiv 2 \pmod{4}. \end{cases}$$

For even values of u , we have the following result.

Lemma 6.1.3. ([10, Chapter 13, Lemma 17]) *Assume that u is even. Then $A_{p^u}^{(s)}(n) = 0$ unless p^{u-1} divides n . If p^{u-1} strictly divides n ,*

$$A_{p^u}^{(s)}(n) = -p^{u-1-\frac{su}{2}} \quad \text{if } n = p^{u-1}\nu, \quad \nu \not\equiv 0 \pmod{p}.$$

If p^u divides n ,

$$A_{p^u}^{(s)}(n) = (p-1)p^{u-1-\frac{su}{2}}.$$

With a complete characterization of $A_{p^u}^{(s)}(n)$, we now turn our attention to the local factors

$$\chi_p^{(s)}(n) = \sum_{j \geq 0} A_{p^j}^{(s)}(n).$$

From this point forward, we will freely utilize the preceding lemmas. Our investigation proceeds by distinguishing between two cases, depending on whether $s \equiv 0$ or $s \equiv 2 \pmod{4}$. We will denote by $\nu_p(n)$ the p -adic valuation of n . We have the following results.

Proposition 6.1.4. *When s is congruent to 0 modulo 4, the local factors $\chi_p^{(s)}(n)$ are given by*

$$\chi_p^{(s)}(n) = \begin{cases} 1 - p^{-\frac{s}{2}} & \text{if } p \nmid n, \\ (1 - p^{-\frac{s}{2}}) \left(\sum_{j=0}^{\nu_p(n)} p^{-j(\frac{s}{2}-1)} \right) & \text{if } p \mid n. \end{cases}$$

Proof. Let $n = 2^\alpha w_1^{a_1} w_2^{a_2} \cdots w_l^{a_l}$ and $\alpha(n)$ be the set

$$\alpha(n) = \{w_1, w_2, \dots, w_l\}.$$

For an odd prime $p \notin \alpha(n)$, we have

$$A_p^{(s)}(n) = -p^{-\frac{1}{2}s},$$

and

$$A_{p^u}^{(s)}(n) = 0$$

for all $u > 1$. Hence,

$$\chi_p^{(s)}(n) = 1 - p^{-\frac{1}{2}s}.$$

Say $p = w_i \in \alpha(n)$. Note that if u is odd and p^{u-1} strictly divides n , we get that

$$A_{p^u}^{(s)}(n) = p^{-(\frac{s}{2}-1)(u-1)} A_p^{(s)}\left(\frac{n}{p^u}\right) = -p^{u-1-\frac{su}{2}}$$

since $A_p^{(s)}(m) = -p^{-s/2}$ for all m which is exactly what we have when u is even as seen in Lemma 6.1.3. Hence, we have that for $\lambda > a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = 0.$$

For $\lambda = a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = -p^{\lambda-1-\frac{s}{2}\lambda} = -p^{-\lambda(\frac{s}{2}-1)-1}.$$

And for $\lambda < a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = (p-1)p^{\lambda-1-\frac{s}{2}\lambda} = (p-1)p^{-\lambda(\frac{s}{2}-1)-1}.$$

Summing them all up, we get

$$\chi_p^{(s)}(n) = 1 + \left(\sum_{j=1}^{a_i} (p-1)p^{-j(\frac{s}{2}-1)-1} \right) - p^{-(a_i+1)(\frac{s}{2}-1)-1}.$$

Splitting the factors in the summation, we get

$$\chi_p^{(s)}(n) = 1 + \left(\sum_{j=1}^{a_i} p^{-j(\frac{s}{2}-1)} - \sum_{j=1}^{a_i} p^{-j(\frac{s}{2}-1)-1} \right) - p^{-(a_i+1)(\frac{s}{2}-1)-1}.$$

This is the same as

$$\chi_p^{(s)}(n) = \left(\sum_{j=0}^{a_i} p^{-j(\frac{s}{2}-1)} - p^{-\frac{s}{2}} \sum_{j=0}^{a_i} p^{-j(\frac{s}{2}-1)-1} \right).$$

Hence we have

$$\chi_p^{(s)}(n) = (1 - p^{-\frac{s}{2}}) \sum_{j=0}^{a_i} p^{-j(\frac{s}{2}-1)}.$$

