PRIME POLYNOMIALS OVER FINITE FIELDS

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by

Paul Pollack

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 1, 2008

Examining Committee:

Carl Pomerance, Chair

Sergi Elizalde

Andrew Granville

Michael Rosen

Thomas Shemanske

Charles Barlowe
Dean of Graduate Studies

Abstract

The ring of univariate polynomials over a finite field shares many foundational arithmetic properties with the ring of rational integers. This similarity makes it possible for many problems in elementary number theory to be translated 'through the looking glass' into the universe of polynomials. In this thesis we look at polynomial analogues of Schinzel's Hypothesis H and other problems related to the multiplicative structure of polynomial values. We obtain results both in the situation where the finite field $\mathbf{F}_q$ is fixed and in the more uniform situation where $\mathbf{F}_q$ is allowed to vary. The most important tool in these investigations is Weil's Riemann Hypothesis for global function fields, which yields an explicit form of the Chebotarev density theorem for such fields.

Acknowledgements

FILL THIS IN.

Contents

Chapter 1

An overview of polynomial prime number theory

This thesis collects a number of results obtained by the author on the arithmetic properties of polynomials over finite fields, most of which concern the distribution of irreducible polynomials. Many of these investigations were motivated by well-known problems in the setting of ordinary (rational) arithmetic. In this introductory chapter we set the stage for our results by recounting the history of polynomial prime number theory.

1.1 The polynomial prime number theorem

It is easy to prove that there are infinitely many (nonassociated) primes in $\mathbf{F}_q[T]$; in fact, Euclid's familiar argument gives this conclusion for any infinite principal ideal domain with a finite unit group. It is, of course, too much to ask that such a general argument offer us any detailed information about the distribution of primes.

For the case of $\mathbf{F}_q[T]$, it is not difficult to formulate a plausible conjecture for the number of monic primes (irreducibles) of a given magnitude (degree). Table 1.1 shows the number of irreducible polynomials over $\mathbf{F}_2$ of degree n for $5 \le n \le 16$. This data suggests that if we set

$$\pi(q;n) := \#\{A \in \mathbf{F}_q[T] : A \text{ monic, irreducible, } \deg A = n\},$$

then $\pi(2;n)$ is approximately $2^n/n$; at the very least we expect that $\pi(2;n) \sim 2^n/n$ as $n \to \infty$. If we put $X = 2^n$, then $2^n/n$ is precisely $X/\log_2 X$, and the asserted asymptotic bears a startling similarity to the statement of the classical prime number theorem. (Here and below, $\log_q(\cdot)$ denotes the base q logarithm.) Moreover, there is nothing special about $q = 2$: a bit more experimentation suggests that for any fixed q,

$$\pi(q;n) \sim \frac{q^n}{n} \quad \text{as } n \to \infty. \tag{1.1}$$

If this is true, then it seems to merit being called the 'polynomial prime number theorem.'

Perhaps surprisingly, given the difficulty that seems inherent in even the simplest proofs of the classical prime number theorem, the polynomial version can be proved in a few lines. For fields with a prime number of elements, the proof appears already in work of Gauss, who thoroughly investigated the ring of polynomials over $\mathbf{F}_p$ for a planned eighth section of his masterwork *Disquisitiones Arithmeticae.* An early manuscript of section eight (*Disquisitiones generales de congruentiis*), attached to a 1797 draft of the *Disquisitiones Arithmeticae*, was found after Gauss's death; this manuscript appears never to have been translated into English, but is available in German as an appendix to Maser's version of the Disquisitiones [50]. For a complete

n	$\pi(2;n)$	ratio: $\pi(2;n)/2^n$	reciprocal ratio
5	6	0.18750000000	5.333333333
6	9	0.14062500000	7.111111111
7	18	0.14062500000	7.111111111
8	30	0.11718750000	8.533333333
9	56	0.10937500000	9.142857143
10	99	0.09667968750	10.34343434
11	186	0.09082031250	11.01075269
12	335	0.08178710938	12.22686567
13	630	0.07690429688	13.00317460
14	1161	0.07086181641	14.11197244
15	2182	0.06658935547	15.01741522
16	4080	0.06225585938	16.06274510

Table 1.1: The number of monic primes $\pi(2;n)$ of degree n over $\mathbf{F}_2$, together with the proportion of irreducibles and the reciprocal of this proportion.

discussion, see [46].

Though Gauss worked over $\mathbf{F}_p$, the argument runs just as well over an arbitrary finite field $\mathbf{F}_q$. Since each of the q^n monic polynomials of degree n over $\mathbf{F}_q$ factor uniquely as a product of prime polynomials, Gauss reasons that

$$q^n = \sum_{\alpha_1+2\alpha_2+3\alpha_3+\cdots=n} (1^{\alpha_1})(2^{\alpha_2})\dots(n^{\alpha_n}),$$

where Gauss's notation (i^{α_i}) refers to the number of ways of choosing α_i monic irreducible polynomials of degree i, with replacement. This identity can be recast in terms of generating functions;

$$\begin{aligned}\prod_{j=1}^{\infty}\left(\frac{1}{1-u}\right)^{\pi(q;j)} &= \prod_{j=1}^{\infty}\left(1+u^j+u^{2j}+\dots\right)^{\pi(q;j)}\\ &= 1+qu+q^2u^2+q^3u^3+\dots=\frac{1}{1-qu}.\end{aligned} \tag{1.2}$$

Taking the logarithmic derivative and multiplying by u, he deduces that

$$\sum_{d\geq 1} d\pi(q;d)\frac{u^d}{1-u^d} = \frac{qu}{1-qu}.$$

Now comparing the coefficients of u^n on both sides, we find that

$$q^n = \sum_{d|n} d\pi(q;d).$$

Gauss inverts this formula to find (adopting modern notation) that

$$\pi(q;n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}. \tag{1.3}$$

The main term in this expression occurs when $d = 1$, and a crude estimate of the remaining terms shows that

$$\pi(q;n) = \frac{1}{n}q^n + O\left(\frac{q^{n/2}}{n}\right), \tag{1.4}$$

with the implied constant 2. Actually it is easy to do somewhat better: Suppose $n > 1$ and let l be the least prime factor of n. The terms with $d > 1$ in the sum on the right of (1.3) are bounded by $q^{n/l}/n$ in absolute value, and decrease at least geometrically with ratio $1/q \leq 1/2$. Hence

$$\left|\pi(q;n) - \frac{q^n}{n}\right| \leq 2\frac{q^{n/l}}{n}. \tag{1.5}$$

We refer to (1.3) as *Gauss's formula for* $\pi(q;n)$, and to either of (1.4) or (1.5) as *Gauss's estimate for* $\pi(q;n)$.

Before proceeding we pause to note that we have proved a bit more than (1.1). The estimate (1.4) shows immediately that $\pi(q;n) \sim q^n/n$ not only when q is fixed and n tends to infinity, but in any case when $q^n \to \infty$. This uniform perspective will be important when we state our results below.

1.2 The Riemann Hypothesis for Function Fields and its consequences

1.2.1 Gauss from the viewpoint of Euler

The Riemann zeta function has proved itself the most fundamental object in the study of the distribution of rational primes, and so it may be surprising that there is no zeta function appearing in Gauss's proof of the prime number theorem for polynomials. Actually it is lurking just beneath the surface. For a nonzero polynomial A over $\mathbf{F}_q$, define its absolute value by $|A| := q^{\deg A}$; thus the absolute value of A measures the size of $\mathbf{F}_q[T]/(A)$ in the same way that the usual absolute value of a nonzero integer n measures the size of $\mathbf{Z}/n\mathbf{Z}$. Define

$$\zeta_q(s) = \sum_{A \text{ monic}} \frac{1}{|A|^s}.$$

As with the Riemann zeta function, our function $\zeta_q(s)$ converges and defines an analytic function for $\Re(s) > 1$. Moreover, because $|A|$ is totally multiplicative in A, there is an Euler factorization (in the region $\Re(s) > 1$):

$$\zeta_q(s) = \prod_{P \text{ monic, irreducible}} \frac{1}{1 - |P|^{-s}}. \tag{1.6}$$

All irreducibles of the same degree have the same absolute value, so that we may reorganize the right-hand product to arrive at

$$\prod_{d=1}^{\infty}\left(\frac{1}{1-q^{-sd}}\right)^{\pi(q;d)}.$$

Remarkably, it is easy to obtain an alternate expression for $\zeta_q(s)$, which at the same time yields its analytic continuation. Working first for $\Re(s) > 1$, we see that

$$\zeta_q(s) = \sum_{n=1}^{\infty} q^n \frac{1}{q^{ns}} = \frac{1}{1-q^{1-s}}. \tag{1.7}$$

But now the right hand side is analytic everywhere except at the obvious poles (viz. $s = 1 + 2\pi i m/\log q$). Putting $u = q^{-s}$, we recover Gauss's identity (1.2). The rest of the proof of the prime number theorem can be run as before.

What have we gained? Actually quite a lot; we can now see that the reason the prime number theorem for polynomials was so easy to obtain is that the appropriate zeta function has a simple form: it is an easily grasped rational function of q^{-s}.

1.2.2 Artin and the zeta functions of quadratic function fields

Artin was the first to obtain results which hinted that this nice behavior of $\zeta_q(s)$ is not an isolated phenomenon. In his 1924 thesis [2], he studies the arithmetic of quadratic function fields of odd characteristic: Let k be a finite field of odd characteristic, and let T be an element transcendental over k. Suppose $K/k(T)$ is a quadratic extension. Artin studies the integral closure R of $k[T]$ in K and treats all of the themes that are familiar from the number field setting:

- ideal theory of R,

- structure of the unit group of R,
- determination of the ramified primes in R,
- connection between ideal classes in R and classes of quadratic forms,
- division of the ideals of R into genera.

(Actually we have again taken some historical liberties; in his thesis Artin treats only the case when $k = \mathbf{F}_p$. He worked out, but never published, the analogous details for general k; see [3].)

These discussions constitute Part I of Artin's thesis, the so-called 'arithmetic' part. More germane for our purposes is the second, 'analytic' part, where Artin introduces the zeta function associated to a quadratic function field. Artin's zeta function is defined in analogy with the Dedekind zeta function and, as Artin showed, encodes much of the same information; e.g.,

- one can prove a class number formula in terms of the residue of the zeta function at $s = 1$,
- the L-functions governing the behavior of the distribution of primes in progressions which come from real characters may be viewed as factors of the zeta function of a quadratic function field.

Artin proves that the zeta function of a quadratic function field is always a rational function in $u = q^{-s}$ of the form

$$\frac{L(u)}{1 - qu},$$

where $L(u)$ is a polynomial in u of predictable degree. He also writes down a functional equation, which can be viewed as describing symmetries among the coefficient of L. Perhaps most stunning of all is that in the roughly forty examples he is able to compute, all the 'nontrivial' zeros of $L(u)$ have absolute value $q^{-1/2}$. (The precise sense of 'nontrivial' here is unimportant; it arises only because Artin's definition of the zeta function is somewhat unnatural, as mentioned below.) In other words, all the nontrivial zeros of the zeta function lie on the line $\Re(s) = 1/2$, in exact analogy with the classical Riemann Hypothesis.

Artin does not prove such a Riemann Hypothesis, but by adapting function-theoretic techniques familiar from the number field setting, he is at least able to show that his zeta function is zero-free on the line $\Re(s) = 1$. This already admits interesting applications. For example, he proves the following version of the prime number theorem for arithmetic progressions:

Theorem 1.2.1. *Fix polynomials $A, M \in \mathbf{F}_q[T]$ with M nonzero and $\gcd(A, M) = 1$. The number of monic irreducible polynomials P of degree n satisfying $P \equiv A \pmod{M}$ is*

$$\frac{1}{\varphi(M)} \frac{q^n}{n} + O\left(\frac{q^{\theta n}}{n}\right),$$

where $\theta < 1$ is a constant depending only on M.

Here and below, we write $\varphi(M)$ for the size of the unit group $(\mathbf{F}_q[T]/(M))^\times$.

This theorem improves on a result of Kornblum [75], according to which each such progression contains infinitely many monic primes P. (Actually Kornblum showed a bit more; see the discussion of his results Chapter 6.) It may seem surprising that Artin was able to obtain a 'power savings' in his error term (i.e., that he could take $\theta < 1$), given that such a result is still not known for the classical prime number theorem. The key is that the L-functions in question here are rational functions of q^{-s}, and so their values remain unchanged if s is shifted by $2\pi i/\log q$. This periodicity implies that if there are no zeros on $\Re(s) = 1$, then all zeros are bounded away from $\Re(s) = 1$.

1.2.3 Weil's Riemann Hypothesis: statement

Artin's definition of the zeta function of a quadratic function field K depends on representing K in the form $\mathbf{F}_q(T)(\sqrt{f(T)})$, and so depends implicitly on the choice of a transcendental element T. This defect can be remedied by working not with ideals but with divisors, as suggested by Schmidt [104]. If K is a global function field, set

$$\zeta_K(s) := \sum_{\mathfrak{a}\geq 0} \frac{1}{|\mathfrak{a}|^s} = \prod_{\mathfrak{p}} \frac{1}{1 - |\mathfrak{p}|^{-s}},$$

where the sum is taken over the effective divisors of K and the product is over the prime divisors. The precise definitions of divisor theory can be sidestepped here; what is important is that we have nailed down a canonical zeta function for every global function field K. When both definitions apply, Schmidt's differs from Artin's (and the definition of $\zeta_q(s)$ that we gave earlier for the rational function field) only in a finite number of Euler-product factors, corresponding to the are poles of T. For example, the zeta function of the rational function field $\mathbf{F}_q(T)$ is precisely

$$\zeta_{\mathbf{F}_q(u)}(s) = \frac{1}{1 - q^{-s}}\zeta_q(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})},$$

which includes an extra factor $1/(1 - q^{-s})$ with respect to (1.7).

As Schmidt showed in 1931 (ibid.), the zeta function $\zeta_K(s)$ is always a rational function of $u = q^{-s}$. Moreover, if K has genus g, then there is a univariate polynomial L_K with integer coefficients, constant term 1 and degree $2g$ with the property that

$$\zeta_K(s) = \frac{L_K(u)}{(1-u)(1-qu)},$$

where $u = q^{-s}$.

For arithmetic applications, it is important to understand the zeros of $\zeta_K(s)$ (equivalently, of $L_K(u)$). In the case when $K = \mathbf{F}_q(u)$, we have $L_K(u) \equiv 1$, and so there are no zeros. This can be seen as a meta-reason for why the prime number theorem in $\mathbf{F}_q[T]$ came to us so easily and with such a strong error term.

In general the situation is not so simple; however, we have the following fundamental and immensely powerful result, proved by Weil in 1948 [122]:

Riemann Hypothesis for Function Fields. *If K is any global function field, then the roots of $\zeta_K(s)$ lie on the line $\Re(s) = 1/2$. Equivalently, the inverse of each root of $L_K(T)$ has absolute value $\sqrt{q}$.*

Weil's original proof required a reworking of the foundations of algebraic geometry. The Riemann Hypothesis now admits a more or less elementary proof, due to Bombieri; see, e.g., [111, Chapter V].

1.2.4 Weil's Riemann Hypothesis: consequences

The Riemann Hypothesis for Function Fields is useful in many circumstances. Here are two examples which will prove important in the sequel:

First, the Riemann Hypothesis offers a handle on the distribution of power residues in finite fields. To take a classical example, fix a positive integer $n \geq 1$, and fix integers $\epsilon_i = \pm 1$ for $1 \leq i \leq n$. If p is an odd prime, how many integers

$a \in [0, p-1]$ satisfy

$$\left(\frac{a+i}{p}\right) = \epsilon_i$$

for all $1 \leq i \leq n$? On probabilistic grounds this number should be roughly $p/2^n$; the Riemann Hypothesis for Function Fields yields a count of

$$\frac{p}{2^n} + O(p^{1/2}),$$

where the implied constant depends only on n. This estimate is easy to prove directly for $n = 1$ and 2, but nontrivial already for $n = 3$. (For these cases, see [1, Chapter 10].) Davenport succeeded in proving the estimate when $n = 4$ or $n = 5$ but only with the weaker error term $O(p^{3/4})$. There is reason to believe that the first result towards Weil's Riemann Hypothesis, namely Hasse's proof of the genus 1 case (which gives the above estimate when $n = 4$), may have been a result of a challenge from the problem-solver Davenport to the theory-builder Hasse to put his algebra to good use! (See [100, §3.3].) In Chapter 3, we will need a result on configurations of power-residues of a very similar flavor, and we will obtain it from an estimate for character sums (essentially due to Lenstra and Wan [119]) that comes from Weil's Riemann Hypothesis.

Second, the Riemann Hypothesis allows one to produce useful, explicit versions of various estimates in prime number theory. For example, one can show that $\theta = 1/2$ is permissible in Artin's Theorem 1.2.1, and at the same make explicit the dependence of the implied constant on p, A and M. In fact one can be a bit more general: as pointed out by Hayes [60] one can obtain analogous formulas for the number of primes which lie in a given arithmetic progression *and* whose first several coefficients are prescribed. We will obtain and apply formulas of this type in Chapter 2, where additional references are given.

The applications appearing in the second half of this thesis depend heavily on a function field analogue of the Chebotarev density theorem. An explicit version of this result, resting on Weil's Riemann Hypothesis, was used by Cohen [27] and Ree [94] to confirm a conjecture of Chowla: for prime $p > p_0(n)$, there is always an irreducible of the form $T^n + T + a$ over $\mathbf{F}_p$. These papers were the inspiration for our work in Chapters 4–7. Cohen has written extensively on this method; see, e.g., [28], which discusses some of the same problems considered by Hayes (op. cit.) but obtains estimates useful in different ranges of the parameters.

Remark. For a complete history of Weil's Riemann Hypothesis, see the series of papers by Roquette ([99], [100], [101]).

1.3 Hypothesis H and its polynomial analogue

> Since the number of all primes is infinite ... we have the question of whether the number of primes, which for example are contained in the form $aa + 1$, is also infinite .... If these are also infinite, one could also ask the same question for the primes of the form $a^4 + 1$ or $a^8 + 1$, etc. – L. Euler [45]

> ...I do not mean to deny that there are mathematical truths, morally certain, which will defy and will probably to the end of time continue to defy proof, as, *e.g.*, that every indecomposable integer polynomial function must represent an infinitude of primes. – J. J. Sylvester [113]

1.3.1 The classical situation

At this point in our historical survey we narrow our focus to a specific class of problems in prime number theory, those concerning prime values of polynomials. As the quotation from Euler demonstrates, particular problems of this type have long been of interest; however, the first formulation of a precise conjecture had to wait until Bunyakovsky in 1857 [14]:

Conjecture 1.3.1 (Bunyakovsky's conjecture)**.** *Suppose $f(T)$ is a nonconstant polynomial with integer coefficients and positive leading coefficient. Moreover, suppose that f is irreducible in $\mathbf{Z}[T]$ and that there is no prime p which divides $f(n)$ for every integer value of n. Then $f(n)$ is prime for infinitely many positive integer values of n.*

The condition on the primes dividing $f(n)$ is needed to exclude examples like $f(T) = T^2 + T + 2$, which assumes only even values.

Bunyakovsky's conjecture was later generalized to a finite family of polynomials by Schinzel, who with Sierpiński [103] gave several applications to elementary number theory:

Conjecture 1.3.2 (Hypothesis H)**.** *Suppose $f_1(T), \dots, f_r(T)$ are nonconstant polynomials with integer coefficients and positive leading coefficients. Moreover, suppose that each f_i is irreducible in $\mathbf{Z}[T]$, and that there is no prime p for which*

$$f_1(n)f_2(n)\cdots f_r(n) \equiv 0 \pmod{p}$$

for every value of n. Then there are infinitely many positive integers n for which $f_1(n), \dots, f_r(n)$ are simultaneously prime.

In the case of a single linear polynomial, Hypothesis H amounts to Dirichlet's 1837 theorem on primes in progressions. Several other cases of Hypothesis H correspond to well-known problems in number theory; e.g., when $r = 1$ and $f_1 = T^2 + 1$ we have exactly Euler's conjecture mentioned above, and when $f_1 = T, f_2 = T + 2$, we have the celebrated twin prime conjecture. But Dirichlet's theorem remains the only proven case of Hypothesis H. In this respect the situation is unchanged from when Sylvester made his rather gloomy prediction.

Despite the difficulties in proving any qualitative conjecture of this type beyond Dirichlet's theorem, it is easy to go a bit further and formulate quantitative predictions along the same lines. The first plausible predictions of this type are due to Hardy and Littlewood [56], via a heuristic application of the circle method. However, similar predictions can also be derived by purely probabilistic reasoning. Let us consider the problem of estimating the number of twin prime pairs $p, p + 2$ with $p \leq x$. The prime number theorem can be viewed as asserting that a number near n is prime with probability roughly $1/\log n$. Thus we expect, under the assumption of independence, that

$$\#\{p \leq x : p, p+2 \text{ prime}\} \approx \sum_{n \leq x} \frac{1}{\log(n) \log{(n+2)}};$$

this last sum is easily shown to be asymptotically $x/\log^2 x$.

However, the assumption of independence is clearly untenable in this case; e.g., if $n > 2$ is prime, then n is odd, and so $n + 2$ is automatically odd. Thus $n + 2$ already has a leg up on being prime!

To obtain a precise conjecture, we need to understand these deviations from independence. An integer is composite exactly when it has a nontrivial prime factor.

This suggests we compare the probability that neither entry of a random pair of integers is divisible by the prime p with the probability that neither element of our special pair $(n, n+2)$ is divisible by p. The former occurs (ignoring the niceties required to quantify 'random') with probability $(1 - 1/p)^2$, and the latter with probability $(1 - \omega(p)/p)$, where

$$\omega(p) := \#\{n \bmod p : n(n+2) \equiv 0 \pmod{p}\}.$$

When $p > 2$, we have $\omega(p) = 2$, and so

$$\frac{(1 - \omega(p)/p)}{(1 - 1/p)^2} = \frac{1 - 2/p}{(1 - 1/p)^2} = 1 - \frac{1}{(p-1)^2}.$$

On the other hand, when $p = 2$ we have $\omega(p) = 1$, and the corresponding ratio is precisely 2. This argument, coupled with a healthy dose of optimism, motivates the following prediction:

Conjecture 1.3.3 (Quantitative twin prime conjecture)**.** *If $\pi_2(x)$ denotes the number of twin prime pairs $p, p+2$ with $p \leq x$, then*

$$\pi_2(x) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{\log^2 x} \quad \textit{as } x \to \infty.$$

This argument appears to originate with Selmer in 1942 [106]. Whatever one's opinion of this reasoning, Conjecture 1.3.3 is supported by a massive accumulation of numerical evidence. See, e.g., the online tables of Nicely [83].

Hardy and Littlewood never formulated a quantitative conjecture of the same generality as Hypothesis H, though this seems to have been within their power. This was left to Bateman and Horn [8]:

Conjecture 1.3.4 (Hardy and Littlewood, Bateman and Horn)**.** *Suppose that $f_1(T), \dots, f_r(T) \in \mathbf{Z}[T]$ are nonassociated polynomials with positive leading coefficients, all irreducible in $\mathbf{Z}[T]$. For each prime p, define*

$$\omega(p) := \#\{n \bmod p : f_1(n)f_2(n)\cdots f_r(n) \equiv 0 \pmod{p}\}.$$

Assume that $\omega(p) < p$ for all p. Then

$$\#\{n \le x : f_1(n), \dots, f_r(n) \text{ are all prime}\} = (1 + o(1))\frac{\mathfrak{S}(f_1, \dots, f_r)}{\prod_{i=1}^{r} \deg f_i} \frac{x}{\log^r x},$$

as $x \to \infty$. Here the "singular series" $\mathfrak{S}(f_1, \dots, f_r)$ is defined by

$$\mathfrak{S}(f_1, \dots, f_r) := \prod_p \left(1 - \frac{\omega(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-r}.$$

We leave to the reader the straightforward task of generalizing the heuristic argument given for the twin prime conjecture to this more general context.

One can show that the singular series $\mathfrak{S}(f_1, \dots, f_r)$ is always positive under the hypotheses of Conjecture 1.3.4, so that Conjecture 1.3.4 implies the qualitative Hypothesis H (Conjecture 1.3.2). Conjecture 1.3.4 is proved only in the case of a single linear polynomial, where it coincides with the prime number theorem for arithmetic progressions.

1.3.2 A surprise in characteristic p, and the work of Conrad, Conrad, and Gross

Is there a plausible function field analogue of Hypothesis H, and if so, what is it? Here the situation is sufficiently complicated that we content ourselves with a discussion of the single-polynomial (Bunyakovsky) situation. Guided by our intuition from the number field setting, it is tempting to conjecture the following:

Conjecture 1.3.5 (Naive Bunyakovsky/Bateman-Horn conjecture over $\mathbf{F}_q[u]$)**.** *Let $f(T)$ be a polynomial in $\mathbf{F}_q[u][T]$. Suppose that $f(T)$ is irreducible in $\mathbf{F}_q[u][T]$, and that there is no prime P of $\mathbf{F}_q[u]$ that divides $f(g(u))$ for every polynomial $g(u) \in \mathbf{F}_q[u]$. Then there are infinitely many $g(u) \in \mathbf{F}_q[u]$ for which $f(g(u))$ is irreducible over $\mathbf{F}_q$. Moreover, the number of such $g(u)$ having degree n is*

$$(1+o(1))\frac{\mathfrak{S}(f)}{\deg_T f}\frac{(q-1)q^n}{n} \quad \textit{as } n \to \infty.$$

Here

$$\mathfrak{S}(f) = \prod_P \left(1 - \frac{\omega(P)}{|P|}\right)\left(1 - \frac{1}{|P|}\right)^{-1},$$
$$\textit{where} \quad \omega(P) = \#\{g(u) \bmod P : f(g(u)) \equiv 0 \pmod{P}\}.$$

Once again, the singular series $\mathfrak{S}(f)$ can be shown to be positive under the given hypotheses, so that the quantitative half of this conjecture is indeed a strengthening of the qualitative part.

One could quibble a bit with our formulation of Conjecture 1.3.5: Bunyakovsky's conjecture is a prediction about prime values of $f(n)$, where n ranges over positive values. One might argue that for the sake of analogy, in Conjecture 1.3.5 we ought only to sample over monic g. We ignore this objection for now but will return briefly to it later.

Is Conjecture 1.3.5 as well-supported by the numerical evidence as Conjecture 1.3.4? For many polynomials, computations (carried out by Conrad, Conrad, and

n	count	prediction	ratio
9	1624	1168.3	1.390
10	4228	3154.5	1.340
11	11248	8603.2	1.307
12	31202	23658.7	1.319
13	87114	65516.5	1.330
14	244246	182510.2	1.338
15	683408	511028.6	1.337
16	1914254	1437268.0	1.332

n	count	prediction	ratio
9	1404	1458.0	0.963
10	7776	3936.6	1.975
11	10476	10736.2	1.001
12	0	29524.5	0
13	82140	81760.2	1.005
14	455256	227760.4	1.999
15	637440	637729.2	1.000
16	0	1793613.4	0

Table 1.2: *Left hand table*: number of g of degree n for which $g(u)^{12}+(u+1)g(u)^6+u^4$ is irreducible over $\mathbf{F}_3$, vs. the number expected from Conjecture 1.3.5. *Right hand table*: number of g of degree n for which $g(u)^3+u$ is irreducible over $\mathbf{F}_3$, vs. expected number.

Gross [32]) do appear to confirm the prediction of Conjecture 1.3.5. Indeed, this seems to be the case whenever $f(T)$ is separable over $\mathbf{F}_q(u)$, i.e., whenever $f(T)$ is *not* a polynomial in T^p (where p is the characteristic of $\mathbf{F}_q$). In the remaining cases the conjecture sometimes appears correct, but there are also examples which point strongly in the opposite direction. See Table 1.3.2 for two such examples over $\mathbf{F}_3$, taken from [33]. Note that in the first example, the ratio appears to be tending not to 1, but to 4/3. In the second example, the ratios appear to be converging to limits depending on n mod 4, which go in the cycle $0, 1, 2, 1$.

As pointed out in [32], the falsity of Conjecture 1.3.5, even in its weaker, qualitative form, is implied by work of Swan [112] from 1962. Let q be a power of 2. Taking $m = 3$ in [112, Example, p.1102] we see that for every $g(u) \in \mathbf{F}_q[u]$, the polynomial

$$g(u)^8 + u^3$$

is either divisible by u, or has an even number of prime factors in $\mathbf{F}_q[u]$. In either case $g(u)^8 + u^3$ is reducible. This is true even though (as is easily checked) $T^8 + u^3$

satisfies all the conditions of Conjecture 1.3.5. Swan does not point out that his formulas falsify the naive polynomial analogue of Hypothesis H, but given that Schinzel's hypothesis had appeared in print only five years before, this omission is certainly understandable.

Driving Swan's result is a formula for the Möbius function of a polynomial in characteristic 2. (The Möbius μ function of a polynomial is defined to be zero if the polynomial is not squarefree, and $(-1)^r$ otherwise, where r is the number of its monic irreducible factors.) Here Swan is generalizing a result that had been derived much earlier in odd characteristic:

Corollary 1.3.6 (Pellet [87])**.** *If $f(T) \in \mathbf{F}_q[T]$ is a nonzero polynomial of degree n over $\mathbf{F}_q$ where q is odd, then*

$$\mu(f) = (-1)^n \chi(\mathrm{disc}(f)),$$

where χ is the quadratic character on $\mathbf{F}_q^\times$, and $\chi(0) = 0$.

(The existence of formulas of this type is rather surprising, as over $\mathbf{Z}$, no algorithm for determining the Möbius function is known which improves on factoring.) Conrad, Conrad, and Gross observe (see [33, Example 4.3]) that one can use this theorem of Pellet to cook up examples similar to Swan's over any finite field of odd order. Set $f(T,u) := T^{4q} + u^{2q-1} \in \mathbf{F}_q[u,T]$; it is easy to check that this polynomial satisfies the hypotheses of Conjecture 1.3.5. However, one can use Pellet's formula to show that $\mu(f(g(u))) = 0$ or 1 for every $g(u) \in \mathbf{F}_q[u]$. Thus $f(T,u)$ is a counterexample to the analogue of Bunyakovsky's conjecture.

These last two examples are quite extreme; the polynomials f involved admit no prime specializations at all. In both cases, this can be traced to the Möbius function only assuming the values 0 or 1 along the $\mathbf{F}_q[u]$-specializations of f. That is, the Möbius function is as biased there as possible. It is reasonable to expect that less severe biases of the Möbius function on the values $f(g(u))$ might skew prime-value statistics also, and that by quantifying these biases one could understand the more complicated and puzzling behavior of the examples in Table 1.3.2.

The idea that studying such Möbius biases could lead to a plausible analogue of Hypothesis H was first developed by Conrad, Conrad, and Gross. (But see [29], where Cohen notes that a similar explanation can be given for anomalous counts of irreducible 'windmill polynomials.') We have already recorded their observation that if f is not a polynomial in T^p, then both the qualitative and quantitative predictions of Conjecture 1.3.5 appears correct. So we may assume f is a polynomial in T^p. In this case Conrad, Conrad and Gross are able to prove a formula for the Möbius function at the specializations of f. Actually this is not quite accurate for $p = 2$, where it appears to be necessary to assume that f is a polynomial in T^4 and not merely T^2. Here is one consequence of their formula:

Theorem 1.3.7 (see [32, Theorem 4.8])**.** *Let $f(T)$ be a squarefree polynomial in $\mathbf{F}_q[u][T]$ with positive T-degree. Assume, moreover, that $f(T)$ is a polynomial in T^p when $p \neq 2$ and is a polynomial in T^4 when $p = 2$. When $p \neq 2$, let χ be the quadratic character on $\mathbf{F}_q^\times$.*

There is a nonzero $M = M_{f,q}$ in $\mathbf{F}_q[u]$ such that for $g_1 = c_1u^{n_1} + \dots$ and $g_2 = c_2u^{n_2} + \dots$ in $\mathbf{F}_q[u]$ with sufficiently large degrees n_1 and n_2,

$$g_1 \equiv g_2 \pmod{M}, \quad n_1 \equiv n_2 \pmod{4}, \quad \chi(c_1) = \chi(c_2) \Longrightarrow \mu(f(g_1)) = \mu(f(g_2))$$

when $p \neq 2$ *and*

$$g_1 \equiv g_2 \pmod{M}, \quad n_1 \equiv n_2 \pmod{4} \Longrightarrow \mu(f(g_1)) = \mu(f(g_2))$$

when $p = 2$.

Thus when g is sufficiently large, $\mu(f(g(T)))$ depends only on g mod M, n mod 4 and the quadratic character of the leading coefficient of g (when $p \neq 2$). The last dependence is our excuse for not insisting that g be monic from the start; it would have prevented us from observing an interesting phenomenon.

We can now describe the correction to Conjecture 1.3.5 proposed by Conrad, Conrad, and Gross: Suppose $f(T)$ satisfies the hypotheses of Theorem 1.3.7. Choose a polynomial $M = M_{f,q}$ as in Theorem 1.3.7 and define

$$\Lambda_q(f;n) := 1 - \frac{\sum_{\deg g = n, (f(g),M)=1} \mu(f(g))}{\sum_{\deg g = n, (f(g),M)=1} |\mu(f(g))|}.$$

Work of Poonen [93] implies that the denominator here is positive for large n; moreover, for large n the value of $\Lambda_q(f;n)$ is independent of the particular choice of M. So the tail-end of this sequence is a well-defined sequence of real numbers in the interval $[0,2]$.

The role of Λ is clearer if we impose a probabilistic interpretation. Let $f(T)$ be as in Conjecture 1.3.5. For $g(u) \in \mathbf{F}_q[u]$ of degree $n \gg 0$, the degree of $f(g(u))$, say N, behaves linearly in n (and, in particular, is independent of the particular choice of $g(u)$). We can now express Λ as a quotient of conditional probabilities: for

$n \gg 0$,

$$\Lambda_q(f;n) = \frac{\mathbf{Prob}(\mu(f(g)) = -1 \text{ for } \deg g = n \mid f(g) \text{ squarefree}, \gcd(f(g), M) = 1)}{\mathbf{Prob}(\mu(A) = -1 \text{ for } \deg A = N \mid A \text{ squarefree}, \gcd(A, M) = 1)}.$$

It is easy to check that this agrees with our earlier definition of Λ, once one verifies that the denominator here is $1/2$ for all large enough N, which is elementary.

Conjecture 1.3.8 (Conrad, Conrad, and Gross)**.** *Suppose $\mathbf{F}_q$ is a field of odd characteristic, and let $f(T) \in \mathbf{F}_q[u][T]$ have positive T-degree. Then $f(g(u))$ is irreducible for infinitely many $g(u) \in \mathbf{F}_q[u]$ if and only if the following conditions hold:*

(i) *$f(T)$ is irreducible in $\mathbf{F}_q(u)[T]$,*

(ii) *no irreducible P in $\mathbf{F}_q[u]$ divides $f(g(u))$ for every $g(u) \in \mathbf{F}_q[u]$,*

(iii) *$f(T) \notin \mathbf{F}_q[u][T^p]$, or $f(T) \in \mathbf{F}_q[u][T^p]$, but the periodic part of the sequence $\Lambda_q(f;n)$ is not identically zero.*

If these conditions hold, then the number of $g(u)$ of degree n for which $f(g(u))$ is irreducible is

$$(1 + o(1))\Lambda_q(f;n)\frac{\mathfrak{S}(f)}{\deg_T(f)}\frac{(q-1)q^n}{n} \quad (n \to \infty), \tag{1.8}$$

where $\Lambda_q(f;n)$ is interpreted as being identically 1 if $f(T) \notin \mathbf{F}_q[u][T^p]$. This asymptotic formula also holds when $\mathbf{F}_q$ has characteristic 2, if in (iii) we assume that $f(T) \notin \mathbf{F}_q[u][T^2]$, or that $f(T) \in \mathbf{F}_q[u][T^4]$.

Unfortunately when $p = 2$ and $f(T) \in \mathbf{F}_q[u,T]$ is a polynomial in T^2 but not in T^4, there is still no satisfactory conjecture (see the remarks in [32, §5] and [31]).

Using the proof of Theorem 1.3.7, Conrad, Conrad and Gross deduce that $\Lambda_q(f; n)$ is eventually periodic with minimal period length dividing 4. Moreover, one can prove (see [32, Examples 6.9, 6.10]) that in the first example of Table 1.3.2, $\Lambda_q(f; n) \equiv 4/3$ for large n, and that in the second example, $\Lambda_q(f; n)$ cycles over $1, 2, 1, 0$. The data of Table 1.3.2 thus serves to confirm Conjecture 1.3.8.

We conclude by remarking that it is not necessary to restrict to the Bunyakovsky situation where only irreducible specializations of a single polynomial are in view; analogous predictions can be given in the more general Hypothesis H scenario. One expects that the naive generalization of Hypothesis H (as well as the direct quantitative analogue of Conjecture 1.3.4) should be correct whenever dealing with a finite family of separable polynomials.

Remark. For a more detailed survey of the results of Conrad, Conrad, and Gross, see K. Conrad's article [33].

1.3.3 Other recent approaches to Hypothesis H in positive characteristic

As we have seen, there are polynomials in $\mathbf{F}_q[u][T]$ which do not admit a single irreducible specialization. It is natural to wonder what conditions could be imposed to preclude this rather unpleasant behavior. Conjecture 1.3.8 of course gives conditions of this type, but does not seem at all easy to prove. In this direction we have the following theorem of Bender and Wittenberg [9]:

Theorem 1.3.9. *Let $f_1, f_2, \ldots, f_r \in \mathbf{F}_q[u, T]$ be irreducible polynomials whose total degrees $\deg(f_i)$ satisfy $p \nmid \deg(f_i)(\deg(f_i) - 1)$ for all i. Assume that the curves*

$C_i \in \mathbf{P}^2(\mathbf{F}_q)$ defined as the Zariski closures of the affine curves

$$f_i(u,T) = 0$$

are smooth. Then for all large s, there are $a, b \in \mathbf{F}_{q^s}$ such that the polynomials $f_1(T, aT+b), \dots, f_r(T, aT+b) \in \mathbf{F}_{q^s}[T]$ are all irreducible over $\mathbf{F}_{q^s}$.

The way we have stated this result, the irreducible specializations are produced only over an extension $\mathbf{F}_{q^s}$ of the ground field. However, it appears from the proof that if q is large compared to the total degree of $f_1 \cdots f_r$, then one may take $s = 1$.

The next result we wish to highlight here is perhaps the most surprising encountered so far. Recall that the naive polynomial analogue of Hypothesis H appears to hold for any finite family of separable polynomials over $\mathbf{F}_q$; in particular, over any field satisfying the necessary local conditions, there should be infinitely many pairs of irreducibles $P, P+1$. These conditions are satisfied whenever $q > 2$; but fail when $q = 2$, as one of P or $P+1$ always has zero constant term (and so is divisible by T).

It therefore appears reasonable to conjecture that when $q > 2$, there are infinitely many 'twin prime pairs' $P, P+1$ over $\mathbf{F}_q$. Remarkably, given the difficulty associated with the classical twin prime conjecture, this polynomial version can be proven. The following result appears in Hall's 2003 doctoral thesis [54] (see also [55]):

Theorem 1.3.10. *If $\mathbf{F}_q$ is a field with $q > 3$ elements, then there are infinitely many pairs of monic irreducibles $P, P+1 \in \mathbf{F}_q[T]$.*

This leaves open the case $q = 3$, but as we will see in Chapter 3, the case $q = 3$ can be handled by a small variation in the argument.

The most surprising feature of Hall's theorem is its simple, short proof. Hall bases the argument on the following irreducibility criterion of Capelli (see, e.g., [76, Chapter VI, Theorem 9.1]):

Theorem 1.3.11 (Capelli)**.** *Let F be any field. Then the polynomial $T^n - a$ is irreducible over F unless one of the following holds:*

(i) *for some prime l dividing n and some $b \in F$, we have $a = b^l$,*

(ii) 4 *divides n and $a = -4b^4$ for some $b \in F$.*

To give the flavor of Hall's proof we describe the $q = 7$ case. There are only three cubes in $\mathbf{F}_7$: 0, 1, and -1. For each $k = 0, 1, 2, 3, \dots$, consider the polynomial $T^{3^k} - 2 \in \mathbf{F}_7[T]$. As a binomial, if it is to factor, it must factor for one of the two reasons given in Capelli's theorem. But since 2 is not on our list of cubes, this is impossible; hence $T^{3^k} - 2$ is irreducible for every value of k. By the same argument, $T^{3^k} - 3$ is irreducible over $\mathbf{F}_7$ for each k. But now we are staring at a twin prime pair: $T^{3^k} - 3$ and $T^{3^k} - 2$. Varying k, we see we have proven an $\mathbf{F}_7$ analogue of the twin prime conjecture!

1.4 Miscellaneous results

There are a number of results on the distribution of irreducible polynomials over finite fields on which we have not yet touched; here we survey some representatives examples.

Perhaps surprisingly, quite a bit can be done under very limited hypotheses. Knopfmacher and Zhang (see [71], [72]) develop much of analytic and probabilistic number theory in the framework of 'arithmetic semigroups satisfying Axiom A$^{\#}$'. The monic polynomials over a finite field form one of the motivating examples of such semigroups, and so all of their results are applicable in this context. This includes, e.g., the Hardy-Ramanujan inequality and Erdős-Kac theorem, estimates for the maximal order of various arithmetic functions, theorems on mean values of multiplicative functions, and quite a bit more. A similar approach is taken in the pair [79] of articles by Liu.

Various authors deal more directly with the polynomial setting. For example, sieve methods are independently generalized to the polynomial setting by Cherly [25], Webb [121], Hsu ([67], [68]), and Bareikis ([6], [7]). From the numerous results obtained by these authors, we choose to quote two 'almost-prime' results. The first is due to Cherly (op. cit.).

Theorem 1.4.1. *All of the following hold, with multiple prime divisors counted multiply:*

(i) *Let $\mathbf{F}_q$ be a finite field, and suppose $q > 2$. Let A be a polynomial of degree n over $\mathbf{F}_q$. If n is sufficiently large, then A can be written in the form $P + Q$, where $\deg P = n - 1$, $\deg Q = n$, and each of P and Q have at most four monic irreducible factors.*

(ii) *Let $\mathbf{F}_q$ be a finite field, and suppose $q > 2$. For each $a \in \mathbf{F}_q^{\times}$, there are infinitely many polynomials P over $\mathbf{F}_q$ for which both P and $P + a$ have at most four monic irreducible factors.*

(iii) *Fix a finite field $\mathbf{F}_q$ with $q \equiv 3 \pmod 4$. Then there are infinitely many polynomials A over $\mathbf{F}_q$ for which $A^2 + 1$ has at most six monic irreducible factors.*

The next result, due to Car [17], generalizes Chen's well-known theorem on Goldbach's problem:

Theorem 1.4.2. *Let $\mathbf{F}_q$ be a finite field, where we suppose first that $q > 2$. Then every $A \in \mathbf{F}_q[T]$ of sufficiently large degree n can be represented as $P + Q$, where P is an irreducible polynomial of degree $\leq n$, and Q is either irreducible or the product of two irreducibles. Moreover, the number of such representations is at least*

$$0.33 \prod_{P|A} \left(1 + \frac{1}{|P| - 1}\right) \prod_{P\nmid A} \left(1 - \frac{1}{(|P| - 1)^2}\right) \frac{q^{n+1}}{n^2},$$

where the products are indexed by monic irreducibles P. The same holds if $q = 2$, if we only consider polynomials $A(T)$ divisible by $T(T + 1)$.

There has also been progress adapting the circle method to study problems in additive prime number theory. In 1966, Hayes proved the first result of this type, an analogue of Vinogradov's 3-primes theorem [61]:

Theorem 1.4.3. *Let A be a polynomial of degree n over $\mathbf{F}_q$. Suppose α, β, γ are nonzero elements of $\mathbf{F}_q$ for which $\alpha + \beta + \gamma$ agrees with the leading coefficient of A. If $q = 2$, suppose also that $\gcd(A, T(T + 1)) = 1$. The number of ordered triples of monic irreducible polynomials P_1, P_2, P_3 over $\mathbf{F}_q$ of degree n with*

$$\alpha P_1 + \beta P_2 + \gamma P_3 = A$$

is

$$\prod_{P|A} \left(1 - \frac{1}{(|P| - 1)^2}\right) \prod_{P\nmid A} \left(1 + \frac{1}{(|P| - 1)^3}\right) \frac{q^{2n}}{n^2} + O\left(q^{1/4} q^{7n/4}\right).$$

Moreover, for A as above, the coefficient of q^{2n}/n^2 is bounded below by an absolute positive constant.

A similar (but somewhat weaker) result was later independently established by

Car [15]. In the same paper she goes on to estimate the exceptional set in the corresponding binary problem:

Theorem 1.4.4. *Let $\mathbf{F}_q$ be a finite field with $q > 2$. Then for every $h > 0$, the number of polynomials A of degree $n \geq 1$ over $\mathbf{F}_q$ which cannot be written in the form $P + Q$, where P and Q are irreducibles of degree $\leq n$, is*

$$\ll \frac{q^n}{n^h},$$

where the implied constant depends at most on q and h. The same holds if $q = 2$, provided we only consider polynomials A divisible by $T(T+1)$.

Theorem 1.4.4 is the analogue of van der Corput's result in [115] that $\ll x/\log^h x$ even integers $\leq x$ are not the sum of two primes.

In [21], Car studies the number of representations of a polynomial in the form $A_1P_1 + A_2P_2 + A_3P_3$, where (in contrast to Hayes's result above) the A_i are not restricted to be constant.

Effinger and Hayes ([41], [40, Chapter 7]) study a variant of the three primes problem. They call a monic polynomial A of degree n over $\mathbf{F}_q$ a 3-*primes polynomial* if it can be written in the form $P_1 + P_2 + P_3$, where P_1 has degree n and P_2, P_3 have smaller degree, and they prove that every monic polynomial $A(T)$ of degree $n \geq 2$ (assumed coprime to $T(T+1)$ in the case $q = 2$) is a 3-primes polynomial, unless $A(T)$ has the form $T^2 + \alpha$ and q is even. This is as complete a classification as one could hope: being prime to $T(T+1)$ in the case $q = 2$ is the polynomial analogue of being 'odd', while the exceptional polynomials $T^2 + \alpha$ are just "too small" to admit a representation. The result of Effinger and Hayes may be compared with the theorem of [36], which asserts that if the RH holds for Dirichlet L-functions, then every odd integer $n > 5$ is a sum of three rational primes.

Applications of the circle method to additive problems mixing primes and powers appear in the work of Webb [120] and Car [16], [18], [19]. Of course the circle method also has applications outside distribution of primes; a recent example in the polynomial context is the work of Liu and Wooley on Waring's problem [80].

We conclude this section by mentioning the recent work of Thorne [114], who shows that Maier's matrix method can be successfully applied in the setting of polynomials over finite fields.

1.5 Summary of later chapters

Chapter 2 treats two problems. In the first half, we revisit the polynomial prime counting function. Suppose p is a prime; then there is a natural correspondence between nonnegative integers and polynomials over $\mathbf{F}_p$, given by sending

$$a_0 + a_1 p + \cdots + a_j p^j \mapsto a_0 + a_1 T + \cdots + a_j T^j,$$

where we assume that the left hand-integer is written in base p (so $0 \leq a_i < p$). Define $\pi_p(X)$ to be the number of integers $0 \leq n < X$ which encode irreducible polynomials. Gauss's prime number theorem gives us information about $\pi_p(X)$ as X goes through powers of p, or through multiples of these powers by $0, 1, 2, \ldots, p-1$, and it is natural to wonder about the behavior of $\pi_p(X)$ for general X.

We prove an unconditional result analogous to the estimate

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(x^{1/2} \log x),$$

which was proved by von Koch [74] under the assumption of the Riemann Hypothesis. We also prove an analogue of the asymptotic series expansion

$$\pi(x) = \frac{x}{\log x} + 1!\frac{x}{\log^2 x} + \cdots + r!\frac{x}{\log^{r+1} x} + O_r\left(\frac{x}{\log^{r+2} x}\right).$$

Our estimates are obtained without assuming p fixed; an easy consequence of our results is that $\pi_p(X) \sim X/\log_p X$ whenever $\log_p X \to \infty$.

The second half of Chapter 2 treats a version of the polynomial twin prime problem. Let n be a positive integer and M a nonzero polynomial over $\mathbf{F}_q$ of degree $< n$. We consider the number of (not necessarily monic) prime pairs $P, P+M$, where P has degree n. For large q, one expects on probabilistic grounds that this is

$$\approx \frac{q^{n+1}}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1},$$

where the product extends over those monic primes Q dividing M. Among other results, we show that this approximation holds as an asymptotic whenever $q/n^2 \to \infty$. Our results both strengthen and generalize work of Hayes [58], who considered the special case when $\deg M = n-1$.

In Chapter 3, we systematize Hall's strategy in his attack on the twin prime problem. We take aim at the following conjecture, which is a restricted polynomial analogue of Hypothesis H:

Conjecture 1.5.1. *Let $f_1(T)$, ..., $f_r(T)$ be irreducible polynomials belonging to $\mathbf{F}_q[T]$. Suppose that there is no prime $P \in \mathbf{F}_q[T]$ for which every $g(T) \in \mathbf{F}_q[T]$ satisfies*

$$f_1(g(T)) \cdots f_r(g(T)) \equiv 0 \pmod{P}. \tag{1.9}$$

Then the specializations $f_1(g(T)), \ldots, f_r(g(T))$ *are simultaneously irreducible for infinitely many monic polynomials* $g(T) \in \mathbf{F}_q[T]$.

The hypotheses here are more stringent than in the conjectures of §1.3.2, since now we are only considering polynomials in T with constant (i.e., $\mathbf{F}_q$) coefficients. This restriction lifts the burden of worrying about the anomalies of that section, as irreducible polynomials over $\mathbf{F}_q$ cannot be polynomials in T^p. So we expect Conjecture 1.5.1 to hold, and we even believe the analogue of the Conjecture 1.3.4 holds without the need for any new correction factors. Note that we have re-introduced in Conjecture 1.5.1 the policy of sampling only over monic $g(T)$; this has the merits of leading to a stronger statement than otherwise, being the true analogue of Schinzel's Hypothesis H (Conjecture 1.3.2), and being easily accommodated in our proofs below.

The number of solutions to the congruence (1.9) is bounded by the degree B (say) of the product $f_1 \cdots f_r$. So we obtain a weakened form of Conjecture 1.5.1 if we replace the local condition there by the assumption that $q > B$. The main result of Chapter 3 is a proof that the conclusion of Conjecture 1.5.1 holds under the stricter hypothesis that $q > \max\{3, 2^{2r-2}B^2\}$.

Chapter 4 introduces, for us, the Chebotarev density theorem as a tool for counting the number of irreducible polynomials of a specified form. Let $f(T, u)$ be an absolutely irreducible polynomial in $\mathbf{F}_q[T, u]$, monic in T. We give conditions which allow us to assert that there are about q/n values of $a \in \mathbf{F}_q$ for which the specialization $f(T, a)$ is irreducible over $\mathbf{F}_q$. The methods used to prove this theorem allow us to establish the following result in the additive theory of prime polynomials: If $\mathbf{F}_q$ is a finite field of characteristic $\neq 2, 3$, then infinitely many monic irreducibles in $\mathbf{F}_q[T]$ have a representation in the form

$$P_1^3 + P_2^3 + P_3^3,$$

where the P_i are also monic irreducibles, and where $\deg P_1 > \{\deg P_2, \deg P_3\}$.

In Chapter 5, we develop the method of Chapter 4 to investigate the following quantitative analogue of Conjecture 1.5.1:

Conjecture 1.5.2. *Suppose that $f_1, \dots, f_r$ are nonassociate irreducible one-variable polynomials over $\mathbf{F}_q$ with the degree of the product $f_1 \cdots f_r$ bounded by B. Suppose that there is no prime P of $\mathbf{F}_q[T]$ for which the map*

$$g(T) \mapsto f_1(g(T)) \cdots f_r(g(T)) \bmod P$$

is identically zero. Then

$$\begin{aligned}\#\{g(T) : g \text{ monic}, \ \deg g = n, \ \text{and } f_1(g(T)), \dots, f_r(g(T)) \text{ all prime}\} \\ = (1 + o_B(1)) \frac{\mathfrak{S}(f_1, \dots, f_r)}{\prod_{i=1}^r \deg f_i} \frac{q^n}{n^r} \quad \text{as } q^n \to \infty.\end{aligned}$$

Here the local factor $\mathfrak{S}(f_1, \dots, f_r)$ is defined by

$$\mathfrak{S}(f_1, \dots, f_r) := \prod_{m=1}^{\infty} \prod_{\substack{\deg P = m \\ P \text{ monic, prime}}} \frac{1 - \omega(P)/q^m}{(1 - 1/q^m)^r},$$

where

$$\omega(P) := \#\{A \bmod P : f_1(A) \cdots f_r(A) \equiv 0 \pmod{P}\}.$$

A key departure from Conjecture 1.3.5 and from Conjecture 1.3.8 is that the asymptotic is stated a uniform manner: rather than fixing q and studying asymptotics as n tends to infinity, Conjecture 1.5.2 proposes an asymptotic formula valid whenever either q or n tends to infinity.

A heuristic argument for Conjecture 1.5.2 is given in §5.2 (and also in the appendix to [90]). The remainder of Chapter 5 is devoted to obtaining an estimate which confirms Conjecture 1.5.2 when q is large compared to n and B and satisfies $\gcd(q, 2n) = 1$. Actually we obtain a more general result; in a similar range of q and n, we are able to describe the joint distribution of the factorization types of $f_1(g(T)), \ldots, f_r(g(T))$. (The *factorization type* of a polynomial is the unordered list of degrees of its irreducible factors.)

Both of these results have a number of applications, which we explore in Chapter 6. For example, our result towards Conjecture 1.5.2 gives us a handle on the distribution of irreducibles in certain short intervals (in a certain range of q); such a result allows one to prove that, in a similar range, irreducible polynomials are Poisson distributed in a sense analogous to that considered by Gallagher [49]. Using the more general result on factorization types mentioned above, we investigate smooth specializations of polynomials and sequences of consecutive smooth polynomials, and we confirm polynomial analogues of conjectures appearing in the work of Martin [81] and of Erdős and Pomerance [44].

We conclude the thesis in Chapter 7 with some remarks on a polynomial analogue of the Goldbach conjecture. Let n be a positive integer, and let α and β be nonzero elements of $\mathbf{F}_q$. Set $\gamma := \alpha + \beta$. If $\gamma \neq 0$, we suppose that A is a polynomial of degree n with leading coefficient γ; otherwise we suppose A is a nonzero polynomial of degree $< n$. Let $R(A)$ be the number of pairs of irreducibles P_1, P_2 of degree n and respective leading coefficients α, β for which $P_1 + P_2 = A$. Heuristically, one expects that

$$R(A) \approx (1+o(1)) \prod_{P|A} \left(1+\frac{1}{|P|-1}\right) \prod_{P\nmid A} \left(1-\frac{1}{(|P|-1)^2}\right) \frac{q^n}{n^2}. \tag{1.10}$$

(Here, as usual, P is restricted to monic prime values.) In fact, one expects that this holds as an asymptotic whenever q^n tends to infinity. We show that (1.10) is a good approximation for most A, by estimating the second moment of the difference between the left and right-hand sides. As a consequence, we obtain an analogue of Hardy and Littlewood's conditional result that the exceptional set in Goldbach's problem has counting function $\ll x^{1/2+\epsilon}$ for each $\epsilon > 0$, which improves on Car's Theorem 1.4.4. Our proof uses the circle method in the form applied by Hayes to the 3-primes problem. We also prove, in the same spirit and by the same methods as in Chapter 5, that (1.10) holds as an asymptotic when q is much larger than n and satisfies $\gcd(q, 2n) = 1$.

This dissertation is largely a synthesis of results that are on their way to being published: The second half of Chapter 2 (from §2.4 onward) is taken from [91]. Chapter 3 is substantially reproduced from [90], which also contains an appendix with the heuristic argument for Conjecture 1.5.2. The main result of Chapter 5, as it relates to Conjecture 1.5.2, appears in [92]. The more general result on factorization types, along with most of the applications of Chapter 6, can be found in [89]. The exceptions are Theorems 6.1.1 and 6.1.2, which appear already in [92]. Chapters 4 and 7 originate with this thesis.

1.6 Notation

For ease of reference, we collect here frequently needed definitions. More localized notation will be defined as it appears.

We write $\pi(q;n)$ for the number of monic irreducibles of degree n in $\mathbf{F}_q[T]$. The term *Gauss's formula for* $\pi(q;n)$ refers to (1.3), while *Gauss's estimate* refers to either of of (1.4), (1.5).

Throughout we make free use of standard notation from elementary and analytic number theory, such as the usual symbols for arithmetic functions and the Bachmann/Landau/Vinogradov symbols ($O(\cdot)$, $o(\cdot)$, $\ll$, etc.) for indicating orders of magnitude.

If A is a polynomial over $\mathbf{F}_q$, we write $|A|$ for $q^{\deg A}$, which is the size of the ring $\mathbf{F}_q[T]/(A)$, and we write $\varphi(A)$ for the size of the corresponding unit group. We write $\varphi_q(A)$ for this latter quantity when the ground field is ambiguous. We write $\mu(A)$ for the Möbius function of A, defined as zero when A is not squarefree, and as $(-1)^r$ otherwise, where r is the number of monic irreducible factors of A.

We reserve the letters P and Q for irreducible polynomials. We will often (but not always) additionally restrict P and Q to monic values; e.g., this is always the case when they are indexing a product.

Chapter 2

Two applications of Hayes's theory of primes in congruence classes

2.1 Introduction

In 1965, Hayes investigated the distribution of monic irreducible polynomials in congruence classes more general than those considered by Kornblum and Artin. We begin by recalling some results of Hayes's paper [60] in the sharp form derived by Rhin [95] on the basis of Weil's Riemann Hypothesis. (Even sharper estimates than these are now available in papers of Hsu [66] and Car [22], but these are not required in the sequel.)

We give two applications of these results. The first is a prime number theorem for $\mathbf{F}_q[T]$ that refines the classical Gauss formula for the number of irreducibles of a given degree. Our second application both corrects and extends work of Hayes

[58] concerning a polynomial analogue of the Goldbach conjecture; here we give an asymptotic formula, valid in a certain range of q and n, for the number of prime pairs of degree n over $\mathbf{F}_q$ with a certain fixed difference. In §2.4.6 we use sieve methods to prove an estimate of the same character valid over all q and n.

Notation

Throughout this chapter Q always denotes a monic irreducible element of $\mathbf{F}_q[T]$.

2.2 The distribution of primes in congruence classes

Let $\mathcal{M}$ be the (multiplicative) monoid of monic polynomials over $\mathbf{F}_q$. If $l \geq 0$ and $M \in \mathcal{M}$, we define a relation $\mathbf{R}_{l,M}$ on $\mathcal{M}$ by saying that $A \equiv B \pmod{\mathbf{R}_{l,M}}$ if and only if A and B have the same first l next-to-leading coefficients and $A \equiv B$ (mod M). Then $\mathbf{R}_{l,M}$ is a congruence relation on $\mathcal{M}$, i.e., an equivalence relation satisfying

$$A \equiv B \bmod \mathbf{R}_{l,M} \Rightarrow AC \equiv BC \bmod \mathbf{R}_{l,M} \quad \text{for all} \quad A, B, C \in \mathcal{M}.$$

Thus there is a well-defined quotient monoid $\mathcal{M}/\mathbf{R}_{l,M}$. It can be shown that an element of $\mathcal{M}$ is invertible modulo $\mathbf{R}_{l,M}$ if and only if it is coprime to M. Thus, the units of this monoid form an abelian group of size $q^l\varphi(M)$, which we denote by $(\mathcal{M}/\mathbf{R}_{l,M})^{\times}$ (cf. [60, Theorem 8.6]).

One of the principal results of Hayes's paper [60, Theorem 1.2] is that the monic irreducibles are uniformly distributed in the unit group modulo $\mathbf{R}_{l,M}$. (When $l = 0$, this reduces to Artin's version of the polynomial prime number theorem in arithmetic progressions.) We now outline a proof of this uniform distribution statement with an explicit error term, optimized to take advantage of Weil's Riemann Hypothesis.

2.2.1 An explicit formula

Fix an integer $l \geq 0$ and $M \in \mathcal{M}$. Let χ be a character of $(\mathcal{M}/\mathbf{R}_{l,M})^{\times}$, and lift χ to a function on $\mathcal{M}$ (defining χ to vanish at elements of $\mathcal{M}$ that are nonunits of $\mathcal{M}/\mathbf{R}_{l,M}$). For $u \in \mathbf{C}$ with $|u| < 1/q$, define

$$L(u,\chi) := \prod_{Q} (1 - \chi(Q) u^{\deg Q})^{-1}. \tag{2.1}$$

If χ is nontrivial, it may be shown that $L(u,\chi)$ is a polynomial in u, and that for some integer $a(\chi) \leq l + \deg M$, we have a factorization

$$L(u,\chi) = \prod_{i=1}^{a(\chi)} (1 - \beta_i(\chi) u), \tag{2.2}$$

where from Weil's Riemann Hypothesis and the work of Rhin [95, Chapter 2] we know that $|\beta_i(\chi)| \leq q^{1/2}$ for $1 \leq i \leq a(\chi)$. (Cf. the proof of [40, Theorem 5.7].) From the Euler product representation (2.1), we deduce

$$\begin{aligned} u\frac{L'(u,\chi)}{L(u,\chi)} &= \sum_{Q} \deg Q \frac{\chi(Q) u^{\deg Q}}{1 - \chi(Q) u^{\deg Q}} \\ &= \sum_{n=1}^{\infty} u^n \sum_{\deg Q^j = n} \chi(Q^j) \deg Q, \end{aligned}$$

while from (2.2), we have

$$u\frac{L'(u,\chi)}{L(u,\chi)} = -\sum_{i=1}^{a(\chi)} \frac{\beta_i(\chi) u}{1 - \beta_i(\chi) u} = -\sum_{n=1}^{\infty} u^n \left(\sum_{i=1}^{a(\chi)} \beta_i(\chi)^n \right).$$

Comparing coefficients in these two expansions, we conclude that

$$\sum_{\deg Q^j = n} \chi(Q^j) \deg Q = -\sum_{i=1}^{a(\chi)} \beta_i(\chi)^n.$$

On the other hand, if $\chi = \chi_0$, then

$$L(u, \chi) = \frac{1}{1-qu} \prod_{Q|M} (1 - u^{\deg Q}) = \frac{1}{1-qu} \prod_{i=1}^{a(\chi_0)} (1 - \beta_i(\chi_0)u),$$

for certain roots of unity $\beta_i(\chi_0)$ (say), the number of which, say $a(\chi_0)$, is exactly

$$\sum_{Q|M} \deg Q \le \deg M.$$

Proceeding as above we find

$$\sum_{\deg Q^j = n} \chi_0(Q^j) \deg Q = q^n - \sum_{i=1}^{a(\chi_0)} \beta_i(\chi_0)^n.$$

It is worth noting for future use that the right hand sum is always nonnegative, since $\sum_{\deg Q^j = n} \deg Q = q^n$.

Combining these results with the orthogonality relations for characters, we deduce the following explicit formula for primes in residue classes modulo $\mathbf{R}_{l,M}$:

Lemma 2.2.1. *Let A be a polynomial prime to M. Then*

$$q^l \varphi(M) \sum_{\substack{Q^j \equiv A \pmod{\mathbf{R}_{l,M}} \\ \deg Q^j = n}} \deg Q = q^n - \sum_{\chi} \bar{\chi}(A) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n,$$

where χ runs over all characters modulo $\mathbf{R}_{l,M}$. Here $a(\chi) \le l + \deg M$ for all χ, *and each* $|\beta_i(\chi)| \leq q^{1/2}$.

2.2.2 A prime number theorem for progressions

As a straightforward consequence of the explicit formula, we obtain the following result (cf. [40, Exercise 3, p. 83]):

Lemma 2.2.2. *Let* M *be a monic polynomial over* $\mathbf{F}_q$ *and* l *a nonnegative integer. Then the number of monic irreducibles of degree* n *belonging to a given unit residue class modulo* $\mathbf{R}_{l,M}$ *is*

$$\frac{1}{n}\frac{q^n}{q^l\varphi(M)} + O\left((l + \deg M + 1)\frac{q^{n/2}}{n}\right).$$

Proof. The right hand side of Lemma 2.2.1 differs from q^n by an error which is

$$O(q^l\varphi(M)(l + \deg M)q^{n/2}),$$

so that

$$\sum_{\substack{Q^j \equiv A \pmod{\mathbf{R}_{l,M}} \\ \deg Q^j = n}} \deg Q = \frac{q^n}{q^l\varphi(M)} + O((l + \deg M)q^{n/2}).$$

The terms of the sum for which $j > 1$ contribute

$$\leq \sum_{\substack{d|n \\ d<n}} d\pi(q;d) \leq \sum_{\substack{d|n \\ d<n}} q^d \leq 2q^{n/2},$$

say. Hence

$$n \sum_{\substack{Q \equiv A \pmod{\mathbf{R}_{l,M}} \\ \deg Q = n}} 1 = \frac{q^n}{q^l \varphi(M)} + O\left((l + \deg M + 1) q^{n/2}\right).$$

Dividing by n gives the result. □

2.3 The prime number theorem for polynomials

2.3.1 The polynomial analogue of von Koch's theorem

Colloquially, the classical prime number theorem asserts that a number n is prime "with probability roughly $1/\log n$." Of course this can only be sensibly interpreted as a heuristic device, but it has proved surprisingly useful in that capacity. For example, it predicts that the number of primes up to X should be well-approximated by the sum

$$\sum_{2 \le n \le X} \frac{1}{\log n},$$

and we know from the work of von Koch [74] that that this approximation is good to within $O(X^{1/2} \log X)$ if and only if the Riemann Hypothesis holds. Here we show that an analogue of von Koch's estimate holds (unconditionally) in the polynomial setting, as a consequence of Weil's Riemann Hypothesis.

For the sake of simplicity, we initially formulate our result only for finite fields of the form $\mathbf{F}_p$, with p a prime. Notice that the nonnegative integers are in bijection with the univariate polynomials over $\mathbf{F}_p$ via the map

$$a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0 \longleftrightarrow a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0,$$

where the integer represented on the left hand side is assumed written in its base p expansion (so that $0 \leq a_i < p$). If the integer a corresponds to the polynomial A, we will write $\|A\| = a$. For an interval of real numbers I, we define

$$\pi_p(I) := \#\{P \in \mathbf{F}_p[T] : \|P\| \in I \text{ and } P \text{ is irreducible}\},$$

and we set

$$\pi_p(X) := \pi_p([0, X)).$$

Our main result is the following:

Theorem 2.3.1. *Let p be a prime and $X \geq p$. Let $n = \lfloor \log X / \log p \rfloor$ (so that $n \geq 1$). Then*

$$\pi_p(X) = \frac{X - p^n}{n} + (p-1) \sum_{m=1}^{n-1} \frac{p^m}{m} + O(np^{n/2+1}),$$

where the O-constant is absolute.

Remark. Gauss's formula implies that a degree n polynomial over $\mathbf{F}_p$ is prime with probability roughly $1/n$. This would lead one to expect that $\pi_p(X)$ should be well-approximated by

$$\sum_{\substack{||f|| \leq X \\ \deg f > 0}} \frac{1}{\deg f}$$

and this is precisely the main term in Theorem 2.3.1. The inside of the O-term in our theorem is $\asymp_p X^{1/2} \log X$, in exact analogy with von Koch's result.

For the proof of Theorem 2.3.1 we may (and do) assume that X is an integer. Write $X = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0$, with each $0 \leq a_i < p$. Then we have the basic decomposition

$$\pi_p(X) = \pi_p([0,p^n)) + \pi_p([p^n, a_n p^n)) + \sum_{j=1}^{n} \pi_p\left(\left[\textstyle\sum_{i=j}^{n} a_i p^i, \sum_{i=j-1}^{n} a_i p^i\right)\right). \quad (2.3)$$

We treat each of these three terms separately.

Lemma 2.3.2. *We have*

$$\pi_p([0,p^n)) = (p-1)\sum_{m=1}^{n-1} \frac{p^m}{m} + O(p^{(n+1)/2}/n).$$

Proof. We have the exact expression $\pi_p([0,p^n)) = (p-1)\sum_{m=1}^{n-1} \pi(p;m)$. The result follows now from Gauss's estimate for $\pi(p;m)$. □

Lemma 2.3.3. *We have*

$$\pi_p([p^n, a_n p^n)) = (a_n - 1)\frac{p^n}{n} + O(p^{n/2+1}/n).$$

Proof. The left hand side counts the number of irreducibles of degree n with leading coefficient one of $1, 2, \ldots, a_n - 1$, so that

$$\pi_p((p^n, a_n p^n]) = (a_n - 1)\left(\frac{p^n}{n} + O(p^{n/2}/n)\right) = (a_n - 1)\frac{p^n}{n} + O(p^{n/2+1}/n). \quad \square$$

Lemma 2.3.4. *For every $1 \le j \le n$, we have*

$$\pi_p\left(\left[\textstyle\sum_{i=j}^{n} a_i p^i, \sum_{i=j-1}^{n} a_i p^i\right)\right) = a_{j-1}\frac{p^{j-1}}{n} + O\left((n-j+2)\frac{p^{n/2+1}}{n}\right).$$

Proof. The left hand side represents the number of degree n primes whose first $n-j+1$ leading coefficients are $a_n, a_{n-1}, \ldots, a_j$, and whose T^{j-1}-coefficient is one of the a_{n-1} values $0, 1, \ldots, a_{n-1} - 1$. For each fixed value of the T^{j-1}-coefficient, the number of such irreducibles is the same as the number of monic irreducibles belonging to a certain prescribed congruence class modulo $\mathbf{R}_{n-j+1,1}$. By Lemma 2.2.2, each such congruence class contains

$$\frac{1}{n}p^{j-1} + O\left((n-j+2)\frac{p^{n/2}}{n}\right)$$

such irreducibles. Summing over the a_{j-1} possible coefficients of T^{j-1} yields the lemma. □

Theorem 2.3.1 follows immediately from (2.3) upon combining Lemmas 2.3.2–2.3.4.

2.3.2 An asymptotic series for $\pi_p(X)$

The estimate of von Koch alluded to before is more often written in the form

$$\pi(X) = \int_2^X \frac{dt}{\log t} + O(X^{1/2}\log X),$$

which is permissible since the integral here (traditionally denoted $\mathrm{li}(X)$) differs by a bounded amount from the sum $\sum_{2 \le n \le X} 1/\log n$. In seeking to approximate $\mathrm{li}(X)$, one is led (by repeated integration by parts) to the approximation

$$\mathrm{li}(X) = \frac{X}{\log X} + 1!\frac{X}{\log^2 X} + 2!\frac{X}{\log^3 X} + \cdots + r!\frac{X}{\log^{r+1} X} + O_r\left(\frac{X}{\log^{r+1} X}\right), \quad (2.4)$$

valid for every $r \ge 1$. (This is one of the canonical examples of an *asympotic series*; for background see, e.g., [35, Chapter 1.5].) Since the difference between $\pi(X)$ and $\mathrm{li}(X)$ is known (unconditionally) to be $O(X/\log^r X)$ for every r, it follows that $\pi(X)$

has the same asymptotic expansion.

It is natural to wonder if there is any analogue for $\pi_p(X)$. This is indeed the case:

Theorem 2.3.5. *Let p be a prime, and $X \geq p$ an integer with $X = \sum_{i=0}^{n} a_i p^i$, and $0 \leq a_i < p$ for each i. Assume $n \geq 2$. For $r \geq 2$, we have*

$$\pi_p(X) = \frac{X}{n} + \sum_{k=2}^{r}(1-1/p)A_{p,k}\frac{p^n}{n^k} + O\left(np^{n/2+1} + A_{p,r+2}\frac{p^n}{n^{r+1}} + \frac{p}{n}\sum_{k=1}^{r}A_{p,k}\right).$$

Here the constants $A_{p,k}$ are defined by

$$A_{p,k} := \sum_{m=1}^{\infty}\frac{m^{k-1}}{p^{m-1}}.$$

Remark. From the definitions it is clear that for every fixed value of $k \geq 1$, the $A_{p,k}$ are well-defined constants, decreasing in p. Consequently, Theorem 2.3.5 implies that (in the stated range)

$$\pi_p(X) = \frac{X}{n} + \sum_{k=2}^{r}(1-1/p)A_{p,k}\frac{p^n}{n^k} + O_r\left(\frac{p^n}{n^{r+1}}\right).$$

In particular, Theorem 2.3.5 makes transparent that

$$\pi_p(X) \sim X/\log_p X$$

whenever $\log_p(X) \to \infty$.

Most of the groundwork for the proof of Theorem 2.3.5 has already been laid in the course of proving Theorem 2.3.1. The only new ingredient required is the following, which is a minor variant of a result of Lenskoi [77]:

Lemma 2.3.6. *For each $r \geq 1$ and $n \geq 2$, we have*

$$\sum_{m=1}^{n-1} \frac{p^m}{m} = \sum_{k=1}^{r} A_{p,k} \frac{p^{n-1}}{n^k} + O\left(\frac{1}{n} \sum_{k=1}^{r} A_{p,k}\right) + O\left(A_{p,r+2} \frac{p^{n-1}}{n^{r+1}}\right),$$

where the constants $A_{p,k}$ are defined as in the statement of Theorem 2.3.1.

Proof. We largely follow Lenskoi. We have

$$\begin{aligned}\frac{1}{p^{n-1}} \sum_{m=1}^{n-1} \frac{p^m}{m} &= \sum_{m=1}^{n-1} \frac{1}{mp^{n-1-m}} = \sum_{m=1}^{n-1} \frac{1}{(n-m)p^{m-1}} \\ &= \sum_{m=1}^{n-1} \frac{1}{p^{m-1}} \sum_{k=1}^{\infty} \frac{m^{k-1}}{n^k} = \sum_{k=1}^{\infty} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}}.\end{aligned}$$

We split this last expression into three parts:

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}} &= \sum_{k=1}^{r} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}} + \sum_{k=r+1}^{\infty} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}} \\ &= \sum_{k=1}^{r} \frac{1}{n^k} A_{p,k} - \sum_{k=1}^{r} \frac{1}{n^k} \sum_{m=n}^{\infty} \frac{m^{k-1}}{p^{m-1}} + \sum_{k=r+1}^{\infty} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}}.\end{aligned}$$

The first sum yields the main term in our theorem, and it remains to show that the latter two contribute only error terms. The first double sum is just

$$\sum_{k=1}^{r} \frac{1}{n^k} \frac{1}{p^{n-1}} \sum_{m=1}^{\infty} \frac{(m-1+n)^{k-1}}{p^{m-1}} \leq \frac{1}{n} \frac{1}{p^{n-1}} \sum_{k=1}^{r} \sum_{m=1}^{\infty} \frac{m^{k-1}}{p^{m-1}} = \frac{1}{n} \frac{1}{p^{n-1}} \sum_{k=1}^{r} A_{p,k},$$

using

$$\frac{m-1+n}{n} = 1 + \frac{m-1}{n} \leq 1 + (m-1) = m.$$

This corresponds to the first O-term above.

To estimate the remaining double sum, notice that

$$\sum_{k=r+1}^{\infty} \frac{1}{n^k} \sum_{m=1}^{n-1} \frac{m^{k-1}}{p^{m-1}} = \frac{1}{n^{r+1}} \sum_{s=0}^{\infty} \frac{1}{n^s} \sum_{m=1}^{n-1} \frac{m^{s+r}}{p^{m-1}}$$
$$= \frac{1}{n^{r+1}} \sum_{m=1}^{n-1} \frac{m^r}{p^{m-1}} \frac{1}{1-m/n} = \frac{1}{n^{r+1}} \sum_{m=1}^{n-1} \frac{m^r}{p^{m-1}} \left(1 + \frac{m}{n-m}\right).$$

Since $m/(n-m) \leq m$, this is bounded above by

$$\frac{1}{n^{r+1}} \left(\sum_{m=1}^{n-1} \frac{m^r}{p^{m-1}} + \sum_{m=1}^{n-1} \frac{m^{r+1}}{p^{m-1}} \right) \leq \frac{A_{p,r+1} + A_{p,r+2}}{n^{r+1}} \leq 2\frac{A_{p,r+2}}{n^{r+1}}.$$

Multiplying through by p^{n-1}, we obtain the second O-term in the estimate of the theorem. □

We can now prove Theorem 2.3.5. According to Lemma 2.3.6, we have

$$(p-1) \sum_{m=1}^{n-1} \frac{p^m}{m} = \sum_{k=1}^{r} (1-1/p) A_{p,k} \frac{p^n}{n^k} + O\left(\frac{p}{n} \sum_{k=1}^{r} A_{p,k} \right) + O\left(A_{p,r+2} \frac{p^n}{n^{r+1}} \right). \quad (2.5)$$

Now the $k=1$ term in the right-hand sum contributes exactly

$$\left((1-1/p) \sum_{m=1}^{\infty} \frac{1}{p^{m-1}} \right) \frac{p^n}{n} = \frac{p^n}{n},$$

so that inserting (2.5) into the result of Theorem 2.3.1 yields Theorem 2.3.5.

While Theorem 2.3.5 gives an asymptotic expansion of $\pi_p(X)$, it is not immediately obvious that the terms of this expansion have much in common with the corresponding terms in the asymptotic expansion of $\pi(X)$ in (2.4). To highlight the similarity, we note the following estimate for the constants $A_{p,k}$:

Lemma 2.3.7. *If p is a prime and k is a positive integer, then*

$$A_{p,k} = p\frac{(k-1)!}{(\log p)^k}\left(1 + O\left(\frac{\log p}{\sqrt{k}}\right)\right).$$

Proof. We have $A_{p,k} := p\sum_{m=1}^{\infty} m^{k-1}p^{-m}$. The Euler-Maclaurin summation formula shows that

$$\sum_{m=1}^{\infty} m^{k-1}p^{-m} = \int_0^{\infty} t^{k-1}\exp(-t\log p)\, dt + O\left(\int_0^{\infty}\left|\frac{d}{dt}\left(t^{k-1}\exp(-t\log p)\right)\right|\, dt\right).$$

A change of variables gives a main term of precisely

$$\frac{\Gamma(k)}{(\log p)^k} = \frac{(k-1)!}{(\log p)^k},$$

while the unimodality of the original integrand ensures that the error term is

$$\ll \max_{t\geq 0} t^{k-1}\exp(-t\log p) = t^{k-1}\exp(-t\log p)|_{t=(k-1)/\log p} =$$
$$((k-1)/e)^{k-1}/(\log p)^{k-1} \ll \frac{(k-1)!}{(\log p)^k}\frac{\log p}{\sqrt{k}}.$$

In the last line we have applied Stirling's formula to estimate $(k-1)!$. □

Now suppose that $X = p^n$ is a power of p; as the proof of Lemma 2.3.6 makes clear, it is these values of X which give rise to the tail of the expansion of Theorem 2.3.5. By Theorem 2.3.5, we have

$$\pi_p(X) = \sum_{k=1}^{r}(1-1/p)A_{p,k}\frac{p^n}{n^k} + O(p^n/n^{r+1}),$$

where $r \geq 2$ is an integer parameter at our disposal. By Lemma 2.3.7, the kth term in this expansion is

$$(p-1)\frac{(k-1)!}{(\log p)^k}\frac{p^n}{n^k}\left(1+O\left(\frac{\log p}{\sqrt{k}}\right)\right) = (p-1)(k-1)!\frac{X}{\log^k X}\left(1+O\left(\frac{\log p}{\sqrt{k}}\right)\right).$$

If k is large compared to $\log p$, then it makes sense to say that the main term here is

$$(p-1)(k-1)!\frac{X}{\log^k X}.$$

This coincides with the kth term in the asymptotic expansion of $\pi(X)$, except for a factor of $p-1$. This factor can be attributed to $\pi_p(X)$ counting all primes irrespective of their leading coefficient, whereas $\pi(X)$ counts only positive primes.

2.3.3 The case of arbitrary finite fields

When q is not prime, then there is no longer an obvious correspondence between the integers $0, 1, 2, \ldots, q-1$ and the elements of $\mathbf{F}_q$. However, if we pick any labeling of the elements of $\mathbf{F}_q$ by $\{0, 1, \ldots, q-1\}$ in which 0 corresponds to 0, then all the results of this section remain true, with O-constants uniform in both q and the choice of labeling. The proofs require only trivial modifications.

2.4 A polynomial analogue of the twin prime conjecture

2.4.1 A uniform conjecture

Let M be a nonzero polynomial over a finite field $\mathbf{F}_q$, and let $R(n; M, q)$ denote the number of 'twin prime pairs' $P, P+M$, where P runs over the irreducible polynomials of degree n. Reasoning in analogy with the usual heuristic arguments offered for configurations of rational primes (compare, e.g., with [96, pp. 409-411]), we are led to expect that for $n > \deg M$,

$$R(n; M, q) \approx R_0(n; M, q), \tag{2.6}$$

where

$$R_0(n; M, q) := (q-1)\frac{q^n}{n^2} \prod_{Q \mid M} \left(1 - \frac{1}{|Q|}\right)^{-1} \prod_{Q \nmid M} \left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2}.$$

The factor of $q - 1$ in front stems from the fact that P is not restricted to monic values.

There are various ways one might attempt to make the approximation (2.6) precise; perhaps the most obvious is to fix q and M, and to read (2.6) as an asymptotic estimate as n tends to infinity. Various special cases of such a conjecture were proposed by Effinger, Hicks & Mullen (see [42]). Little is known in this direction; in fact it was only recently that Hall [55, p. 140] showed the existence of infinitely many twin prime pairs $P, P + M$ over $\mathbf{F}_q$ in the special case when M is constant (and $q > 3$), but his clever proof only yields very weak lower bounds on the number of such pairs. Hall's result together with some generalizations is discussed in Chapter 3.

A different approach is suggested by another result from the same paper of Effinger, Hicks & Mullen. A special case of these authors' Proposition 1 (op. cit.) is that for M a nonzero constant polynomial, one has $R(n; M, q) > 0$ for $q \geq 2n$. This suggests that $R(n; M, q)$ may be more amenable to study as a function of multiple parameters. Once in this frame of mind, it is easy to formulate a more uniform conjecture, justified by the same classical heuristic alluded to above:

Conjecture 2.4.1. *Let M be a nonzero polynomial of degree $< n$ over $\mathbf{F}_q$. Then*

$$R(n; M, q) = (1 + o(1))R_0(n; M, q) \quad \text{as} \quad q^n \to \infty,$$

uniformly in M. In other words: For every $\epsilon > 0$, there is a constant $B = B(\epsilon)$ with the property that whenever M is a nonzero polynomial over $\mathbf{F}_q$ of degree $< n$ and $q^n > B$, we have

$$|R(n; M, q) - R_0(n; M, q)| < \epsilon R_0(n; M, q).$$

Here we use the explicit formula of §2.2.1 to prove an estimate for $R(n; M, q)$ which confirms Conjecture 2.4.1 whenever q/n^2 tends to infinity (uniformly in the choice of $M \in \mathbf{F}_q[T]$ of degree $< n$). In §2.4.6, we use Selberg's upper bound sieve to derive an upper estimate for $R(n; M, q)$ valid uniformly in n, M and q.

2.4.2 Statement of the main result

Considering again the right hand side of the approximation (2.6), we observe that each factor in the second product is $1 + O(|Q|^{-2})$. From this one may deduce that

$$R_0(n; M, q) = (1 + O(1/q))\frac{q^{n+1}}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1}.$$

In particular, Conjecture 2.4.1 would imply that as $q \to \infty$, we have

$$R(n; M, q) = (1 + o(1))\frac{q^{n+1}}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1}, \tag{2.7}$$

uniformly in n and M (with $0 \leq \deg M < n$).

We can now state our main result. Recall that $\prod_{Q|M}(1-1/|Q|)^{-1} = |M|/\varphi(M)$.

Theorem 2.4.2. *Let $k \geq 0$ and $n \geq 2$ be integers with $0 \leq k < n$. Let M be a polynomial of degree k over $\mathbf{F}_q$. Then*

$$-\frac{q^n}{n} - 4\frac{|M|}{\varphi(M)}\frac{q^{n/l+1}}{n^2} \leq R(n; M, q) - \frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2} \leq q^n - \frac{q^n}{n} + 2\frac{q^{n/l}}{n},$$

where l is the least prime divisor of n.

In the omitted case $k = 0$ and $n = 1$, it is easy to see that one has the exact expression $R(n; M, q) = q^2 - q$.

Remark. As a consequence of Theorem 2.4.2, we see that

$$1 + O(n/q) \leq \frac{R(n; M, q)}{(|M|/\varphi(M))q^{n+1}/n^2} \leq 1 + O(n^2/q).$$

Thus if q^n tends to infinity in such a way that n^2/q tends to zero, we have the asymptotic for $R(n; M, q)$ predicted by (2.7), while the lower bound aspect of this asymptotic holds already if n/q tends to zero. These estimates can be compared with the uniform upper bound

$$R(n; M, q) \leq 8\frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2} \tag{2.8}$$

which follows from an application of Selberg's upper-bound sieve, as developed in the polynomial setting by Webb (see [121]). The details of the proof of (2.8) are supplied in §2.4.6.

When $k = n - 1$, a weaker version of Theorem 2.4.2 was stated by Hayes [58, Theorem 2]. However, the proof of his lower bound on $R(n; M, q)$ contained a gap [59], and he salvaged his main result only under additional hypotheses. Our argument for the upper bound in Theorem 2.4.2 closely follows Hayes. Our proof of the lower bound rests on a simple averaging argument applied to the well-known formula for the number of prime polynomials of a given degree.

Finally, we remark that if we let P run over only monic primes, then we still believe the analogue of Conjecture 2.4.1, but obtaining an analogue of Theorem 2.4.2 appears substantially more difficult. A weaker result in this direction is contained in Theorem 7.1.4 of Chapter 7.

Notation

For the remainder of this chapter, l denotes the least prime factor of the integer n.

2.4.3 A heuristic

Let M be a polynomial of degree k over $\mathbf{F}_q$ and suppose $n > k$. Let $h(T)$ range over a set of representatives of the units modulo $\mathbf{R}_{n-1-k,M}$, and let N_h be the number of monic primes of degree n congruent to $h(T)$ modulo $\mathbf{R}_{n-1-k,M}$. (If we choose our representatives $h(T)$ from the set of monic, degree n polynomials, then N_h can be interpreted as the number of prime polynomials in the q-element set $\{h(T) + \alpha M\}$, where α ranges over $\mathbf{F}_q$.) Then $\sum_h N_h^2$ is precisely the number of monic prime pairs Q, Q' of degree n whose difference is an $\mathbf{F}_q$-multiple of M. If $Q' - Q$ is nonzero for such a pair, then necessarily $Q' - Q = \alpha M$ for some $\alpha \in \mathbf{F}_q^{\times}$. But then $\alpha^{-1}Q$ and $\alpha^{-1}Q'$ form a pair of primes differing by M. Thus, removing the pairs where $Q = Q'$, we find that

$$R(n; M, q) = \sum_h N_h^2 - \pi(q; n). \tag{2.9}$$

There are a total of $q^n\varphi(M)/|M|$ monic, degree n polynomials which are prime to M, of which about q^n/n are irreducible. Thus, a random monic, degree n polynomial coprime to M is irreducible with probability about $n^{-1}|M|/\varphi(M)$. Hence it is natural to guess that N_h is roughly $(q/n)|M|/\varphi(M)$ for each h, and this leads us to expect that

$$\sum_h N_h^2 \approx (q/n)^2(|M|/\varphi(M))^2\#(\mathcal{M}/\mathbf{R}_{n-1-k,M})^\times = \frac{q^2}{n^2}\frac{|M|^2}{\varphi(M)^2}q^{n-1-k}\varphi(M) = \frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2}.$$

2.4.4 Lower bound of Theorem 2.4.2

To obtain a lower bound it is not necessary to understand the numbers N_h individually. Since every monic prime of degree n belongs to some unit residue class modulo $\mathbf{R}_{n-1-k,M}$, we have $\sum_h N_h = \pi(q;n)$, so that by the Cauchy-Schwarz inequality and Gauss's estimates,

$$\sum_h 1^2 \sum_h N_h^2 \geq \left(\sum_h N_h\right)^2 \geq \frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/p)}}{n^2},$$

and so

$$\begin{aligned}\sum_h N_h^2 &\geq \frac{1}{q^{n-1-k}\varphi(M)}\left(\frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/l)}}{n^2}\right)\\ &= \frac{|M|}{\varphi(M)}\left(\frac{q^{n+1}}{n^2} - 4\frac{q^{n/l+1}}{n^2}\right).\end{aligned}$$

The relation (2.9) now implies that

$$R(n;M,q) \geq \frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2} - 4\frac{|M|}{\varphi(M)}\frac{q^{n/l+1}}{n^2} - \pi(q;n). \tag{2.10}$$

The upper estimate $\pi(q;n) \leq q^n/n$ completes the proof of the lower bound.