□

Before we proceed to the next result, we define $\chi_{-4}(n)$ to be the non-trivial character modulo 4 defined by

$$\chi_{-4}(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 6.1.5. *When s is congruent to 2 modulo 4, the local factors $\chi_p^{(s)}(n)$ are given by*

$$\chi_p^{(s)}(n) = \begin{cases} 1 - \chi_{-4}(p)p^{-\frac{s}{2}} & \text{if } p \nmid n, \\ (1 - \chi_{-4}(p)p^{-\frac{s}{2}}) \left(\sum_{j=0}^{\nu_p(n)} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)} \right) & \text{if } p \mid n. \end{cases}$$

Proof. Let $n = 2^\alpha w_1^{a_1} w_2^{a_2} \cdots w_l^{a_l}$ and $\alpha(n)$ be the set

$$\alpha(n) = \{w_1, w_2, \dots, w_l\}.$$

For an odd prime $p \notin \alpha(n)$, we have

$$A_p^{(s)}(n) = -(-1)^{\frac{1}{2}(p-1)} p^{-\frac{1}{2}s},$$

and

$$A_{p^u}^{(s)}(n) = 0$$

for all $u > 1$. Hence,

$$\chi_p^{(s)}(n) = 1 - \chi_{-4}(p) p^{-\frac{1}{2}s}.$$

Say $p = w_i \in \alpha(n)$. For $\lambda > a_i + 1$, irrespective of whether a_i is odd or even, we have

$$A_{p^\lambda}^{(s)}(n) = 0.$$

For $\lambda = a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = -\chi_{-4}(p) p^{\lambda-1-\frac{s}{2}\lambda} = -\chi_{-4}(p) p^{-\lambda(\frac{s}{2}-1)-1}.$$

And for $\lambda < a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = \begin{cases} (p-1) p^{\lambda-1-\frac{s}{2}\lambda} = (p-1) p^{-\lambda(\frac{s}{2}-1)-1} & \text{if } \lambda \text{ is even,} \\ \chi_{-4}(p) (p-1) p^{\lambda-1-\frac{s}{2}\lambda} = \chi_{-4}(p) (p-1) p^{-\lambda(\frac{s}{2}-1)-1} & \text{if } \lambda \text{ is odd.} \end{cases}$$

Hence for $\lambda < a_i + 1$,

$$A_{p^\lambda}^{(s)}(n) = (\chi_{-4}(p))^\lambda (p-1) p^{-\lambda(\frac{s}{2}-1)-1}.$$

Summing them all up, we get

$$\chi_p^{(s)}(n) = 1 + \left(\sum_{j=1}^{a_i} (\chi_{-4}(p))^j (p-1) p^{-j(\frac{s}{2}-1)-1} \right) - \chi_{-4}(p) p^{-(a_i+1)(\frac{s}{2}-1)-1}.$$

Splitting the factors in the summation, we get

$$\chi_p^{(s)}(n) = 1 + \left(\sum_{j=1}^{a_i} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)} - \sum_{j=1}^{a_i} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)-1} \right) - \chi_{-4}(p) p^{-(a_i+1)(\frac{s}{2}-1)-1}.$$

This is the same as

$$\chi_p^{(s)}(n) = \left(\sum_{j=0}^{a_i} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)} - \chi_{-4}(p) p^{-\frac{s}{2}} \sum_{j=0}^{a_i} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)-1} \right).$$

Hence we have

$$\chi_p^{(s)}(n) = \left(1 - \chi_{-4}(p)p^{-\left(\frac{s}{2}-1\right)-1}\right) \sum_{j=0}^{\nu_p(n)} (\chi_{-4}(p))^j p^{-j\left(\frac{s}{2}-1\right)}.$$

□

Having determined the local factors, we can now proceed to evaluate the singular series, as established in the following result. Let χ_1 and χ_2 represent the principal Dirichlet characters modulo 1 and 2, respectively.