2.4.5 Upper bound of Theorem 2.4.2

From Lemma 2.2.1, if h represents a unit residue class modulo $\mathbf{R}_{n-1-k,M}$, then

$$\begin{aligned} q^{n-1-k}\varphi(M)nN_h &\leq q^{n-1-k}\varphi(M) \sum_{\substack{Q^j \equiv h \pmod{\mathbf{R}_{n-1-k,M}} \\ \deg Q^j = n}} \deg Q \\ &= q^n - \sum_{\chi} \overline{\chi}(h) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n. \end{aligned}$$

Now square both sides and sum over h:

$$\begin{aligned} n^2 q^{2(n-1-k)}\varphi(M)^2 \sum_h N_h^2 \leq \sum_h q^{2n} - 2q^n \sum_h \sum_\chi \overline{\chi}(h) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n \\ + \sum_h \sum_{\chi,\chi'} \overline{\chi}(h)\overline{\chi}'(h) \sum_{\substack{1\leq i\leq a(\chi) \\ 1\leq j\leq a(\chi')}} \beta_i(\chi)^n \beta_j(\chi')^n. \end{aligned}$$

Interchanging the sums over h with the sums over χ and χ', and using the orthogonality relations once again, we find that the right hand side simplifies to

$$q^{n-1-k}\varphi(M)q^{2n} - 2q^n q^{n-1-k}\varphi(M)\sum_{i=1}^{a(\chi_0)}\beta_i(\chi_0)^n$$
$$+\sum_h\sum_\chi\sum_{\substack{1\le i\le a(\chi)\\ 1\le j\le a(\chi^{-1})}}\beta_i(\chi)^n\beta_j(\chi^{-1})^n.$$

As noted above, the first sum appearing here is nonnegative, and so the entire term it belongs to is nonpositive and can therefore be ignored, since we are looking for an upper bound. Moreover, since $|\beta_i(\chi)|$ and $|\beta_j(\chi^{-1})|$ are bounded by $q^{1/2}$, and both $a(\chi)$ and $a(\chi^{-1})$ are bounded by $n-1$, the triple sum here is bounded in absolute value by

$$(q^{n-1-k}\varphi(M))^2(q^{n/2})^2n^2 = q^{3n-2-2k}\varphi(M)^2n^2.$$

Thus

$$\sum_h N_h^2 \le \frac{q^{3n-1-k}\varphi(M) + q^{3n-2-2k}\varphi(M)^2n^2}{n^2q^{2n-2-2k}\varphi(M)^2},$$

so that

$$\begin{aligned} R(n;M,q) &= \sum_h N_h^2 - \pi(q;n)\\ &\le \frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2} + q^n - \pi(q;n). \end{aligned}$$

Inserting Gauss's lower estimate for $\pi(q;n)$ completes the proof of the upper bound.

2.4.6 An upper bound for twin prime pairs in $\mathbf{F}_q[T]$

In this section we establish the following estimate:

Proposition 2.4.3. *Let $n \geq 2$ be an integer, and let $M \neq 0$ be a polynomial of degree $< n$ over the finite field $\mathbf{F}_q$. Then*

$$\#\{P : P, P+M \text{ are both monic irreducibles of degree } n\} \leq 8\frac{|M|}{\varphi(M)}\frac{q^n}{n^2}.$$

As a corollary, we have

$$R(n; M, q) \leq 8\frac{|M|}{\varphi(M)}\frac{q^{n+1}}{n^2},$$

whenever $0 \leq \deg M < n$.

The estimate of Proposition 2.4.3 is analogous to an explicit upper bound on generalized twin prime pairs obtained by Riesel and Vaughan ([97, Lemma 5]), but working in the polynomial setting enables us to give a much simpler proof. We begin with a statement of Selberg's upper-bound sieve for polynomials (cf. [121, Theorem 1]).

Lemma 2.4.4 (Selberg's Λ^2-sieve for $\mathbf{F}_q[T]$)**.** *Let $\mathcal{A}$ be a multiset of polynomials over $\mathbf{F}_q$, and let $\mathcal{Q}$ be a finite set of monic irreducibles over $\mathbf{F}_q$. Suppose that f is a multiplicative function defined on the squarefree divisors of $\prod_{Q \in \mathcal{Q}} Q$ with $1 < f(Q) \leq |Q|$ for each $Q \in \mathcal{Q}$, and write*

$$\sum_{\substack{A \in \mathcal{A} \\ D \mid A}} 1 = \frac{\#\mathcal{A}}{f(D)} + R_D. \tag{2.11}$$

Let $\mathcal{D}$ be any nonempty subset of the monic divisors of $\prod_{Q \in \mathcal{Q}} Q$ which is divisor *closed (i.e., every monic divisor of an element of $\mathcal{D}$ belongs to $\mathcal{D}$). Then*

$$\sum_{\substack{A\in\mathcal{A}\\ \gcd(A,\prod_{Q\in\mathcal{Q}}Q)=1}} 1 \le \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1}\prod_{Q\mid D}\left(1-f(Q)^{-1}\right)^{-1}} + \sum_{D_1,D_2\in\mathcal{D}} |X_{D_1}X_{D_2}R_{[D_1,D_2]}|,$$

where

$$X_D = \mu(D)f(D)\frac{\sum_{C\in\mathcal{D},D\mid C} f(C)^{-1}\prod_{Q\mid C}\left(1-f(Q)^{-1}\right)^{-1}}{\sum_{C\in\mathcal{D}} f(C)^{-1}\prod_{Q\mid C}\left(1-f(Q)^{-1}\right)^{-1}}.$$

Before proceeding we introduce a bit more notation. Let A be a nonzero polynomial over $\mathbf{F}_q$. Then we can express A uniquely in the form

$$A = \varepsilon Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r},$$

where $\varepsilon \in \mathbf{F}_q^\times$, the Q_i are distinct monic irreducibles, and the e_i are positive integers. We define the arithmetic functions $\Omega(\cdot), d(\cdot)$, and $\operatorname{rad}(\cdot)$ in analogy with their integer counterparts by setting

$$\Omega(A) := \sum_{i=1}^r e_i, \quad d(A) := \prod_{i=1}^r (e_i+1), \quad \operatorname{rad}(A) := \prod_{i=1}^r Q_i.$$

Proof of Proposition 2.4.3. In the case when $q = 2$, we may assume that $T(T+1)$ divides M, since otherwise there are no prime pairs $P, P+M$ of degree n. Thus $|Q| > 2$ for every prime Q not dividing M. Define the multiset

$$\mathcal{A} := \{A(A+M) : A \text{ monic}, \deg A = n\}.$$

Let $\mathcal{Q}$ be the set of monic primes of degree $\leq n/2$. Then the number of monic, degree n prime pairs $P, P+M$ is precisely the number of elements of $\mathcal{A}$ coprime to $\prod_{Q\in\mathcal{Q}} Q$, a quantity which may be estimated with Lemma 2.4.4.

We take $\mathcal{D}$ to be the (divisor-closed) set of squarefree, monic polynomials of degree $\leq n/2$. Define the multiplicative function f appearing in Lemma 2.4.4 by setting (for monic primes Q)

$$f(Q) = \begin{cases} |Q|/2 & \text{if } Q \text{ does not divide } M, \\ |Q| & \text{if } Q \text{ divides } M, \end{cases}$$

and extending f to be a completely multiplicative function on the monoid of monic polynomials. It is easy to check that if the squarefree polynomial D has degree $\leq n$, then (2.11) holds without any error term, i.e., with $R_D = 0$.

Since the least common multiple of any pair $D_1, D_2 \in \mathcal{D}$ has degree $\leq n$, we obtain from Lemma 2.4.4 the following clean inequality:

$$\sum_{\substack{A\in\mathcal{A} \\ \gcd(A,\prod_{Q\in\mathcal{Q}} Q)=1}} 1 \leq \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1} \prod_{Q|D} \left(1-f(Q)^{-1}\right)^{-1}}. \tag{2.12}$$

To proceed we need a lower bound on the denominator in this expression. For each $D \in \mathcal{D}$, write $D = D_1 D_2$, where D_1 divides M and D_2 is prime to M. Then we have

$$f(D)^{-1} \prod_{Q|D} \left(1-f(Q)^{-1}\right)^{-1} = \prod_{Q|D_1} \frac{1}{|Q|-1} \prod_{Q|D_2} \frac{2}{|Q|-2},$$

using $|Q| > 2$ for every Q dividing D_2. Thus we have reduced the problem to obtaining a lower bound on

$$\sum_{D\in\mathcal{D}}\prod_{Q|D_1}\frac{1}{|Q|-1}\prod_{Q|D_2}\frac{2}{|Q|-2}$$
$$=\sum_{D\in\mathcal{D}}\prod_{Q|D_1}\left(\frac{1}{|Q|}+\frac{1}{|Q|^2}+\frac{1}{|Q|^3}+\dots\right)\prod_{Q|D_2}\left(\frac{2}{|Q|}+\frac{4}{|Q|^2}+\frac{8}{|Q|^3}+\dots\right).$$

We may rewrite this expression as

$$\sum_{A\text{ monic}}\frac{2^{\Omega(A_2)}}{|A|}\sum_{\substack{D\in\mathcal{D}\\ \mathrm{rad}(A)=D}}1,$$

where A_2 denotes that part of A supported on the primes not dividing M. The inner sum is at least 1 whenever $\deg A\le n/2$, which yields a lower bound of

$$\sum_{\substack{A_2\text{ monic}\\ \deg A_2\le n/2\\ \gcd(A_2,M)=1}}\frac{2^{\Omega(A_2)}}{|A_2|}\sum_{\substack{A_1\text{ monic}\\ \deg A_1\le n/2-\deg A_2\\ \mathrm{rad}(A_1)|M}}\frac{1}{|A_1|}. \tag{2.13}$$

Now $2^{\Omega(A_2)}\ge d(A_2)$, while for the inner sum we have

$$\sum_{\substack{A_1\text{ monic}\\ \deg A_1\le n/2-\deg A_2\\ \mathrm{rad}(A_1)|M}}\frac{1}{|A_1|}=\frac{\varphi(M)}{|M|}\sum_{\substack{A_1\text{ monic}\\ \deg A_1\le n/2-\deg A_2\\ \mathrm{rad}(A_1)|M}}\frac{1}{|A_1|}\prod_{Q|M}\left(1-\frac{1}{|Q|}\right)^{-1}$$
$$=\frac{\varphi(M)}{|M|}\sum_{\substack{A_1\text{ monic}\\ \deg A_1\le n/2-\deg A_2\\ \mathrm{rad}(A_1)|M}}\frac{1}{|A_1|}\sum_{\substack{B\text{ monic}\\ \mathrm{rad}(B)|M}}\frac{1}{|B|}$$
$$\ge\frac{\varphi(M)}{|M|}\sum_{\substack{C\text{ monic}\\ \deg C\le n/2-\deg A_2\\ \mathrm{rad}(C)|M}}\frac{d(C)}{|C|}.$$

Assembling these results, we find that (2.13) is bounded below by

$$\frac{\varphi(M)}{|M|} \sum_{\substack{A \text{ monic} \\ \deg A \leq n/2}} \frac{d(A)}{|A|}.$$

By an easy result of Carlitz, we have $\sum_{\substack{A \text{ monic} \\ \deg A = k}} d(A) = (k+1)q^k$ (see [23]), and so our last-displayed sum is just

$$\sum_{0 \leq k \leq n/2} (k+1) \geq \frac{n^2}{8},$$

so that (2.13) is bounded below by $(\varphi(M)/|M|)n^2/8$. Since the numerator in (2.12) is $\#\mathcal{A} = q^n$, we obtain the stated result. □

Remark. Let $\mathcal{I}_q(n)$ denote the set of monic irreducibles of degree n over $\mathbf{F}_q$. Then our argument shows that for any nonzero polynomial M (without any restriction on its degree) there are at most $8(|M|/\varphi(M))q^n/n^2$ values of $P \in \mathcal{I}_q(n)$ for which $P + M$ is free of prime factors of degree $\leq n/2$. As a consequence, there are at most

$$8\frac{|M|}{\varphi(M)}\frac{q^n}{n^2} + q^{\lfloor n/2 \rfloor + 1}$$

values of $P \in \mathcal{I}_q(n)$ for which $P + M$ is irreducible, where the $q^{\lfloor n/2 \rfloor + 1}$ term can be omitted unless M has degree n and leading coefficient -1. (The extra term is due to irreducible values of $P + M$ which are nevertheless removed in the sieve because $\deg(P + M) \leq n/2$.)

Chapter 3

The substitution method

3.1 Introduction

In Chapter 1 we alluded to the following finite field analogue of Schinzel's Hypothesis H:

Conjecture 3.1.1. *Let $f_1(T)$, …, $f_r(T)$ be irreducible polynomials belonging to $\mathbf{F}_q[T]$. Suppose that there is no prime $P \in \mathbf{F}_q[T]$ for which every $g(T) \in \mathbf{F}_q[T]$ satisfies*

$$f_1(g(T)) \cdots f_r(g(T)) \equiv 0 \pmod{P}. \tag{3.1}$$

Then the specializations $f_1(g(T)), \ldots, f_r(g(T))$ are simultaneously irreducible for infinitely many monic polynomials $g(T) \in \mathbf{F}_q[T]$.

The first nontrivial result towards this Conjecture is due to Hall ([54]; see also [55]), who settled (in the affirmative) the cases when $f_1(T) = T, f_2(T) = T + 1$ and $q > 3$. The first theorem we prove here is an extension of this result:

Theorem 3.1.2 (Twin prime polynomial theorem)**.** *For every $q \neq 2$ and every $\alpha \in \mathbf{F}_q^\times$, there are infinitely many monic twin prime polynomials $f, f+\alpha$ in $\mathbf{F}_q[T]$.*

The main result of this Chapter is that Conjecture 3.1.1 holds for an arbitrary family of polynomials, provided q is large in a suitable sense:

Theorem 3.1.3. *Let $f_1(T), \ldots, f_r(T)$ be irreducible polynomials over $\mathbf{F}_q$. If q is large compared to both r and the sum of the degrees of the f_i, then there is a prime l dividing $q-1$ and an element $\beta \in \mathbf{F}_q$ for which every subsitution*

$$T \mapsto T^{l^k} - \beta \quad \textit{with} \quad k = 0, 1, 2, \ldots$$

leaves all of $f_1, \ldots, f_r$ irreducible. Explicitly, the above conclusion holds provided

$$q > \max\left\{3, 2^{2r-2}\left(\sum\nolimits_{i=1}^{r} \deg f_i\right)^2\right\}. \tag{3.2}$$

Actually we obtain the theorem for q satisfying a slightly weaker (but more complicated) inequality than (3.2). It may be initially surprising that we have not included a local condition in our statement of Theorem 3.1.3. But such a condition is actually implicit in our requirements on q: the number of incongruent solutions to (3.1) is bounded by the sum of the degrees of the f_i, so that the local condition of Conjecture 3.1.1 is automatically satisfied for $q > \sum_{i=1}^{r} \deg f_i$, an inequality less stringent than (3.2).

Treating smaller q appears more difficult. Here we restrict ourselves to some remarks concerning those cases when $r = 1$ and q is fixed. This corresponds to searching for irreducible specializations of a single polynomial, so to a polynomial analogue of Buniakowsky's conjecture.

Our best result is conditional on the following well-known conjecture of Masser and Oesterlé (see [84]):

abc Conjecture. *Let $\epsilon > 0$, For any three coprime positive integers a, b and c satisfying $a + b = c$, we have*

$$c \ll_\epsilon \left(\prod_{p \mid abc} p \right)^{1+\epsilon}.$$

Using this result, we can prove the following. Below $l_a(m)$ denotes the multiplicative order of a modulo m.

Theorem 3.1.4. *Fix a finite field $\mathbf{F}_q$. For each $d \geq 2$, define*

$$\mathcal{A}_d := \{f \in \mathbf{F}_q[T] : \deg f = d; \text{ for some prime } l \mid q^d - 1, \\ f(T^{l^k}) \text{ is irreducible for } k = 0, 1, 2, \dots\},$$

and let $\mathcal{E}_d$ denote the set of monic irreducibles of degree d not in $\mathcal{A}_d$. Then for any $\epsilon > 0$,

$$\#\mathcal{E}_d \ll q^d/d^2 \qquad (\textit{unconditionally}), \tag{3.3}$$

$$\ll_\epsilon q^{1+\epsilon d} \qquad (\textit{assuming the abc Conjecture}). \tag{3.4}$$

Moreover, if we assume that

$$\sum_{\substack{r \text{ prime} \\ r \nmid q}} \frac{1}{l_q(r^2)} < \infty, \tag{3.5}$$

then $\mathcal{E}_d$ is empty for almost all d (in the sense of asymptotic density).

The complicated-looking assumption (3.5) asserts, in crude terms, that there are not too many q-Wieferich primes (i.e., primes r for which $q^{r-1} \equiv 1 \pmod{r^2}$). For example, in order for (3.5) to hold, it suffices that there be $\ll (\log x)^{1-\delta}$ such primes up to x; the natural conjecture is that there are only $\ll \log\log x$. We note that in the case $q = 2$ an assumption equivalent to (3.5) already appears in the work of Granville & Soundararajan (cf. [53, Theorem 4]).

Notation and conventions

We use $\mathrm{rad}(n) := \prod_{p|n} p$ to denote the *radical* of the positive integer n and $\mathrm{rad}'(n)$ to denote the odd part of $\mathrm{rad}(n)$, i.e., $\mathrm{rad}'(n) := \prod_{p|n, p>2} p$. We remind the reader that $l_a(m)$ denotes the multiplicative order of a modulo m.

3.2 The substitution method: Overview

Suppose $f(T)$ is an irreducible polynomial over a finite field. Under what conditions is the composition $f(g(T))$ also irreducible? At the heart of the substitution method is the observation that this question has a simple answer when $g(T)$ is a binomial polynomial $T^m - \beta$.

Since the linear substitution $T \mapsto T - \beta$ always preserves irreducibility, to understand the effect of binomial substitutions it suffices to study the case when $g(T) = T^m$. This question was considered by Serret in the case of prime fields [107] and Dickson in the general case ([38], p. 382; see also [39], §34). Since it is somewhat simpler and suffices for us, we restrict ourselves to the case when m is a prime power. Recall that the *order* of an irreducible polynomial $f(T) \in \mathbf{F}_q[T]$, not an associate of T, is the multiplicative order of any of its roots.

Lemma 3.2.1 (Serret, Dickson). *Let f be an irreducible polynomial over $\mathbf{F}_q$ of degree d and order e. Let l be an odd prime. Suppose that f has a root $\alpha \in \mathbf{F}_{q^d}$ which is not an lth power, or equivalently that*

$$l \text{ divides } e \quad \text{but} \quad l \text{ does not divide } (q^d - 1)/e. \tag{3.6}$$

Then the substitution $T \mapsto T^{l^k}$ leaves f irreducible for every $k = 1, 2, 3, \ldots$. The same holds for the prime $l = 2$ under the additional hypothesis $q^d \equiv 1 \pmod 4$.

The proof depends on the following well-known elementary result:

Lemma 3.2.2. *Let a be an integer and suppose $a \equiv 1 \pmod l$, where l is an odd prime. Then for every pair of positive integers k and r, we have*

$$l^k \mid \frac{a^r - 1}{a - 1} \iff l^k \mid r.$$

The same holds in the case when $l = 2$, if we suppose now that $a \equiv 1 \pmod 4$.

Proof. Write $v_l(\cdot)$ for the l-adic valuation; then we are claiming that

$$v_l(r) = v_l\left(\frac{a^r - 1}{a - 1}\right). \tag{3.7}$$

We consider first the case when $r = l$. Suppose that $l = 2$. Then $a \equiv 1 \pmod 4$, and

$$\frac{a^2 - 1}{a - 1} = a + 1 \equiv 2 \pmod 4,$$

which implies (3.7). If $l > 2$, write $a = 1 + lk$. Then $a^i \equiv 1 + ikl \pmod{l^2}$, and so

$$\frac{a^l - 1}{a - 1} = \sum_{i=0}^{l-1} a^i \equiv l + \frac{l(l-1)}{2} kl \equiv l \pmod{l^2},$$

and again (3.7) holds.

Next consider the case when l does not divide r. Then

$$\frac{a^r - 1}{a - 1} = \sum_{i=0}^{r-1} a^i \equiv r \pmod{l},$$

so that (3.7) holds in this case as well.

We now consider the general case: write $r = l^j r_0$, where $l \nmid r_0$. Then

$$\frac{a^r - 1}{a - 1} = \left(\prod_{i=1}^{j} \frac{a^{l^i r_0} - 1}{a^{l^{i-1} r_0} - 1} \right) \cdot \frac{a^{r_0} - 1}{a - 1}.$$

Using the above, $v_l((a^r - 1)/(a - 1)) = \sum_{i=1}^{j} 1 = j = v_l(r)$. □

Proof of Lemma 3.2.1. Clearly $\alpha \neq 0$. Let k be a positive integer, and let β be an l^k-th root of α taken from the algebraic closure of $\mathbf{F}_q$. Showing that $f(T^{l^k})$ is irreducible is equivalent to showing that β has degree dl^k over $\mathbf{F}_q$. This, in turn, is equivalent to showing that

$$\beta^{q^i} = \beta \Longleftrightarrow dl^k \mid i.$$

We first show that $\beta^{q^d - 1}$ is a primitive l^k-th root of unity. Since $\beta^{l^k} = \alpha$ and $\alpha^{q^d - 1} = 1$, it is clear that β^{q^d-1} is an l^k-th root of unity. Moreover, since α is not an lth power it must be that l divides $\#\mathbf{F}_{q^d}^{\times} = q^d - 1$, and that

$$\left(\beta^{q^d - 1}\right)^{l^{k-1}} = \alpha^{(q^d-1)/l} \neq 1.$$

Thus the order of β^{q^d-1} must be a divisor of l^k that is not a divisor of l^{k-1}; since l is prime, the only possibility for this order is l^k itself, giving our claim.

If $\beta^{q^i} = \beta$, then raising both sides to the l^k-th power we find that $\alpha^{q^i} = \alpha$; since

α has degree d, this implies that d divides i. So write $i = di'$. Then

$$\beta^{q^i} = \beta \iff \beta^{q^{di'}-1} = 1 \iff \left(\beta^{q^d-1}\right)^{\frac{q^{di'}-1}{q^d-1}} = 1.$$

From the above, the last equality holds precisely when

$$l^k \mid \frac{q^{di'}-1}{q^d-1}.$$

By Lemma 3.2.2 (applied with the prime l and the integer $a = q^d$), this last possibility holds if and only if l^k divides i', which in turn holds if and only if dl^k divides i. □

Applied to polynomials of the form $T - \beta$, this Lemma immediately yields the following result (which can also be deduced from Capelli's classification of irreducible binomials; see, e.g., [76, Chapter VI, Theorem 9.1]):

Corollary 3.2.3. *Let l be an odd prime. If $\beta \in \mathbf{F}_q$ is not an lth power, then*

$$T^{l^k} - \beta \quad \textit{is irreducible over } \mathbf{F}_q \textit{ for every } k = 0, 1, 2, \ldots.$$

The same result holds for $l = 2$ if also $q \equiv 1 \pmod 4$.

How are these results useful? Consider, e.g., the problem of producing twin prime pairs $f, f+1$ over a finite field. With l a prime to be chosen conveniently, we consider the binomials $T^{l^k} + \alpha$ and $T^{l^k} + \alpha + 1$. Corollary 3.2.3 tells us that whether or not both of these polynomials are irreducible depends (at least if $l > 2$) only on the lth power character of α and $\alpha + 1$. (In particular, there is no dependence on k!) Thus, if we can choose l and α appropriately, then varying k gives us an infinite family of twin prime pairs. This was Hall's strategy, and it is also our strategy in proving Theorem 3.1.2.

Consider now the situation of Theorem 3.1.3. Thus we are given irreducibles $f_1, \dots, f_r$ over $\mathbf{F}_q$ and we seek a prime l and a $\beta \in \mathbf{F}_q$ for which each $f_i(T^{l^k} - \beta)$ is irreducible (for all $k \geq 0$). If l is a prime for which the hypotheses of Lemma 3.2.1 are satisfied simultaneously with respect to every $f_i(T)$, then our job is easy: use this l and take $\beta = 0$. Of course there is no guarantee that such an l exists. We prove Theorem 3.1.3 by showing that we can always satisfy the hypotheses of Lemma 3.2.1 for some l if we allow ourselves to replace the given family $\{f_i(T)\}_{i=1}^r$ by the translated family $\{f_i(T - \beta)\}_{i=1}^r$ for an appropriate $\beta \in \mathbf{F}_q$.

To summarize, in both cases our success hinges on the existence of an appropriate configuration of lth power nonresidues. In the proof of Theorem 3.1.2, the arguments guaranteeing that these configurations exist are usually combinatorial. To prove Theorem 3.1.3, we take a different tack, detecting configurations of nonresidues via estimates for character sums.

3.3 Proof of Theorem 3.1.2

The following near-trivial combinatorial lemma is at the heart of Theorem 3.1.2:

Lemma 3.3.1. *Let α be a nonzero element of $\mathbf{F}_q$. Suppose that for every pair a, b of elements of $\mathbf{F}_q$ which differ by α, either a or b belongs to some given set S. Then $\#S \geq q/2$; i.e., S contains at least half the elements of $\mathbf{F}_q$.*

Proof. Indeed, in this case $\mathbf{F}_q \subset S \cup S'$, where $S' := \{s - \alpha : s \in S\}$. □

The remainder of the proof is divided into three cases:

3.3.1 Case I: $q > 4$ and $q \equiv 1 \pmod{l}$ for some odd prime l

Theorem 3.1.2 for a given α then follows from Corollary 3.2.3 if we can produce a pair of lth power nonresidues of $\mathbf{F}_q$ differing by α. The set of lth powers in $\mathbf{F}_q$ has cardinality $1+(q-1)/l$, and this is strictly smaller than $q/2$ except when $q=4$ and $l=3$ (which will be treated in Case III). We now appeal to Lemma 3.3.1, taking for S the set of lth powers in $\mathbf{F}_q$; this finishes the proof whenever $q-1$ has an odd prime divisor and $q \neq 4$.

3.3.2 Case II: $q > 5$ and $q = 1+2^k$ for some k

One can show elementarily that the only prime powers q meeting this requirement are $q=9$ and the Fermat primes greater than 5 (see [108], p. 374, Exercise 1). We apply Corollary 3.2.3 with $l=2$, noting that all the q under consideration satisfy $q \equiv 1 \pmod 4$. It is straightforward to check directly that every nonzero element of $\mathbf{F}_9$ is a difference of nonsquares. To treat the case when q is a Fermat prime, we note that if p is any odd prime and α any nonzero element of $\mathbf{F}_p$, then the number of pairs of nonsquares in $\mathbf{F}_p$ differing by α is

$$\frac{1}{4}\sum_{\substack{a \pmod p \\ a\not\equiv 0,\ a+\alpha\not\equiv 0 \pmod p}} \left(1-\left(\frac{a}{p}\right)\right)\left(1-\left(\frac{a+\alpha}{p}\right)\right) =$$

$$\frac{1}{4}\left(p+\sum_{a \pmod p}\left(\frac{a}{p}\right)\left(\frac{a+\alpha}{p}\right)-\left(1-\left(\frac{\alpha}{p}\right)\right)-\left(1-\left(\frac{-\alpha}{p}\right)\right)\right).$$

Simplifying this expression using the evaluation $\sum \left(\frac{a}{p}\right)\left(\frac{a+\alpha}{p}\right) = -1$ of the Jacobsthal sum (cf. [10], Theorem 2.1.2) gives a count of

$$\frac{1}{4}\left(p - 3 + \left(\frac{\alpha}{p}\right) + \left(\frac{-\alpha}{p}\right)\right),$$

which is always positive if $p > 5$. This settles all cases when $q - 1$ has no odd prime divisor, except those corresponding to $q = 3$ and $q = 5$.

3.3.3 Case III: $q = 3$, 4 or 5

The cases not covered by the above analysis are handled by a direct appeal to Lemma 3.2.1. For each q and α, we find a pair of twin prime polynomials $f, f + \alpha$ and a prime l for which the conditions of Lemma 3.2.1 hold simultaneously for both f and $f + \alpha$. The pairs $f, f + \alpha$ and the information needed to verify the hypotheses of the lemma are presented in Table 3.1. For example, the first line of Table 3.1 describes the proof that the polynomials

$$T^{3\cdot 13^k} - T^{13^k} + 1, \quad T^{3\cdot 13^k} - T^{13^k} + 2$$

form a twin prime pair over $\mathbf{F}_3$ for each $k = 1, 2, 3, \ldots$. □

Without giving the details, we mention the analogous theorem for prime triplets:

Theorem 3.3.2 (Prime triplet theorem). *Let $\mathbf{F}_q$ be a finite field with $q > 3$. If α and β are distinct elements of $\mathbf{F}_q^\times$, then there are infinitely many monic prime triplets $f, f + \alpha, f + \beta$ in $\mathbf{F}_q[T]$.*

That such a result is valid for all but finitely many q is immediate from Theorem 3.1.3; all that remains is to check the validity of this result over the remaining "small"

q	α	**Twin Prime Pair** $f, f+\alpha$	**Orders**	q^d-1	l
3	1	$T^3-T+1,\ T^3-T+2$	$2\cdot 13,\ 13$	$2\cdot 13$	13
4	1	$T-\beta,\ T-\beta+1$	3, 3	3	3
	β	$T^2+(\beta+1)T+1, T^2+(\beta+1)T+\beta+1$	$5,\ 3\cdot 5$	$3\cdot 5$	5
	$\beta+1$	$T^2+\beta T+1, T^2+\beta T+\beta$	$5,\ 3\cdot 5$	$3\cdot 5$	5
5	1	$T+2,\ T+3$	$2^2,\ 2^2$	2^2	2
	2	$T^3+T+4,\ T^3+T+1$	$31,\ 2\cdot 31$	$2^2\cdot 31$	31

Table 3.1: Explicit monic twin prime pairs for small q, where β is such that $\mathbf{F}_4 = \mathbf{F}_2(\beta)$. In odd characteristic we include only one of $\{\alpha, -\alpha\}$.

finite fields $\mathbf{F}_q$, as in our Table 3.1. This is a straightforward (if somewhat tedious) computation.

3.4 Proof of Theorem 3.1.3

3.4.1 A character sum estimate

The following consequence of Weil's Riemann Hypothesis appears as [119, Corollary 2.2]:

Lemma 3.4.1 (Lenstra)**.** *Suppose we are given an n-dimensional commutative $\mathbf{F}_q$-algebra A, an element $x \in A$ and a character χ of the multiplicative group $A^\times$ (extended by zero to all of A) which is nontrivial on $\mathbf{F}_q[x]$. Then*

$$\left|\sum_{\beta\in\mathbf{F}_q} \chi(\beta+x)\right| \leq (n-1)\sqrt{q}.$$

Lemma 3.4.2. *Let $f_1(T), \dots, f_s(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$. Fix roots $\alpha_1, \dots, \alpha_s$ of $f_1, \dots, f_s$, respectively, lying in an algebraic closure of $\mathbf{F}_q$. Suppose that for every $1 \leq i \leq s$ we are given a multiplicative character χ_i of*

$\mathbf{F}_q(\alpha_i)$ and that at least one of these χ_i is nontrivial. Then

$$\left|\sum_{\beta\in\mathbf{F}_q} \chi_1(\alpha_1+\beta)\cdots\chi_s(\alpha_s+\beta)\right| \leq (D-1)\sqrt{q}, \tag{3.8}$$

where D is the sum of the degrees of the f_i.

Proof. We argue as in [119, Corollary 2.4]. Define $F := \prod_{i=1}^{s} f_i$ and set $A := \mathbf{F}_q[T]/(F)$. Thus A is generated over $\mathbf{F}_q$ by the residue class $T \bmod F$. By the Chinese remainder theorem, we obtain a multiplicative character χ on A by setting $\chi(g \bmod F) := \prod_{i=1}^{s} \chi_i(g(\alpha_i))$. Since some χ_i is nontrivial on $\mathbf{F}_q(\alpha_i)$, we see that χ is nontrivial on A. Moreover, for $\beta \in \mathbf{F}_q$, we have $\chi((\beta+T) \bmod F) = \prod_{i=1}^{s} \chi(\alpha_i + \beta)$. The result now follows from Lemma 3.4.1, since A is an $\mathbf{F}_q$-algebra of dimension $\deg F = \sum_{i=1}^{s} \deg f_i = D$. □

3.4.2 Proof of Theorem 3.1.3

We now turn to the proof of Theorem 3.1.3. We may assume that the f_i are nonassociate. We will prove that the conclusion of Theorem 3.1.3 holds provided $q > 3$ and

$$q + \left(2^r - 1 - 2^{r-1}\sum_{i=1}^{r} \deg f_i\right)\sqrt{q} - 2^{r-1}r > 0. \tag{3.9}$$

Note that if the condition (3.2) from Theorem 3.1.3 holds, then (3.9) also holds. To see this, write $D = \sum \deg f_i$. If (3.2) holds, then $\sqrt{q} > 2^{r-1}D$; thus

$$\begin{aligned} q + \left(2^r - 1 - 2^{r-1}\sum_{i=1}^{r} \deg f_i\right)\sqrt{q} &= \sqrt{q}\left(\sqrt{q} - 2^{r-1}D\right) + \sqrt{q}(2^r-1) \\ &> \sqrt{q}(2^r-1) > (2^{r-1}D)(2^r-1) \geq 2^{r-1}r(2^r-1) \geq 2^{r-1}r, \end{aligned}$$

which gives (3.9).

Choose roots $\alpha_1, \ldots, \alpha_r$ of $f_1, \ldots, f_r$, respectively, from a fixed algebraic closure of $\mathbf{F}_q$. We can fix l so that one of the following two conditions holds:

(i) l is an odd prime dividing $q-1$,

(ii) $l = 2$ and $q \equiv 1 \pmod 4$.

Indeed, since $q > 3$, if there is no l for which (i) holds, then the choice $l = 2$ always satisfies (ii).

Lemma 3.4.3. *Assuming the above notation and hypotheses, there always exists an element $\beta \in \mathbf{F}_q$ with the property that for every $1 \leq i \leq r$,*

$$\alpha_i + \beta \textit{ is not an } l\textit{th power (vanishing or otherwise) in } \mathbf{F}_q(\alpha_i).$$

Proof. For each $i = 1, 2, \ldots, r$, fix a multiplicative character χ_i of order l on $\mathbf{F}_q(\alpha_i)$. Consider the sum

$$\sum_{\beta \in \mathbf{F}_q} (1 - \chi_1(\alpha_1 + \beta))(1 - \chi_2(\alpha_2 + \beta)) \cdots (1 - \chi_r(\alpha_r + \beta)). \tag{3.10}$$

Multiplying this out, it is

$$q + \sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ \mathcal{I} \neq \emptyset}} \sum_{\beta \in \mathbf{F}_q} \prod_{i \in \mathcal{I}} \chi_i(\alpha_i + \beta).$$

By Lemma 3.4.2, we can bound this from below by

$$\begin{aligned} q - \sum_{\substack{\mathcal{I}\subset\{1,2,\ldots,r\}\\ \mathcal{I}\neq\emptyset}} \left(-1 + \sum_{i\in\mathcal{I}} \deg f_i\right)\sqrt{q} \\ &= q + (2^r - 1)\sqrt{q} - \sum_{i=1}^{r} \deg f_i \left(\sum_{\substack{\mathcal{I}\subset\{1,2,\ldots,r\}\\ i\in I}} 1\right)\sqrt{q} \\ &= q + (2^r - 1)\sqrt{q} - 2^{r-1}\left(\sum_{i=1}^{r} \deg f_i\right)\sqrt{q} > 2^{r-1}r, \quad (3.11) \end{aligned}$$

using (3.9) for the last inequality. Suppose the lemma is false and so for each $\beta \in \mathbf{F}_q$, there is an $i = i(\beta)$ for which $\alpha_i + \beta$ is an lth power in $\mathbf{F}_q(\alpha_i)$. If $\alpha_i + \beta$ is nonzero for this i, then the summand corresponding to β in (3.10) vanishes, while if $\alpha_i + \beta = 0$, then the corresponding summand has absolute value at most 2^{r-1}. Since the latter is possible for at most r values of β, the sum (3.10) is bounded above by $2^{r-1}r$, contradicting (3.11). □

Proof of Theorem 3.1.3. With β as in Lemma 3.4.3, apply the substitution $T \mapsto T - \beta$ to the sequence of polynomials $f_1, \ldots, f_r$. This yields a new sequence $h_1, \ldots, h_r$ (say) of irreducible polynomials over $\mathbf{F}_q$ with corresponding nonzero roots $\alpha_1 + \beta, \ldots, \alpha_r + \beta$. By Lemma 3.2.1 all the polynomials

$$h_1(T^{l^k}) = f_1(T^{l^k} - \beta), \ldots, h_r(T^{l^k}) = f_r(T^{l^k} - \beta) \quad \text{for } k = 0, 1, 2, \ldots$$

are irreducible, which proves the theorem. □

Example. Let α be any nonsquare in $\mathbf{F}_q^{\times}$; we show that there are infinitely many monic primes in $\mathbf{F}_q[T]$ of the form $f^2 - \alpha$. By Theorem 3.1.3 (with $r = 1$ and

$f_1(T) = T^2 - \alpha$), we know this is true for all large q; referring to (3.9) shows that $q > 3$ is large enough. When $q = 3$, we must have $\alpha = -1$, and we can treat this case directly. Indeed, the irreducible polynomial $(T+1)^2+1$ has order $8 = 3^2-1$, and so Lemma 3.2.1 shows that $(T^{2^k}+1)^2+1$ is irreducible over $\mathbf{F}_3$ for every $k = 0, 1, 2, \ldots$.

Example. Let $f(x, y)$ be an irreducible binary form over $\mathbf{F}_q$ of degree $n \geq 2$. We claim that if $q > n^2$, then $f(A, A+1)$ is irreducible for infinitely many monic A. Since $n \geq 2$, we may express f as the homogenization of an irreducible degree n polynomial g:

$$f(x, y) = y^n g(x/y), \quad \text{where} \quad g(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_0.$$

The polynomial $f(T, T+1)$ has degree n and leading coefficient $g(1) \neq 0$. Let α be a root of $f(T, T+1)$; since $f(-1, 0) = a_n(-1)^n \neq 0$, we have $\alpha \neq -1$. Now $\alpha/(\alpha+1)$ is a root of g and so has degree n over $\mathbf{F}_q$. But then α must also have degree n, which yields the irreducibility of $f(T, T+1)$. The original assertion is now obtained by applying Theorem 3.1.3 to $f(T, T+1)$. Actually for $q > 16(n+2)^2$, the same statement holds even if we require also that A and $A+1$ are prime, as we see by applying Theorem 3.1.3 to the three polynomials T, $T+1$, and $f(T, T+1)$.

3.5 Proof of Theorem 3.1.4

Lemma 3.5.1. *Fix a finite field $\mathbf{F}_q$. For each $d \geq 2$,*

$$\#\mathcal{E}_d \leq \frac{1}{\mathrm{rad}'(q^d-1)} \frac{q^d-1}{d}. \tag{3.12}$$

Proof. Let E be the set of elements of $\mathbf{F}_{q^d}$ whose minimal polynomials belong to

$\mathcal{E}_d$. By Lemma 3.2.1, each α in E is an lth power for every odd prime $l \mid q^d - 1$, so is an Lth power for

$$L := \prod_{\substack{l \text{ odd prime} \\ l \mid q^d - 1}} l = \operatorname{rad}'(q^d - 1).$$

Thus $\#E \leq \#((\mathbf{F}_{q^d}^{\times})^L) = (q^d - 1)/L$. But the action of $\operatorname{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q)$ partitions E into orbits of length d, each of which corresponds to a single element of $\mathcal{E}_d$. This proves (3.12). □

Before proceeding we recall an 1886 result of Bang [5] (see, e.g., [98] for a modern proof):

Bang's theorem. *Let a and n be integers > 1. There is a prime l which divides $a^n - 1$ but not $a^m - 1$ for any $m < n$, except in the following cases:*

(i) *$n = 2$, $a = 2^s - 1$, where $s \geq 2$,*

(ii) *$n = 6$, $a = 2$.*

Proof of the upper bounds (3.3) *and* (3.4) *on $\#\mathcal{E}_d$.* By Bang's theorem, if $d > 6$ (as we can assume), then there is a primitive prime divisor l of $q^d - 1$. Then $l \equiv 1 \pmod{d}$, and so in particular $L \geq l > d$. Lemma 3.5.1 now gives (3.3). The abc Conjecture implies that for each $\epsilon > 0$,

$$L \geq \frac{1}{2}\operatorname{rad}(q^d - 1) \gg_\epsilon q^{d(1-\epsilon)-1},$$

and this proves (3.4). □

Remark. Actually one can do a bit better unconditionally than stated in Theorem 3.1.4; for example, the results of Stewart & Yu toward the abc Conjecture [110] imply that $\mathrm{rad}'(q^d - 1) \geq d^{3+o_q(1)}$ as $d \to \infty$, leading to a corresponding (unconditional but no longer elementary) upper bound of $q^d/d^{4+o_q(1)}$.

Proof that $\mathcal{E}_d$ is empty for almost all d, assuming (3.5). It is enough to prove that for almost all d, no element of $\mathbf{F}_{q^d}$ of degree d over $\mathbf{F}_q$ is an Lth power for $L := \mathrm{rad}'(q^d - 1)$. Suppose, contrariwise, that α is such an element. Let

$$Q := \frac{q^d - 1}{L} \quad \text{and let} \quad m := l_q(Q).$$

Then trivially $m \leq d$. Now $\alpha^Q = 1$ (as α is a nonzero Lth power), so that

$$\alpha^{q^m} = \alpha \left(\alpha^Q\right)^{\frac{q^m - 1}{Q}} = \alpha.$$

Thus α has degree $\leq m$ over $\mathbf{F}_q$ and so $d \leq m \leq d$. So $m = d$.

Now fix a large positive number B. We may restrict attention to those d with a prime factor $> B$, since the exceptional d have density 0. Given d of this type, let $l > B$ be its largest prime factor. As $m = d$, it follows that l divides $m = l_q(Q)$, and so l divides $l_q(R)$ for some prime power $R \parallel Q$. If R is a power of the prime r, then necessarily $r \geq l > B$, and from $r \mid Q$ we deduce that

$$r^2 \mid rQ = \frac{q^d - 1}{L/r} \mid q^d - 1,$$

so that $l_q(r^2) \mid d$.

Thus d is divisible by $l_q(r^2)$ for some prime $r > B$. But the number of such

$d \leq x$ is

$$\leq \epsilon_B x, \quad \text{where} \quad \epsilon_B := \sum_{\substack{r>B \\ r \text{ prime} \\ r \nmid q}} \frac{1}{l_q(r^2)}.$$

So the upper density of such d is bounded by ϵ_B; but (3.5) implies that $\epsilon_B \to 0$ as $B \to \infty$. □

Example. In practice it is rare that $d = m$, which as we have just seen is forced upon us if $\mathcal{E}_d \neq \emptyset$. Consider, e.g., the case $q = 2$. At the time of writing, the first d for which the complete factorization of $2^d - 1$ is not known is $d = 787$ (see [12]). Using the known factorizations for smaller d, one can calculate that $m < d$ for all $d < 787$, except for $d = 364$. In that case

$$\frac{2^{364} - 1}{\mathrm{rad}'(2^{364} - 1)} = 1093 \quad \text{and} \quad l_2(1093) = 364.$$

Thus the only polynomials $f(T)$ of degree 364 over $\mathbf{F}_2$ for which Buniakowsky's conjecture can fail are those with a root $\alpha \in \mathbf{F}_{2^{364}}$ with $\alpha^{1093} = 1$. Now if $f(T)$ has this property, replace $f(T)$ with $f(T-1)$. This has the root $\alpha + 1$, and we cannot have both

$$\alpha^{1093} = 1 \quad \text{and} \quad (\alpha + 1)^{1093} = 1 \quad \text{in } \mathbf{F}_{2^{364}},$$

since one can compute that the resultant

$$\mathrm{Res}(T^{1093} - 1, (T+1)^{1093} - 1) \not\equiv 0 \pmod{2}.$$

So Bouniakowsky's conjecture must hold for $f(T-1)$, and so also for our original f. We conclude that Bouniakowsky's conjecture holds for every irreducible of degree

$d < 787$.