Theorem 1.1.10. *The singular series $\mathcal{S}^{(s)}(n)$ converges to*

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \sigma_{\frac{s}{2}-1}(\chi_2, \chi_1; n)}{L\left(\frac{s}{2}, \chi_2\right)} \quad \text{if } s \equiv 0 \pmod{4},$$

and

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \sigma_{\frac{s}{2}-1}(\chi_{-4}, \chi_1; n)}{L\left(\frac{s}{2}, \chi_{-4}\right)} \quad \text{if } s \equiv 2 \pmod{4},$$

where $\sigma_k(\chi_1, \chi_2; n)$ denotes the generalised divisor function.

Proof. In the case $s \equiv 0 \pmod{4}$, for an odd prime p ,

$$\begin{aligned} \chi_p^{(s)}(n) &= \left(1 - p^{-\frac{s}{2}}\right) \sum_{j=0}^{\nu_p(n)} p^{-j\left(\frac{s}{2}-1\right)} \\ &= \left(1 - p^{-\frac{s}{2}}\right) p^{-\nu_p(n)\left(\frac{s}{2}-1\right)} \sum_{j=0}^{\nu_p(n)} p^{j\left(\frac{s}{2}-1\right)} \end{aligned}$$

Recall that our singular series is given by

$$\mathcal{S}^s(n) = \sum_{k \text{ odd}} A_k^{(s)}(n) = \prod_{p \text{ odd}} \chi(p).$$

Hence taking the product over the local factors, we get

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1}}{2^{-\nu_2(n)\left(\frac{s}{2}-1\right)}} \prod_{p \neq 2} \left(1 - p^{-\frac{s}{2}}\right) \prod_{p|n} \left(\sum_{j=0}^{\nu_p(n)} p^{j\left(\frac{s}{2}-1\right)}\right),$$

Observe that the second product on the right-hand side corresponds to the divisor function $\sigma_{\frac{s}{2}-1}(\chi_1, \chi_2; n)$ as we are only summing over the odd divisors. Identifying the zeta function within the first product, we obtain,

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \sigma_{\frac{s}{2}-1}(\chi_1, \chi_2; n)}{2^{-\nu_2(n)(\frac{s}{2}-1)} (1 - 2^{-\frac{s}{2}}) \zeta\left(\frac{s}{2}\right)}.$$

Noting that

$$\sigma_{\frac{s}{2}-1}(\chi_2, \chi_1; n) = 2^{\nu_2(n)(\frac{s}{2}-1)} \sigma_{\frac{s}{2}-1}(\chi_1, \chi_2; n)$$

and

$$L\left(\frac{s}{2}, \chi_2\right) = (1 - 2^{-\frac{s}{2}}) \zeta\left(\frac{s}{2}\right),$$

we have our result. In the case $s \equiv 2 \pmod{4}$,

$$\begin{aligned} \chi_p^{(s)}(n) &= \left(1 - \chi_{-4}(p) p^{-(\frac{s}{2}-1)-1}\right) \sum_{j=0}^{\nu_p(n)} (\chi_{-4}(p))^j p^{-j(\frac{s}{2}-1)} \\ &= \left(1 - \chi_{-4}(p) p^{-\frac{s}{2}}\right) (\chi_{-4}(p))^{\nu_p(n)} p^{-\nu_p(n)(\frac{s}{2}-1)} \sum_{j=0}^{\nu_p(n)} (\chi_{-4}(p))^j p^{j(\frac{s}{2}-1)}. \end{aligned}$$

Hence, taking the product over the local factors, we get

$$\mathcal{S}^{(s)}(n) = \frac{n^{-\frac{s}{2}+1} \chi_{-4}(n_{\text{odd}}) \sigma_{\frac{s}{2}-1}(\chi_1, \chi_{-4}; n)}{2^{-\nu_2(n)(\frac{s}{2}-1)} L\left(\frac{s}{2}, \chi_{-4}\right)},$$

where n_{odd} denotes the odd part of n . Noting that

$$\sigma_{\frac{s}{2}-1}(\chi_{-4}, \chi_1; n) = \chi_{-4}(n_{\text{odd}}) 2^{\nu_2(n)(\frac{s}{2}-1)} \sigma_{\frac{s}{2}-1}(\chi_1, \chi_{-4}; n),$$

we have our result. □

6.2 Number of representations by triangular numbers

At last, we will use the expressions obtained for the singular series to find formulas for the representation function $t_s(n)$. Recall that the generalised Bernoulli number $B_{n,\chi}$ is defined by the relation

$$\sum_{a=1}^M \frac{\chi(a) t e^{at}}{e^{Mt} - 1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n.$$

We have the following result.