3.6 Other applications of the substitution method

Consider the problem of studying $\mathbf{F}_q[T]$-points on algebraic sets defined over $\mathbf{F}_q$. In other words, suppose that we have a system of equations

$$f_i(X_1, \dots, X_N) = 0$$

where each f_i belongs to $\mathbf{F}_q[X_1, \dots, X_N]$. Suppose that $(A_1(T), \dots, A_N(T)) \in \mathbf{F}_q[T]^N$ is an initial solution. Then trivially, $(A_1(h(T)), \dots, A_N(h(T)))$ is also a solution for every polynomial $h(T)$. It follows that if there is a single $\mathbf{F}_q[T]$-valued point on this algebraic set, not having all its coordinates constant, then there are infinitely many. The importance of Theorem 3.1.3 is that it allows us to obtain results of the same kind when some of the coordinates X_i are restricted to irreducible values, provided that q is large compared to the sum of the degrees of the initial solution $(A_1(T), \dots, A_N(T))$.

For example, suppose we are interested in exhibiting infinitely many irreducibles which are sums of three irreducibles cubes. Then we are looking for solutions to the equation

$$X_1^3 + X_2^3 + X_3^3 = X_4 \tag{3.13}$$

where all of $X_1, \dots, X_4$ are prescribed to be irreducible. If we can write down a single solution to (3.13) with all the X_i small (say of absolutely bounded degree), then Theorem 3.1.3 implies that as long as q is large enough, this equation has infinitely many solutions. Moreover, the solutions provided by Theorem 3.1.3 arise from the initial solution in a very explicit way, so that properties of the initial solution translate predictably to properties of the entire family of solutions. (For example, if all the X_i in the initial solution are monic, then so are all the X_i in the infinite family, etc.)

Following this strategy, in Chapter 4 we will prove the following result:

Theorem. *If* $\mathbf{F}_q$ *is a finite field with characteristic* > 3*, then infinitely many monic primes* P *over* $\mathbf{F}_q$ *have a representation in the form*

$$P = A^3 + B^3 + C^3, \quad \textit{where } A, B, C \textit{ are monic primes,}$$
$$\deg A > \max\{\deg B, \deg C\}.$$

The difficulty in proving this result lies in showing that for any field $\mathbf{F}_q$ of characteristic $\neq 2, 3$, one can find an initial solution to (3.13) with each X_i of bounded degree.

If one is content in proving the preceding theorem for a positive proportion of fields, then the proof is much easier: Start with the universal identity

$$T^3 + (T+1)^3 + (T^2+1)^3 = T^6 + 3T^4 + 2T^3 + 6T^2 + 3T + 2. \tag{3.14}$$

The polynomial on the right-hand side of this identity has Galois group over $\mathbf{Q}$ the full symmetric group on six letters. Moreover, its splitting field has odd discriminant, and so is linearly disjoint over $\mathbf{Q}$ from the splitting field $\mathbf{Q}(i)$ of $T(T+1)(T^2+1)$. So by the Chebotarev density theorem for number fields, the four polynomials involved in the identity (3.14) are irreducible modulo q for precisely $\frac{1}{2} \cdot \frac{1}{6} = \frac{1}{12}$ of all primes q. And for these primes q, we may take (3.14) as our initial input to Theorem 3.1.3.

To obtain an initial solution for *all* fields of characteristic $\neq 2, 3$, we will again appeal to the Chebotarev density theorem. However, what is needed is not the number field version applied above, but an effective version for *function fields.* It is to this circle of ideas that we now turn our attention.

Chapter 4

Preliminary applications of the Chebotarev density theorem

4.1 Introduction

In this chapter we show how the Chebotarev density theorem for function fields can be used to settle certain problems concerning the distribution of irreducible polynomials over finite fields. The proofs exhibit a similar structure to the applications towards Hypothesis H that will be given in the next chapter, but the technical details are far less daunting.

We take as our primary target an analogue of the classical Hilbert irreducibility theorem. In its simplest form, that theorem asserts that if $f(T, u)$ is a polynomial in two variables irreducible over $\mathbf{Q}$, then there are infinitely many choices of $a \in \mathbf{Q}$ for which $f(T, a)$ is irreducible as a one-variable polynomial over $\mathbf{Q}$. It is not obvious how to formulate a finite field analogue; if $f(T, u)$ is irreducible over $\mathbf{F}_q$, there need not be any values of $a \in \mathbf{F}_q$ for which $f(T, u)$ is irreducible. (For example, $T^n - u$

is always irreducible over $\mathbf{F}_q$, but if n is coprime to $q-1$ then $T^n - a$ always has a linear factor.)

The following theorem can be seen as a partial result in this direction:

Theorem 4.1.1. *Let $f(T,u)$ be an absolutely irreducible polynomial in two variables over $\mathbf{F}_q$, monic in T, with $\deg_T f(T,u) = n$ and $\deg_u f(T,u) = m$. Suppose that the characteristic of $\mathbf{F}_q$ exceeds n. Assume further that the T-discriminant of $f(T,u)$ is squarefree in $\mathbf{F}_q[u]$. Then there are*

$$q/n + O(n!mq^{1/2})$$

values of $a \in \mathbf{F}_q$ for which $f(T,a)$ is irreducible in $\mathbf{F}_q[T]$. Here the implied constant is absolute.

Theorem 4.1.1 is no doubt far from optimal in both the conditions imposed on f and in the shape of the error-term. However, formulating a satisfactory conjecture at any level of generality appears difficult.

Example. Fix a positive integer $n \geq 2$. Chowla conjectured [26] that for $p > p_0(n)$, one can always find an irreducible polynomial over $\mathbf{F}_p$ of the form $T^n + T + a$, where $a \in \mathbf{F}_p$. Moreover, he predicted that the number of such a is asymptotically p/n as $p \to \infty$, and proved this in the first nontrivial case, when $n = 3$.

Theorem 4.1.1 is immediately applicable to this problem. Let p be a prime larger than n. The T-discriminant of $T^n + T + u$ is

$$(-1)^{\binom{n}{2}}(n^n u^{n-1} + (1-n)^{n-1}),$$

which is easily checked to be squarefree in $\mathbf{F}_p[u]$ (since $p \nmid n(n-1)$). It follows from

Theorem 4.1.1 that the number of $a \in \mathbf{F}_p$ for which $T^n + T + a$ is irreducible is $p/n + O(n!p^{1/2})$. This confirms Chowla's predicted asymptotic formula, and at the same time shows that one can take $p_0(n) = C((n+1)!)^2$ for an appropriate constant C. In fact, a bit of attention to detail in the proofs below shows that one may take $C = 2$.

Chowla's asymptotic formula was confirmed independently but almost simultaneously by Cohen [27] and Ree [94], using the theory of algebraic function fields and Weil's effective form of the Chebotarev density theorem. (However, neither author made explicit the dependence on n to obtain a value for C_0.) The proof of Theorem 4.1.1 was inspired by these authors' arguments and exhibits a very similar structure.

The second goal of this chapter is to establish the following result, alluded to in Chapter 3:

Theorem 4.1.2. *If $\mathbf{F}_q$ is a finite field with characteristic > 3, then infinitely many monic primes P over $\mathbf{F}_q$ have a representation in the form*

$$P = A^3 + B^3 + C^3, \quad \textit{where } A, B, C \textit{ are monic primes,}$$
$$\textit{and } \deg A > \max\{\deg B, \deg C\}.$$

The proof technique was already hinted at in the preceding chapter: For $q \gg 0$, the substitution method shows that is enough to exhibit an identity of the shape

$$P(T) = T^3 + (T+1)^3 + (T^2 + a)^3,$$

where $a \in \mathbf{F}_q$, and both $P(T)$ and $T^2 + a$ are irreducible. Were it not for the requirement that $T^2 + a$ be irreducible, such a result would follow (for large q and with certain restrictions on the characteristic) from Theorem 4.1.1 applied to the polynomial $f(T, u) = T^3 + (T+1)^3 + (T^2 + u)^3$. While Theorem 4.1.1 cannot be applied as it stands, we shall see that it is possible to modify its proof to yield Theorem 4.1.2.

4.2 Preparation for the proof of Theorem 4.1.1

4.2.1 Algebraic function fields

The proof of Theorem 4.1.1 depends on the arithmetic theory of *global function fields*: finite extensions of the field of rational functions over a finite field.

For the convenience of the reader, we summarize some of the relevant definitions. Readable introductions to the theory of algebraic function fields include Stichtenoth's monograph [111] where the subject is developed alongside applications to coding theory, Rosen's textbook [102], and the very thorough recent treatment of Villa Salvador [117].

We say that K is an *algebraic function field* over k if K/k is a finitely generated extension of transcendence degree 1. (Thus a *global function field* is an algebraic function field K/k with k finite.) If K/k is a function field, the set of elements of K algebraic over k is called the *field of constants of* K. Henceforth we adopt the usual convention that whenever we are given a function field K/k, the field k is the full field of constants of K. (To satisfy this requirement, it suffices to replace k with its algebraic closure in K.)

To each function field K/k there is an important nonnegative integer invariant, known as the *genus* of K. When $k = \mathbf{C}$ is the field of complex numbers, this admits a topological interpretation: One can identify the function field K/k as the field of meromorphic functions of a compact Riemann surface (uniquely determined up to conformal equivalence). Such a Riemann surface is a compact orientable 2-manifold, and so is homeomorphic to a g-holed torus for a unique integer $g \geq 0$; this integer g is called the *genus* of K. For an arbitrary function field K/k, the definition of the genus of K goes through the theory of the adeles of K, and is too complicated to be given here. (See [117, §3.3] for the details.)

If L/l and K/k are two function fields, we say that L/l is an *extension* of K/k if K is a subfield of L and $l \cap K = k$. We say that L/l is a *geometric extension* of K/k if $l = k$. One can show that if L is a finite (resp. algebraic) extension of K, then l is a finite (resp. algebraic) extension of k ([117, Propositions 5.1.8, 5.1.9]). As a consequence, if k is algebraically closed, then every algebraic extension of K is geometric.

To each function field K/k, there is an associated theory of divisors, which is foundational to the arithmetic of function fields in the same way that ideal theory is for number fields. (See [117, Chapters 2, 3].) The theory of the decomposition of prime divisors under extensions is also quite analogous to the corresponding theory for prime ideals. For example, if L is a finite extension of K, then every prime $\mathfrak{P}$ of L lies over a unique prime P of K. Moreover, in this case there are well-defined positive integers $e(\mathfrak{P}/P)$ and $f(\mathfrak{P}/P)$, the ramification index and residual degree, respectively (cf. [117, Definition 5.1.5, Proposition 5.1.8]). A prime P of K is said to be *unramified* in L if $e(\mathfrak{P}/P) = 1$ for every prime $\mathfrak{P}$ of L that lies over P. We say that the prime P of K is *tamely ramified* in L if for every prime $\mathfrak{P}$ of L above P, the characteristic of K does not divide $e(\mathfrak{P}/P)$. We say that L/K is *unramified* (resp. *tamely ramified*) if every prime $\mathfrak{P}$ of K is unramified in L (resp. tamely ramified).

Suppose L/K is a Galois extension of function fields. If P is a prime of K unramified in L, then proceeding as in the number field case, one can define the *Frobenius of P in L/K*, denoted $(L/K, P)$; it is a well-defined conjugacy class of the Galois group of L/K. Moreover, such Frobenius elements are "uniformly distributed" in an appropriate sense – i.e., there is an analogue of the Chebotarev density theorem in this context. (See [117, §11.2].) We shall meet a precise version of this last result in the sequel.

4.2.2 A criterion of Hayes

Here we establish a criterion for certain Galois groups to be the full symmetric group on n letters. This can be considered as making explicit results which are already, for the most part, implicit in Hayes's paper [62].

Lemma 4.2.1. *Let K be a rational function field and L a finite, geometric, tamely ramified extension of K. Let P be a prime of K of degree* 1*. Suppose that L/K is unramified except possibly at primes lying above P. Then $L = K$.*

Proof. This is more or less an immediate consequence of the Riemann-Hurwitz genus formula ([117, Theorem 9.4.2]) but we give the details for the sake of completeness.

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ denote the primes which lie above P. Since L/K is tamely ramified and unramified except at the $\mathfrak{P}_i$, writing $e_i = e(\mathfrak{P}_i/P)$ we have that the different $\mathfrak{D}_{L/K}$ is given by

$$\mathfrak{D}_{L/K} = \sum_{i=1}^{r} (e_i - 1)\mathfrak{P}_i.$$

(See [117, Theorem 5.6.3].) Thus, by the Riemann-Hurwitz genus formula,

$$\begin{aligned}2g_L - 2 &= [L:K](2g_K - 2) + \sum_{i=1}^{r}(e_i - 1)\deg \mathfrak{P}_i \\ &= -2[L:K] + [L:K] - \sum_{i=1}^{r}\deg \mathfrak{P}_i \\ &= -[L:K] - r.\end{aligned}$$

Since $g_L \geq 0$, we must have $r = 1 = [L:K]$, so that $L = K$ as claimed. □

Before proceeding we recall Hensel's lemma in the form in which we need it (see [117, Theorems 2.2.20, 2.3.14]):

Hensel's lemma. *Let K be a field complete with respect to a discrete, nonarchimedean valuation, k the corresponding residue field, $\mathcal{O}$ the valuation ring, and $\mathcal{M}$ the maximal ideal (so that $k = \mathcal{O}/\mathcal{M}$). Suppose $f(T) \in \mathcal{O}[T]$ is a polynomial with leading coefficient not in $\mathcal{M}$. Let $\bar{f}(T) = f(T) \bmod \mathcal{M} \in k[T]$, and suppose that $\bar{f}(T) = h(T)g(T)$ with $h(T), g(T) \in k[T]$ and $h(T), g(T)$ relatively prime. Then there exist $H(T), G(T) \in K[T]$ with*

$$f(T) = H(T)G(T), \quad \bar{H}(T) = h(T), \quad \bar{G}(T) = g(T),$$

and

$$\deg H(T) = \deg h(T), \quad \deg G(T) = \deg g(T).$$

The next two lemmas constitute the main results of this section:

Lemma 4.2.2. *Let $f(T,u)$ be an absolutely irreducible polynomial in $\mathbf{F}_q[T,u]$ which is monic in T of T-degree n, where n is coprime to q. Let K be the splitting field* *of $f(T,u)$ over $\mathbf{F}_q(u)$, and let $\bar{K} = K\overline{\mathbf{F}}_q$ be the splitting field of $f(T,u)$ over $\overline{\mathbf{F}}_q(u)$. Suppose that*

(i) *the prime P_∞ corresponding to the $(1/u)$-adic valuation on $\overline{\mathbf{F}}_q(u)$ is tamely ramified in the extension $\bar{K}/\overline{\mathbf{F}}_q(u)$,*

(ii) *for each $\beta \in \overline{\mathbf{F}}_q$, the polynomial $f(T,\beta)$ has at most one multiple root, which is then a root of exact multiplicity* 2*.*

Then $\mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u))$ *is the full symmetric group on the n roots of $f(T,u)$. Consequently,* $\mathrm{Gal}(K/\mathbf{F}_q(u))$ *is also the full symmetric group on the roots of $f(T,u)$.*

Proof. Since n is coprime to q, the (absolutely irreducible) polynomial $f(T,u)$ is automatically separable, so that $\bar{K}/\overline{\mathbf{F}}_q(u)$ (as well as $K/\mathbf{F}_q(u)$) is Galois. Let $\bar{G}$ denote the Galois group of $\bar{K}/\overline{\mathbf{F}}_q(u)$, and let H be the subgroup of $\bar{G}$ generated by the decomposition groups of all the ramified primes of $\bar{K}$ that do not lie over P_∞. Let F be the fixed field of $\bar{G}$. Then $F/\overline{\mathbf{F}}_q(u)$ is unramified except possibly at primes above P_∞, where (by hypothesis) the ramification is tame. (See [111, III.8.3. Theorem].) Moreover, since $\overline{\mathbf{F}}_q$ is algebraically closed, $F/\overline{\mathbf{F}}_q(u)$ is geometric. By Lemma 4.2.1, we must have $F = \overline{\mathbf{F}}_q(u)$, so that $H = \bar{G}$.

Now to complete the proof that $\bar{G}$ is the full symmetric group, it suffices to show that H is generated by transpositions. (Here we use that the symmetric group has no proper transitive subgroups generated by transpositions – see [117, Lemma 14.4.13].) Let $\mathfrak{P}$ be a ramified prime of $\bar{K}$. Then $\mathfrak{P}$ lies over a prime of $\overline{\mathbf{F}}_q(u)$ corresponding to the $(u-\beta)$-adic valuation for some $\beta \in \overline{\mathbf{F}}_q$; call this prime P_β.

The decomposition group of $\mathfrak{P}/P_\beta$ can be canonically identified with the Galois group of the extension of local fields $\bar{K}_{\mathfrak{P}}/\overline{\mathbf{F}}_q(u)_{P_\beta}$ ([117, Theorem 5.4.10]). By Hensel's lemma and our hypothesis (ii), all but two of the roots of $f(T,u)$ belong to

$\overline{\mathbf{F}}_q(u)_{P_\beta}$, so that $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/\bar{\mathbf{F}}_q(u)_{P_\beta})$ is generated by a transposition of the remaining two roots.

Thus $\mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u))$ is the full symmetric group. Since $\mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u))$ injects (via restriction) into $\mathrm{Gal}(K/\mathbf{F}_q(u))$, this latter group must also be the full symmetric group. □

Lemma 4.2.3. *Under the same hypotheses as Lemma 4.2.2 (and with the same notation), the extension $K/\mathbf{F}_q(u)$ is geometric.*

Proof. In the proof of Lemma 4.2.2 we saw that restriction induces an isomorphism between $\mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u))$ and $\mathrm{Gal}(K/\mathbf{F}_q(u))$. Suppose that $\alpha \in K$ is algebraic over $\mathbf{F}_q$; then α is fixed by every element of $\mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u))$ and so also by every element of $\mathrm{Gal}(K/\mathbf{F}_q(u))$. The latter forces α to belong to $\mathbf{F}_q(u)$. But since α is algebraic over $\mathbf{F}_q$, it follows that α belongs to $\mathbf{F}_q$. □

4.2.3 Remarks on the conditions of Lemma 4.2.2

Let $f(T,u)$ be an absolutely irreducible polynomial over $\mathbf{F}_q$. Suppose moreover that f is monic in T and that $\deg_T f(T,u) = n$, where n is coprime to q. We make a few remarks in connection with Theorem 4.1.1 about the additional conditions (i) and (ii) on $f(T,u)$ imposed in Lemmas 4.2.2 and 4.2.3.

Firstly, condition (i) of Lemma 4.2.2 is automatically satisfied if $p > n$. Indeed, in this case P_∞ is, for trivial reasons, tamely ramified in each of the degree n extensions obtained by adjoining a single root of $f(T,u)$ to $\overline{\mathbf{F}}_q(u)$. That P_∞ is also tamely ramified in their compositum $\bar{K}$ now follows from repeated application of the following result (see [117, Theorem 12.4.4]):

Abhyankar's lemma. *Let F'/F be a finite separable extension of function fields.*

Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields $F \subset F_1, F_2 \subset F'$. Let P be a prime of F and P' a prime of F' lying above P. With $P_i := P' \cap F_i$ for $i = 1$ and 2, assume that at least one of the extensions P_1/P or P_2/P is tame. Then

$$e(P'/P) = \operatorname{lcm}[e(P_1/P), e(P_2/P)].$$

In particular, if both P_1/P and P_2/P are tamely ramified, then so is P'/P.

Secondly, condition (ii) of Lemma 4.2.2 holds provided that

$$\operatorname{disc}_T f(T, u) \quad \text{is a squarefree polynomial in } u.$$

To see this, we recall Zeuthen's rule, as it appears in [32, Lemma 4.6] (with minor changes in notation):

Zeuthen's rule. *Let $g_1(T, u) = 0$ and $g_2(T, u) = 0$ be (possibly empty) plane curves over an algebraically closed field K, and assume that these zero loci do not share a common irreducible component and that the leading T-coefficients of g_1 and g_2 do not have a common zero at $\beta \in K$. Then the resultant $\operatorname{res}_T(g_1, g_2)$ vanishes at β to order*

$$\sum_{c \in K} i_{(c,\beta)}(g_1, g_2),$$

where $i_{\mathbf{x}}(g_1, g_2)$ is the intersection number of the curves g_1 and g_2 at the point $\mathbf{x}$.

Remark. For the definition of the intersection number and the development of its properties, see [48, Chapter 3, §3]. For our purposes the following suffices: Let K be an algebraically closed field and suppose g_1 and g_2 are two affine plane curves over K. Let $\mathbf{x} \in \mathbf{A}^2(K)$. Then the intersection number $i_{\mathbf{x}}(g_1, g_2)$ of g_1 and g_2 at $\mathbf{x}$ is either a nonnegative integer or ∞, the latter occurring exactly when $\mathbf{x}$ belongs to a common component of g_1 and g_2. Also, $i_{\mathbf{x}}(g_1, g_2) \geq 1$ if and only if $\mathbf{x}$ belongs to the intersection of g_1 and g_2, and equality holds precisely when $\mathbf{x}$ is a nonsingular point of both g_1 and g_2 and g_1 and g_2 have distinct tangent lines at $\mathbf{x}$.

We are assuming that $f(T, u)$ is absolutely irreducible, monic in T of T-degree n, and that n is coprime to q. It follows that

$$\operatorname{disc}_T f(T, u) = (-1)^{n(n-1)/2} \operatorname{res}_T \left(f(T, u), \frac{\partial}{\partial T} f(T, u) \right)$$

vanishes at $u = \beta$ to order

$$\sum_{c \in \overline{\mathbf{F}}_q} i_{(c,\beta)} \left(f, \frac{\partial}{\partial T} f \right),$$

where $i_{(c,\beta)}(f, \frac{\partial}{\partial T} f)$ is the intersection number at (c, β) of the affine plane curves $f(T, u) = 0$ and $\frac{\partial}{\partial T} f(T, u) = 0$. Suppose $\beta \in \overline{\mathbf{F}}_q$ is such that either $f(T, \beta)$ has more than one multiple root or $f(T, \beta)$ has a root of multiplicity ≥ 3. In the former case at least two of the above intersection multiplicities are positive, and in the latter case some intersection multiplicity is ≥ 2. In either case, $\operatorname{disc}_T f(T, u)$ vanishes at $u = \beta$ to order ≥ 2, so that $\operatorname{disc}_T f(T, u)$ is not squarefree.

4.3 Proof of Theorem 4.1.1

We now make precise the connection we alluded to before between the factorization of $(u - a)$ and the irreducibility of $f(T, a)$. The following is one version of a result often useful in the theory of global fields (cf. [117, Theorem 5.8.2]):

Kummer's theorem. *Let F/k be a function field. Suppose we are given an extension $F' = F(\alpha)$, where α is integral over the valuation ring $\mathcal{O}_P$ corresponding to the prime P of F. Let $\pi(T) \in \mathcal{O}_P[T]$ be the minimal polynomial of α over F, and* *suppose that the reduction of $\pi(T)$ factors, over the residue field $\bar{F} := \mathcal{O}_P/P$, into distinct irreducibles:*

$$\bar{\pi}(T) = \prod_{i=1}^{r} \gamma_i(T).$$

Then P is unramified in F', and there are r distinct places $P_1, \dots, P_r$ of F' that lie over P which can be ordered so that the residue field corresponding to P_i is isomorphic to $\bar{F}[T]/(\gamma_i(T))$. In particular, the P_i can be ordered so that $f(P_i/P) = \deg \gamma_i(T)$.

Lemma 4.3.1. *Suppose $f(T,u) \in \mathbf{F}_q[u,T]$ is monic in T of positive T-degree and irreducible in $\mathbf{F}_q(u)[T]$ (or, what amounts to the same thing by Gauss's lemma, in $\mathbf{F}_q[u][T]$). Assume that $a \in \mathbf{F}_q$ is not a root of the polynomial*

$$Z(u) := \operatorname{disc}_T f(T,u) \in \mathbf{F}_q[u].$$

Then $f(T,a)$ is irreducible over $\mathbf{F}_q$ if and only if the prime of $\mathbf{F}_q(u)$ corresponding to the $(u-a)$-adic valuation remains prime when a root of $f(T,u)$ is adjoined to $\mathbf{F}_q(u)$.

Proof. Let P be the prime corresponding to the $(u-a)$-adic valuation on $\mathbf{F}_q(u)$. Then $\mathcal{O}_P/P \cong \mathbf{F}_q$, and under this identification the reduction of $f(T,u)$ modulo P becomes $f(T,a) \in \mathbf{F}_q[T]$. Kummer's theorem now shows that the conclusion of the corollary holds for all values of a except possibly those for which $f(T,a)$ has a multiple root. Any such value of a is a zero of $Z(u)$. □

Our hypothesis that $Z(a) \neq 0$ is a mild one for large q, excluding at most $(2n-1)m$ values of a. Indeed, one can express $Z(u)$ as the determinant of a $(2n-1) \times (2n-1)$ Sylvester matrix, from which it follows immediately that the degree of $Z(u)$ is at most $(2n-1)m$. Moreover, $Z(u)$ is not identically zero: if it were, then $f(T,u)$ would have a multiple root in the algebraic closure of $\mathbf{F}_q(u)$. But we have already noted that $f(T,u)$ is a separable irreducible polynomial over $\mathbf{F}_q(u)$.

Lemma 4.3.2. *Suppose $f(T,u) \in \mathbf{F}_q[u,T]$ is monic in T of positive T-degree and irreducible in $\mathbf{F}_q(u)[T]$. Suppose also that $f(T,u)$ is separable over $\mathbf{F}_q(u)$, and let K be the splitting field of $f(T,u)$ over $\mathbf{F}_q(u)$. Suppose that $a \in \mathbf{F}_q$ is not a root of $Z(u) := \operatorname{disc}_T f(T,u)$. Let P_a be the prime of $\mathbf{F}_q(u)$ corresponding the $(u-a)$-adic valuation. Then $f(T,a)$ is irreducible over $\mathbf{F}_q$ precisely when the Frobenius conjugacy class $(K/\mathbf{F}_q(u), P_a)$ coincides with the class of n-cycles.*

Proof. Everything is trivial unless $n \geq 2$, so we assume that here.

Since a is not a root of $Z(u)$, the polynomial $f(T,a)$ is squarefree. Thus by Kummer's theorem, the prime P_a is unramified in each extension obtained by adjoining a single root of $f(T,u)$ to $\mathbf{F}_q(u)$, and so also in their compositum K. In particular, $(K/\mathbf{F}_q(u), P_a)$ is a well-defined conjugacy class of $\operatorname{Gal}(K/\mathbf{F}_q(u))$.

Let σ be any element of the conjugacy class $(K/\mathbf{F}_q(u), P_a)$. Let α be a root of $f(T,u)$, and let $K_0 = \mathbf{F}_q(u)(\alpha)$. Then P_a stays prime precisely when

$$\operatorname{Gal}(K/\mathbf{F}_q(u)) = \dot{\bigcup}_{l=0}^{n-1} \operatorname{Gal}(K/K_0)\sigma^l. \tag{4.1}$$

(Compare with [69, Theorem 2.7].) This, in turn, holds precisely when σ acts an n-cycle on the roots of $f(T,u)$. Indeed, suppose that σ acts as an n-cycle: then for any $\psi \in \operatorname{Gal}(K/\mathbf{F}_q(u))$, there is a unique $0 \leq l < n$ for which $\psi\sigma^{-l}$ fixes α, and this implies (4.1). Conversely, if (4.1) holds then $\sigma \notin \operatorname{Gal}(K/K_0)$, so that σ must move α. Thus in the decomposition of σ into disjoint cycles, α must occur in a nontrivial cycle. If this cycle has length $l < n$, then both σ^l and σ^0 belong to $\operatorname{Gal}(K/K_0)$, and this contradicts that (4.1) is a disjoint union. □

By Lemma 4.3.2, to complete the proof of Theorem 4.2.2, it suffices to estimate the number of a for which the Frobenius of P_a belongs to the conjugacy class of n-cycles. This is precisely the sort of estimate that comes out of the Chebotarev density theorem. The following explicit form of that theorem is a consequence of Weil's Riemann Hypothesis. (The proof is implicit Fried & Jarden's treatment of the Chebotarev density theorem; cf. their proof of [47, Proposition 6.4.8].)

Explicit Chebotarev density theorem for degree one sprimes. *Let $M/\mathbf{F}_q(u)$ be a finite, geometric Galois extension. Let $\mathcal{C}$ be a conjugacy class of* $\mathrm{Gal}(M/\mathbf{F}_q(u))$*, and let $\mathcal{M}$ be the set of first-degree primes P of $\mathbf{F}_q(u)$ for which the Frobenius $(M/\mathbf{F}_q(u), P) = \mathcal{C}$. Then*

$$\left|\#\mathcal{M} - \frac{\#\mathcal{C}}{[M:\mathbf{F}_q(u)]}q\right| \leq 2\frac{\#\mathcal{C}}{[M:\mathbf{F}_q(u)]}(gq^{1/2} + g + [M:\mathbf{F}_q(u)]),$$

where g denotes the genus of $M/\mathbf{F}_q$.

To take advantage of this result we need an estimate for the genus of $K/\mathbf{F}_q$.

Lemma 4.3.3. *Let $f(T,u)$ satisfy the hypotheses of Lemma 4.2.2. Suppose moreover that the characteristic of $\mathbf{F}_q$ is odd. Then the genus of $K/\mathbf{F}_q$ is $O(nn!m)$, with an absolute implied constant.*

Proof. Since $\overline{\mathbf{F}}_q$ is separably generated over $\mathbf{F}_q$, the genus of $K/\mathbf{F}_q$ coincides with the genus of of $\bar{K}/\overline{\mathbf{F}}_q$ (see [117, Theorem 8.5.2]). Thus it is enough to estimate the latter, which we accomplish by means of the Riemann-Hurwitz genus formula.

The extension $\bar{K}/\overline{\mathbf{F}}_q(u)$ is tamely ramified. Indeed, the prime P_∞ is assumed tamely ramified in the hypotheses of Lemma 4.2.2, while in the course of the proof of that lemma it was shown that all other ramified primes had ramification index 2. (Recall that we are supposing $\mathbf{F}_q$ is of odd characteristic.) Therefore

$$\begin{aligned}
2g_{\bar{K}} - 2 &= [\bar{K} : \overline{\mathbf{F}}_q(u)](2g_{\overline{\mathbf{F}}_q(u)} - 2) + \sum_{P \text{ ramified}} \sum_{\mathfrak{P}|P} (e(\mathfrak{P}/P) - 1) \\
&= n!(-2) + \sum_{\mathfrak{P}|P_\infty} (e(\mathfrak{P}/P_\infty) - 1) + \sum_{\substack{P_\beta \text{ ramified} \\ \beta \in \overline{\mathbf{F}}_q}} \sum_{\mathfrak{P}|P_\beta} (e(\mathfrak{P}/P_\beta) - 1) \\
&\leq -2n! + \sum_{\mathfrak{P}|P_\infty} e(\mathfrak{P}/P_\infty) + \frac{1}{2} \sum_{\substack{P_\beta \text{ ramified} \\ \beta \in \overline{\mathbf{F}}_q}} \sum_{\mathfrak{P}|P_\beta} e(\mathfrak{P}/P_\beta) \\
&= n!(M/2 - 1), \qquad (4.2)
\end{aligned}$$

where M is the number of $\beta \in \overline{\mathbf{F}}_q$ for which P_β ramifies. If P_β ramifies, then by Kummer's theorem, the polynomial $f(T, \beta)$ has a multiple root, so that β is a root of $\operatorname{disc}_T f(T, u)$. We showed above that $\operatorname{disc}_T f(T, u)$ is a nonzero polynomial of degree $\leq (2n-1)m$, so that $M \leq 2nm$. The result follows. □

Lemma 4.3.4. *Let $f(T, u)$ be an absolutely irreducible polynomial over $\mathbf{F}_q$, monic in T and with $\deg_T f(T, u) = n$. Suppose that q is prime to $2n$, and that both conditions of Lemma 4.2.2 are satisfied. Then the number of $a \in \mathbf{F}_q$ for which $f(T, a)$ is irreducible is*

$$q/n + O(n!mq^{1/2}),$$

where the O-constant is absolute.

Proof. By Lemmas 4.2.2 and 4.2.3, $K/\mathbf{F}_q(u)$ is a geometric Galois extension with Galois group the full symmetric group on the roots of $f(T, u)$. We apply the explicit form of the Chebotarev density theorem to the extension $K/\mathbf{F}_q(u)$, taking $\mathcal{C}$ to be the $(n-1)!$-element conjugacy class consisting of n-cycles.

From that theorem and our estimate for the genus of $K/\mathbf{F}_q$ (Lemma 4.3.3), we see that there are

$$q/n + O(n!mq^{1/2}) \tag{4.3}$$

values of $a \in \mathbf{F}_q$ for which P_a is unramified and for which $(M/\mathbf{F}_q(u), P_a) = \mathcal{C}$. Suppose a is not a root of $\operatorname{disc}_T f(T,u)$; this excludes only $O(nm)$ values of a. Then by Lemma 4.3.2, any such a for which $f(T,a)$ is irreducible is counted in (4.3). Conversely, any value of a which is counted in (4.3) either is such that $f(T,a)$ is irreducible or such that P_a ramifies, the latter being possible again for at most $O(nm)$ values of a. It follows that the number of a satisfying the conclusion of Theorem 4.1.1 is given by (4.3) up to an additional error term of $O(nm)$, which is negligible. □

Proof of Theorem 4.1.1. We have already seen that the hypotheses of Theorem 4.1.1 imply the hypotheses of Lemma 4.2.2. Moreover, unless $n = 1$ (in which case Theorem 4.1.1 is trivial) the hypothesis that the characteristic of $\mathbf{F}_q$ is larger than n implies that $\mathbf{F}_q$ is not of characteristic 2. The result is therefore immediate from Lemma 4.3.4. □

4.4 Proof of Theorem 4.1.2

4.4.1 Field-theoretic preliminaries

Theorem on the Newton polygon (see [117, Theorem 12.4.2]). *Let K be a field complete with to the discrete valuation v, and suppose that*

$$f(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_2T^2 + a_1T + a_0 \in K[T], \quad \textit{where} \quad a_0a_n \neq 0.$$

Extend v to the splitting field L of $f(T)$ over K. The lower convex hull of the set of points $\{(i, v(a_i)) : 1 \leq i \leq n, a_n \neq 0\}$ forms a polygonal chain called the Newton polygon of $f(T)$. *This polygon consists of a sequence of line segments $S_1, S_2, \ldots$ of increasing slopes with the following property: If $(r, v(a_r)) \leftrightarrow (s, v(a_s))$ is a line segment of slope $-m$ occurring in the Newton polygon of $f(T)$, then $f(T)$ has exactly $s-r$ roots $\alpha_1, \ldots, \alpha_{s-r} \in L$ for which*

$$v(\alpha_1) = \cdots = v(\alpha_{s-r}) = m.$$

Lemma 4.4.1. *Let $\mathbf{F}_q$ be a finite field with characteristic $p \notin S$, where S is the finite set of primes*

$$S := \{2, 3, 11, 19, 53, 431, 4434631\}. \tag{4.4}$$

Let

$$f(T, u) := T^3 + (T+1)^3 + (T^2 + u)^3 \in \mathbf{F}_q[T, u].$$

Then $f(T, u)$ satisfies the hypotheses of Lemma 4.2.2. In particular, $\bar{K}/\overline{\mathbf{F}}_q(u)$ as well as $K/\mathbf{F}_q(u)$ are geometric, Galois extensions with Galois group the entire symmetric group on the roots of f.

Proof. It is clear that $f(T,u)$ is monic in T of degree 6, which is prime to p by hypothesis. So it remains to verify conditions (i) and (ii). We start with (ii). By the discussion of §4.2.3, it is enough to check that $\operatorname{disc}_T f(T,u)$ is squarefree in $\mathbf{F}_q[u]$. By explicit computation, we find that

$$\begin{aligned}\operatorname{disc}_T f(T,u) = {}&-746496u^9 + 1119744u^8 - 2099520u^7 + 746496u^6 + 559872u^5 \\ &- 1889568u^4 + 1154736u^3 - 26244u^2 - 813564u + 152361. \quad (4.5)\end{aligned}$$

For $p \neq 2,3$ (so in particular for $p \notin S$), this is a polynomial of degree 9, with u-discriminant

$$2^{68} \cdot 3^{105} \cdot 19^3 \cdot 53^2 \cdot 431^3 \cdot 4434631^2,$$

which is nonzero for $p \notin S$. Thus $\operatorname{disc}_T f(T,u)$ is squarefree and we have (ii).

If p exceeds the T-degree of $f(T,u)$, then the tame ramification of P_∞ in $\bar{K}$ is immediate. This leaves open the case $p = 5$, which necessitates another approach. For this case we consider the Newton polygon for $f(T,u)$ over the completion F (say) of $\overline{\mathbf{F}}_q(u)$ at P_∞. This polygon is shown, for characteristic $\neq 2$ or 3, in Figure 4.1. Let L be the splitting field of $f(T,u)$ over F, and let v be the extension of the P_∞-adic valuation on F to L. From the theorem on the Newton polygon, we find that all the roots α_i $(1 \leq i \leq 6)$ of $f(T,u)$ in L have $v(\alpha_i) = 1/2$.

Let $\bar{K}_0$ be a field obtained by adjoining a root α of $f(T,u)$ to $\overline{\mathbf{F}}_q(u)$. To prove that P_∞ is tamely ramified in $\bar{K}$, it suffices by Abhyankar's lemma to show it is tamely ramified for every choice of $\bar{K}_0$. So suppose that $\mathfrak{P}$ is a prime of $\bar{K}_0$ that lies above P_∞. We can view the completion E of $\bar{K}_0$ at $\mathfrak{P}$ as an extension of F of degree $e(\mathfrak{P}/P_\infty)f(\mathfrak{P}/P_\infty) = e(\mathfrak{P}/P_\infty)$ (see [117, Theorem 5.4.8]). (Note that $f(\mathfrak{P}/P_\infty) = 1$ automatically since $\overline{\mathbf{F}}_q$ is algebraically closed.) Then $E = F(\alpha)$,

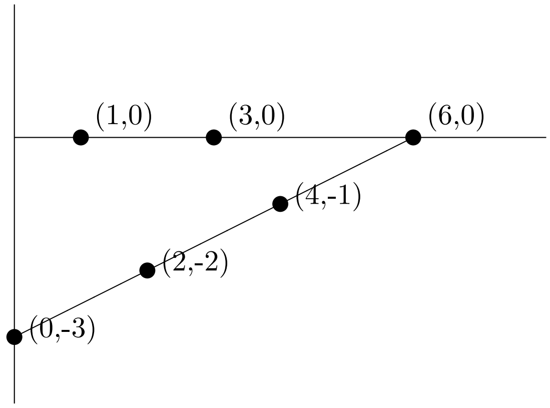

Figure 4.1: The Newton polygon for $T^3 + (T+1)^3 + (T^2+u)^3$ over the completion of $\overline{\mathbf{F}}_q(u)$ with respect to P_∞.

as the latter field contains K_0 and is already complete (cf. [117, Theorem 5.4.7]). Consequently, there is an F-isomorphism between E and some subfield $F(\alpha_i)$ of L.

Since $v(\alpha_i) = 1/2$, it must be that 2 divides $[F(\alpha_i) : F] = [E : F] = e(\mathfrak{P}/P_\infty)$. Trivially $e(\mathfrak{P}/P_\infty) \leq [\bar{K} : \overline{\mathbf{F}}_q(u)] = 6$, so that $e(\mathfrak{P}/P_\infty) = 2, 4$, or 6. In every case, $p \nmid e(\mathfrak{P}/P_\infty)$. □

Lemma 4.4.2. *Let $g(T,u) = T^2 + u \in \mathbf{F}_q[T]$. If $p \neq 2$, then the splitting field of $g(T,u)$ over $\overline{\mathbf{F}}_q(u)$ is a geometric, Galois extension with Galois group the symmetric group on the two roots of g. The same holds for the splitting field of $g(T,u)$ over $\mathbf{F}_q(u)$.*

Lemma 4.4.2 is straightforward to check directly, but it is amusing to note it also follows immediately from our Lemmas 4.2.2 and 4.2.3.

Lemma 4.4.3. *Suppose $p \notin S$, where S is the set* (4.4)*. The splitting fields of T^2+u and $f(T,u) = T^3+(T+1)^3+(T^2+u)^3$ are linearly disjoint over $\overline{\mathbf{F}}_q(u)$.*

Proof. Since each of the splitting fields are Galois over $\overline{\mathbf{F}}_q(u)$, it is enough to verify that their intersection F (say) is $\overline{\mathbf{F}}_q(u)$. By Lemma 4.2.1, it is enough to show that $F/\overline{\mathbf{F}}_q(u)$ is tamely ramified and unramified except possibly at primes above P_∞.

The multiplicativity of ramification indices in towers shows immediately that $F/\overline{\mathbf{F}}_q(u)$ is tamely ramified, since the splitting field of T^2+u is a tamely ramified extension of $\overline{\mathbf{F}}_q(u)$.

To prove that F is unramified except at primes above P_∞, suppose that P_a ramifies in F. Then P_a must ramify in $\overline{\mathbf{F}}_q(\sqrt{-u})$, forcing $a=0$. Moreover, P_0 must also ramify in the field obtained by adjoining a single root of $f(T,u)$ to $\overline{\mathbf{F}}_q(u)$. By Kummer's criterion, this is only possible if the reduction of $f(T,u)$ modulo P_0, viz. $T^3+(T+1)^3+T^6$, has a multiple root in $\overline{\mathbf{F}}_q$. But

$$\mathrm{disc}_T(T^3+(T+1)^3+T^6) = 3^6 \cdot 11 \cdot 19 \neq 0,$$

since $p \notin S$. □

Lemma 4.4.4. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \notin S$, and define $f(T,u) = T^3+(T+1)^3+(T^2+u)^3$. Let K be the splitting field of $f(T,u)$ over $\mathbf{F}_q(u)$ and $\bar{K} = K\overline{\mathbf{F}}_q$ the splitting field of $f(T,u)$ over $\overline{\mathbf{F}}_q(u)$. Let L be the splitting field of $f(T,u)(T^2+u)$ over $\mathbf{F}_q(u)$, and let $\bar{L} = L\overline{\mathbf{F}}_q$ be the corresponding splitting field over $\overline{\mathbf{F}}_q(u)$. Then $\bar{L}/\overline{\mathbf{F}}_q(u)$ and $L/\mathbf{F}_q(u)$ are geometric Galois extensions. Moreover, the* *map*

$$\begin{aligned} \mathrm{Gal}(L/\mathbf{F}_q(u)) &\to \mathrm{Gal}(K/\mathbf{F}_q(u)) \times \mathrm{Gal}(\mathbf{F}_q(\sqrt{-u})/\mathbf{F}_q(u)) \\ \sigma &\mapsto (\sigma|_K, \sigma|_{\mathbf{F}_q(\sqrt{-u})}) \end{aligned}$$

is an isomorphism.

Proof. The last claim follows immediately upon observing that we have a commutative square

$$\begin{tikzcd} \mathrm{Gal}(\bar{L}/\overline{\mathbf{F}}_q(u)) \arrow[r, "\sigma\mapsto(\sigma|_{\bar{K}},\sigma|_{\overline{\mathbf{F}}_q(\sqrt{-u})})"] \arrow[d, "\sigma\mapsto\sigma|_L"'] & \mathrm{Gal}(\bar{K}/\overline{\mathbf{F}}_q(u)) \times \mathrm{Gal}(\overline{\mathbf{F}}_q(\sqrt{-u})/\overline{\mathbf{F}}_q(u)) \arrow[d, "(\tau_1,\tau_2)\mapsto(\tau_1|_K,\tau_2|_{\mathbf{F}_q(\sqrt{-u})})"'] \\ \mathrm{Gal}(L/\mathbf{F}_q(u)) \arrow[r, "\sigma\mapsto(\sigma|_K,\sigma|_{\mathbf{F}_q(\sqrt{-u})})"] & \mathrm{Gal}(K/\mathbf{F}_q(u)) \times \mathrm{Gal}(\mathbf{F}_q(\sqrt{-u})/\mathbf{F}_q(u)) \end{tikzcd} \quad , \tag{4.6}$$

in which all the maps except that of the bottom row are known to be isomorphisms. (The top map is an isomorphism by Lemma 4.4.3; the latter maps are isomorphisms by counting arguments, since each of the Galois groups has the largest possible size.)

To prove that $\mathbf{F}_q(u)$ is the full field of constants of L, we mimic the proof of Lemma 4.2.3: any $\alpha \in L$ algebraic over $\mathbf{F}_q$ is fixed by every element of $\mathrm{Gal}(\bar{L}/\overline{\mathbf{F}}_q(u))$; by the left vertical isomorphism above, α is also fixed by $\mathrm{Gal}(L/\mathbf{F}_q(u))$, so must belong to $\mathbf{F}_q(u)$. But then α, being algebraic over $\mathbf{F}_q$, is forced to belong to $\mathbf{F}_q$. □

Lemma 4.4.5. *Let L be as in Lemma 4.4.4, and let g_L be the genus of $L/\mathbf{F}_q$. Then $g_L \leq 3241$.*

Before giving the proof we recall a useful auxiliary result (see [117, Theorem 14.1.3]):

Castelnuovo-Severi inequality. *Let F/k be a function field with full constant field k. Suppose we are given two subfields F_1/k and F_2/k of F/k satisfying*

(i) *$F = F_1F_2$ is the compositum of F_1 and F_2,*

(ii) *$[F : F_i] = n_i$ and F_i/k has genus g_i for $i = 1, 2$.*

Then the genus g of F/k obeys the bound

$$g \leq n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

Proof of Lemma 4.4.5. Let K be the splitting field of $f(T, u) = T^3 + (T + 1)^3 + (T^2 + u)^3$ over $\mathbf{F}_q(u)$. According to equation (4.2) of Lemma 4.3.3, the genus g_K of $K/\mathbf{F}_q$ satisfies

$$2g_K - 2 \leq 6!(M/2 - 1),$$

where M is the number of $\beta \in \overline{\mathbf{F}}_q$ for which P_β ramifies in K. Any such β is a root of the nonzero, degree 9 polynomial $\operatorname{disc}_T f(T, u)$, so that $M \leq 9$. Hence $g_K \leq 1261$.

On the other hand, the splitting field of $T^2 + u$ over $\mathbf{F}_q(u)$ has genus zero. Since L is the compositum of K and $\mathbf{F}_q(\sqrt{-u})$, the Castelnuovo-Severi inequality yields

$$\begin{aligned} g_L &\leq [L : K]g_K + ([L : K] - 1)([L : \mathbf{F}_q(\sqrt{-u})] - 1) \\ &\leq 2 \cdot 1261 + (2 - 1)(6! - 1) = 3241, \end{aligned}$$

as we sought to show. □

So far, the results of this section suffice to prove Theorem 4.1.2 for large q, subject to the restriction $p \notin S$. We would like to weaken this to the requirement that $p \neq 2, 3$. The easiest way to accomplish this seems to go via the following lemma:

Lemma 4.4.6. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \notin S'$,where*

$$S' := \{2, 3, 5, 71, 89, 461, 3469\}.$$

Let K' be the splitting field of

$$g(T, u) := T^3 + (T + 1)^3 + (T^2 + T + u)^3 \in \mathbf{F}_q(u)[T]$$

over $\mathbf{F}_q(u)$. Then $\operatorname{Gal}(K'/\mathbf{F}_q(u))$ is the full symmetric group on the roots of g. Let L' be the compositum of K' and the splitting field $\mathbf{F}_q(\sqrt{1 - 4u})$ of $T^2 + T + u$ over $\mathbf{F}_q(u)$. Then $L'/\mathbf{F}_q(u)$ is a geometric Galois extension. Moreover,

$$\begin{aligned} \operatorname{Gal}(L'/\mathbf{F}_q(u)) &\to \operatorname{Gal}(K'/\mathbf{F}_q(u)) \times \operatorname{Gal}(\mathbf{F}_q(\sqrt{1-4u})/\mathbf{F}_q(u)) \\ \sigma &\mapsto (\sigma|_{K'}, \sigma_{\mathbf{F}_q(\sqrt{1-4u})}) \end{aligned}$$

is an isomorphism. Finally, the genus $g_{L'}$ of $L'/\mathbf{F}_q$ obeys the bound $g_{L'} \leq 3241$.

Proof. For the most part the proofs run parallel to those already given. We begin by verifying condition (ii) of Lemma 4.2.2. Direct computation shows that

$$\begin{aligned} \operatorname{disc}_T g(T, u) = {} & -746496u^9 + 3919104u^8 - 8678016u^7 + 10614240u^6 \\ & - 7899444u^5 + 3698217u^4 - 1268460u^3 + 616734u^2 - 367416u + 111537. \end{aligned}$$

This polynomial is squarefree over $\mathbf{F}_q$, since its discriminant involves only the primes $2, 3, 71, 89, 3469$, all of which belong to S. This implies (ii). Also, since $p \notin S$, we have $p > 6 = \deg_T g(T, u)$, which shows that (i) also holds.

So by Lemmas 4.2.2 and 4.2.3, $K'\overline{\mathbf{F}}_q/\overline{\mathbf{F}}_q(u)$ is a geometric Galois extension with Galois group the full symmetric group on the roots of $g(T, u)$, and similarly for $K'/\mathbf{F}_q(u)$. We now check that $K'\overline{\mathbf{F}}_q$ is linearly disjoint from $\overline{\mathbf{F}}_q(\sqrt{1-4u})$. Arguing as in the proof of Lemma 4.4.3, we observe that the only prime P_a, $a \in \overline{\mathbf{F}}_q$, that could possibly ramify in both $K'\overline{\mathbf{F}}_q$ and $\overline{\mathbf{F}}_q(\sqrt{1-4u})$ is $P_{1/4}$. But then

$$\operatorname{disc}_T f(T, 1/4) = \frac{3024621}{64} = \frac{3^8 \cdot 461}{2^6} = 0,$$

which is impossible since $p \notin S$. So as before an appeal to Lemma 4.2.1 yields the desired linear disjointness.

Now arguing as in Lemma 4.4.4 yields that $L'/\mathbf{F}_q(u)$ is a geometric Galois extension and that the given map of Galois groups is an isomorphism. The bound on the genus of L' is handled exactly as in Lemma 4.4.5. □

4.4.2 Proof of Theorem 4.1.2 for large q

In Chapter 3 we established the following result, which may be considered the kernel of the substitution method:

Theorem. *Let $f_1(T), \ldots, f_r(T)$ be irreducible polynomials over $\mathbf{F}_q$, and suppose that*

$$\deg f_1(T) \cdots f_r(T) \leq B.$$

If

$$q > \max\{3, 2^{2r-2}B^2\},$$

then there is a prime l dividing $q - 1$ and an element $\beta \in \mathbf{F}_q$ for which every *subsitution*

$$T \mapsto T^{l^k} - \beta \quad \text{with} \quad k = 0, 1, 2, \ldots$$

leaves all of $f_1, \ldots, f_r$ irreducible.

Lemma 4.4.7. *Let $\mathbf{F}_q$ be a finite field with $q > 6400$. If there is a single $a \in \mathbf{F}_q$ for which both $T^2 + a$ and $T^3 + (T+1)^3 + (T^2+a)^3$ are irreducible, then the conclusion of Theorem 4.1.2 holds for the field $\mathbf{F}_q$. The same conclusion holds if there is a single $a \in \mathbf{F}_q$ for which both $T^2 + T + a$ and $T^3 + (T+1)^3 + (T^2+T+a)^3$ are prime.*

Proof. The proofs of both statements are almost identical, so we treat only the first. Suppose $q > 6400$ and that both $T^2 + a$ and $T^3 + (T+1)^3 + (T^2+a)^3$ are irreducible over $\mathbf{F}_q$. Then

$$P(T) := T^3 + (T+1)^3 + (T^2+a)^3 \tag{4.7}$$

is a representation of the monic irreducible polynomial P as a sum of three cubes of monic irreducibles, where

$$\deg (T^2 + a) > \max\{\deg T, \deg (T+1)\}.$$

We apply Theorem 4.4.2 to the four polynomials $T, T+1, T^2+a$, and $P(T)$ to obtain that for

$$q > 2^{2 \cdot 4 - 2} (1 + 1 + 2 + 6)^2 = 6400,$$

there is a prime l and a $\beta \in \mathbf{F}_q$ for which every substitution $T \mapsto T^{l^k} - \beta$ preserves the irreducibility of each term of (4.7). Making these substitutions in 4.7 for $k = 0, 1, 2, \ldots$, we obtain infinitely many irreducible polynomials $P(T^{l^k} - \beta)$ which have representations of the desired form. □

Lemma 4.4.8. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \neq 2, 3$. Suppose also that $q \geq 5 \times 10^7$. Then the conclusion of Theorem 4.1.2 holds for $\mathbf{F}_q$.*

Proof. We prove the result first for $p \notin S$ and then for $p \notin S'$. Since $S \cap S' = \{2, 3\}$, the lemma follows.

Suppose $p \notin S$. As before let $f(T, u) = T^3 + (T + 1)^3 + (T^2 + u)^3$ and let K be the splitting field of $f(T, u)$ over $\mathbf{F}_q(u)$. Let $\alpha \in K$ be a root of $f(T, u)$.

Suppose $a \in \mathbf{F}_q$ is not a zero of $\operatorname{disc}_T f(T, u)$. From (4.5) we see this excludes at most 9 values of a. Then by Kummer's lemma, P_a is unramified and the factorization of $f(T, a)$ over $\mathbf{F}_q$ mirrors the factorization of P_a in the extension $\mathbf{F}_q(u)(\alpha)$. In particular, $f(T, a)$ is irreducible exactly when P_a is inert in $\mathbf{F}_q(u)(\alpha)$. Arguing as in the proof of Lemma 4.3.2, we see this is equivalent to the Frobenius conjugacy class $(K/\mathbf{F}_q(u), P_a)$ being a 6-cycle in $\operatorname{Gal}(K/\mathbf{F}_q(u))$. Similarly, for $a \neq 0$, the polynomial $T^2 + a$ is irreducible over $\mathbf{F}_q$ precisely when $(\mathbf{F}_q(\sqrt{-u})/\mathbf{F}_q(u), P_a)$ is represented by a 2-cycle in $\operatorname{Gal}(\mathbf{F}_q(\sqrt{-u})/\mathbf{F}_q)$. Putting these facts together and using the isomorphism of Lemma 4.4.4, we deduce that there is a conjugacy class $\mathcal{C}$ of $\operatorname{Gal}(L/\mathbf{F}_q(u))$ with

$$\frac{\#\mathcal{C}}{[L : \mathbf{F}_q(u)]} = \frac{5!}{6!} \cdot \frac{1!}{2!} = \frac{1}{12}$$

which possesses the property that excepting at most 10 values of $a \in \mathbf{F}_q$,

$$(L/\mathbf{F}_q(u), P_a) = \mathcal{C} \Longleftrightarrow \text{both } f(T, a) \text{ and } T^2 + a \text{ are irreducible over } \mathbf{F}_q.$$

By the explicit version of the Chebotarev density theorem given above and the estimate for the genus of L given by Lemma 4.4.5, we see that the left hand inequality holds for at least

$$\frac{q}{12} - 2\frac{1}{12}(3241q^{1/2} + 3241 + 1440) - 1$$

values of $a \in \mathbf{F}_q$. (The -1 comes from taking account of the possible contribution of the term P_∞.) This lower bound exceeds 10 for $q \geq 4.3 \times 10^7$, and so for these q there is at least one value of a for which $f(T, a)$ and $T^2 + a$ are simultaneously irreducible over $\mathbf{F}_q$. The result now follows, when $p \notin S$, from Lemma 4.4.7.

If $p \notin S'$, then we argue exactly as above but with Lemma 4.4.6 in place of Lemmas 4.4.4 and 4.4.5. □

4.4.3 Mopping up

It is now straightforward to complete the proof of Theorem 4.1.2. Using a computer algebra system, one can check that for fields $\mathbf{F}_q$ with $6400 < q < 5 \cdot 10^7$ (and characteristic $\neq 2, 3$), there is an $a \in \mathbf{F}_q$ for which for which $T^2 + a$ and $T^3 + (T + 1)^3 + (T^2 + a)^3$ are simultaneously irreducible. Together with Lemma 4.4.7, this shows that Theorem 4.1.2 holds in the range $q > 6400$.

The remaining q can be treated individually, again with the assistance of a computer algebra system. One searches for an irreducible polynomial over $\mathbf{F}_q$ either of the form

$$T^3 + (T + 1)^3 + (T^2 + a)^3, \quad \text{where also } T^2 + a \text{ is irreducible,}$$

or of the form

$$T^3 + (T + 1)^3 + (T^2 + T + a)^3, \quad \text{where also } T^2 + T + a \text{ is irreducible.}$$

In either case we have an irreducible $P(T)$ represented as a sum of three cubes of monic irreducibles, satisfying the given degree restrictions. Thinking of this as a 'seed solution,' we seek an l dividing $q-1$ and a $\beta \in \mathbf{F}_q$ for which the Dickson-Serret lemma (Lemma 3.2.1) guarantees that each substitution $T \mapsto T^{l^k} - \beta$ preserves the irreducibility of every term in the representation. This strategy turns out to be successful except in the lone case of the field with 7 elements.

In that case, one begins with the representation

$$P(T) := T^3 + (T+2)^3 + (T^2 + 3T + 1)^3,$$

(which does not belong to either family given above) and uses the Dickson-Serret lemma to show that each substitution $T \mapsto T^{3^k} + 2$ preserves the irreducibility of all the summands.

Chapter 5

The Chebotarev density theorem and Hypothesis H

5.1 Introduction

Having investigated a qualitative finite field version of Hypothesis H in Chapter 3, we now turn our attention to a quantitative version:

Conjecture 5.1.1 (A quantitative constant-coefficient Hypothesis H)**.** *Suppose that $f_1, \dots, f_r$ are nonassociate irreducible one-variable polynomials over $\mathbf{F}_q$ with the degree of the product $f_1 \cdots f_r$ bounded by B. Suppose that there is no prime P of $\mathbf{F}_q[T]$ for which the map*

$$g(T) \mapsto f_1(g(T)) \cdots f_r(g(T)) \bmod P$$

is identically zero. Then

$$\#\{g(T) : g \textit{ monic},\ \deg g = n,\ \textit{and } f_1(g(T)), \ldots, f_r(g(T)) \textit{ all prime}\}$$
$$= (1 + o_B(1)) \frac{\mathfrak{S}(f_1, \ldots, f_r)}{\prod_{i=1}^r \deg f_i} \frac{q^n}{n^r} \quad \textit{as } q^n \to \infty. \quad (5.1)$$

Here the local factor $\mathfrak{S}(f_1, \ldots, f_r)$ *is defined by*

$$\mathfrak{S}(f_1, \ldots, f_r) := \prod_{m=1}^{\infty} \prod_{\substack{\deg P = m \\ P \text{ monic, prime}}} \frac{1 - \omega(P)/q^m}{(1 - 1/q^m)^r},$$

where

$$\omega(P) := \#\{A \bmod P : f_1(A) \cdots f_r(A) \equiv 0 \pmod{P}\}.$$

It is notable that the asymptotic relation (5.1) is conjectured to hold as $q^n \to \infty$, so when *either* q or n tends to infinity. In §5.2 we explain the heuristic leading us to Conjecture 5.1.1. Two properties of the singular series $\mathfrak{S}(f_1, \ldots, f_r)$ are worth extracting from that discussion:

(i) Under the hypotheses of Conjecture 5.1.1, the product defining $\mathfrak{S}(f_1, \ldots, f_r)$ converges to a positive constant. In particular, fixing $f_1, \ldots, f_r$ (and so also q) and letting n tend to infinity, we see that Conjecture 5.1.1 implies the qualitative Conjecture 3.1.1.

(ii) Putting equation (5.5) together with Lemma 5.2.1 yields the estimate

$$\frac{\mathfrak{S}(f_1, \ldots, f_r)}{\prod_{i=1}^r \deg f_i} = 1 + O_B(1/q). \quad (5.2)$$

This is useful in explaining the form of Corollary 5.1.3 below.

The primary goal of this chapter is to verify Conjecture 5.1.1 when q is much larger than n and satisfies $\gcd(q, 2n) = 1$. Actually we prove a more general result, which we now explain.

First some notational preliminaries: We use λ to denote a partition of the positive integer n, i.e., λ is a sequence of positive integers $(t_1, t_2, \dots)$ with $t_1 \geq t_2 \geq \dots$ and $\sum t_i = n$. Alternatively, we may write $\lambda = \langle 1^{\alpha_1}, 2^{\alpha_2}, \dots \rangle$, where α_j is the number of times j occurs in the sequence of summands t_i. If d is a positive integer and $\lambda = (t_1, t_2, \dots)$ is a partition of n, we write $d \times \lambda$ for the partition of dn given by $(dt_1, dt_2, \dots)$.

If $f(T)$ is a degree-n polynomial over a field, the partition corresponding to the list of degrees of its irreducible factors is referred to as the *cycle type* or *factorization type* of $f(T)$. Similarly, the *cycle type* of a permutation on n letters refers to the partition $\langle 1^{\alpha_1}, \dots, n^{\alpha_n} \rangle$, where α_j is the number of j-cycles in its decomposition into disjoint cycles. We use the notation $T(\lambda)$ for the proportion of permutations on n letters with cycle type λ. If $\lambda = \langle 1^{\alpha_1}, 2^{\alpha_2}, \dots \rangle$ is a partition of n, then a classical formula of Cauchy [24, p. 193] asserts that

$$T(\lambda) = \frac{1}{1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n} \alpha_1! \cdots \alpha_n!}.$$

We can now state our main theorem:

Theorem 5.1.2. *Let n be a positive integer and let $\lambda_1, \dots, \lambda_r$ be partitions of the integer n. Let $f_1(T), \dots, f_r(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$ of respective degrees $d_1, \dots, d_r$, with $\sum_{i=1}^{r} d_i \leq B$. The number of univariate monic polynomials h of degree n for which $f_i(h(T))$ has factorization type $d_i \times \lambda_i$ for every*

$1 \le i \le r$ is

$$q^n \prod_{i=1}^{r} T(\lambda_i) + O((nB)n!^B q^{n-1/2}),$$

provided $\gcd(q, 2n) = 1$*. Here the implied constant is absolute.*

Remark. It is worth explaining why Theorem 5.1.2 is stated in terms of partitions of the form $d_i \times \lambda_i$ and not in terms of arbitrary partitions of $d_i n$. Suppose that $f(T)$ is irreducible of degree d. Then if $h(T)$ is any polynomial over $\mathbf{F}_q$, every irreducible factor of $f(h(T))$ has degree divisible by d, so that the cycle type of $f(h(T))$ must have the form $d \times \lambda$. Indeed, if the prime $P(T)$ divides $f(h(T))$, then f has a root in the field $\mathbf{F}_q[T]/(P)$. Thus the extension of $\mathbf{F}_q$ of degree $\deg P$ must contain a copy of the extension of $\mathbf{F}_q$ of degree d, which gives the claim.

As a corollary, we obtain the promised result towards Conjecture 5.1.1:

Corollary 5.1.3. *Let n be a positive integer. Let $f_1(T), \ldots, f_r(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$ with the degree of the product $f_1 \cdots f_r$ bounded by B. The number of univariate monic polynomials g of degree n for which all of $f_1(g(T)), \ldots, f_r(g(T))$ are irreducible over $\mathbf{F}_q$ is*

$$q^n/n^r + O((nB)n!^B q^{n-1/2}) \tag{5.3}$$

provided $\gcd(q, 2n) = 1$.

Proof. Apply Theorem 5.1.2 with each $\lambda_i = (n)$. Since there are precisely $(n-1)!$ n-cyles in the symmetric group on n letters, each $T(\lambda_i) = (n-1)!/n! = 1/n$, and the result follows. □

The relationship between Corollary 5.1.3 and Conjecture 5.1.1 is perhaps not so obvious. To relate the two, we use the estimate (5.2), which shows that the factor in front of q^n/n^r in Conjecture 5.1.1 is close to 1 when q is large. In fact, this estimate implies that Corollary 5.1.3 remains true with q^n/n^r in (5.3) replaced by

$$\frac{\mathfrak{S}(f_1, \ldots, f_r)}{\prod_{i=1}^{r} \deg f_i} \frac{q^n}{n^r},$$

making evident that Corollary 5.1.3 implies Conjecture 5.1.1 in an appropriate range. (For example, for fixed B, Conjecture 5.1.1 holds as long as q tends to infinity faster than any power of n^n).

5.2 A heuristic

When q is fixed and n tends to infinity, Conjecture 5.1.1 is totally analogous to the Bateman-Horn conjecture [8] and is suggested by a completely parallel argument. In order to explain why we should expect the asymptotic relation (5.1) to hold in the wider range $q^n \to \infty$, we need to revisit the heuristic. The following approach leads to a uniform prediction that looks superficially different from that of Conjecture 5.1.1, but which will be shown identical in Lemma 5.2.1.

Write d_i for the degree of f_i. Fix roots $\alpha_1, \ldots, \alpha_r$ of $f_1, \ldots, f_r$ from an algebraic closure of $\mathbf{F}_q$. It is not hard to prove (and is a special case of our Lemma 5.5.1 below) that $f_i(g(T))$ is irreducible over $\mathbf{F}_q$ precisely when $g(T) - \alpha_i$ is irreducible over $\mathbf{F}_{q^{d_i}}$. Thus the left hand side of (5.1) counts the number of monic, degree n polynomials $g(T)$ in $\mathbf{F}_q[T]$ for which the r-tuple $(g(T) - \alpha_1, \ldots, g(T) - \alpha_r)$ has its ith coordinate irreducible over $\mathbf{F}_{q^{d_i}}$ for each $1 \leq i \leq r$. A random monic polynomial of degree n over $\mathbf{F}_{q^{d_i}}$ is prime with probability about $1/n$. So if our r-tuple behaves randomly in the appropriate sense, we expect the left hand side of (5.1) to be roughly q^n/n^r.

A more precise answer requires us to quantify the deviations from randomness.

To each monic prime P of $\mathbf{F}_q[T]$, we assign a correction factor C_P, viz. the ratio of the probability that P is coprime to all the polynomials $g(T) - \alpha_i$ compared to the probability that P is coprime to all the members of a randomly chosen r-tuple of polynomials with the ith one in $\mathbf{F}_{q^{d_i}}[T]$. (Note that being coprime to P is the same as being coprime to every prime of $\mathbf{F}_{q^{d_i}}[T]$ that lies over P.) Since P has coefficients from $\mathbf{F}_q$, we know that P has a factor in common with $g(T) - \alpha_i$ precisely when P divides

$$\prod_{\sigma \in \mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q)} (g(T) - \sigma(\alpha_i)) = f_i(g(T)).$$

It follows that P has a factor in common with some $g(T) - \alpha_i$ precisely when $g(T)$ belongs to one of $\omega(P)$ residue classes mod P.

On the other hand, a random r-tuple of monic polynomials whose ith component has coefficients from $\mathbf{F}_{q^{d_i}}$ has all its components coprime to P with probability

$$\prod_{i=1}^{r} \frac{\varphi_{q^{d_i}}(P)}{q^{d_i \deg P}}.$$

Suppose $\deg P = m$. Over $\mathbf{F}_{q^{d_i}}$, the prime P splits into (m, d_i) distinct monic irreducibles of degree $m/(m, d_i)$, and hence

$$\frac{\varphi_{q^{d_i}}(P)}{q^{d_i \deg P}} = \left(1 - \frac{1}{q^{d_i m/(m,d_i)}}\right)^{(m,d_i)}.$$

We therefore set

$$C_P := \frac{1 - \omega(P)/q^m}{\prod_{i=1}^{r} \left(1 - q^{-d_i m/(m,d_i)}\right)^{(m,d_i)}}.$$

Notice that since the f_i are coprime univarate polynomials over $\mathbf{F}_q$, we can write $\omega(P) = \sum \omega_i(P)$, where $\omega_i(P)$ is the number of incongruent roots of f_i modulo P.

Moreover, $\omega_i(P)$ is zero unless d_i divides m, in which case $\omega_i(P) = d_i$. Thus

$$C_P = \left(\frac{1 - \sum_{\substack{1 \le i \le r \\ d_i | m}} d_i/q^m}{\prod_{\substack{1 \le i \le r \\ d_i | m}} (1 - q^{-m})^{d_i}} \right) \prod_{\substack{1 \le i \le r \\ d_i \nmid m}} \frac{1}{\left(1 - q^{-d_i m/(m,d_i)}\right)^{(m,d_i)}} = 1 + O_B(q^{-2m}), \tag{5.4}$$

as both factors above are $1 + O_B(q^{-2m})$.

We now set

$$\mathfrak{S}'(f_1, \dots, f_r) := \prod_{m=1}^{\infty} \prod_{\deg P = m} C_P.$$

Notice that C_P depends on P only through its degree m; thus (5.4), along with the estimate $q^m/m + O(q^{m/2}/m)$ for the number of monic primes of degree m, together imply that the contribution to the product from degree m primes is $1+O_B(m^{-1}q^{-m})$. It follows that the product is absolutely convergent and that

$$\mathfrak{S}'(f_1, \dots, f_r) = 1 + O_B(1/q). \tag{5.5}$$

Since our local condition guarantees every term in the product is positive, we also have $\mathfrak{S}'(f_1, \dots, f_r) > 0$.

So our revised guess for the number of monic degree n polynomials g for which all of $f_1(g(T)), \dots, f_r(g(T))$ are irreducible is

$$\mathfrak{S}'(f_1, \dots, f_r)\frac{q^n}{n^r}.$$

There is perhaps some reason for suspicion here: e.g., we might think that the product defining $\mathfrak{S}'(f_1, \dots, f_r)$ should be restricted to primes of degree bounded in terms of n. However, since the degree m primes contribute $1 + O_B(m^{-1}q^{-m})$, as long as the bound for the degree of P tends to infinity with n, the resulting partial product is still $(1+o_B(1))\mathfrak{S}'(f_1,\dots,f_r)$ as $q^n \to \infty$.

These considerations suggest the truth of a modified Conjecture 5.1.1, where the factor $\mathfrak{S}(f_1,\dots,f_r)/\prod_{1\le i\le r} d_i$ is replaced by $\mathfrak{S}'(f_1,\dots,f_r)$. Hence the derivation will be complete if we can establish the following identity:

Lemma 5.2.1. *With notation as above,*

$$\mathfrak{S}'(f_1,\dots,f_r) = \frac{\mathfrak{S}(f_1,\dots,f_r)}{\prod_{1\le i\le r} d_i}.$$

Write $\zeta_q(s)$ for the zeta function of the ring $\mathbf{F}_q[T]$, defined for $\Re(s)>1$ by

$$\zeta_q(s) = \sum_{A \text{ monic}} \frac{1}{|A|^s}.$$

For $\Re(s)>1$, the function $\zeta_q(s)$ admits the Euler product expansion $\zeta_q(s)=\prod_P(1-q^{-s\deg P})^{-1}$. Moreover,

$$\zeta_q(s) = \sum_{m=0}^{\infty} \frac{q^m}{q^{ms}} = \frac{1}{1-q^{1-s}},$$

which provides a meromorphic continuation to the entire complex plane. Note that $\zeta_q(s)$ coincides with the usual zeta function of the rational function field $\mathbf{F}_q(T)$ up to a missing factor from the $(1/T)$-adic valuation.

Proof of Lemma 5.2.1. Comparing the product definitions of $\mathfrak{S}$ and $\mathfrak{S}'$, we see that

$$\mathfrak{S}'(f_1,\dots,f_r) = \mathfrak{S}(f_1,\dots,f_r) \prod_{m=1}^{\infty} \prod_{\deg P = m} \frac{(1-1/q^m)^r}{\prod_{i=1}^{r}(1-q^{-d_i m/(m,d_i)})^{(m,d_i)}}. \tag{5.6}$$

Using Q to denote a generic monic prime polynomial over $\mathbf{F}_{q^{d_i}}$, we have

$$\begin{aligned}\zeta_{q^{d_i}}(s) &= \prod_{Q} \left(1 - 1/q^{sd_i \deg Q}\right)^{-1} \\ &= \prod_{P} \prod_{Q|P} (1 - 1/q^{sd_i \deg Q})^{-1} = \prod_{P} (1 - 1/q^{sd_i m/(m,d_i)})^{-(m,d_i)},\end{aligned}$$

where as before we write m for the degree of P. Thus for $s > 1$,

$$\begin{aligned}\prod_{m=1}^{\infty} \prod_{\deg P = m} \frac{(1 - 1/q^{ms})^r}{\prod_{i=1}^{r} (1 - q^{-sd_i m/(m,d_i)})^{(m,d_i)}} &= \frac{1}{\zeta_q(s)^r} \prod_{i=1}^{r} \zeta_{q^{d_i}}(s) \\ = \prod_{i=1}^{r} \frac{1 - q^{1-s}}{1 - q^{d_i(1-s)}} &= \prod_{i=1}^{r} \frac{1}{1 + q^{1-s} + \cdots + q^{(d_i - 1)(1-s)}}. \quad (5.7)\end{aligned}$$

So if we know that the double product (5.7) is continuous for $s \geq 1$, then taking the limit in (5.7) as $s \downarrow 1$ shows that the right hand side of (5.6) is precisely $\mathfrak{S}(f_1, \dots, f_r)/\prod_{1 \leq i \leq r} d_i$, as desired.

To prove continuity, it is enough to show that for fixed $f_1, \dots, f_r$, the series

$$\sum_{m=1}^{\infty} \log \prod_{\deg P = m} \frac{(1 - 1/q^{ms})^r}{\prod_{i=1}^{r} (1 - q^{-sd_i m/(m,d_i)})^{(m,d_i)}} \tag{5.8}$$

converges uniformly for $s \geq 1$. Let $a_m = r - \sum_{\substack{d_i | m \\ 1 \leq i \leq r}} d_i$, so that the term in (5.8) corresponding to m is

$$\left(\frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right)\right) \left(-\frac{a_m}{q^{ms}} + O_B(q^{-2ms})\right) = -\frac{a_m}{mq^{m(s-1)}} + O_B(m^{-1} q^{-m(s-1/2)}).$$

Note that the partial sums $\sum_{m \le x} a_m$ are bounded; indeed,

$$\sum_{m \le x} \sum_{\substack{i=1 \\ d_i | m}}^{r} d_i = \sum_{i=1}^{r} d_i \left\lfloor \frac{x}{d_i} \right\rfloor = rx + O_B(1).$$

The uniform convergence of (5.8) for $s \ge 1$ now follows by Abel summation. □

5.3 Preparation for the proof of Theorem 5.1.2

5.3.1 Notation

As in the preceding chapter, the proofs go through the theory of algebraic function fields and the Chebotarev density theorem.

We fix once and for all an algebraically closed field Ω_q of infinite transcendence degree over $\mathbf{F}_q$ and assume for the remainder of the paper that all extensions of $\mathbf{F}_q$ which appear are subfields of Ω_q.

Our work also requires variants of the usual polynomial resultant and discriminant (as before denoted res and disc), which we introduce as follows: If $f = \sum_{i=0}^{n} a_i u^i$ and $g = \sum_{j=0}^{m} b_j u^j$ are polynomials in u of degrees *at most* n and m respectively over a domain R (so that a_n and b_m may vanish), we define

$$\mathrm{res}_u^{n,m}(f,g) := \mathrm{res}_u \left(\sum_{i=0}^{n} A_i u^i, \sum_{j=0}^{m} B_j u^j \right) \Bigg|_{A_0=a_0,\dots,A_n=a_n,B_0=b_0,\dots,B_m=b_m},$$

where the right-hand resultant is computed over the ring $R[A_0, \dots, A_n, B_0, \dots, B_m]$ of polynomials obtained by adjoining the indeterminates A_i and B_j to R. Similarly, if $f = \sum_{i=0}^{n} a_i T^i$ is a polynomial in T of degree at most n, we define

$$\operatorname{disc}_T^n(f) := \operatorname{disc}_T\left(\sum_{i=0}^{n} A_i T^i\right)\Bigg|_{A_0=a_0,\dots,A_n=a_n},$$

the right-hand discriminant being taken over $R[A_0, \dots, A_n]$. If n and m represent the actual degrees of f and g, respectively, then $\operatorname{res}_u^{n,m}(f, g) = \operatorname{res}_u(f, g)$, and similarly for $\operatorname{disc}_T^n(f)$. We work with $\operatorname{res}_u^{n,m}$ and disc_T^n rather than the usual resultant and discriminant in order to obtain uniform formulas without needing to worry about "degree-dropping" in intermediate calculations.

The fundamental property of $\operatorname{res}_u^{n,m}$ that we need is that $\operatorname{res}_u^{n,m}(f, g)$ is an $R[u]$-linear combination of f and g. (This follows from our definitions above and the analogous result for the usual resultant.) In particular, if R is a field and $\operatorname{res}_u^{n,m}(f, g)$ is a nonzero constant, then f and g have no common roots in R.

We use $\operatorname{Sym}(S)$ to denote the symmetric group on the set S.

5.3.2 Further preliminaries for the proof of Theorem 5.1.2

Since the case $n = 1$ of Theorem 5.1.2 is trivial, we always suppose that $n \geq 2$. We also suppose the following setup:

$f_1, \dots, f_r$ nonassociate irreducible univariate polynomials over $\mathbf{F}_q$,

$d_1, \dots, d_r$ degrees of $f_1, \dots, f_r$ respectively,

$\theta_1, \dots, \theta_r$ fixed roots of $f_1, \dots, f_r$, respectively, from $\overline{\mathbf{F}}_q$,

$\theta_i^{(j)}$ jth conjugate of θ_i with respect to Frobenius, i.e., $\theta_i^{(j)} := \theta_i^{q^j}$.

If $h(T)$ is a fixed polynomial of degree $n \geq 2$ over $\mathbf{F}_q$, we define the function

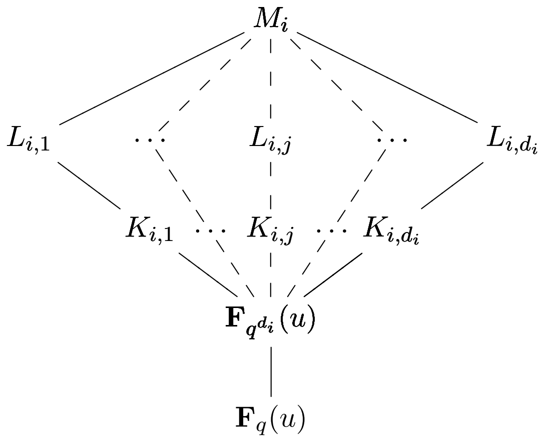

Figure 5.1: Tower of fields illustrating the inclusion relations between $\mathbf{F}_q(u), \mathbf{F}_{q^{d_i}}(u)$, the $K_{i,j}$, the $L_{i,j}$ and M_i.

fields $K_{i,j}/\mathbf{F}_q$, $L_{i,j}/\mathbf{F}_q$, and $M_i/\mathbf{F}_q$ (for $1 \leq i \leq r, 1 \leq j \leq d_i$) as follows, suppressing in our notation the dependence on h:

$K_{i,j}$	field obtained by adjoining a fixed root of $h(T) - u - \theta_i^{(j)}$ to $\mathbf{F}_{q^{d_i}}(u)$,
$L_{i,j}$	normal closure of $K_{i,j}$ over $\mathbf{F}_{q^{d_i}}(u)$,
M_i	compositum of the fields $L_{i,j}$ for $j = 1, 2 \ldots, d_i$.

We let D be the least common multiple of $d_1, \ldots, d_r$ and denote with a tilde the corresponding fields obtained by extending the constant field by $\mathbf{F}_{q^D}$. (That is, we set $\widetilde{K}_{i,j} := K_{i,j}\mathbf{F}_{q^D}, \widetilde{L}_{i,j} := L_{i,j}\mathbf{F}_{q^D}$ and $\widetilde{M_i} := M_i\mathbf{F}_{q^D}$.) Finally, we let $\widetilde{M}$ denote the compositum of $\widetilde{M_1}, \ldots, \widetilde{M_r}$. The inclusion relations between these fields are illustrated in Figures 5.1 and 5.2.

Lemma 5.3.1. *Assume that $h(T)$ is a polynomial of degree $n \geq 2$ over $\mathbf{F}_q$ which is not a polynomial in T^p, where p is the characteristic of $\mathbf{F}_q$. Then the extensions*

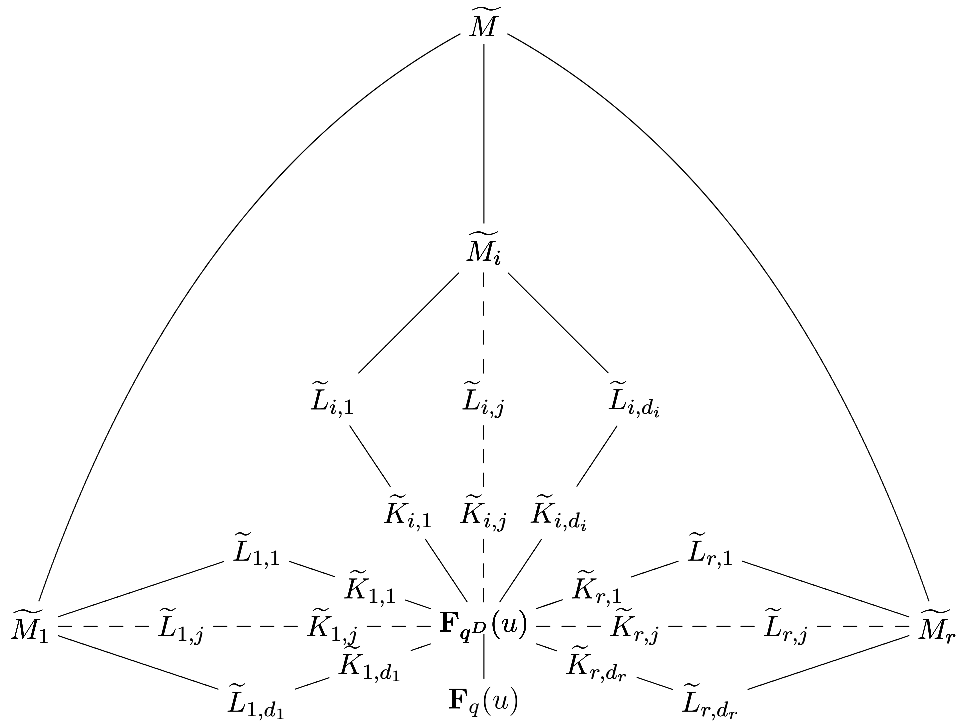

Figure 5.2: Field diagram illustrating the inclusion relations between $\mathbf{F}_q(u), \mathbf{F}_{q^D}(u)$, the $\widetilde{K}_{i,j}$, the $\widetilde{L}_{i,j}$, $\widetilde{M}_i$ and $\widetilde{M}$. Here moving to a larger field is signified by moving outward from $\mathbf{F}_q(u)$.

$M_i/\mathbf{F}_q(u)$ are Galois for each $i = 1, 2, \ldots, r$. The same assertion holds for the extensions $\widetilde{M_i}/\mathbf{F}_q(u)$ and $\widetilde{M}/\mathbf{F}_q(u)$.

Proof. Observe that M_i is the splitting field over $\mathbf{F}_q(u)$ of $f_i(h(T) - u)$, so that the first half of the lemma follows immediately once we show that the irreducible factors of $f_i(h(T) - u)$ are separable over $\mathbf{F}_q(u)$. Moving to the finite extension $\mathbf{F}_{q^{d_i}}(u)$ of $\mathbf{F}_q(u)$ we have

$$f_i(h(T) - u) = \prod_{j=1}^{d_i}(h(T) - u - \theta_i^{(j)}).$$

The d_i factors on the right-hand side are pairwise coprime (in $\overline{\mathbf{F}_q(u)}[T]$), so that it suffices to verify that each factor $h(T) - u - \theta_i^{(j)}$ has no repeated roots. Any such repeated root is also a root of $h'(T)$. But our hypothesis on h ensures that h' is not identically zero, so each root of $h'(T)$ is algebraic over $\mathbf{F}_q$, while $h(T) - u - \theta_i^{(j)}$ has no roots algebraic over $\mathbf{F}_q$.

The second half of the lemma is a consequence of the first. Indeed, since $\mathbf{F}_{q^D}(u)/\mathbf{F}_q(u)$ is Galois, what we have just proved implies that $\widetilde{M_i} = M_i\mathbf{F}_{q^D} = M_i\mathbf{F}_{q^D}(u)$ is also Galois over $\mathbf{F}_q(u)$, and thus so is the compositum $\widetilde{M}$ of the $\widetilde{M_i}$. □

The groups $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ and $\mathrm{Gal}(M_i/\mathbf{F}_q(u))$ will play an important role and so we study them in some detail. Let $S_{i,j}$ denote the full set of roots of $h(T)-u-\theta_i^{(j)}$ (so that for each i, the set $S_{i,j}$ depends only on $j \bmod d_i$). We begin by observing that under the hypothesis of Lemma 5.3.1, which ensures that the extensions appearing below are Galois, we have for each $k = 1, 2, \ldots, r$ a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u)) \arrow[r, "\iota_1"] \arrow[d, "\sigma\mapsto\sigma|_{M_k}"'] & \mathrm{Gal}(\mathbf{F}_{q^D}/\mathbf{F}_q) \times \prod_{i=1}^{r} \mathrm{Sym}(\cup_{j=1}^{d_i} S_{i,j}) \arrow[d, "\pi"'] \\
\mathrm{Gal}(M_k/\mathbf{F}_q(u)) \arrow[r, "\iota_2"] & \mathrm{Gal}(\mathbf{F}_{q^{d_k}}/\mathbf{F}_q) \times \mathrm{Sym}(\cup_{j=1}^{d_k} S_{k,j})
\end{tikzcd} . \qquad (5.9)$$

Here the maps ι_1, ι_2 are given by

$$\begin{aligned}
\iota_1 \colon \sigma &\mapsto (\sigma|_{\mathbf{F}_{q^D}}, \sigma|_{\cup_{j=1}^{d_1} S_{1,j}}, \dots, \sigma|_{\cup_{j=1}^{d_r} S_{r,j}}), \\
\iota_2 \colon \sigma &\mapsto (\sigma|_{\mathbf{F}_{q^{d_k}}}, \sigma|_{\cup_{j=1}^{d_k} S_{k,j}}),
\end{aligned}$$

and

$$\pi \colon (\tau, \sigma_1, \dots, \sigma_r) \mapsto (\tau|_{\mathbf{F}_{q^{d_k}}}, \sigma_k).$$

Note that ι_1 and ι_2 are embeddings while π is a surjection.

The remainder of this section is devoted to an explicit description of the images of ι_1 and ι_2 under a mild restriction on h. This characterization is obtained under the following two hypotheses:

$$\mathrm{disc}_u^{n-1} \mathrm{disc}_T^n(h(T) - u - \theta_i^{(j)}) \neq 0 \quad \text{for all} \quad 1 \leq i \leq r, \quad 1 \leq j \leq d_i, \tag{5.10}$$

and

$$\mathrm{res}_u^{n-1,n-1} \left(\mathrm{disc}_T^n(h(T) - u - \theta_i^{(j)}), \mathrm{disc}_T^n(h(T) - u - \theta_{i'}^{(j')})\right) \neq 0$$
$$\text{whenever } i, i', j, j' \text{ are as above and } (i,j) \neq (i',j'). \tag{5.11}$$

That together (5.10) and (5.11) impose only a mild restriction on h is borne out by the following lemma, which we prove in §5.4:

Lemma 5.3.2. *Let $h(T)$ range over the polynomials of the form $T^n + a_{n-1}T^{n-1} + \cdots + a_1 T$, with all coefficients a_i belonging to $\mathbf{F}_q$. Assume that q is prime to $2n$. Then both of the following hold:*

(i) *The number of such h for which* (5.10) *fails is bounded above by*

$$4n^2q^{n-2}. \tag{5.12}$$

(ii) *For any fixed pairs of indices $(i,j) \neq (i',j')$, the same bound holds for the number of such h which fail to satisfy* (5.11).