Theorem 1.1.11. *The number $t_s(n)$ of representations of n as a sum of s triangular numbers satisfies the asymptotic formulas*

$$t_{4k}(n) \sim \frac{(-1)^k \cdot 8k}{B_{2k, \chi_2}} \sigma_{2k-1}(\chi_2, \chi_1; 2n+k)$$

and

$$t_{4k+2}(n) \sim \frac{(-1)^{k+1}(8k+4)}{B_{2k+1, \chi_{-4}}} \sigma_{2k}(\chi_{-4}, \chi_1; 4n+2k+1),$$

where $B_{n, \chi}$ denotes the generalised Bernoulli number associated to the Dirichlet character χ .

Proof. We begin by considering the case when $s = 4k$. Recalling from equation (6.1), we have the expression

$$t_s(n) = 2^{3-s} \frac{\pi^{\frac{s}{2}}}{\Gamma(\frac{s}{2})} (8n+s)^{\frac{s}{2}-1} \sum_{k \text{ odd} > 0} A_k^{(s)}(8n+s) + O((8n+s)^{\frac{s}{4}}).$$

Substituting $s = 4k$ into this formula, we obtain

$$t_{4k}(n) = 2^{3-4k} \frac{\pi^{2k}}{\Gamma(2k)} (8n+4k)^{2k-1} \mathcal{S}^{(4k)}(8n+4k) + O((8n+4k)^k). \quad (6.2)$$

Applying Theorem 1.1.10, it follows that

$$\mathcal{S}^{(4k)}(8n+4k) = \frac{(8n+4k)^{-2k+1} \sigma_{2k-1}(\chi_2, \chi_1; 8n+4k)}{L(2k, \chi_2)}.$$

Furthermore, we use the relation

$$\sigma_{2k-1}(\chi_2, \chi_1; 8n+4k) = 4^{2k-1} \sigma_{2k-1}(\chi_2, \chi_1; 2n+k).$$

Substituting these expressions back into equation (6.2), we obtain

$$t_{4k}(n) = \frac{2\pi^{2k}}{\Gamma(2k)L(2k, \chi_2)} \sigma_{2k-1}(\chi_2, \chi_1; 2n+k) + O((8n+4k)^k).$$

The value of the Dirichlet L -function $L(2k+1, \chi_{-4})$ can be computed, using [8, Theorem 3.4.14] as

$$L(2k, \chi_2) = \frac{(-1)^k (2\pi)^{2k} B_{2k, \chi_2}}{2^{2k+1} (2k)!},$$

Utilizing the explicit formulas for $\Gamma(2k)$ and $L(2k, \chi_2)$, we arrive at the simplified result:

$$t_{4k}(n) = \frac{(-1)^k 8k}{B_{2k, \chi_2}} \sigma_{2k-1}(\chi_2, \chi_1; 2n+k) + O((8n+4k)^k)$$

We now consider the case when $s = 4k+2$. Substituting $s = 4k+2$ in (6.1), we obtain

$$t_{4k+2}(n) = \frac{2^{1-4k} \pi^{2k+1}}{\Gamma(2k+1)} (8n+4k+2)^{2k} \mathcal{S}^{(4k+2)}(8n+4k+2) + O\left((8n+4k+2)^{k+\frac{1}{2}}\right). \quad (6.3)$$

Applying Theorem 1.1.10, it follows that

$$\mathcal{S}^{(4k+2)}(8n+4k+2) = \frac{(8n+4k+2)^{-2k} \sigma_{2k}(\chi_{-4}, \chi_1; 8n+4k+2)}{L(2k+1, \chi_{-4})}.$$

Furthermore, we use the relation

$$\sigma_{2k}(\chi_{-4}, \chi_1; 8n+4k+2) = 2^{2k} \sigma_{2k}(\chi_{-4}, \chi_1; 4n+2k+1).$$