Consequently, for all but at most

$$4n^2\left(1+\binom{d_1+\cdots+d_r}{2}\right)q^{n-2}$$

values of h as above, both (5.10) *and* (5.11) *hold for all distinct pairs of indices (i,j) and (i',j').*

We now present the promised descriptions of the images of ι_1 and ι_2, beginning with ι_2:

Lemma 5.3.3. *Let $n \geq 2$. Assume that the characteristic of $\mathbf{F}_q$ is prime to $2n$. Suppose $h(T)$ has the form*

$$h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T, \quad \textit{with each } a_i \in \mathbf{F}_q,$$

and $h(T)$ satisfies both (5.10) *and* (5.11). *Then all of the following hold:*

(i) *The $L_{i,j}$ are Galois over $\mathbf{F}_{q^{d_i}}(u)$ with Galois group $\mathrm{Sym}(S_{i,j})$ for each $1 \leq i \leq r, 1 \leq j \leq d_i$.*

(ii) *For every $1 \leq i \leq r, 1 \leq j \leq d_i$, the field $L_{i,j}$ is linearly disjoint from the compositum of all other fields $L_{i,j'}$ with $1 \leq j' \neq j \leq d_i$.*

(iii) $\mathbf{F}_{q^{d_i}}$ *is the full field of constants of* $M_i/\mathbf{F}_{q^{d_i}}$.

(iv) *The extension* $M_i/\mathbf{F}_{q^{d_i}}(u)$ *is Galois with*

$$\mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Gal}(L_{i,j}/\mathbf{F}_{q^{d_i}}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Sym}(S_{i,j}),$$

the first isomorphism being induced by restriction in each component.

(v) *Fix* $1 \leq i \leq r$. *Let* Frob *denote the qth power map, so that* Frob *generates the group* $\mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q)$. *The image of* ι_2 *consists of all pairs* $(\mathrm{Frob}^k, \sigma)$ *which obey the following compatibility condition:*

$$\sigma(S_{i,j}) \subset S_{i,j+k}. \tag{5.13}$$

A similar lemma characterizes the image of ι_1:

Lemma 5.3.4. *Let* $n \geq 2$. *Assume that the characteristic of* $\mathbf{F}_q$ *is prime to* $2n$. *Suppose* $h(T)$ *has the form*

$$h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T, \quad \textit{with each } a_i \in \mathbf{F}_q,$$

and $h(T)$ *satisfies both* (5.10) *and* (5.11). *Then all of the following hold:*

(i) *The* $\widetilde{L}_{i,j}$ *are Galois over* $\mathbf{F}_{q^D}(u)$ *with Galois group* $\mathrm{Sym}(S_{i,j})$ *for each* $1 \leq i \leq r, 1 \leq j \leq d_i$.

(ii) *For every* $1 \leq i \leq r, 1 \leq j \leq d_i$, *the field* $\widetilde{L}_{i,j}$ *is linearly disjoint from the compositum of all other fields* $\widetilde{L}_{i',j'}$ *with* $1 \leq i' \leq r, 1 \leq j' \leq d_{i'}$ *and* $(i,j) \neq (i',j')$.

(iii) $\mathbf{F}_{q^D}$ *is the full field of constants of* $\widetilde{M}$.

(iv) *We have*

$$\mathrm{Gal}(\widetilde{M}/\mathbf{F}_{q^D}(u)) \cong \prod_{i=1}^{r} \mathrm{Gal}(\widetilde{M}_i/\mathbf{F}_{q^D}(u))$$

while for each $1 \leq i \leq r$,

$$\mathrm{Gal}(\widetilde{M}_i/\mathbf{F}_{q^D}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Gal}(\widetilde{L}_{i,j}/\mathbf{F}_{q^D}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Sym}(S_{i,j}).$$

Here all isomorphisms are induced by restriction.

(v) *The image of* ι_1 *consists of all pairs* $(\mathrm{Frob}^k, \sigma)$ *which obey the compatibility condition*

$$\sigma(S_{i,j}) \subset S_{i,j+k} \qquad \textit{for every } i = 1, 2, \ldots, r.$$

5.4 Proofs of Lemmas 5.3.2, 5.3.3, and 5.3.4

5.4.1 Proof of Lemma 5.3.2

The proof of Lemma 5.3.2 rests on the following elementary bound for the number of affine zeros of a polynomial:

Lemma 5.4.1. *Let* $E/\mathbf{F}_q$ *be an arbitrary field extension and let* $P(T_1, \ldots, T_m)$ *be a nonzero polynomial in* m *variables over* E *with total degree bounded by* d. *Then there are at most* dq^{m-1} *solutions to* $P(x_1, \ldots, x_m) = 0$ *in* $\mathbf{F}_q^m$.

This lemma is well-known when $E = \mathbf{F}_q$ (see, e.g., [78, Theorem 6.13]), and the general case reduces to this one upon writing the coefficients of P with respect to an $\mathbf{F}_q$-basis of E.

Our computations also require the following evaluation of the discriminants of certain trinomials (cf. [112, Theorem 2]):

Lemma 5.4.2. *Let R be any integral domain, and let a and b be any elements of R. Then*

$$\operatorname{disc}_T(T^n + aT + b) = (-1)^{\binom{n}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

Lemma 5.4.3. *Let F be a field of characteristic p relatively prime to $2n$. Then*

$$\widehat{P}(T_1, \ldots, T_{n-1}) := \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(T^n + T_{n-1}T^{n-1} + \cdots + T_1T - u) \in F[T_1, \ldots, T_{n-1}] \tag{5.14}$$

is a nonzero polynomial over F with total degree bounded by $(2n-1)(2n-3)$.

Proof. First suppose that p is also relatively prime to $(n-1)$. Then successive application of Lemma 5.4.2 shows that

$$\begin{aligned}\widehat{P}(1, 0, \ldots, 0) &= \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(T^n + T - u)\\ &= \operatorname{disc}_u^{n-1}\left((-1)^{\binom{n}{2}}\left(n^n(-u)^{n-1} + (-1)^{n-1}(n-1)^{n-1}\right)\right)\\ &= \operatorname{disc}_u^{n-1}(n^n u^{n-1} + (n-1)^{n-1}) = \pm(n-1)^{(n-1)^2} n^{n(n-2)},\end{aligned}$$

which is nonzero. We can therefore assume that p divides $n-1$. In this case we consider

$$\widehat{P}(1, 1, \ldots, 1) = \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(T^n + T^{n-1} + \cdots + T - u).$$

To understand the inner discriminant, note that

$$(T-1)(T^n+T^{n-1}+\cdots+T-u)=T^{n+1}-T-(T-1)u.$$

By Lemma 5.4.2, the T-discriminant of the right-hand polynomial is given explicitly by

$$(-1)^{\binom{n+1}{2}}\left((n+1)^{n+1}u^n-n^n(u+1)^{n+1}\right). \tag{5.15}$$

We can relate this to the discriminant we are after by using the relations

$$\begin{aligned}
&\operatorname{disc}_T((T-1)(T^n+T^{n-1}+\cdots+T-u))\\
&\quad=\pm\left((T^n+T^{n-1}+\cdots+T-u)|_{T=1}\right)^2\operatorname{disc}_T(T^n+T^{n-1}+\cdots+T-u)\\
&\qquad\qquad\qquad=\pm(n-u)^2\operatorname{disc}_T(T^n+T^{n-1}+\cdots+T-u).
\end{aligned}$$

Piecing this all together we obtain

$$\widehat{P}(1,1,\ldots,1)=\operatorname{disc}_u^{n-1}\left(\frac{(n+1)^{n+1}u^n-n^n(u+1)^{n+1}}{(u-n)^2}\right).$$

Let $Q(u)$ denote the polynomial in u appearing in the argument of disc_u here, so that Q has degree $n-1$ in u. If $\widehat{P}(1,1,\ldots,1)$ vanishes, then Q has a multiple root, which is necessarily also a multiple root of (5.15). One computes easily that unless p divides $n+1$, the only common root of (5.15) and its derivative is $u=n$. If $u=n$ is a multiple root of Q, then it must be a root of multiplicity at least 4 of (5.15), which forces the second derivative of (5.15) to vanish at $u=n$. But this second derivative is given by

$$(-1)^{\binom{n+1}{2}}\left((n+1)^{n+1}n(n-1)n^{n-2}-n^{n+1}(n+1)(n+1)^{n-1}\right) \\ = (-1)^{\binom{n+1}{2}+1}n^{n-1}(n+1)^{n}.$$

Since the characteristic p is prime to n, this can only vanish if p divides $n+1$. So we are forced to the conclusion that $\widehat{P}(1,\ldots,1)$ is nonvanishing except possibly if p divides $n+1$. However, p divides $n-1$ in the case we are considering, so that p can divide $n+1$ only if $p=2$, which is excluded.

To bound the degree of P, observe (from the definition of the discriminant in terms of the determinant of a $(2n-1)\times(2n-1)$ Sylvester matrix) that the inner T-discriminant on the right of (5.14) is a polynomial in u of degree at most $n-1$, each coefficient of which is a polynomial in $T_1,\ldots,T_{n-1}$ of total degree bounded by $2n-1$. These coefficients determine the entries of the $(2n-3)\times(2n-3)$ determinant used to compute $\widehat{P}$, whence $\widehat{P}$ has total degree at most $(2n-1)(2n-3)$ in $T_1,\ldots,T_{n-1}$, as claimed. □

Proof of Lemma 5.3.2(i). Write $h(T)=T^n+a_{n-1}T^{n-1}+\cdots+a_1T$. For every pair of i and j with $1\le i\le r$ and $1\le j\le d_i$, we have

$$\operatorname{disc}_u^{n-1}\operatorname{disc}_T^{n}(h(T)-u-\theta_i^{(j)})=\operatorname{disc}_u^{n-1}\operatorname{disc}_T^{n}(h(T)-u)=\widehat{P}(a_1,\ldots,a_{n-1}). \quad (5.16)$$

Indeed, the T-discriminant in the first expression differs from that of the second only in that u is replaced by $u-\theta_i^{(j)}$, and such a shift leaves the outer u-discriminant unaffected. By Lemma 5.4.3, $\widehat{P}$ is a nonzero polynomial of total degree bounded by $(2n-1)(2n-3)$. The bound (5.12) on the number of h which fail to satisfy (5.10) now follows from Lemma 5.4.1. □

Proof of Lemma 5.3.2(ii). We proceed as in the proof of Lemma 5.3.2(i). Write $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T$ as usual. Fix pairs (i, j) and (i', j') with $(i, j) \neq (i', j')$ and set

$$P(a_1, \ldots, a_{n-1}) := \operatorname{res}_u^{n-1,n-1}\left(\operatorname{disc}_T^n(h(T) - u - \theta_i^{(j)}), \operatorname{disc}_T^n(h(T) - u - \theta_{i'}^{(j')})\right).$$

Arguing as in Lemma 5.3.2(i), we see that there is some polynomial $\widehat{P}(T_1, \ldots, T_{n-1})$ over $\overline{\mathbf{F}}_q$ of degree at most $(2n-1)(2n-2)$ for which

$$P(a_1, \ldots, a_{n-1}) = \widehat{P}(a_1, \ldots, a_{n-1}) \quad \text{for all } a_1, \ldots, a_{n-1} \in \mathbf{F}_q.$$

Then (5.11) is satisfied (for the fixed pairs (i, j) and (i', j')) as long as $\widehat{P}$ is nonvanishing. This nonvanishing is easily checked: indeed, the constant term of $\widehat{P}$ is

$$\begin{aligned}\widehat{P}(0, \ldots, 0) &= \operatorname{res}_u^{n-1,n-1}(\operatorname{disc}_T(T^n - u - \theta_i^{(j)}), \operatorname{disc}_T(T^n - u - \theta_{i'}^{(j')}))\\ &= \operatorname{res}_u^{n-1,n-1}(\operatorname{disc}_T(T^n - u), \operatorname{disc}_T(T^n - u + \theta_i^{(j)} - \theta_{i'}^{(j')}))\\ &= (-1)^{n+1} n^{n(2n-2)} (\theta_i^{(j)} - \theta_{i'}^{(j')})^{(n-1)^2} \neq 0.\end{aligned}$$

Lemma 5.4.1 now implies that $\widehat{P}$ has at most $(2n-1)(2n-2)q^{n-2}$ zeros in $\mathbf{F}_q^{n-1}$. □

5.4.2 Proofs of Lemmas 5.3.3 and 5.3.4

Our fundamental tool is the following criterion of Birch and Swinnerton-Dyer [11] for certain polynomials to have the full symmetric group as their Galois group. We state their result in an alternative form attributed by the same authors to Davenport:

A Criterion of Birch and Swinnerton-Dyer. Let $h(T)$ be a polynomial of degree $n \geq 2$ with coefficients from a finite field F whose characteristic is prime to n. Suppose that with u an indeterminate over F, we have

$$\operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(h(T) - u) \neq 0. \tag{5.17}$$

Then the Galois group of $h(T) - u$ over the rational function field $\overline{F}(u)$ is the full symmetric group on the n roots of $h(T) - u$. Consequently, if E is any algebraic extension of F, then the Galois group of $h(T) - u$ over $E(u)$ is also the full symmetric group.

Proof (Hayes [62]). We apply Lemma 4.2.2, taking $f(T, u) := h(T) - u$. To verify its hypotheses, recall from the discussion of §4.2.3 that condition (ii) of that lemma follows immediately once one knows that $\operatorname{disc}_T f(T, u)$ is squarefree. This, in turn, follows at once from (5.17) if $\operatorname{disc}_T f(T, u)$ has degree $n - 1$ in u. In fact this last polynomial has leading term $\pm n^n u^{n-1}$, which one sees easily upon viewing the discriminant as the determinant of the $(2n - 1) \times (2n - 1)$ Sylvester matrix.

Thus it is enough to verify condition (i) of Lemma 4.2.2, that the first-degree prime $P = P_\infty$ of $\overline{F}(u)$ is tamely ramified in the splitting field $\widetilde{L}$ (say) of $f(T, u)$ over $\overline{F}(u)$. In fact we show that if $\mathfrak{P}$ is any prime of $\widetilde{L}$ that lies above P, then $e(\mathfrak{P}/P) = n$.

Since $\overline{F}$ is algebraically closed, we can write this ramification index as the degree of an extension of completions, viz.

$$e(\mathfrak{P}/P) = [\widetilde{L}_{\mathfrak{P}} : \overline{F}(u)_P]. \tag{5.18}$$

Let v be the exponential valuation on $\overline{F}(u)$ corresponding to P; then v induces a valuation on the completion of $\overline{F}(u)$ at P, and it extends uniquely to a valuation on $\widetilde{L}_{\mathfrak{P}}$, which (by abuse of notation) we continue to denote by v.

If y is any root of $h(T) - u$ in L, then $v(h(y)) = v(u) = -1$. Since v is non-Archimedean, we easily deduce that $v(y) = -1/n$, which shows that y has degree n over $\overline{F}(u)_P$. Let K be the field obtained by adjoining y to $\overline{F}(u)_P$. By (5.18), it now suffices to show that K is all of $\widetilde{L}_{\mathfrak{P}}$. Equivalently, we would like to show that $h(T) - u$ splits completely over K.

We make a simple change of variables: it is enough to show that the polynomial

$$y^{-n}h(yT) - y^{-n}u \tag{5.19}$$

has all its roots in K. The reason for this change of variables is to allow the application of Hensel's lemma (p. 89): in the residue field associated to v, which may be identified with $\overline{F}$, the polynomial (5.19) has the shape $c_1T^n - c_2$ for constants $c_1, c_2 \in \overline{F}$ and $c_1 \neq 0$. Since p does not divide n, this splits completely into linear factors over $\overline{F}$. Hensel's lemma now implies that (5.19) splits completely into linear factors over K.

The last claim follows immediately from the observation that the Galois group of $h(T) - u$ over $\overline{F}(u)$ injects (via restriction) into the Galois group of $h(T) - u$ over $E(u)$. □

Proof of Lemmas 5.3.3(i) and 5.3.4(i). Suppose that h satisfies conditions (5.10) and (5.11). Then part (i) of Lemma 5.3.3 is immediate from the criterion of Birch and Swinnerton-Dyer. Since $\widetilde{L}_{i,j}$ is the splitting field of $h(T) - u - \theta_i^{(j)}$ over $\mathbf{F}_{q^D}$, the same argument also establishes Lemma 5.3.4(i). □

Before continuing we extract a result from the proof given above for the Birch and Swinnerton-Dyer criterion:

Lemma 5.4.4 (Hayes). *Let $h(T)$ be a polynomial of degree $n \geq 2$ over the finite field $\mathbf{F}_q$ which satisfies the hypotheses of the Birch and Swinnerton-Dyer criterion with $F = \mathbf{F}_q$. Let L be the splitting field of $h(T) - u$ over $\overline{\mathbf{F}}_q(u)$. Let P_∞ be the prime of $\overline{\mathbf{F}}_q(u)$ corresponding to the $(1/u)$-adic valuation on $\overline{\mathbf{F}}_q[1/u]$, and let P be any prime of L lying above above P_∞. Then $e(P|P_\infty) = n$, where $e(P|P_\infty)$ denotes the ramification index of P over P_∞.*

Proof of Lemmas 5.3.3(ii) and 5.3.4(ii). Define the constant field extensions

$$\widehat{K}_{i,j} := K_{i,j}\overline{\mathbf{F}}_q, \quad \widehat{L}_{i,j} := L_{i,j}\overline{\mathbf{F}}_q, \quad \text{and} \quad \widehat{M}_i := M_i\overline{\mathbf{F}}_q.$$

Thus $\widehat{L}_{i,j}$ is the splitting field of $h(T) - u - \theta_i^{(j)}$ over $\overline{\mathbf{F}}_q$. To prove Lemma 5.3.3(ii), it suffices to show that for each fixed i,

$$\widehat{L}_{i,j} \text{ is linearly disjoint from the compositum of } \widehat{L}_{i,j'} \text{ for } 1 \leq j' \neq j \leq d_i. \quad (5.20)$$

Indeed, once (5.20) is known, we may deduce that

$$\mathrm{Gal}(\widehat{M}_i/\overline{\mathbf{F}}_q(u)) \cong \mathrm{Gal}(\widehat{L}_{i,1}/\overline{\mathbf{F}}_q(u)) \times \cdots \times \mathrm{Gal}(\widehat{L}_{i,d_i}/\overline{\mathbf{F}}_q(u)).$$

By the Birch and Swinnerton-Dyer criterion the right-hand Galois groups each have size $n!$, so that the left-hand Galois group has size $n!^{d_i}$. But the left-hand Galois group injects (via restriction) into $\mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u))$, and degree counting shows that this injection must be an isomorphism; thus

$$\begin{aligned}[M_i : \mathbf{F}_{q^{d_i}}(u)] &= [L_{i,1}L_{i,2}\cdots L_{i,d_i} : \mathbf{F}_{q^{d_i}}(u)] \\ &= [L_{i,1} : \mathbf{F}_{q^{d_i}}(u)][L_{i,2} : \mathbf{F}_{q^{d_i}}(u)]\cdots[L_{i,d_i} : \mathbf{F}_{q^{d_i}}(u)],\end{aligned}$$

which implies Lemma 5.3.3(ii).

To prove (5.20), consider the intersection N of $\widehat{L}_{i,j}$ with the compositum of the fields $\widehat{L}_{i,j'}$ for $1 \leq j \neq j' \leq d_i$. The only primes of $\overline{\mathbf{F}}_q(u)$ that can ramify in N ramify in both $\widehat{K}_{i,j}$ and some $\widehat{K}_{i,j'}$ with $1 \leq j \neq j' \leq d_i$. But by (5.11), the polynomials

$$\operatorname{disc}_T^n(h(T) - u - \theta_i^{(j)}) \quad \text{and} \quad \operatorname{disc}_T^n(h(T) - u - \theta_i^{(j')}) \quad \text{have no common roots,}$$

and so the only prime that can possibly ramify in both extensions is P_∞. By emma 5.4.4 and repeated application of Abhyankar's Lemma (p. 92), P_∞ is tamely ramified in $\widehat{L}_{i,j}$ and hence also in N. (Here we again use our hypothesis that q is prime to n.) Thus N is a finite, tamely ramified geometric extension of $\overline{\mathbf{F}}_q(u)$ unramified except possibly at primes above the degree 1 prime P_∞. It follows that $N = \overline{\mathbf{F}}_q(u)$ (by Lemma 4.2.1). This proves (5.20) and together with the above argument completes the proof of Lemma 5.3.3(ii).

The proof of Lemma 5.3.4(ii) is nearly identical but is based instead on the claim that

$$\widehat{L}_{i,j} \text{ is linearly disjoint from the compositum of } \widehat{L}_{i',j'} \text{ for } (i,j) \neq (i',j'); \qquad (5.21)$$

we omit the details. □

Proof of Lemma 5.3.3(iii) and 5.3.4(iii). In the course of proving Lemma 5.3.3(ii), we showed that restriction induces an isomorphism

$$\mathrm{Gal}(\widehat{M_i}/\overline{\mathbf{F}}_q(u)) \cong \mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u)).$$

If $\alpha \in M_i \cap \overline{\mathbf{F}}_q$, then α is fixed by every element of the left-hand Galois group appearing above, and so must be fixed by all elements of the right-hand Galois group. But this forces α to lie in the field of rational functions $\mathbf{F}_{q^{d_i}}(u)$. Since α is algebraic over $\mathbf{F}_q$, it must belong to $\mathbf{F}_{q^{d_i}}$. So $\mathbf{F}_{q^{d_i}}$ is the full field of constants of M_i. Lemma 5.3.4(iii) can be proved similarly, using that restriction induces an isomorphism $\mathrm{Gal}(\widehat{M_i}/\overline{\mathbf{F}}_q(u)) \cong \mathrm{Gal}(\widetilde{M}/\mathbf{F}_{q^D}(u))$. □

Proof of Lemmas 5.3.3(iv) and 5.3.4(iv). Immediate from parts (i) and (ii) of Lemmas 5.3.3 and 5.3.4. □

Proof of Lemma 5.3.3(v) and Lemma 5.3.4(v). Suppose $\sigma \in \mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u))$ satisfies $\sigma|_{\mathbf{F}_{q^{d_i}}} = \mathrm{Frob}^k$. Then σ takes $\theta_i^{(j)}$ to $\theta_i^{(j+k)}$ and so takes every root of $h(T) - u - \theta_i^{(j)}$ to a root of $h(T) - u - \theta_i^{(j+k)}$. It follows that the image of ι_2 is contained within the set of elements obeying the compatibility condition specified in Lemma 5.3.3(v). A straightforward counting argument shows that there are $d_i n!^{d_i}$ such elements of $\mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q) \times \mathrm{Sym}(\cup_{j=1}^{d_i} S_{i,j})$. On the other hand, we know that $M_i/\mathbf{F}_q(u)$ is Galois of degree $[M_i : \mathbf{F}_q(u)] = [M_i : \mathbf{F}_{q^{d_i}}(u)][\mathbf{F}_{q^{d_i}}(u) : \mathbf{F}_q(u)] = d_i n!^{d_i}$. Since ι_2 is injective, it follows that the image of ι_2 must coincide with the set specified in (v).

A similar argument establishes Lemma 5.3.4(v): in that case $\widetilde{M}$ is Galois over $\mathbf{F}_q(u)$ of degree $Dn!^{d_1+\cdots+d_r}$, and this degree coincides with the number of elements obeying the compatibility condition of Lemma 5.3.4(v). □

5.5 Proof of Theorem 5.1.2

Throughout this section $f_1(T), \ldots, f_r(T)$ denote nonassociate irreducible polynomials of respective degrees $d_1, \ldots, d_r$ over $\mathbf{F}_q$ and $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T$ denotes a monic polynomial over $\mathbf{F}_q$ of degree $n \geq 2$ without constant term satisfying conditions (5.10) and (5.11).

Lemma 5.5.1. *Let $g(T)$ be a squarefree polynomial of degree n over $\mathbf{F}_{q^d}$ which is coprime to all its conjugates over $\mathbf{F}_q$: i.e., $\gcd(g(T), \sigma(g(T))) = 1$ for every $\sigma \in \mathrm{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q)$. If λ is the factorization type of $g(T)$, then $d \times \lambda$ is the factorization type of $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(g(T)) := \prod_{\sigma \in \mathrm{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q)} \sigma(g(T))$.*

Proof. Since $g(T)$ is squarefree, so are all the polynomials $\sigma(g(T))$, and as $g(T)$ is coprime to its conjugates, $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(g(T))$ is also squarefree.

Suppose that Q is a monic prime of $\mathbf{F}_{q^d}[T]$ that divides $g(T)$, and let P be the monic prime of $\mathbf{F}_q[T]$ that lies below Q. Let $f(Q/P)$ be the inertial degree of Q over P. Since $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(Q) = P^{f(Q/P)}$ divides the squarefree polynomial $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(g(T))$, we must have $f(Q/P) = 1$ and $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(Q) = P$. In particular, $\deg P = d \deg Q$.

Thus, starting with a factorization of $g(T)$ exhibiting cycle type λ, takings norms gives us a corresponding factorization of $\mathrm{Nm}_{\mathbf{F}_{q^d}/\mathbf{F}_q}(g(T))$ with cycle type $d \times \lambda$. □

The next result is analogous to Lemma 4.3.2. For $a \in \mathbf{F}_q$, we write P_a for the prime of $\mathbf{F}_q(u)$ corresponding to the $(u-a)$-adic valuation.

Lemma 5.5.2. *Assume $h(T)$ obeys the nondegeneracy conditions* (5.10) *and* (5.11). *If $\lambda_1, \ldots, \lambda_r$ are arbitrary partitions of n, then the group $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ contains a* *conjugacy class $\mathcal{C}$, of size*

$$n!^{d_1+\cdots+d_r}\prod_{i=1}^{r}T(\lambda_i),$$

with the following property: Suppose that a is an element of $\mathbf{F}_q$ which is not a zero of any of the polynomials

$$\operatorname{disc}_T(h(T)-u-\theta_i^{(j)}) \quad \textit{for} \quad 1\le i\le r, \quad 1\le j\le d_i. \tag{5.22}$$

Then $f_i(h(T)-a)$ has factorization type λ_i for every $1\le i\le r$ exactly when $\mathcal{C}$ coincides with the Frobenius conjugacy class $(\widetilde{M}/\mathbf{F}_q(u),P_a)$.

Proof. Since a is not a root of any of the polynomials (5.22), P_a is unramified in $\widetilde{M}$ and the polynomials $h(T)-a-\theta_i^{(j)}$ are squarefree for all i and j. Now fix $1\le i\le r$. Applying Lemma 5.5.1 with $g(T)=h(T)-a-\theta_i^{(1)}$, we see that

$$h(T)-a-\theta_i^{(1)} \text{ has type } \lambda_i \text{ over } \mathbf{F}_{q^{d_i}} \Longleftrightarrow f_i(h(T)-a) \text{ has type } d\times\lambda_i \text{ over } \mathbf{F}_q.$$

There is a unique prime Q_a of $\mathbf{F}_{q^{d_i}}(u)$ that lies over P_a, and for this prime we have

$$f(Q_a/P_a)=d_i \quad \text{and} \quad e(Q_a/P_a)=1. \tag{5.23}$$

By Kummer's theorem (p. 94), the factorization of $h(T)-a-\theta_i^{(1)}$ mirrors the factorization of Q_a in $K_{i,1}$. So if $\lambda_i=(t_1,\dots,t_s)$, then $f_i(h(T)-a)$ has type $d_i\times\lambda_i$ if and only if Q_a factors in $K_{i,1}$ into primes of relative degrees $t_1,\dots,t_s$. By (5.23), this in turn occurs exactly when P_a factors in $K_{i,1}$ into primes of degrees $d_it_1,\dots,d_it_s$.

This last possibility can be recast in terms of the action of Frobenius. Let σ denote any element of the Frobenius conjugacy class $(M_i/\mathbf{F}_q(u), P_a)$; then necessarily

$$\sigma \text{ restricts to the } q\text{th power map on } \mathbf{F}_{q^{d_i}}, \tag{5.24}$$

so that the image of σ under ι_2 has the form (Frob, σ') for some permutation σ' of $\cup_{j=1}^{d_i} S_{i,j}$ (obeying the compatibility condition (5.13) with $k = i$ and $l = 1$). Then P_a factors as indicated above if only if σ has cycles of lengths $d_i t_1, \ldots, d_i t_s$ when acting by right-multiplication on the right-cosets of $H = \mathrm{Gal}(M_i/K_{i,1})$ in the group $\mathrm{Gal}(M_i/\mathbf{F}_q(u))$. (Cf. [69, Theorem 2.7].) We claim that this is equivalent to σ', considered as a permutation of the nd_i-element set $\cup_{j=1}^{d_i} S_{i,j}$, decomposing as a product of s disjoint cycles of lengths $d_i t_1, \ldots, d_i t_s$. To prove this, we exhibit a bijective length-preserving correspondence between the cycles in the decomposition of σ' and the cycles appearing when σ acts by right-multiplication on the right-cosets of H.

We set this correspondence up as follows. Write $K_{i,1} = \mathbf{F}_{q^{d_i}}(u)(\alpha)$, where $\alpha \in S_{i,1}$. Let C' be a cycle appearing in the decomposition of σ', and let β be an element appearing in C'. Choose an element τ of of $\mathrm{Gal}(M_i/\mathbf{F}_q(u))$ with $\tau(\beta) = \alpha$. (The existence of such an element follows from our description of the image of ι_2 above.) We define our bijection by sending

$$C' \mapsto C, \quad \text{where } C \text{ is that cycle of the right-action containing } H\tau. \tag{5.25}$$

We must check that this does not depend on the particular choices of τ and β. To this end, suppose that $\tau_1(\beta) = \tau_2(\beta) = \alpha$. Then $\tau_1\tau_2^{-1}$ fixes both α and $\mathbf{F}_q(u)$, so must also fix the entire field

$$\mathbf{F}_q(u)(\alpha) = \mathbf{F}_q(u)(h(\alpha), \alpha) = \mathbf{F}_q(u)(\theta_i^{(1)})(\alpha) = \mathbf{F}_{q^{d_i}}(u)(\alpha) = K_{i,1}.$$

Thus $\tau_1\tau_2^{-1} \in \mathrm{Gal}(M/K_{i,1}) = H$, and so $H\tau_1 = H\tau_2$, proving that our map is independent of the choice of τ. Now suppose β_1 and β_2 both appear in the cycle C'; then $\beta_2 = \sigma^j(\beta_1)$ for some j. If $\tau(\beta_1) = \alpha$, then $(\tau\sigma^j)(\beta_2) = \alpha$. Thus (5.25) associates to C' both the cycle containing $H\tau$ and the cycle containing $H\tau\sigma^j$. But these coincide, since our action is right-multiplication by σ.

Suppose now that two cycles C_1' and C_2' are mapped to the same cycle C. Choose elements β_1 and β_2 which appear in the cycles C_1' and C_2' respectively, and choose τ_1 and τ_2 from $\mathrm{Gal}(M_i/\mathbf{F}_q(u))$ with $\tau_1(\beta_1) = \alpha$ and $\tau_2(\beta_2) = \alpha$. It follows that $H\tau_1$ and $H\tau_2$ appear in the same cycle of our right-action, so that $H\tau_1 = H\tau_2\sigma^j$ for some j. Hence the *left*-cosets $\tau_1^{-1}H$ and $\sigma^{-j}\tau_2^{-1}H$ coincide. But elements of the former coset send α to β_1 and elements of the latter send α to $\sigma^{-j}(\beta_2)$. It follows that β_1 and β_2 belong to the same cycle of σ; i.e., $C_1' = C_2'$. This proves injectivity.

Now we show that the association (5.25) takes cycles C' to cycles C of the same length. Using $|\cdot|$ for the length of a cycle in both cases, we observe that for an arbitrary integer j,

$$\begin{aligned} |C| \text{ divides } j &\iff H\tau\sigma^j = H\tau \iff \tau^{-1}H = \sigma^{-j}\tau^{-1}H \\ &\iff \tau^{-1}(\alpha) = \sigma^{-j}\tau^{-1}(\alpha) \iff \beta = \sigma^{-j}(\beta) \iff |C'| \text{ divides } j. \end{aligned}$$

This forces $|C| = |C'|$.

The surjectivity of our map now follows, as the lengths of the cycles of C and the lengths of the cycles of C' must both sum to n. This completes the proof that (5.25) defines a bijective, length-preserving map.

At this point we have reduced the problem to a consideration of those permutations σ' of $\cup_{j=1}^{d_i} S_{i,j}$ which obey the compatibility condition (5.13) (with $k = i$ and $l = 1$) and which decompose into disjoint cycles of lengths $d_i t_1, \ldots, d_i t_s$. Such cycles can be explicitly constructed as follows: Take any permutation of $S_{i,1}$ of cycle type λ_i; there are $T(\lambda_i)n!$ of these. This permutation serves as a template for a permutation σ' with the desired properties: use the given permutation to fill in every dth element in the cycles of σ', and fill in the remaining spots arbitrarily, subject only to the compatibility condition. The latter task can be done in $n!^{d_i-1}$ ways, and this shows that the total number of such σ' is $T(\lambda)n!^{d_i}$.

Let $\gamma \in \mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ be an element from the conjugacy class of $(\widetilde{M}/\mathbf{F}_q(u), P_a)$. Then in order that $f_i(h(T) - a)$ have cycle type $d_i \times \lambda_i$ for every $i = 1, 2, \ldots, r$, it is necessary and sufficient that $\gamma|_{M_i}$ obey the conditions imposed on σ' above for every i. That is, it is necessary and sufficient that γ (identified with its image under ι_1) has the form $(\mathrm{Frob}, \sigma_1, \ldots, \sigma_r)$, where each σ_i is one of the previously-constructed $n!^{d_i}T(\lambda_i)$ permutations on $\cup_{j=1}^{d_i} S_{i,j}$. There are $n!^{d_1+\cdots+d_r} \prod_{i=1}^{r} T(\lambda_i)$ possible tuples $(\mathrm{Frob}, \sigma_1, \ldots, \sigma_r)$, and because the σ_i obey the stated compatibility conditions, these correspond to distinct, well-defined elements of $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$.

Finally, Lemma 5.3.4(i), (ii) shows that

$$\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u)) \supset \mathrm{Gal}(\widetilde{M}/\mathbf{F}_{q^D}(u)) = \prod_{\substack{1 \le i \le r \\ 1 \le j \le d_i}} \mathrm{Sym}(S_{i,j}), \tag{5.26}$$

where each $\mathrm{Sym}(S_{i,j})$ is thought of as a subgroup of $\mathrm{Sym}(\cup_{\substack{1 \le i \le r \\ 1 \le j \le d_i}} S_{i,j})$. From (5.26) and our construction of the σ_i, it is easy to convince oneself that the set of elements

$\mathcal{C}$ (say) constructed above constitute a single conjugacy class of $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$. □

To apply the Chebotarev density theorem we require an estimate for the genus of $\widetilde{M}/\mathbf{F}_{q^D}$. This is a consequence of the following genus estimate due to Cohen (see [30, Theorem 1.1]):

Lemma 5.5.3. *Let $f(T)$ be a nonconstant polynomial over $\mathbf{F}_q$ which is not a polynomial in T^p, and let L be the splitting field of $f(T)-u$ over $\mathbf{F}_q(u)$. Then the genus of L is bounded above by*

$$\frac{1}{2}(\deg f - 3)[L : \mathbf{F}_q(u)] + 1.$$

Corollary 5.5.4. *Let $f_1(T), \dots, f_r(T)$ be nonassociate monic irreducible polynomials of respective degrees $d_1, \dots, d_r$ over $\mathbf{F}_q$ and suppose that $h(T)$ is a polynomial of degree $n \geq 2$ without constant term satisfying conditions* (5.10) *and* (5.11). *Then the genus of $\widetilde{M}/\mathbf{F}_{q^D}$ is bounded above by*

$$(d_1 + \cdots + d_r)n \cdot n!^{d_1+\cdots+d_r}.$$

Proof. Write g_N for the genus of a function field N with constant field $\mathbf{F}_{q^D}$. Since $\widetilde{L}_{i,j}$ is the splitting field of $h(T) - u - \theta_i^{(j)}$ over $\mathbf{F}_{q^D}$ (for $1 \leq i \leq r$ and $1 \leq j \leq d_i$), Lemma 5.5.3 implies that

$$g_{\widetilde{L}_{i,j}} \leq \frac{1}{2}(n-3)n! + 1 \leq \frac{1}{2}n \cdot n!.$$

To continue we enumerate the $\widetilde{L}_{i,j}$ as $\widetilde{L}^{(1)}, \dots, \widetilde{L}^{(d_1+\cdots+d_r)}$, so that $\widetilde{M}$ is the compositum of the $\widetilde{L}^{(i)}$ for $1 \leq i \leq d_1 + \cdots + d_r$. By the Castelnuovo-Severi inequality, we have for any $k \leq d_1 + \cdots + d_r$ that

$$g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k)}} \leq [\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(k)}]g_{\widetilde{L}^{(k)}} + [\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(1)}\cdots\widetilde{L}^{(k-1)}]g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}} + \\ ([\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(k)}]-1)([\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(1)}\cdots\widetilde{L}^{(k-1)}]-1);$$

thus

$$\begin{aligned} g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k)}} &\leq n!^{k-1}\cdot\frac{1}{2}n\cdot n! + n!g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}} + (n!^{k-1}-1)(n!-1) \\ &\leq \frac{1}{2}n\cdot n!^k + n!g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}} + n!^k \leq n\cdot n!^k + n!g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}}. \end{aligned}$$

By induction we deduce that

$$g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k)}} \leq kn\cdot n!^k.$$

Taking $k = d_1 + d_2 + \cdots + d_r$ gives the result. □

We can now complete the proof of Theorem 5.1.2 appealing to the explicit form of the Chebotarev density theorem that appeared in the last chapter (p. 96).

Proof of Theorem 5.1.2. As always we may assume $n \geq 2$, since Theorem 5.1.2 is trivial otherwise. Let X be the number of polynomials $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T \in \mathbf{F}_q[T]$ satisfying both nondegeneracy conditions (5.10) and (5.11).

Suppose $h(T)$ is one of the polynomials counted by X, and let N_h be the number of $a \in \mathbf{F}_q$ with the property that $f_i(h(T)-a)$ has cycle type λ_i for all $1 \leq i \leq r$. For all but at most $(n-1)B$ values of a, Lemma 5.5.2 asserts that this property is equivalent to $(\widetilde{M}/\mathbf{F}_q(u), P_a)$ coinciding with the conjugacy class $\mathcal{C}$ of that lemma.

Since

$$|\mathcal{C}| = n!^{d_1+\cdots+d_r}\prod_{i=1}^{r} T(\lambda_i) \quad \text{and} \quad [\widetilde{M} : \mathbf{F}_{q^D}(u)] = n!^{d_1+\cdots+d_r},$$

the Chebotarev density theorem gives us that

$$\left| N_h - q\prod_{i=1}^{r} T(\lambda_i) \right| \leq \left(2\prod_{i=1}^{r} T(\lambda_i) \right) (gq^{1/2} + g + n!^{d_1+\cdots+d_r}) + (n-1)B. \qquad (5.27)$$

Since $g \leq Bnn!^B$ (Lemma 5.5.4), the right-hand side here is $O((Bn)n!^B q^{n-1/2})$. Thus the total number of polynomials $\tilde{h}(T)$ for which $f_i(\tilde{h}(T))$ has cycle type λ_i for all $1 \leq i \leq r$ is

$$Xq\prod_{i=1}^{r} T(\lambda_i) + O(X(Bn)n!^B q^{1/2}) + O((q^{n-1} - X)q).$$

Making use of the bounds

$$q^{n-1} - 4n^2 q^{n-2}\left(1 + \binom{B}{2}\right) \leq X \leq q^{n-1},$$

we find that this number is

$$q^n \prod_{i=1}^{r} T(\lambda_i) + O((Bn)n!^B q^{n-1/2}) + O(n^2B^2q^{n-1}).$$

The proof is completed by the (easy) verification that the first O-term is dominant (using $n \geq 2$). □

Chapter 6

Further applications

6.1 Introduction

In this chapter we give several applications of Theorem 5.1.2 to the multiplicative properties of polynomials.

6.1.1 Prime values of polynomials

The first two applications constitute further results towards a polynomial analogue of Hypothesis H. In Chapter 3 we showed that if $f_1(T), \ldots, f_r(T)$ is a finite collection of irreducible polynomials over $\mathbf{F}_q$, and if q is large compared to the degree of the product $f_1(T) \cdots f_r(T)$, then the conclusion of Hypothesis H holds for the given collection. However, our proof produced only a sparse set of substitutions $T \mapsto h(T)$ leaving all the f_i irreducible. A weak consequence of Conjecture 5.1.1 is that there should be such $h(T)$ of every sufficiently large degree.

Our first application uses Corollary 5.1.3 to establish that the degrees of these polynomials $h(T)$ are "dense" with respect to arithmetic progressions, in the following sense:

Theorem 6.1.1. *Let $f_1(T), \dots, f_r(T)$ be nonassociate irreducibles over $\mathbf{F}_q$ with the degree of $f_1 \cdots f_r$ bounded by B. Let $a \bmod m$ be an arbitrary infinite arithmetic progression of integers. If the finite field $\mathbf{F}_q$ is sufficiently large, depending just on m, r, and B, and if q is prime to $2\gcd(a, m)$, then there are infinitely many univariate monic polynomials h over $\mathbf{F}_q$ with*

$$\deg h \equiv a \pmod{m} \quad \textit{and} \quad f_1(h(T)), \dots, f_r(h(T)) \textit{ all irreducible over } \mathbf{F}_q.$$

Theorem 6.1.1 is no doubt true without any restriction on the characteristic of $\mathbf{F}_q$, but we have not been able to show this.

Tweaking the methods involved in the proof of Theorem 6.1.1 we can also prove the following result, the first half of which settles a problem posed by Hall [55, p. 140]:

Theorem 6.1.2. *Let $\mathbf{F}_q$ be any finite field with more than two elements. Then there are infinitely many monic prime pairs $f, f+1$ of odd degree over $\mathbf{F}_q$. The same holds for the case of even degree.*

Even for large q this is not immediate from Theorem 6.1.1, since that theorem says nothing about prime specializations over fields of characteristic 2.

Theorem 6.1.2 is the twin prime analogue of Kornblum's result that every coprime residue class of polynomials over $\mathbf{F}_q$ contains infinitely many monic irreducibles of odd degree, as well as infinitely many of even degree. In a posthumously-published version of Kornblum's paper [75], Landau presents a modification of Kornblum's argument to the effect that the degrees can be taken from an arbitrary arithmetic progression. Theorem 6.1.1 can be seen as an effort in the same direction.

6.1.2 Twin primes and Brun's constant

We begin by recalling Brun's classical result [13] towards the twin prime problem:

Theorem A (Brun). *The sum of the reciprocals of those primes which are members of a twin prime pair converges (or is a finite sum); that is,*

$$B := \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots < \infty.$$

While constants like π and e are known to billions of digits, our knowledge of Brun's constant B is surprisingly modest. The sharpest known unconditional bounds are (roughly)

$$1.830 < B < 2.347.$$

(Thus we do not know B to even one decimal place!) The lower bound here is due to Sebah [105], who computed all the twin prime pairs up to 10^{16} and summed their reciprocals. The upper bound is due to Crandall and Pomerance ([34, pp. 16-17], see also [70, Chapter 3]), who bound the sum of the twin prime pairs past 10^{16} using an explicit upper estimate of Riesel and Vaughan [97] for the number of twin prime pairs. Much sharper estimates for Brun's constant are available if one assumes a suitable quantitative version of the twin prime conjecture; e.g., it is plausible that

$$B = 1.902160583121 \pm 4.08 \times 10^{-8}.$$

This last estimate is taken from the recent thesis of Klyve [70], which the reader should consult for references to earlier work.

If $\mathbf{F}_q$ is a finite field containing the nonzero element α, we define the *Brun constant associated to q and α* by

$$B_{q,\alpha} := \sum_{P, P+\alpha \text{ monic primes}} \frac{1}{|P|}.$$

The proof of Theorem A can be adapted to show that $B_{q,\alpha}$ is finite for every q and α (cf. [121, Corollary, p. 349] or [67, Theorem 5.5]). Actually we can be far more precise about the values of $B_{q,\alpha}$:

Theorem 6.1.3. *If $\mathbf{F}_q$ is a finite field with characteristic $p > 2$, then*

$$B_{q,\alpha} = \frac{\pi^2}{6} + O(1/p + \log\log q/\log q), \tag{6.1}$$

uniformly for $\alpha \in \mathbf{F}_q^{\times}$. Moreover, for every finite field $\mathbf{F}_q$,

$$\frac{1}{q-1} \sum_{\alpha \in \mathbf{F}_q^{\times}} B_{q,\alpha} = \frac{\pi^2}{6} + O(q^{-1/2}). \tag{6.2}$$

Thus $B_{q,\alpha}$ tends to $\pi^2/6$ as the characteristic of $\mathbf{F}_q$ tends to infinity, for example if q tends to infinity through prime values. Moreover, the error term in this approximation is rather small on average over α once q is large (regardless of the characteristic). We suspect that $B_{q,\alpha}$ tends to $\pi^2/6$, uniformly in α, whenever q tends to infinity, but we have not so far succeeded in showing this.

6.1.3 The distribution of prime gaps

The following conjecture is a well-known consequence of Cramér's probabilistic model (see, e.g., [52] for background):

Conjecture A. *Fix $\lambda > 0$. Suppose h and N tend to infinity in such a way that $h \sim \lambda \log N$. Then*

$$\lim_{N\to\infty} \frac{1}{N}\#\{n \le N : \pi(n+h) - \pi(n) = k\} = e^{-\lambda}\frac{\lambda^k}{k!}$$

for every fixed integer $k = 0, 1, 2, \dots$.

Additional support for Conjecture A comes from the work of Gallagher [49], who shows that it follows from a plausible uniform version of Hardy and Littlewood's prime k-tuples conjecture.

Granville (personal communication) has suggested the following polynomial analogue of Conjecture A. For a prime p and an integer a, let $\overline{a}$ denote the residue class of a in $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. For each prime p and each integer $h \ge 0$, define

$$I(p;h) := \{\overline{a_0} + \overline{a_1}T + \cdots + \overline{a_j}T^j : 0 \le a_0, \dots, a_j < p \text{ with } \sum a_i p^i < h\}. \tag{6.3}$$

Let $P_k(p;h,n)$ be the number of polynomials $A(T)$ of degree n over $\mathbf{F}_p$ for which the translated "interval" $A + I(p;h)$ contains exactly k primes.

Conjecture 6.1.4. *Fix $\lambda > 0$. Suppose h and n tend to infinity in such a way that $h \sim \lambda n$. Then*

$$\frac{1}{p^n}P_k(p;h,n) \to e^{-\lambda}\frac{\lambda^k}{k!} \quad (\textit{as } n \to \infty) \tag{6.4}$$

for each fixed $k = 0, 1, 2, 3, \dots$, uniformly in the prime p.

In §6.5.1, we show that, in analogy with Gallagher's result, this conjecture follows from a suitable uniform version of the prime k-tuples conjecture. Our main result towards Conjecture 6.1.4 is the following, which shows that (6.4) holds whenever p tends to infinity faster than any power of n^{n^2}, as long as $k = o(\sqrt{n})$:

Theorem 6.1.5. *For each compact set $I \subset (0, \infty)$, there is a constant C with the following property: For integers n, h and k with $n \geq 2, h \geq 1, 0 \leq k \leq h$, and $h/n \in I$, we have upon setting $\lambda := h/n$,*

$$\frac{1}{p^n} P_k(p; h, n) = e^{-\lambda} \frac{\lambda^k}{k!} \left(1 + O_I\left(\frac{(k+1)^2}{n}\right)\right) + O\left(p^{-1/2} \exp(Cn^2 \log n)\right),$$

where the second O-constant is absolute.

6.1.4 Smooth values of polynomials

To this point, all of our applications have been towards polynomial analogues of problems in the distribution of primes. On the opposite end of the multiplicative spectrum one has the smooth numbers, those composed only of small prime factors. (More precisely, an integer n is called *y-smooth* if its largest prime factor $P(n)$ is $\leq y$.) Dickman has shown [37] that for fixed u, the number of $n \leq x$ which are $x^{1/u}$-smooth is asymptotic to $\rho(u)x$, where ρ is the (unique) continuous solution of the differential-delay equation

$$u\rho'(u) = -\rho(u-1) \quad \text{satisfying the initial condition} \quad \rho(u) = 1 \text{ for } 0 \leq u \leq 1.$$

One could ask, more generally, for an asymptotic formula for the number of $x^{1/u}$-smooth values assumed by a polynomial $F(T)$ on integers $1 \leq n \leq x$. Denote this number by $\Psi(F;x,x^{1/u})$. Then we have the following conjecture of Martin [81], which we state in a slightly strengthened form:

Conjecture B (Martin)**.** *Let F be an arbitrary but fixed nonzero integer-valued polynomial and let $d_1,\dots,d_K$ be the degrees of the nonassociate irreducible factors of F. Then for each $U>0$, the asymptotic formula*

$$\Psi(F;x,x^{1/u}) \sim x\rho(d_1u)\cdots\rho(d_Ku)$$

holds as $x\to\infty$, uniformly for $0<u\leq U$.

This can be viewed as a smooth number analogue of Schinzel's Hypothesis H. Martin links the two conjectures by showing that a sufficiently uniform quantitative version of Hypothesis H implies the truth of Conjecture B for every $U<(d-1/K)^{-1}$, where d is the maximal degree of an irreducible factor of F and K is the number of nonassociate irreducible factors of F of degree d. (Note that Conjecture B is trivial in the narrower range $U<d^{-1}$.)

The distribution of smooth polynomials mimics the distribution of smooth integers: e.g., the number of polynomials of degree n over $\mathbf{F}_q$ all of whose prime factors have degree $\leq n/u$ is asymptotically $\rho(u)q^n$ (in large ranges of u and uniformly in q; see, e.g., [20], [86]). This motivates the following analogue of Conjecture B. For a polynomial $F(T)$ over $\mathbf{F}_q$, define $\Psi(F;n,m)$ as the number of monic, degree n polynomials $g(T)$ over $\mathbf{F}_q$ for which every prime factor of $F(g(T))$ has degree bounded by m.

Conjecture 6.1.6. *Fix $B,U\geq 1$. Let $F(T)$ be a nonconstant polynomial over $\mathbf{F}_q$ of degree at most B. Let K be the number of distinct monic irreducible factors of*

F, and let $d_1, \ldots, d_K$ be the degrees of those factors. Then as $n \to \infty$,

$$\Psi(F; n, n/u) \sim q^n \rho(d_1 u) \cdots \rho(d_K u)$$

uniformly for $0 < u \leq U$ and uniformly for all q, F, and K.

Theorem 5.1.2 allows us to confirm this conjecture when q grows much faster than n (say when q grows faster than any power of n^n) and satisfies $\gcd(q, 2n) = 1$:

Theorem 6.1.7. *Fix $B, U \geq 1$. Let $F(T)$ be a nonconstant polynomial over $\mathbf{F}_q$ of degree at most B. Let K be the number of distinct monic irreducible factors of F, and let $d_1, \ldots, d_K$ be the degrees of these factors. If $n \geq BU$ and $(q, 2n) = 1$, then*

$$\Psi(F; n, n/u) = q^n \rho(d_1 u) \cdots \rho(d_K u) + O_B(uq^n/n) + O_B(q^{n-1/2} n!^{2B}),$$

for $0 < u \leq U$.

Without giving details, we remark that minor modifications of our arguments give analogous results for the number of smooth values of $F(h(T))$ when $h(T)$ is restricted to monic prime values (cf. Martin's prediction [81, equation (1.8)]).

6.1.5 Smooth values of consecutive integers

The final conjecture we consider can be viewed as a smooth number analogue of the prime k-tuples conjecture:

Conjecture C. *Let $0 \leq \alpha < \beta \leq 1$, and let A be the set of integers $n \geq 2$ whose largest prime factor $P(n)$ satisfies $n^\alpha \leq P(n) \leq n^\beta$. Then for every k, one can find k consecutive integers $n + 1, \ldots, n + k$ all of which belong to A.*

The origin of this problem lies with Erdős (see, e.g., [43]), who asked for a proof in the case when $k = 2$ and $[\alpha, \beta] = [1 - \epsilon, 1]$. The case $k = 2$ was settled in its entirety by Hildebrand [63] (via the solution of a more general conjecture of Balog). Moreover, when $\alpha = 0$, Conjecture C follows (for any $\beta > 0$ and every k) from the results of Balog and Wooley [4]. (All of these theorems in fact can be proved in stronger, quantitative forms.) Nevertheless, Conjecture C remains open in general. A partial result when $k > 2$ is contained in [64]. See also the survey [65].

A similar problem appears in the work of Erdős and Pomerance [44]; they ask whether the largest prime factors of n and $n + 1$ are independent events, in the sense that the proportion of $n \leq x$ with $P(n) > x^{\alpha_1}$ and $P(n + 1) > x^{\alpha_2}$ tends to $a(\alpha_1)a(\alpha_2)$, where $a(t) := 1 - \rho(1/t)$. This is still unsolved. Even the weaker assertion that asymptotically half of all positive integers n have $P(n) > P(n + 1)$ remains open. This last problem goes all the way back to correspondence in the 1930s between Erdős and Turán (see [109, pp. 100-101]).

The results of Balog and Wooley mentioned above have been translated into the polynomial setting by Masuda and Panario [82]. However, it seems that there are no results for polynomials in the direction of Conjecture C when $\alpha > 0$. Our next theorem deals with this case, and at the same time proves an independence statement for the largest prime factors of neighboring polynomials.

Write $L(A)$ for the degree of the largest irreducible factor of a polynomial A. Suppose that $I = [\alpha, \beta]$ is a compact subinterval of $[0, 1]$. (Here and in what follows, intervals are always understood to be of nonzero length, so that $\alpha < \beta$.) If $\alpha \neq 0$, we define $\kappa(I) = 1/\alpha$, otherwise we set $\kappa(I) = 1/\beta$.

Theorem 6.1.8. *Let k be a positive integer, and let S be a k-element subset of $\mathbf{F}_q$. Suppose that for each $s \in S$ we are given a compact subinterval $I_s = [\alpha_s, \beta_s] \subset [0, 1]$*

and let $C := \max_{s\in S} \kappa(I_s)$*.*

(i) *The number of monic, degree* n *polynomials* $A(T) \in \mathbf{F}_q[T]$ *with*

$$\alpha_s \deg A(T) \le L(A(T)+s) \le \beta_s \deg A(T) \quad \text{for every } s \in S \tag{6.5}$$

is given by

$$q^n \prod_{s\in S} \left(\rho(\beta_s^{-1}) - \rho(\alpha_s^{-1})\right) + O_{k,C}(q^n/n) + O(n!^{2k} q^{n-1/2}),$$

provided that $\gcd(q, 2n) = 1$*.*

(ii) *Suppose that the length of each interval* I_s *is bounded below by* $\epsilon > 0$*. If* q *is odd and sufficiently large (depending only on* k *and* ϵ*), then there are infinitely many monic polynomials* $A(T) \in \mathbf{F}_q[T]$ *for which* (6.5) *holds.*

We emphasize that the estimate in (i) is only nontrivial when q is large compared to n, since otherwise our bound on the error term exceeds the total number of monic, degree n polynomials.

To illustrate Theorem 6.1.8, fix $\alpha_1, \alpha_2 \ge 0$. Then applying Theorem 6.1.8 with $I_0 = [\alpha_1, 1]$, $I_1 = [\alpha_2, 1]$, and $S = \{0, 1\} \subset \mathbf{F}_q$, we see that the proportion of degree n polynomials $A(T)$ over $\mathbf{F}_q$ with

$$L(A(T)) \ge \alpha_1 n \quad \text{and} \quad L(A(T)+1) \ge \alpha_2 n$$

is asymptotic to $a(\alpha_1)a(\alpha_2)$, provided n and q tend to infinity with $q \ge n^{4n}$ (say) and $\gcd(q, 2n) = 1$. This confirms, in a certain range, the polynomial analogue of the independence result conjectured by Erdős and Pomerance.

Notation

Throughout this chapter, we reserve the letter P for monic irreducibles. For an arbitrary polynomial A, we write $\omega(A)$ for the number of distinct monic prime divisors of A. This should not be confused with the functions $\omega(\cdot)$ appearing in conjectures of Hypothesis H type, or the function $\omega_{\mathcal{D}}(\cdot)$ appearing in §6.5.

6.2 Proof of Theorem 6.1.1

We begin with some comments on the relationship between the referenced Theorem 3.1.3 and Theorem 6.1.1. For q large in terms of r and B, Theorem 3.1.3 asserts the existence of infinitely many irreducibility preserving substitutions $T \mapsto T^{l^k} - \beta$ for some prime l dividing $q-1$ and some $\beta \in \mathbf{F}_q$. So we obtain irreducibility-preserving substitutions whose degrees are exactly the powers of l. In the proof of Theorem 3.1.3, there is some control over the choice of l, and this could be used to establish Theorem 6.1.1 in a number of special cases.

In order to prove Theorem 6.1.1 in full, we require two additional ingredients:

(i) the existence of a preliminary irreducibility-preserving substitution $T \mapsto h(T)$ of degree d, for some d belonging to the progression $a \bmod m$,

(ii) the existence of some l coprime to m and some $\beta \in \mathbf{F}_q$ for which all the substitutions $T \mapsto T^{l^k} - \beta$ preserve the irreducibility of the polynomials $f_i(h(T))$, where $h(T)$ is as in (i).

If we can establish (i) and (ii), then Theorem 6.1.1 follows immediately, since $h(T^{l^k} - \beta)$ has degree from the progression $a \bmod m$ whenever k is divisible by $\varphi(m)$. The most difficult part of the proof is obtaining (i), which requires Corollary 5.1.3. By contrast, the techniques necessary for the proof of (ii) are present already in Chapter 3. However, the details here are slightly different; this is because in proving Theorem 6.1.1 we take l as a divisor of $q^d - 1$ (with d as in (i) above), while in that chapter l is always chosen as a divisor of $q - 1$.

Now for the details:

Corollary 6.2.1. *Let m be a positive integer. Then every integer $d > \max\{2, \varphi(m)\}$ has the following property: if q is any odd integer ≥ 3, then $q^d - 1$ has an odd prime divisor not dividing m.*

Proof. Suppose $d > \max\{2, \varphi(m)\}$. By Bang's theorem (p. 77) there is a prime l for which q has order d in $(\mathbf{Z}/l\mathbf{Z})^\times$. Since $d > 1$, we must have $l \neq 2$. Moreover, l is necessarily prime to m: for if l divides m, then the order of q in $(\mathbf{Z}/l\mathbf{Z})^\times$ is a divisor of $\varphi(l)$, hence also a divisor of $\varphi(m)$ and so less than d, a contradiction. Hence l is an odd prime divisor of $q^d - 1$ which is prime to m. □

We can now establish the following variant of Theorem 3.1.3:

Lemma 6.2.2. *Let $f_1(T), \ldots, f_r(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$ with each f_i of degree $d_i > 1$ and the degree of $f_1 \cdots f_r$ bounded by B. Suppose that l is an odd prime dividing $q^{d_i} - 1$ for each $i = 1, 2, \ldots, r$. If*

$$q > (2^{r-1}B - 2^r + 1)^2,$$

then there is a $\beta \in \mathbf{F}_q$ for which all the polynomials $f_1(T^{l^k} - \beta), \ldots, f_r(T^{l^k} - \beta)$ are irreducible for each $k = 0, 1, 2, 3, \ldots$.

Proof. Fix roots $\alpha_1, \ldots, \alpha_r$ of $f_1(T), \ldots, f_r(T)$, respectively. By Lemma 3.2.1 it suffices to produce an element $\beta \in \mathbf{F}_q$ with the property that $\alpha_i + \beta$ is an lth power nonresidue in $\mathbf{F}_q(\alpha_i)$ for every $i = 1, 2, \ldots, r$. Since l divides $q^{d_i} - 1$ for each i, there are multiplicative characters χ_i of order l on each of the fields $\mathbf{F}_q(\alpha_i)$. If for every choice of β, there is an $i \in \{1, 2, \ldots, r\}$ for which $\alpha_i + \beta$ is an lth power in $\mathbf{F}_q(\alpha_i)$, then the sum

$$\sum_{\beta \in \mathbf{F}_q} (1 - \chi_1(\alpha_1 + \beta))(1 - \chi_2(\alpha_2 + \beta)) \cdots (1 - \chi_r(\alpha_r + \beta))$$

vanishes. (Note that it is impossible for any of the arguments $\alpha_i + \beta$ inside a character to vanish, since each α_i belongs to a nontrivial extension of $\mathbf{F}_q$.) But by Lemma 3.4.2, the absolute value of this sum is bounded below by

$$q - \sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ \mathcal{I} \neq \emptyset}} \left(-1 + \sum_{i \in \mathcal{I}} \deg f_i(T)\right) \sqrt{q} =$$

$$q + (2^r - 1)\sqrt{q} - \sum_{i=1}^{r} d_i \left(\sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ i \in I}} 1 \right) \sqrt{q} \geq q + (2^r - 1)\sqrt{q} - 2^{r-1} B \sqrt{q},$$

and this is positive for q as in the hypothesis of the lemma. □

Proof of Theorem 6.1.1. Suppose that $f_1, \ldots, f_r$ are irreducible polynomials over $\mathbf{F}_q$, where $\mathbf{F}_q$ is a finite field with characteristic p coprime to $2 \gcd(a, m)$. Let d be the smallest integer exceeding $\max\{2, \varphi(m)\}$ relatively prime to p and satisfying $d \equiv a \pmod{m}$. Since p is prime to $\gcd(a, m)$, it follows that p divides at most one of any two consecutive terms from the progression $a \bmod m$, so that $d \leq 3m$. In particular d is bounded solely in terms of m. So by Corollary 5.1.3, as long as q is sufficiently large (depending just on B and m), there is a polynomial h of degree d for which all of $f_1(h(T)), \ldots, f_r(h(T))$ are irreducible over $\mathbf{F}_q$. Using Corollary

q	f	q^3-1	**order of** f	**order of** $f+1$	l
3	T^3-T+2	$2\cdot 13$	13	26	13
9	T^3-T+2	$2^3\cdot 7\cdot 13$	13	26	13
5	T^3+3T+2	$2^2\cdot 31$	$2^2\cdot 31$	$2^2\cdot 31$	31
17	T^3+T+8	$2^4\cdot 307$	$2^2\cdot 307$	$2^2\cdot 307$	307
257	T^3+T+15	$2^8\cdot 61\cdot 1087$	$2^5\cdot 61\cdot 1087$	$2^2\cdot 61\cdot 1087$	61
65537	T^3+T+18	$2^{16}\cdot 37\cdot P_9$	$2^{15}\cdot 37\cdot P_9$	$2^{15}\cdot 37\cdot P_9$	37

Table 6.1: Monic twin prime pairs of odd degree over small finite fields $\mathbf{F}_q$, where $q = 1 + 2^N$. We write P_9 for the 9-digit prime 116085511.

6.2.1, choose a prime l dividing $q^d - 1$ which is relatively prime to m. Then l also divides $q^{\deg f_i(h(T))} - 1$ for each $i = 1, 2, \ldots, r$. According to Lemma 6.2.2 (applied to the polynomials $f_1(h(T)), \cdots, f_r(h(T))$), if

$$q > (2^{r-1}dB - 2^r + 1)^2,$$

then there is some $\beta \in \mathbf{F}_q$ with the property that the polynomials $f_i(h(T^{l^k} - \beta))$ are all irreducible over $\mathbf{F}_q$ for $k = 0, 1, 2, 3, \ldots$. Since

$$\deg h(T^{l^k} - \beta) = dl^k \equiv al^k \equiv a \pmod{m}$$

whenever k is a multiple of $\varphi(m)$, the proof of Theorem 6.1.1 is complete. □

6.3 Application to a question of Hall

We prove Theorem 6.1.2 in two parts:

6.3.1 Part I: Infinitely many twin prime pairs of odd degree

In the case when $q-1$ has an odd prime divisor, the monic twin prime pairs $f, f+1$ constructed in the proof of Theorem 3.1.2 already have odd degree, so we may suppose that $q - 1$ is a power of 2. As noted in Chapter 3, if q is an odd prime power for which $q - 1$ is a power of 2, then either $q = 9$ or q is a Fermat prime.

Theorem 6.1.1 guarantees the existence of a monic twin prime pair $f, f + 1$ of odd degree over all sufficiently large finite fields $\mathbf{F}_q$ with q odd. The next lemma is an explicit version of a slightly weaker result:

Lemma 6.3.1. *Suppose $q > 200000$ is a prime power coprime to 6. Then there are infinitely many monic twin prime pairs $f, f+1$ over $\mathbf{F}_q$ for which $\deg f = \deg (f + 1)$ is odd.*

It is worth remarking that no Fermat primes > 200000 are known, and it is plausible that none exist.

Proof. By Corollary 5.1.3, if q is large enough and prime to 6, then we may choose a monic prime pair $f, f + 1$ of degree 3 over $\mathbf{F}_q$. In fact, referring to the estimate (5.27) (with $B = 2$ and $n = 3$), we see that such pairs exist as long as

$$\frac{q}{9} - \frac{2}{9}(gq^{1/2} + g + 6^2) - 2 \cdot 2 > 0, \tag{6.6}$$

where g is the genus of an appropriate function field. By Corollary 5.5.4, we have

$$g \leq 2 \cdot 3 \cdot 3!^2 = 216;$$

and so (6.6) holds as soon as

$$\frac{1}{9}q - 48\sqrt{q} - 60 > 0,$$

which is valid for $q \geq 187703$, so certainly for $q > 200000$. To complete the proof,

Table 6.2: Monic twin prime pairs of even degree over some small finite fields.

q	f	q^d-1	**order of** f	**order of** $f+1$	l
3	$T^6+T^5+2T^3+2T^2+1$	$2^3\cdot 7\cdot 13$	$2^2\cdot 7\cdot 13$	$2^3\cdot 7\cdot 13$	7
4	$T^2+T+\alpha$	$3\cdot 5$	$3\cdot 5$	$3\cdot 5$	3
5	T^2+T+1	$2^3\cdot 3$	3	$2^3\cdot 3$	3
7	T^2+T+3	$2^4\cdot 3$	$2^4\cdot 3$	$2^3\cdot 3$	3
8	$T^2+(\beta+1)T+\beta^2+\beta$	$3^2\cdot 7$	$3^2\cdot 7$	$3^2\cdot 7$	7
9	$T^2+(\gamma+1)T+\gamma+1$	$2^4\cdot 5$	$2^4\cdot 5$	$2^4\cdot 5$	5
11	T^2+3	$2^3\cdot 3\cdot 5$	$2^2\cdot 5$	$2^2\cdot 5$	5
13	T^2+6	$2^3\cdot 3\cdot 7$	$2^3\cdot 3$	$2^3\cdot 3$	3
16	$T^2+(\delta^2+\delta)T+\delta$	$3\cdot 5\cdot 17$	$3\cdot 5\cdot 17$	$3\cdot 5\cdot 17$	3
17	T^2+T+2	$2^5\cdot 3^2$	$2^4\cdot 3^2$	$2^5\cdot 3^2$	3
19	T^2+4	$2^3\cdot 3^2\cdot 5$	$2^2\cdot 3^2$	$2^2\cdot 3^2$	3
23	T^2+2	$2^4\cdot 3\cdot 11$	$2^2\cdot 11$	$2^2\cdot 11$	11
25	$T^2+4\epsilon T+4\epsilon+2$	$2^4\cdot 3\cdot 13$	$3\cdot 13$	$2^2\cdot 3\cdot 13$	3

Here $\alpha^2+\alpha+1=0$, $\beta^3+\beta+1=0$, $\gamma^2+1=0$, $\delta^4+\delta+1=0$, and $\epsilon^2+2=0$.

choose an odd prime divisor l of q^3-1 (e.g., any prime divisor of q^2+q+1) and apply Lemma 6.2.2 to the pair $f, f+1$ (taking $B=6$ and $r=2$). We obtain that for $q>81$, there is some $\beta \in \mathbf{F}_q$ for which both $f(T^{l^k}-\beta)$ and $f(T^{l^k}-\beta)+1$ are simultaneously irreducible for $k=1,2,3,\ldots$. This is an infinite family of monic twin prime pairs of odd degree. □

To finish off this half of Theorem 6.1.2, it remains to consider the cases when $q=9$ or when q is a Fermat prime less than 200000. These small finite fields are treated by hand. For each such q, Table 6.1 exhibits the first member f of a monic twin prime pair $f, f+1$ of odd degree together with all the information necessary to verify that the Serret-Dickson Lemma (Lemma 3.2.1) can be applied to both f and $f+1$ with the specified odd prime l.

6.3.2 Part II: Infinitely many twin prime pairs of even degree

We first argue that for $q \geq 4$, there is always a monic, quadratic twin prime pair $f, f+1$ over $\mathbf{F}_q$. In the proof of this result it is convenient to consider odd and even q separately.

Lemma 6.3.2. *Let $\mathbf{F}_q$ be a finite field of odd characteristic with $q \geq 5$. Then there is a pair $f, f+1$ of monic irreducible quadratic polynomials over $\mathbf{F}_q$.*

Lemma 6.3.2 could be established using Corollary 5.1.3, in analogy with the proof of Lemma 6.3.1 in Part I. However, the direct approach below leads to better bounds.

Proof. It suffices to show that there is some pair of consecutive quadratic nonresidues in $\mathbf{F}_q$. Letting χ denote the quadratic character on $\mathbf{F}_q$, the number of such pairs is $\frac{1}{4}$ of the sum $\sum(1-\chi(\alpha))(1-\chi(\alpha+1))$, the sum being taken over $\alpha \neq 0, -1$ from $\mathbf{F}_q$. Now a straightforward calculation using the evaluation $\sum_{\alpha\in\mathbf{F}_q}\chi(\alpha)\chi(\alpha+1) = -1$ (cf. [10, Theorem 2.1.2]) results in a count of

$$\frac{1}{4}\left(q-3+\chi(1)+\chi(-1)\right) = \frac{1}{4}\left(q-2+\chi(-1)\right)$$

such pairs, which is positive for $q > 3$. □

Lemma 6.3.3. *Let $\mathbf{F}_q$ be a finite field of characteristic 2 with $q \geq 4$. Then there is a pair $f, f+1$ of monic quadratic polynomials both of which are irreducible over $\mathbf{F}_q$.*

Proof. For any fixed $\gamma \in \mathbf{F}_q$, the map $\psi\colon \mathbf{F}_q \to \mathbf{F}_q$ defined by $\psi(\beta) := \beta^2 + \gamma\beta$ is an endomorphism of the underlying additive group of $\mathbf{F}_q$. We choose γ so that $\gamma \neq 0$ and the image of ψ contains 1 (and so contains all of $\mathbf{F}_2$). This is possible as soon as $\mathbf{F}_q$ is a nontrivial extension of $\mathbf{F}_2$; merely choose any $\beta \in \mathbf{F}_q \setminus \mathbf{F}_2$ and define γ so that $\beta^2 + \gamma\beta = 1$.

We claim that with this choice of γ, there is a pair $f, f+1$ of irreducibles where f has the form $T^2 + \gamma T + \delta$. A polynomial of this form is irreducible if and only if δ is not in the image of ψ. But by our choice of γ, the element δ is missing from the image of ψ if and only if the same is true for $\delta + 1$. So the lemma follows provided that ψ is not onto. Since ψ is a map from $\mathbf{F}_q$ to itself, if ψ were onto it would also be injective. But $\psi(\gamma) = \psi(0) = 0$. □

Lemma 6.3.4. *Let $\mathbf{F}_q$ be a finite field with $q > 25$. Then there are infinitely many monic twin prime pairs $f, f+1$ of even degree over $\mathbf{F}_q$.*

Proof. Lemmas 6.3.2 and 6.3.3 show that for $q \geq 4$ there is a monic twin prime pair $f, f+1$ of degree 2 over $\mathbf{F}_q$. Since $q > 3$, it is impossible for both $q-1$ and $q+1$ to be powers of 2, and so there must be an odd prime divisor l of $q^2 - 1$. Lemma 6.2.2 (with $r = 2$ and $B = 4$) implies that for $q > 25$, there is some $\beta \in \mathbf{F}_q$ for which both $f(T^{l^k} - \beta)$ and $f(T^{l^k} - \beta) + 1$ are simultaneously irreducible for $k = 0, 1, 2, 3, \ldots$. Since these twin prime pairs have even degree, the lemma follows. □

To complete the proof of Theorem 6.1.2 it suffices to consider those finite fields with at most 25 elements, and these are treated in Table 6.2.

6.4 Brun's constant: Proof of Theorem 6.1.3

For $\alpha \in \mathbf{F}_q^{\times}$, let $\pi_2(q; n, \alpha)$ denote the number of monic primes P of degree n over $\mathbf{F}_q$ for which $P + \alpha$ is also prime.

Lemma 6.4.1. *Let n be a positive integer. If $\alpha \in \mathbf{F}_q^\times$ and $(q, 2n) = 1$, then*

$$\pi_2(q; n, \alpha) = \frac{q^n}{n^2} + O(q^{n-1/2} nn!^2). \tag{6.7}$$

Moreover,

$$\sum_{\alpha \in \mathbf{F}_q^\times} \pi_2(q; n, \alpha) = \frac{q^{n+1}}{n^2} \left(1 + O(n^2/q)\right). \tag{6.8}$$

Proof. Estimate (6.7) follows immediately from Corollary 5.1.3 if we take $f_1(T) = T$ and $f_2(T) = T + \alpha$. To prove (6.8), note that the left hand side of (6.8) can be viewed as counting the number of not necessarily monic prime pairs $f, f+1$ of degree n over $\mathbf{F}_q$. (In fact, the term corresponding to α here counts the number of such pairs with leading coefficient α^{-1}.) In this guise the estimate (6.8) is contained in Theorem 2.4.2. □

Proof of Theorem 6.1.3. We have

$$B_{q,\alpha} = \sum_{n=1}^{\infty} \frac{1}{q^n} \pi_2(q; n, \alpha). \tag{6.9}$$

We split the sum (6.9) at a number A with $0 < A < p/2$. Then $(q, 2n) = 1$ for every $n \leq A$, so that (6.7) yields

$$B_{q,\alpha} = \sum_{n \leq A} \frac{1}{n^2} + O\left(q^{-1/2} \sum_{n \leq A} nn!^2\right) + O\left(\sum_{n > A} q^{-n} \pi_2(q; n, \alpha)\right).$$

The first O-term is $\ll q^{-1/2} A^{2A}$. To estimate the latter O-term, we use the bound (valid uniformly over all q, n, and α)

$$\pi_2(q; n, \alpha) \ll \frac{q^n}{n^2}, \tag{6.10}$$

which is a special case of the estimate (2.8) from Chapter 2. This shows that the second O-term is $\ll \sum_{n>A} n^{-2} \ll 1/A$. Hence

$$B_{q,\alpha} = \frac{\pi^2}{6} + O(1/A + q^{-1/2}A^{2A}),$$

say. Now take $A = \min\{\frac{1}{3}p, \frac{1}{6}\log q/\log\log q\}$ to obtain (6.1).

Turning to (6.2), we observe that for any $A > 0$,

$$\frac{1}{q-1}\sum_{\alpha\in\mathbf{F}_q^\times} B_{q,\alpha} = \frac{1}{q-1}\sum_{n\le A}\frac{1}{q^n}\sum_{\alpha\in\mathbf{F}_q^\times} \pi_2(q;n,\alpha) + O\left(\frac{1}{q-1}\sum_{n>A}\sum_{\alpha\in\mathbf{F}_q^\times}\frac{1}{n^2}\right).$$

(Note that we have once again applied (6.10).) The error term here is $O(1/A)$. Using (6.8) to estimate the inner sum, we obtain a main term of

$$\begin{aligned}\frac{q}{q-1}\sum_{n\le A}\frac{1}{n^2}\left(1+O\left(\frac{n^2}{q}\right)\right) &= \frac{q}{q-1}\sum_{n\le A}\frac{1}{n^2} + O\left(\frac{A}{q}\right)\\ &= \frac{\pi^2}{6} + O(1/A + A/q).\end{aligned}$$

Taking $A = q^{1/2}$ yields (6.2). □

6.5 The distribution of prime gaps

6.5.1 Gallagher's theorem for polynomials over finite prime fields

For $\mathcal{D} = (D_1, \dots, D_r)$ an r-tuple of distinct polynomials over $\mathbf{F}_q$, define

$$\mathfrak{S}_{\mathcal{D}} = \prod_P \frac{|P|^{r-1}(|P| - \omega_{\mathcal{D}}(P))}{(|P|-1)^r},$$

where $\omega_{\mathcal{D}}(P)$ is the number of residue classes modulo P occupied by $D_1, \ldots, D_r$. Let $\pi_{\mathcal{D}}(n;q)$ be the number of monic polynomials A of degree n for which all of $A+D_1, \ldots, A+D_r$ are irreducible. Then the usual heuristics offered in favor of the Hardy-Littlewood conjectures suggest that

$$\pi_{\mathcal{D}}(n;q) = (\mathfrak{S}_D + o(1))\frac{q^n}{n^r} \quad (n \to \infty). \tag{6.11}$$

In fact these heuristics suggest that this relation should hold not merely when $\mathcal{D}$ is fixed and $n \to \infty$, but also whenever $q^n \to \infty$, uniformly in $\mathcal{D}$, provided only that every D_i has degree less than n. This suggests the plausibility of the hypothesis in the following theorem, which is an analogue of Gallagher's principal result in [49]:

Theorem 6.5.1. *Fix $\lambda > 0$, and suppose that h and n tend to infinity with $h \sim \lambda n$. Then* (6.4) *holds uniformly in p, under the following hypothesis:*

(A) For each fixed r, (6.11) *holds as n tends to infinity, uniformly in p, and uniformly for $D_1, \ldots, D_r \in I(p;h)$ with the D_i distinct and $\mathfrak{S}_{(D_1,\ldots,D_r)} \neq 0$.*

As in Gallagher's paper, the theorem follows from a suitable estimate for the average value of $\mathfrak{S}_{\mathcal{D}}$.

Lemma 6.5.2. *Fix $r \geq 1$. Under hypothesis (A) of Theorem 6.5.1, we have*

$$\sum_{\substack{D_1,\ldots,D_r \in I(p;h) \\ \text{distinct}}} \mathfrak{S}_{\mathcal{D}} \sim h^r \quad (h \to \infty),$$

uniformly in p.

Suppose now that this lemma is proved. Fix $k \geq 0$, and let $M_k(\lambda)$ be the kth moment of the Poisson distribution with parameter λ. Then as $n \to \infty$, the argument of [49, pp. 5-6] shows that

$$\frac{1}{p^n} \sum_{\substack{A(T)\in\mathbf{F}_p[T]\\ A(T)\text{ monic, degree } n}} |\{P \in A + I(p;h) : P \text{ prime}\}|^k \to M_k(\lambda),$$

where the convergence is uniform in p. Theorem 6.5.1 then follows by an application of the method of moments.

Thus to prove Theorem 6.5.1 it remains only to prove Lemma 6.5.2.

Lemma 6.5.3. *Let M be a nonzero polynomial over $\mathbf{F}_p$. If $|M| \leq h$, then the number of elements of $I(p;h)$ which lie in a given residue class modulo M is $h/|M| + O(1)$, where the implied constant here is absolute.*

Proof. Write h in base p, so that $h = h_0 + h_1 p + \cdots + h_k p^k$ with each $0 \leq h_i < p$ and $h_k \geq 1$. Represent the given residue class as $A \bmod M$, where $\deg A < \deg M$. Then $|M| \leq h$ implies that $j := \deg M \leq k$. Assume (with no loss in generality) that M is monic, and write

$$M = T^j + m_{j-1}T^{j-1} + \cdots + m_1 T + m_0.$$

We wish to count the number of $B \in \mathbf{F}_p[T]$ for which $A + MB$ belongs to $I(p;h)$. Any such B can be written in the form

$$B = b_{k-j}T^{k-j} + b_{k-j-1}T^{k-j-1} + \cdots + b_0,$$

and then (writing $A = \sum a_i T^i$),

$$A + MB = b_{k-j}T^k + (b_{k-j}m_{j-1} + b_{k-j-1} + a_{k-1})T^{k-1} + \cdots + a_0 + b_0 m_0.$$

Looking at the leading coefficient of $A+MB$, we see that $A+MB$ belongs to $I(p;h)$ whenever b_{k-j} is any of $\overline{0}, \overline{1}, \dots, \overline{h_k - 1}$ (regardless of the values of the other b_i). There are $h_k p^{k-j}$ such choices of B. All other choices of B with $A + MB \in I(p;h)$ have $b_{k-j} = \overline{h_k}$. For these B, the condition $A + MB \in I(p;h)$ restricts the next-to-leading coefficient of B: if

$$b_{k-j}m_{j-1} + b_{k-j-1} + a_{k-1} = \overline{0}, \overline{1}, \overline{2}, \dots, \text{ or } \overline{h_{k-1} - 1}, \tag{6.12}$$

then automatically $A + MB$ belongs to $I(p;h)$. This gives rise to an additional $h_{k-1}p^{k-j-1}$ permissible values of B. Any B not counted so far for which $A + MB$ belongs to $I(p;h)$ has both $b_{k-j} = \overline{h_k}$ and the left hand side of (6.12) equal to $\overline{h_{k-1}}$. Continuing this process, we find

$$N := h_k p^{k-j} + h_{k-1}p^{k-j-1} + \dots + h_j = \lfloor h/|M| \rfloor$$

values of B which guarantee that $A + MB$ belongs to $I(p;h)$. Moreover, there is at most one other value of B for which $A + MB$ belongs to $I(p;h)$, namely that B for which

$$|A + MB - (\overline{h_k}T^k + \overline{h_{k-1}}T^{k-1} + \dots + \overline{h_j}T^j)| < p^j.$$

If $A + MB$ lies outside $I(p;h)$ for this final value of B, then the quantity to be enumerated is N, otherwise it is $N + 1$. In either case the stated estimate holds. □

Proof of Lemma 6.5.2 (sketch). Define $\Delta := \prod_{1 \le i < j \le r}(D_i - D_j)$. Write the Pth factor of $\mathfrak{S}_{\mathcal{D}}$ in the form

$$1 + \frac{|P|^r - \omega_{\mathcal{D}}(P)|P|^{r-1} - (|P| - 1)^r}{(|P| - 1)^r} = 1 + a(P, \omega_{\mathcal{D}}(P)).$$

For monic, squarefree Q define $a_{\mathcal{D}}(Q) := \prod_{P|Q} a(P, \omega_{\mathcal{D}}(P))$. Then (in analogy with [49, eq. (7)]) we find that

$$a_{\mathcal{D}}(P) \ll \begin{cases} (|P|-1)^{-2} & \text{when } \omega_{\mathcal{D}}(P) = r, \\ (|P|-1)^{-1} & \text{when } \omega_{\mathcal{D}}(P) < r, \end{cases}$$

these two cases occurring respectively when P does not or does divide Δ. Here the implied constant, say C, depends only on r. It follows from these estimates that we have an absolutely convergent series expansion

$$\mathfrak{S}_{\mathcal{D}} = \sum_{Q} a_{\mathcal{D}}(Q).$$

For the tail of this expansion, we have

$$\begin{aligned} \sum_{|Q|>x} |a_{\mathcal{D}}(Q)| &\leq \sum_{|Q|>x} \frac{\mu^2(Q) C^{\omega(Q)}}{\varphi(Q)^2} \varphi((Q, \Delta)) \\ &= \sum_{A|\Delta} \frac{\mu^2(A) C^{\omega(A)}}{\varphi(A)} \sum_{\substack{|B|>x/|A| \\ (B,\Delta)=1}} \frac{\mu^2(B) C^{\omega(B)}}{\varphi(B)^2}, \end{aligned} \tag{6.13}$$

where in the last line we have written $Q = AB$ with $A \mid \Delta$ and $(B, \Delta) = 1$. In [49], the analogous double sum is

$$\ll_{r,\epsilon} x^{-1}(xh)^{\epsilon}; \tag{6.14}$$

we proceed to establish that this estimate is also valid for (6.13). Observe that

$$\begin{aligned}\sum_{|B|\le x}\frac{\mu^2(B)C^{\omega(B)}}{\varphi(B)^2}|B| &\le \prod_{|P|\le x}\left(1+\frac{C|P|}{(|P|-1)^2}\right)\\ &\le \prod_{|P|\le x}\left(1+\frac{4C}{|P|}\right)\le \exp\left(4C\sum_{|P|\le x}\frac{1}{|P|}\right).\end{aligned}$$

The number of prime polynomials P of degree n over $\mathbf{F}_p$ is bounded above by p^n/n, and this implies that

$$\exp\left(4C\sum_{|P|\le x}\frac{1}{|P|}\right)\le \exp\left(4C\sum_{1\le n\le\frac{\log x}{\log p}}\frac{1}{n}\right)\ll(\log x)^{4C}.$$

Partial summation now shows that the inner sum in (6.13) is $\ll |A|x^{-1}\log^{4C}x$, so that (6.13) is

$$\begin{aligned}&\ll\left(x^{-1}\log^{4C}x\right)\sum_{A|\Delta}\mu^2(A)C^{\omega(A)}\frac{|A|}{\varphi(A)}\le\left(x^{-1}\log^{4C}x\right)\prod_{P|\Delta}(1+2C)\\ &\le(x^{-1}\log^{4C}x)|\Delta|^{\epsilon}\prod_{\substack{P\in\mathbf{F}_p[T]\\|P|<(1+2C)^{1/\epsilon}}}(1+2C)|P|^{-\epsilon}\ll_{\epsilon}(x^{-1}\log^{4C}x)h^{\epsilon\binom{r}{2}},\end{aligned}\tag{6.15}$$

for any $\epsilon>0$. (Note that the last product over P is finite for each fixed p and empty for $p>(1+2C)^{1/\epsilon}$, and so is $\ll_{\epsilon}1$.) To obtain (6.14), we replace ϵ in (6.15) with ϵr^{-2} (say). From this point the proof proceeds exactly as in [49], save that the "lattice point argument" of [49, p. 7] now requires an appeal to Lemma 6.5.3. □

Remark. The restriction to prime fields $\mathbf{F}_p$ was introduced to ensure a canonical embedding from $[0,p-1]$ into $\mathbf{F}_p$. This restriction is in some sense merely cosmetic.

More precisely, suppose that for each q we have fixed a bijection $a \mapsto \overline{a}$ between $\{0, 1, \ldots, q-1\}$ and $\mathbf{F}_q$. Define $I(q; h)$ as in (6.3) with p replaced by q. Then the proofs of this section show that Theorem 6.5.1 remains valid with p replaced by q throughout.

6.5.2 Proof of Theorem 6.1.5

Proof. We may assume that $p > \max\{h, n\}$, for otherwise the theorem is trivial. Thus $I(p; h)$ is a subset of the constant polynomials over $\mathbf{F}_p$, and Corollary 5.1.3 can be employed to count the occurrence of prime r-tuples $A + D_1, \ldots, A + D_r$ with $D_i \in I(p; h)$.