Substituting these expressions back into equation (6.3), we obtain

$$t_{4k+2}(n) = \frac{2^{1-2k} \pi^{2k+1}}{\Gamma(2k+1) L(2k+1, \chi_{-4})} \sigma_{2k}(\chi_{-4}, \chi_1; 4n+2k+1) + O\left((8n+4k+2)^{k+\frac{1}{2}}\right).$$

The value of the Dirichlet L -function $L(2k+1, \chi_{-4})$ can be computed, using [8, Theorem 3.4.14] as

$$L(2k+1, \chi_{-4}) = \frac{(-1)^{k+1} (2\pi)^{2k+1} B_{2k+1, \chi_{-4}}}{2^{4k+2} (2k+1)!},$$

Utilizing the explicit formulas for $\Gamma(2k+1)$ and $L(2k+1, \chi_{-4})$, we arrive at

$$t_{4k+2}(n) = \frac{(-1)^{k+1} 4(2k+1)}{B_{2k+1, \chi_{-4}}} \sigma_{2k}(\chi_{-4}, \chi_1; 4n+2k+1) + O\left((8n+4k+2)^{k+\frac{1}{2}}\right).$$

□

References

- [1] Amir Akbary and Zafer Selcuk Aygin. Sums of triangular numbers and sums of squares. *J. Math. Anal. Appl.*, 517(1):Paper No. 126580, 26, 2023.
- [2] Atanas Atanasov, Rebecca Bellovin, Ivan Loughman-Pawelko, Laura Peskin, and Eric Potash. An asymptotic for the representation of integers as sums of triangular numbers. *Involve*, 1(1):111–121, 2008.
- [3] Lior Bary-Soroker, Yotam Smilansky, and Adva Wolf. On the function field analogue of Landau’s theorem on sums of squares. *Finite Fields Appl.*, 39:195–215, 2016.
- [4] Paul T. Bateman, Boris A. Datskovsky, and Marvin I. Knopp. Sums of squares and the preservation of modularity under congruence restrictions. In *Symbolic computation, number theory, special functions, physics and combinatorics (Gainesville, FL, 1999)*, volume 4 of *Dev. Math.*, pages 59–71. Kluwer Acad. Publ., Dordrecht, 2001.
- [5] Jonathan Michael Borwein and Kwok-Kwong Stephen Choi. Dirichlet series for squares of sums of squares: a summary. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 27–34. Amer. Math. Soc., Providence, RI, 2004.
- [6] Mireille Car. Sommes de deux carrés dans $\mathbf{F}_q[X]$ et problèmes de diviseurs. *Ann. Fac. Sci. Toulouse Math. (5)*, 5(2):89–108, 1983.
- [7] Mireille Car. Quadratic forms on $\mathbf{F}_q[T]$. *J. Number Theory*, 61(1):145–180, 1996.
- [8] Henri Cohen and Fredrik Strömberg. *Modular forms*, volume 179 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017. A classical approach.
- [9] R. D. Connors and J. P. Keating. Degeneracy moments for the square billiard. *J. Phys. A*, 32(3):555–562, 1999.

- [10] Leonard Eugene Dickson. *Studies in the Theory of Numbers*. Chelsea Publishing Company, New York, 1930. Reprint of the first edition; © 1930 by the University of Chicago and © 1957 by Eleanor D. Higinbotham.
- [11] G. H. Hardy. On the representation of a number as the sum of any number of squares, and in particular of five. *Trans. Amer. Math. Soc.*, 21(3):255–284, 1920.
- [12] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
- [13] S. Karlin and J. McGregor. Addendum to a paper of W. Ewens. *Theoret. Population Biol.*, 3:113–116, 1972.
- [14] Edmund Landau. *Vorlesungen über Zahlentheorie. Erster Band, zweiter Teil; zweiter Band; dritter Band*. Chelsea Publishing Co., New York, 1969.
- [15] Ken Ono, Sinai Robins, and Patrick T. Wahl. On the representation of integers as sums of triangular numbers. *Aequationes Math.*, 50(1-2):73–94, 1995.
- [16] R. A. Rankin. Sums of squares and cusp forms. *Amer. J. Math.*, 87:857–860, 1965.
- [17] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [18] Yash Totani. On the number of representations by quadratic forms and triangular numbers, Masters Thesis, 2019-2021.