Fix one of the $\binom{h}{k}$ subsets $S \subset I(p; h)$ with k elements. We first count the number of monic, degree-n polynomials A for which $A + s$ is prime for all $s \in S$ and reducible for all $s \in I(p; h) \setminus S$. By the principle of inclusion-exclusion, this is given by

$$\sum_{\substack{T \supseteq S \\ T \subseteq I(p;h)}} (-1)^{|T|-|S|} \#\{A : \text{every element of } A + T \text{ is irreducible}\}.$$

According to Corollary 5.1.3,

$$\#\{A : \text{every element of } A + T \text{ is irreducible}\} = \frac{p^n}{n^{|T|}} + O((hn)n!^{h} p^{n-1/2}).$$

We insert this estimate above, and sum over the $\binom{h}{k}$ k-element subsets S of

$I(p;h)$ to find that

$$\begin{aligned}P_k(p;h,n) = \binom{h}{k}\left(\frac{p^n}{n^k} - \binom{h-k}{1}\frac{p^n}{n^{k+1}} + \cdots + (-1)^{h-k}\frac{p^n}{n^h}\right)&\\ + O\left(\binom{h}{k}2^{h-k}(hn)n!^h p^{n-1/2}\right)&.\end{aligned}$$

The error term here is

$$\ll 2^{2h}(nh)n^{nh}p^{n-1/2} \ll \exp(Cn^2\log n)p^{n-1/2}.$$

for a constant C depending on I, and the main term is

$$\binom{h}{k}\frac{p^n}{n^k}\left(1-\frac{1}{n}\right)^{h-k}.$$

The theorem follows upon inserting into this expression for the main term the estimates

$$\begin{aligned}\binom{h}{k} &= \frac{h^k}{k!}\left(1-\frac{1}{h}\right)\left(1-\frac{2}{h}\right)\cdots\left(1-\frac{k-1}{h}\right)\\ &= \frac{h^k}{k!}\left(1+O\left(\frac{k^2}{h}\right)\right) = \frac{h^k}{k!}\left(1+O_I\left(\frac{k^2}{n}\right)\right),\end{aligned}$$

and

$$\begin{aligned}\left(1-\frac{1}{n}\right)^{h-k} &= \left(1+O_I\left(\frac{k}{n}\right)\right)\left(1-\frac{1}{n}\right)^h\\ &= \exp(-h/n)\left(1+O_I\left(\frac{k}{n}\right)\right)\left(1+O_I\left(\frac{1}{n}\right)\right)\\ &= \exp(-h/n)\left(1+O_I\left(\frac{k+1}{n}\right)\right),\end{aligned}$$

once we recall that we are writing λ for h/n. □

6.6 Smooth values of polynomials: Proof of Theorem 6.1.7

For a permutation σ on a finite set, let $L(\sigma)$ denote the length of the longest cycle in the decomposition of σ into disjoint cycles. The following result is extracted from the thesis of X. Gourdon (cf. [51, Chapitre VII, Théorème 1]).

Lemma 6.6.1 (Gourdon)**.** *Let n be a positive integer and suppose $m > 0$. Then the proportion of permutations σ on n letters with $L(\sigma) \leq m$ is $\rho(n/m) + O(1/m)$.*

Thus, by the results mentioned to in the introduction just before Conjecture 6.1.6, the proportion of permutations on n letters with largest cycle length $\leq n/u$ is close to the proportion of degree n polynomials over a finite field with largest prime factor of degree $\leq n/u$. (The idea that the decomposition of random permutations should mimic the decomposition of random arithmetic structures seems to appear first in the work of Knuth and Trabb Pardo [73] in their study of the rth largest prime factor of a random integer.)

Remarks.

(i) In the original theorem of Gourdon, m is restricted to integral values in the interval $[2, n]$. However, the restriction to integral values is inessential; for any real m with $2 \leq m \leq n$,

$$\rho(n/m) - \rho(n/\lfloor m \rfloor) = \int_{n/m}^{n/\lfloor m \rfloor} \frac{\rho(u-1)}{u}\, du \ll \log \frac{m}{\lfloor m \rfloor} \ll \frac{1}{m}.$$

Moreover, for $m < 2$ or $m > n$, Lemma 6.6.1 is trivial.

(ii) By a simple inductive argument, Omar et al. obtain Lemma 6.6.1 under the additional hypothesis that $m \geq \epsilon n$ for an arbitrary fixed $\epsilon > 0$ (see [85, Theorem 1]). This result gives Theorem 6.1.7 with its first error term term replaced with the less uniform bound $O_{B,U}(uq^n/n)$. However, it suffices to establish Theorem 6.1.8(i) as stated.

Proof of Theorem 6.1.7. Let $P_1, \ldots, P_K$ be the distinct monic irreducible factors of F, numbered so that $\deg P_i = d_i$. Then $F(h(T))$ has all its prime factors of degree $\leq n/u$ precisely when the same is true for each of the polynomials $P_i(h(T))$. For $1 \leq i \leq K$, let λ_i run over the cycle types of permutations on n letters corresponding to permutations σ with $L(\sigma) \leq \frac{n}{d_i u}$. By Theorem 5.1.2, we have

$$\Psi(F; n, n/u) = \sum_{\lambda_1,\ldots,\lambda_K} q^n \prod_{i=1}^{K} T(\lambda_i) + O_B\left(\sum_{\lambda_1,\ldots,\lambda_K} n n!^B q^{n-1/2}\right).$$

Since the number of possibilities for each λ_i is (crudely) bounded above by 2^n, the error here is

$$\ll_B 2^{nK} n n!^B q^{n-1/2} \leq 2^{2nB} n!^B q^{n-1/2} \ll_B n!^{2B} q^{n-1/2}.$$

Using Lemma 6.6.1, we see that the main term here is

$$\begin{aligned} q^n \prod_{i=1}^{K} \left(\sum_{\lambda_i} T(\lambda_i)\right) &= q^n \prod_{i=1}^{K} (\rho(d_i u) + O(d_i u/n)) \\ &= q^n \rho(d_1 u) \cdots \rho(d_K u) + O_B(uq^n/n). \end{aligned}$$

Combining these two estimates completes the proof of Theorem 6.1.7. □

6.7 Smoothness of neighboring polynomials: Proof of Theorem 6.1.8

Proof of Theorem 6.1.8(i). We may assume $n \geq 2$, since the estimate is trivial for $n = 1$ (or for any absolutely bounded n). By Lemma 6.6.1, the proportion of permutations σ on n letters for which

$$\alpha n \leq L(\sigma) \leq \beta n \tag{6.16}$$

is given by

$$\rho(\beta^{-1}) - \rho(\alpha^{-1}) + O(\kappa/n),$$

where $\kappa = \kappa([\alpha, \beta])$, provided we adopt the convention that $\rho(0^{-1}) = 0$. (Recall that if $I = [\alpha, \beta]$, then $\kappa(I) = 1/\alpha$ if $\alpha \neq 0$ and $\kappa(I) = 1/\beta$ otherwise.) For each $s \in S$, let λ_s run over the cycle types of permutations satisfying (6.16) with $[\alpha, \beta] = [\alpha_s, \beta_s]$. Proceeding as in the proof of Theorem 6.1.7, we find that the number of polynomials $A(T)$ satisfying the conclusion of part (i) is

$$q^n \prod_{s \in S} \left(\sum_{\lambda_s} T(\lambda_s) \right) + O\left(\sum_{\lambda_1, \ldots, \lambda_k} (nk) n!^k q^{n-1/2} \right).$$

The error term here is

$$\ll 2^{nk} (nk) n!^k q^{n-1/2} \ll n!^{2k} q^{n-1/2}.$$

Moreover, since $\kappa([\alpha_s, \beta_s]) \le C$ for each s, the main term here is

$$q^n \prod_{s \in S} \big(\rho(\beta_s^{-1}) - \rho(\alpha_s^{-1}) + O(C/n)\big) = q^n \prod_{s \in S} (\rho(\beta_s^{-1}) - \rho(\alpha_s^{-1})) + O_{k,C}(q^n/n).$$

Combining these estimates finishes the proof. □

Proof of Theorem 6.1.8(ii). Let n be the least positive integer which is prime to q and exceeds $2\epsilon^{-1}$; then $n = O_\epsilon(1)$. For each $s \in S$, choose a $\lfloor \frac{1}{2}(\alpha_s + \beta_s)n \rfloor$-cycle σ_s from S_n. Since $n \ge 2\epsilon^{-1} \ge 2(\beta_s - \alpha_s)^{-1}$, we have

$$\alpha_s n \le L(\sigma_s) \le \beta_s n$$

for each $s \in S$. Let λ_s be the cycle type of σ_s. By Theorem 5.1.2 (applied to the k linear polynomials $f_s(T) = T + s$), if q is chosen large enough (depending on k and ϵ), then we can find a monic, degree n polynomial $A(T)$ for which $A(T) + s$ has cycle type λ_s for all $s \in S$. For this choice of $A(T)$, we have

$$\alpha_s n \le L(A(T) + s) \le \beta_s n$$

for all $s \in S$. We have thus constructed a polynomial satisfying (6.5).

If q is large, we can use this polynomial $A(T)$ to construct an infinite sequence of solutions to (6.5): For each $s \in S$, let $P_s(T)$ be a monic prime of maximal degree dividing $A(T) + s$. Then the degree of $\prod_{s \in S} P_s(T)$ is $O_{k,\epsilon}(1)$, and so by Theorem 3.1.3, if q is large enough (again depending only on k and ϵ) one can find a prime l and a $\beta \in \mathbf{F}_q$ for which all the polynomials $P_s(T^{l^k} - \beta)$ are irreducible for every $k \ge 0$. It is now easy to check that all the polynomials $A(T^{l^k} - \beta)$, with $k = 0, 1, 2, 3, \ldots$, have the desired property. □

Chapter 7

Remarks on the polynomial Goldbach problem

7.1 Introduction

Up to this point we have focused on problems of Hypothesis H type, the quintessential example being the twin prime conjecture. There is another class of problems which Hardy and Littlewood [56, p. 34] call 'conjugate' to these, the most famous of which is Goldbach's conjecture that every even $n > 2$ can be expressed as a sum of two primes. This conjecture remains open, but there has been a great deal of exciting progress, much of which finds its genesis in the already-cited paper of Hardy and Littlewood. There the circle method is used to derive, under the Riemann Hypothesis for Dirichlet L-functions, an asymptotic formula for the number of representations of an odd integer as a sum of three primes. (This formula was later proved unconditionally by Vinogradov [118].) The circle method does not appear to resolve the usual binary Goldbach problem (even assuming Riemann hypotheses), but it does provide a heuristic derivation of a plausible asymptotic formula for the number of representations of an even integer as a sum of two primes.

In this chapter we focus our energies on a polynomial analogue of this latter formula. Specifically, we examine the following conjecture: Let α, β be nonzero elements of $\mathbf{F}_q$, and let $\gamma := \alpha + \beta$. Let n be a positive integer. If $\gamma \neq 0$, we suppose that A is a polynomial of degree n over $\mathbf{F}_q$ with leading coefficient γ; otherwise we suppose A is a nonzero polynomial of degree $< n$ over $\mathbf{F}_q$. We let $R(A) = R_{\alpha,\beta,n,\mathbf{F}_q}(A)$ denote the number of pairs of degree-n monic primes P_1, P_2 over $\mathbf{F}_q$ for which $\alpha P_1 + \beta P_2 = A$.

Conjecture 7.1.1. *Let A be a polynomial of degree n over $\mathbf{F}_q$, assumed divisible by $T(T+1)$ in the case when $q = 2$. Then (with notation as above)*

$$R(A) = (1 + o(1))\mathfrak{S}(A)\frac{q^n}{n^2} \quad \textit{as } q^n \to \infty,$$

where

$$\mathfrak{S}(A) := \prod_{P|A}\left(1 + \frac{1}{|P| - 1}\right)\prod_{P\nmid A}\left(1 - \frac{1}{(|P| - 1)^2}\right).$$

Remarks. (i) It will be useful to observe that for A as above, $\mathfrak{S}(A)$ is bounded below by an absolute positive constant. To see this, notice that for every field $\mathbf{F}_q$ and every A as above, we have

$$\mathfrak{S}(A) \geq \prod_{|P|>2}\left(1 - \frac{1}{(|P| - 1)^2}\right).$$

We show that the product here is bounded below by a positive constant, independent of q. Let us first check that the product is positive. For this it is enough to show that $\sum_P(|P|-1)^{-2}$ is convergent. In fact,

$$\sum_P \frac{1}{(|P|-1)^2} \leq \sum_P \frac{4}{|P|^2} \leq \sum_{d\geq 1} \frac{4}{q^{2d}}\frac{q^d}{d} < 4\sum_{d\geq 1}\frac{1}{q^d} = \frac{4}{q-1}. \tag{7.1}$$

This estimate shows moreover that for $q \geq 9$,

$$\prod_{|P|>2}\left(1-\frac{1}{(|P|-1)^2}\right) \geq 1-\sum_P \frac{1}{(|P|-1)^2} \geq 1-\frac{4}{q-1} \geq \frac{1}{2}. \tag{7.2}$$

The claim follows.

(ii) When $\gamma = 0$, the quantity $R(A)$ counts the number of twin prime pairs $\{P, P+A\}$ where P has degree n and leading coefficient α. In Chapter 2, we considered a polynomial analogue of the twin prime conjecture; our prediction (2.6) there follows from Conjecture 7.1.1 upon summing over α.

Conjecture 7.1.1 appears difficult, but Hayes has successfully attacked the corresponding ternary problem ' [61]:

Polynomial three primes theorem. *Let A be a polynomial of degree n over $\mathbf{F}_q$. Suppose α, β, γ are nonzero elements of $\mathbf{F}_q$ for which $\alpha+\beta+\gamma$ agrees with the leading coefficient of A. If $q = 2$, suppose also that $\gcd(A, T(T+1)) = 1$. The number of ordered triples of monic irreducible polynomials P_1, P_2, P_3 over $\mathbf{F}_q$ of degree d with*

$$\alpha P_1 + \beta P_2 + \gamma P_3 = A$$

is

$$\mathfrak{S}^{(3)}(A)\frac{q^{2n}}{n^2} + O\left(q^{(7n+1)/4}\right).$$

Here

$$\mathfrak{S}^{(3)}(A) := \prod_{P|A}\left(1 - \frac{1}{(|P|-1)^2}\right)\prod_{P\nmid A}\left(1 + \frac{1}{(|P|-1)^3}\right)$$

and the implied constant is absolute. Moreover, for A as above, $\mathfrak{S}^{(3)}(A)$ is bounded below by an absolute positive constant.

This paper of Hayes is of additional interest in that it marks the first time the circle method was developed and applied in the polynomial setting.

Our first result in this chapter is an estimate for the 'exceptional set' in Conjecture 7.1.1, i.e., for the number of A which do not admit a representation in the desired form. In the rational setting, such a result goes back again to Hardy and Littlewood. In [57], they show (again assuming the Riemann Hypothesis for Dirichlet L-functions) that the number of even $n \leq x$ not representable as a sum of two primes is is $O(x^{1/2+\epsilon})$ for each $\epsilon > 0$. We prove an unconditional polynomial analogue of this result by using Hayes's version of the circle method; the details are based on the paper of Hardy and Littlewood but with some nods to the monograph of Vaughan [116, Chapter 3]. (In the rational setting, the best unconditional result is due to Pintz, who shows the Hardy-Littlewood result holds with $\epsilon = 1/6$; see the announcement and discussion in [88].)

To simplify the statement of our result, we introduce some psychologically useful terminology. Call a polynomial $A \in \mathbf{F}_q[T]$ *even* if A is divisible by every prime of absolute value 2 over $\mathbf{F}_q$ and*odd* if A is divisible by none of the primes of absolute value 2. Then Hayes's three primes theorem is about 'odd' polynomials and our Goldbach analogue (Conjecture 7.1.1) is about even polynomials. However, it is important to keep in mind that not everything is completely analogous to the rational case; e.g., if $q \neq 2$, all polynomials A over $\mathbf{F}_q$ are both even and odd.

Theorem 7.1.2. *Let α, β be nonzero elements of $\mathbf{F}_q$, and let $\gamma := \alpha + \beta$. Suppose first that $\gamma \neq 0$. Then the number of even polynomials of degree n and leading coefficient γ that cannot be written in the form $\alpha P_1 + \beta P_2$ for prime polynomials P_1, P_2 is*

$$\ll q^{(n+1)/2} n^3.$$

If $\gamma = 0$, then the same bound holds for the number of even polynomials of degree $< n$ that cannot be represented in this form. Here the implied constant is absolute.

Actually we prove a stronger result, which shows that most polynomials have approximately the correct number of representations:

Theorem 7.1.3. *Let α, β be nonzero elements of $\mathbf{F}_q$, and let $R(A)$ be defined as above. Then*

$$\sum_{A}{}' \left| R(A) - \mathfrak{S}(A) \frac{q^n}{n^2} \right|^2 \ll q^{(5n+1)/2} n^{-1}. \tag{7.3}$$

Here the $'$ indicates that the sum is taken over degree n polynomials with leading coefficient γ in the case $\gamma \neq 0$, but over all nonzero polynomials of degree $< n$ when $\gamma = 0$.

Remark. Let us check that Theorem 7.1.3 implies Theorem 7.1.2. Suppose A is an even polynomial of degree n and leading coefficient γ for which $R(A) = 0$; then A contributes $\mathfrak{S}(A)^2 q^{2n}/n^4 \gg q^{2n}/n^4$ to the sum (7.3), using that $\mathfrak{S}(A) \gg 1$. So the number of such A must be

$$\ll \frac{q^{(5n+1)/2} n^{-1}}{q^{2n}/n^4} = q^{(n+1)/2} n^3,$$

which is the assertion of Theorem 7.1.2.

Our second result shows that Conjecture 7.1.1 holds in a certain range of q and n, and should be viewed as analogous to Corollary 5.1.3.

Theorem 7.1.4. *Let α, β be nonzero elements of $\mathbf{F}_q$. If $\alpha + \beta \neq 0$, let A be a polynomial of degree n over $\mathbf{F}_q$ with leading coefficient $\alpha + \beta$, otherwise let A be a nonzero polynomial of degree $< n$. Then*

$$R(A) = \frac{q^n}{n^2} + O((n-1)!n!q^{n-1/2}),$$

where the implied constant is absolute.

Remark. Thus for pairs q, n with $\gcd(q, 2n) = 1$ and $q/(n!^4 n^2)$ tending to infinity, we have $R(A) \sim q^n/n^2$. It is easy to see that in this range of q and n, one has $\mathfrak{S}(A) \sim 1$, so that Theorem 7.1.4 agrees with Conjecture 7.1.1. Indeed, whenever $q > 2$, we have (cf. (7.2))

$$1 - \frac{4}{q-1} < \mathfrak{S}(A) < \prod_{P|A} \left(1 + \frac{1}{|P|-1}\right) \leq \exp\left(\sum_{P|A} \frac{1}{|P|-1}\right) \leq \exp\left(\frac{2n}{q}\right),$$

and both sides of this inequality tend to 1 once q/n tends to infinity.

Note that Theorem 7.1.4 implies that the exceptional set considered in Theorem 7.1.2 is empty when $q > Cn!^4 n^2$, for an appropriate choice of constant C.

7.2 The exceptional set in the polynomial Goldbach problem

Notation and Conventions

The proof of Theorems 7.1.2 and 7.1.3 go through the circle method as developed by Hayes [61]. We remind the reader of the basic setup.

We write $\mathbf{F}_q(T)_\infty$ for the completion of $\mathbf{F}_q(T)$ at the prime associated to the $(1/T)$-adic valuation. It is usual to identify this with the field of finite-tailed Laurent series in $1/T$:

$$\mathbf{F}_q(T)_\infty = \mathbf{F}_q((1/T)) = \left\{ \sum_{i=-\infty}^{n} a_i T^i : a_i \in \mathbf{F}_q, n \in \mathbf{Z} \right\}.$$

We let $|\cdot|$ denote the induced absolute value on $\mathbf{F}_q(T)_\infty$, so that (with the above identification)

$$\left| \sum_{i=-\infty}^{n} a_i T^i \right| = q^n \quad \text{if } a_n \neq 0.$$

The *unit interval* $\mathcal{U}$ is defined as

$$\mathcal{U} := \left\{ \sum_{i<0} a_i T^i : a_i \in \mathbf{F}_q \right\}.$$

Then $\mathcal{U}$ is a compact abelian group; we use ν to denote the Haar measure on $\mathcal{U}$, normalized so that $\nu(\mathcal{U}) = 1$. For notational simplicity, we always abbreviate $\int f(\theta)\, d\nu(\theta)$ to $\int f(\theta)\, d\theta$.

For $\theta \in \mathcal{U}$ and integers $r \geq 1$, we define

$$B(\theta, r) = \{\eta \in \mathcal{U} : |\eta - \theta| < q^{-r}\}.$$

Then the ν-measure of $B(\theta, r)$ is q^{-r} (see [61, Corollary 3.2]).

We write $e\colon \mathbf{F}_q(T)_\infty \to S^1$ for the map defined by

$$e\left(\sum_{i=-\infty}^{n} a_i T^i\right) = \exp\left(\frac{2\pi i}{p}\mathrm{Tr}(a_{-1})\right),$$

where the trace is from $\mathbf{F}_q$ to its prime field $\mathbf{F}_p$.

Throughout we reserve the letter P for monic irreducible elements of $\mathbf{F}_q[T]$.

7.2.1 The fundamental approximation

Let n be a positive integer. To study additive problems concerning degree-n primes, one is led to investigate the behavior of the function $f\colon \mathcal{U} \to \mathbf{C}$ defined by

$$f(\theta) := \sum_{\deg P = n} e(P\theta),$$

where the sum is over monic irreducibles of degree n. We introduce the decomposition

$$\mathcal{U} = \bigcup_{\substack{\deg H \le n/2 \\ H \text{ monic}}} \bigcup_{\substack{\deg G < \deg H \\ \gcd(G,H)=1}} \mathcal{I}_{G/H},$$

$$\text{where} \quad \mathcal{I}_{G/H} = \left\{\eta \in \mathcal{U} : |\eta - G/H| < \frac{1}{q^{\deg H} q^{\lfloor n/2 \rfloor}}\right\}.$$

(Thus $I_{G/H} = B(G/H, \lfloor n/2 \rfloor + \deg H)$.) The sets $\mathcal{I}_{G/H}$, with G and H as above, form a disjoint open cover of $\mathcal{U}$ ([61, Theorem 4.3]). We define $\mathcal{U}_1$ as the union of those intervals $\mathcal{I}_{G/H}$ with $\deg H \le n/4$, and we take $\mathcal{U}_2 := \mathcal{U} \setminus \mathcal{U}_1$.

The function f can be well-approximated on each $I_{G/H}$ by a simpler function g.

For $\theta \in \mathcal{I}_{G/H}$, set

$$g(\theta) := \begin{cases} \frac{\mu(H)}{\varphi(H)} \frac{q^n}{n} e\left(T^n(\theta - G/H)\right) & \text{if } |\theta - G/H| < 1/q^n, \\ 0 & \text{otherwise.} \end{cases}$$

The following fundamental estimate is proved by Hayes as a consequence of Weil's Riemann Hypothesis (see [61, Theorem 5.3, Lemma 7.1]):

Lemma 7.2.1. *For all $\theta \in \mathcal{U}$, we have $|f(\theta) - g(\theta)| < 2q^{(3n+1)/4}$.*

7.2.2 Two lemmas on arithmetic functions

A complex-valued function f, defined on the semigroup $\mathcal{M}$ of monic polynomials over $\mathbf{F}_q$, is said to be *multiplicative* if $f(AB) = f(A)f(B)$ whenever A and B are relatively prime.

We require basic estimates for certain sums of multiplicative functions. For our purposes the following crude lemma suffices:

Lemma 7.2.2. *If G is a nonnegative multiplicative function, then*

$$\sum_{\substack{\deg A \leq d \\ A \text{ monic}}} G(A) \ll q^d \prod_{\deg P \leq d} \left(1 + \frac{|G(P) - 1|}{|P|} + \frac{|G(P^2) - G(P)|}{|P|^2} + \dots\right),$$

where the implied constant is absolute.

Proof. Define a new function $g\colon \mathcal{M} \to \mathbf{C}$ so that $G(A) = \sum_{\substack{D|A \\ D \text{ monic}}} g(D)$. Then g is multiplicative; in fact, $g(A) = \sum_{\substack{D|A \\ D \text{ monic}}} \mu(D)G(A/D)$. In particular, $g(P^k) =$

$G(P^k) - G(P^{k-1})$. Hence

$$\sum_{\substack{\deg A \le d \\ A \text{ monic}}} G(A) = \sum_{\substack{\deg A \le d \\ A \text{ monic}}} \sum_{\substack{D \mid A \\ D \text{ monic}}} g(D) \le (q^d + q^{d-1} + \cdots + q^{\deg D}) \sum_{\substack{\deg D \le d \\ D \text{ monic}}} \frac{|g(D)|}{|D|}$$
$$\le 2q^d \prod_{\deg P \le d} \left(1 + \frac{|G(P) - 1|}{|P|} + \frac{|G(P^2) - G(P)|}{|P|^2} + \ldots\right),$$

which gives the result. □

Lemma 7.2.3. *For every real $i \ge 1$, we have*

$$\sum_{\substack{\deg A = d \\ A \text{ monic}}} \frac{1}{\varphi(A)^i} = O(q^{(1-i)d}),$$

where the implied constant depends only on i.

Proof. Define a multiplicative function G on $\mathcal{M}$ by setting

$$G(A) := \left(\frac{|A|}{\varphi(A)}\right)^i = \prod_{P \mid A} \left(1 - \frac{1}{|P|}\right)^{-i}.$$

Since $|A| = q^d$ when $\deg A = d$, to prove the lemma it is enough to show that

$$\sum_{\substack{\deg A = d \\ A \text{ monic}}} G(A) = O(q^d). \tag{7.4}$$

For each monic prime P we have $|G(P) - 1| \ll_i 1/|P|$. Moreover, since $G(A)$ depends only on the primes dividing A, every difference $G(P^k) - G(P^{k-1})$ with

$k > 1$ vanishes. So 7.2.2 shows that

$$\sum_{\substack{\deg A=d\\ A \text{ monic}}} G(A) \ll q^d \prod_{\deg P\leq d}\left(1+O\left(\frac{1}{|P|^2}\right)\right) = q^d \exp\left(O\left(\sum_P \frac{1}{|P|^2}\right)\right).$$

Now (7.4) follows since $\sum |P|^{-2}$ is absolutely bounded (cf. (7.1)). □

7.2.3 Proof of Theorem 7.1.3

For distinct polynomials A, the functions $e(A\theta)$ define orthonormal elements of $L^2(\mathcal{U})$ (see [61, Theorem 3.5]). Thus

$$\int_{\mathcal{U}} f(\alpha\theta)f(\beta\theta)e(-A\theta)\,d\theta = \sum_{P_1,P_2}\int_{\mathcal{U}} e((\alpha P_1+\beta P_2)\theta)e(-A\theta)\,d\theta = R(A).$$

We decompose $R(A) = R_1(A) + R_2(A)$, where in R_1 the integration is taken over $\mathcal{U}_1$ and in R_2 the integration is taken over $\mathcal{U}_2$. Then

$$\sum_A{}' \left|R(A) - \mathfrak{S}(A)\frac{q^n}{n^2}\right|^2 \ll \sum_A{}' |R_2(A)|^2 + \sum_A{}' \left|R_1(A) - \mathfrak{S}(A)\frac{q^n}{n^2}\right|^2. \qquad (7.5)$$

Lemma 7.2.4. *We have*

$$\int_{\mathcal{U}} |f(\theta)|^2\,d\theta \ll q^n/n \quad \textit{and} \quad \int_{\mathcal{U}} |g(\theta)|^2\,d\theta \ll q^n/n.$$

Proof. The first estimate is almost immediate: We have

$$\int_{\mathcal{U}} |f(\theta)|^2\,d\theta = \sum_{P_1,P_2}\int_{\mathcal{U}} e(\theta(P_1-P_2))\;d\theta = \sum_{P_1} = 1 = \pi(q;n) \leq \frac{q^n}{n}.$$

For the second, we observe that

$$\begin{aligned}\int_{\mathcal{U}} |g(\theta)|^2\,d\theta &= \sum_{\substack{\deg H \le n/2\\ H \text{ monic}}} \sum_{\substack{\deg G < \deg H\\ (G,H)=1}} \int_{B(G/H,n)} \left(\frac{\mu(H)}{\varphi(H)}\right)^2 \frac{q^{2n}}{n^2}\,d\theta\\ &\le \frac{q^n}{n^2} \sum_{\substack{\deg H \le n/2\\ H \text{ monic}}} \left(\frac{\mu(H)}{\varphi(H)}\right)^2 \sum_{\substack{\deg G < \deg H\\ (G,H)=1}} 1 = \frac{q^n}{n^2} \sum_{\substack{\deg H \le n/2\\ H \text{ monic, squarefree}}} \frac{1}{\varphi(H)},\end{aligned}$$

and that the final sum here is $\ll n$ by Corollary 7.2.3. □

Now recall the following elementary result from linear algebra:

Lemma 7.2.5 (Bessel's inequality, finite version)**.** *Let $e_1, \ldots, e_n$ be a finite collection of orthonormal vectors in a complex inner product space V. Then for any $x \in V$,*

$$\sum_{k=1}^{m} |\langle x, e_k\rangle|^2 \le \|x\|^2.$$

Lemma 7.2.6. *We have $\sum_A{}' |R_2(A)|^2 \ll q^{(5n+1)/2} n^{-1}$.*

Proof. We view $R_2(A)$ as the A-th Fourier coefficient of the function $f(\alpha\theta)f(\beta\theta)\mathbf{1}_{\mathcal{U}_2}$, where $\mathbf{1}_{\mathcal{U}_2}$ is the indicator function of the set $\mathcal{U}_2$. So by Bessel's inequality, with the functions $e(A\theta)$ playing the role of the e_i, we see that

$$\sum_A{}' |R_2(A)|^2 \le \int_{\mathcal{U}_2} |f(\alpha\theta)f(\beta\theta)|^2\,d\theta,$$

which, in turn, is bounded by

$$\left(\int_{\mathcal{U}_2} |f(\alpha\theta)|^4\,d\theta\right)^{1/2} \left(\int_{\mathcal{U}_2} |f(\beta\theta)|^4\,d\theta\right)^{1/2}$$

by an application of Cauchy-Schwarz. Since multiplication by an element of $\mathbf{F}_q^\times$

preserves the ν-measure of Borel subsets of $\mathcal{U}$, a change of variables reveals that both the integrals appearing above coincide with $\int_{\mathcal{U}_2} |f(\theta)|^4 \, d\theta$. Now

$$\int_{\mathcal{U}_2} |f(\theta)|^4 \, d\theta \ll \int_{\mathcal{U}_2} |g(\theta)|^4 \, d\theta + \int_{\mathcal{U}_2} |f(\theta) - g(\theta)|^4 \, d\theta.$$

By Lemmas 7.2.1 and 7.2.4, the second integral is

$$\ll \sup |f(\theta) - g(\theta)|^2 \int_{\mathcal{U}_2} (|f(\theta)|^2 + |g(\theta)|^2) \, d\theta$$
$$\ll q^{(3n+1)/2} \left(q^n/n + q^n/n\right) \ll q^{(5n+1)/2} n^{-1}.$$

For the first integral we have (applying Corollary 7.2.3)

$$\begin{aligned}\int_{\mathcal{U}_2} |g(\theta)|^4 \, d\theta &= \frac{q^{4n}}{n^4} \sum_{\substack{n/4 < \deg H \leq n/2 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\varphi(H)}\right)^4 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} \int_{B(G/H,n)} 1 \, d\theta \\ &= \frac{q^{3n}}{n^4} \sum_{\substack{n/4 < \deg H \leq n/2 \\ H \text{ monic, squarefree}}} \frac{1}{\varphi(H)^3} \ll \frac{q^{3n}}{n^4} \sum_{n/4 < r \leq n/2} \frac{1}{q^{2r}} \ll \frac{q^{5n/2}}{n^4}.\end{aligned}$$

The result follows. □

For H a monic polynomial over $\mathbf{F}_q$ and A any element of $\mathbf{F}_q[T]$, define $c_H(A)$ by

$$c_H(A) := \sum_{\substack{G \bmod H \\ (G,H)=1}} e(AG/H).$$

(Here G runs over a reduced residue system modulo H, which will usually be chosen as the set of polynomials of degree $< \deg H$ and coprime to H.) Then $c_H(A)$ is a polynomial analogue of the usual Ramanujan sum. It is multiplicative in H (for fixed A) and satisfies

$$c_H(A) = \frac{\varphi(H)\mu(H/(H,A))}{\varphi(H/(H,A))}. \tag{7.6}$$

(Compare [61, Theorem 6.1].)

Lemma 7.2.7. *We have*

$$R_1(A) = \mathfrak{S}'(A)\frac{q^n}{n^2} + E(A),$$

where

$$\mathfrak{S}'(A) := \sum_{\substack{\deg H \leq n/4 \\ H \ monic}} \left(\frac{\mu(H)}{\varphi(H)}\right)^2 c_H(A)$$

and

$$E(A) := \int_{\mathcal{U}_1} (f(\alpha\theta)f(\beta\theta) - g(\alpha\theta)g(\beta\theta))e(-A\theta)\, d\theta.$$

Proof. We have

$$\begin{aligned} R_1(A) &= \int_{\mathcal{U}_1} g(\alpha\theta)g(\beta\theta)e(-A\theta)\, d\theta + \int_{\mathcal{U}_1} (f(\alpha\theta)f(\beta\theta) - g(\alpha\theta)g(\beta\theta))e(-A\theta)\, d\theta \\ &= \int_{\mathcal{U}_1} g(\alpha\theta)g(\beta\theta)e(-A\theta)\, d\theta + E(A), \end{aligned}$$

and we need to show that the remaining integral is $\mathfrak{S}'(A)q^n/n^2$. Inserting the definition of g, we can rewrite this integral as

$$\frac{q^{2n}}{n^2} \sum_{\substack{\deg H \leq n/4 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\varphi(H)}\right)^2 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} \int_{B(G/H,n)} e((\alpha+\beta)T^n(\theta - G/H))e(-A\theta)\, d\theta$$

Write $e(-A\theta) = e(-AG/H)e(-A(\theta - G/H))$ and make the change of variables $\theta \mapsto \theta + G/H$, so that the integration takes place over $B(0,n)$. This transforms the expression into

$$\frac{q^{2n}}{n^2}\sum_{\substack{\deg H\le n/4\\ H\text{ monic}}}\left(\frac{\mu(H)}{\varphi(H)}\right)^2\sum_{\substack{\deg G<\deg H\\ (G,H)=1}} e(-AG/H)\int_{B(0,n)} e(((\alpha+\beta)T^n-A)\theta)\,d\theta.$$

By the choice of A, the polynomial $(\alpha+\beta)T^n - A$ has degree $< n$; it follows that

$$|((\alpha+\beta)T^n-A)\theta| < q^{-1}\quad\text{for each } \theta\in B(0,n).$$

Recalling the definition of $e(\cdot)$, we see that the integrand here is identically 1. Since the measure of $B(0,n)$ is q^{-n}, the above simplifies to

$$\frac{q^{n}}{n^2}\sum_{\substack{\deg H\le n/4\\ H\text{ monic}}}\left(\frac{\mu(H)}{\varphi(H)}\right)^2\sum_{\substack{\deg G<\deg H\\ (G,H)=1}} e(-AG/H).$$

But the last sum here is exactly $c_H(-A) = c_H(A)$. □

Lemma 7.2.8. *We have* ${\sum}'_A |\mathfrak{S}(A)-\mathfrak{S}'(A)|^2 \ll q^{n/2}n^3$.

Proof. Since $c_H(A)$ is multiplicative in H, we have

$$\sum_{H\text{ monic}}\left(\frac{\mu(H)}{\varphi(H)}\right)^2 c_H(A) = \prod_P\left(1+\frac{1}{(|P|-1)^2}c_P(A)\right) = \mathfrak{S}(A).$$

(The factorization here is justified by the absolute convergence of the left-hand sum, which follows from (7.6).) Hence

$$\begin{aligned}\left|\mathfrak{S}(A)-\mathfrak{S}'(A)\right| &= \sum_{\substack{\deg H>n/4\\ H\text{ monic}}}\left(\frac{\mu(H)}{\varphi(H)}\right)^2\frac{\varphi(H)\mu(H/(H,A))}{\varphi(H/(H,A))}\\ &= \sum_{\substack{D\mid A\\ D\text{ squarefree, monic}}}\ \sum_{\substack{\deg H>n/4\\ H\text{ monic}\\ D\mid H,\ (H/D,A)=1}}\frac{\mu(H)^2}{\varphi(H)}\frac{\mu(H/D)}{\varphi(H/D)}\\ &= \sum_{\substack{D\mid A\\ D\text{ monic, squarefree}}}\frac{1}{\varphi(D)}\sum_{\substack{\deg E>n/4-\deg D\\ E\text{ monic, }(E,A)=1}}\frac{\mu(E)}{\varphi(E)^2}.\end{aligned}$$

Appealing to Lemma 7.2.3, this last double sum is

$$\ll q^{-n/4}\sum_{\substack{D\mid A\\ D\text{ monic, squarefree}}}\frac{|D|}{\varphi(D)}.$$

Thus

$$\left|\mathfrak{S}(A)-\mathfrak{S}'(A)\right|^2\ll q^{-n/2}K(A),\quad\text{where}\quad K(A):=\left(\sum_{\substack{D\mid A\\ D\text{ monic, squarefree}}}\frac{|D|}{\varphi(D)}\right)^2.$$

Applying Lemma 7.2.2,

$$\sum_A{}' K(A)\le q^n\prod_{\deg P\le n}\left(1+\frac{|K(P)-1|}{|P|}\right). \tag{7.7}$$

Now

$$\frac{K(P)-1}{|P|}=\frac{2}{|P|-1}+\frac{|P|}{(|P|-1)^2}=\frac{3}{|P|}+O\left(\frac{1}{|P|^2}\right),$$

and so the product on the right-hand side of (7.7) is

$$\exp\left(\sum_{\deg P\le n}\frac{3}{|P|}+O(1)\right)\ll\exp\left(\sum_{r\le n}\frac{3}{q^r}\frac{q^r}{r}\right)=\exp(3\log n+O(1))\ll n^3.$$

Piecing it all together, $\sum_A{}^{'}|\mathfrak{S}(A)-\mathfrak{S}'(A)|^2\ll q^{-n/2}q^nn^3=q^{n/2}n^3$, as desired. □

Lemma 7.2.9. *We have* $\sum_A{}^{'}|E(A)|^2\ll q^{(5n+1)/2}n^{-1}$.

Proof. By another application of Bessel's inequality,

$$\sum_A{}^{'}|E(A)|^2\le\int_{\mathcal{U}_1}|f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2\,d\theta.$$

Since

$$|f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2\ll|f(\alpha\theta)-g(\alpha\theta)|^2|f(\beta\theta)|^2+|f(\beta\theta)-g(\beta\theta)|^2|g(\alpha\theta)|^2,$$

we have by Lemmas 7.2.1 and 7.2.4,

$$\begin{aligned}\int_{\mathcal{U}_1}|f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2&\ll\sup|f-g|^2\left(\int_{\mathcal{U}}|f(\beta\theta)|^2+\int_{\mathcal{U}}|g(\alpha\theta)|^2\right)\\&\ll q^{(3n+1)/2}\left(\int_{\mathcal{U}}|f(\theta)|^2+\int_{\mathcal{U}}|g(\theta)|^2\right)\ll q^{(3n+1)/2}q^nn^{-1}=q^{(5n+1)/2}n^{-1},\end{aligned}$$

as desired. □

Lemma 7.2.10. *We have* $\sum_A{}^{'}|R_1(A)-\mathfrak{S}(A)q^n/n^2|^2\ll q^{(5n+1)/2}n^{-1}$.

Proof. Observe that

$$\begin{aligned}\sum_A{}' \left|R_1(A) - \mathfrak{S}(A)\frac{q^n}{n^2}\right|^2 \\ &\ll \sum_A{}' \left|R_1(A) - \mathfrak{S}'(A)\frac{q^n}{n^2}\right|^2 + \sum_A{}' \left|\mathfrak{S}'(A)\frac{q^n}{n^2} - \mathfrak{S}(A)\frac{q^n}{n^2}\right|^2 \\ &= \sum_A{}' |E(A)|^2 + \frac{q^{2n}}{n^4}\sum_A{}' |\mathfrak{S}(A) - \mathfrak{S}'(A)|^2.\end{aligned}$$

By Lemmas 7.2.8 and 7.2.9, this is

$$\ll q^{(5n+1)/2}n^{-1} + \frac{q^{2n}}{n^4}q^{n/2}n^3 \ll q^{(5n+1)/2}n^{-1},$$

as desired. □

Theorem 7.1.3 follows immediately upon combining (7.5) with the results of Lemmas 7.2.6 and 7.2.10.

7.3 Proof of Theorem 7.1.4

We apply the explicit form of the Chebotarev density theorem as explained in detail in Chapter 4. We assume throughout that $n \geq 2$, since Theorem 7.1.4 is trivial otherwise.

Recall that $\gcd(q, 2n) = 1$ and that

$$A(T) = \gamma T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$$

with $a_i \in \mathbf{F}_q$. Here $\gamma = \alpha + \beta$, and we might have $\gamma = 0$.

Lemma 7.3.1. *For all but $O(n^2q^{n-2})$ choices of $(h_1, \ldots, h_{n-1}) \in \mathbf{F}_q^{n-1}$, all of the following hold with*

$$H(T) := \alpha T^n + h_{n-1}T^{n-1} + \cdots + h_1 T. \tag{7.8}$$

(i) *If K_1 is the splitting field of $H(T) - u$ over $\mathbf{F}_q(u)$ and K_2 the splitting field of $H(T) - A(T) - u$ over $\mathbf{F}_q(u)$, then $K_1/\mathbf{F}_q(u)$ and $K_2/\mathbf{F}_q(u)$ are Galois with Galois groups the full symmetric group on n letters.*

(ii) *Let L be the compositum of K_1 and K_2. Then $L/\mathbf{F}_q(u)$ is a geometric Galois extension. Moreover, the map*

$$\begin{gathered}\mathrm{Gal}(L/\mathbf{F}_q(u)) \to \mathrm{Gal}(K_1/\mathbf{F}_q(u)) \times \mathrm{Gal}(K_2/\mathbf{F}_q(u)) \\ \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})\end{gathered}$$

is an isomorphism.

(iii) *The genus of L is $O(nn!^2)$.*

Here all implied constants are absolute.

Proof. We claim that (i)-(iii) all hold if we assume that

$$\mathrm{disc}_u^{n-1}\,\mathrm{disc}_T^n(H(T) - u) \neq 0, \tag{7.9}$$

$$\mathrm{disc}_u^{n-1}\,\mathrm{disc}_T^n(H(T) - A(T) - u) \neq 0, \tag{7.10}$$

$$\mathrm{res}_u^{n-1,n-1}(\mathrm{disc}_T^n(H(T) - u), \mathrm{disc}_T^n(H(T) - A(T) - u)) \neq 0. \tag{7.11}$$

Let us first show that (7.9)-(7.11) exclude $O(n^2q^{n-2})$ choices of $(h_1, \ldots, h_{n-1}) \in$

$\mathbf{F}_q^{n-1}$. Define polynomials $Y(u_1, \ldots, u_{n-1}, u)$ and $Z(u_1, \ldots, u_{n-1})$ by setting

$$\begin{aligned} Y(u_1, \ldots, u_{n-1}, u) &:= \operatorname{disc}_T^n(T^n + u_{n-1}T^{n-1} + \cdots + u_1 T - u), \\ Z(u_1, \ldots, u_{n-1}) &:= \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(T^n + u_{n-1}T^{n-1} + \cdots + u_1 T - u). \end{aligned}$$

Lemma 5.4.3 asserts that Z is a nonzero polynomial of degree at most $(2n-1)(2n-3)$; hence $Z(h_1, \ldots, h_{n-1}) = 0$ for at most $4n^2 q^{n-2}$ choices of $(h_1, \ldots, h_{n-1}) \in \mathbf{F}_q^{n-1}$. Now observe that

$$\begin{aligned} \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(H(T) - u) &= \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(\alpha T^n + h_{n-1}T^{n-1} + \cdots + h_1 T - u) \\ &= \operatorname{disc}_u^{n-1} \alpha^{2n-2} Y(h_1\alpha^{-1}, \ldots, h_{n-1}\alpha^{-1}, u\alpha^{-1}) \\ &= \alpha^{(2n-2)(2n-4)} \operatorname{disc}_u^{n-1} Y(h_1\alpha^{-1}, \ldots, h_{n-1}\alpha^{-1}, u\alpha^{-1}). \end{aligned}$$

But

$$\begin{aligned} &\operatorname{disc}_u^{n-1} Y(h_1\alpha^{-1}, \ldots, h_{n-1}\alpha^{-1}, u\alpha^{-1}) \\ &\qquad = \alpha^{-(n-1)(n-2)} \operatorname{disc}_u^{n-1} Y(h_1\alpha^{-1}, \ldots, h_{n-1}\alpha^{-1}, u) \\ &\qquad\qquad = \alpha^{-(n-1)(n-2)} Z(h_1\alpha^{-1}, \ldots, h_{n-1}\alpha^{-1}). \end{aligned}$$

It follows that (7.9) holds for all but $O(n^2 q^{n-2})$ choices of $h_1, \ldots, h_{n-1}$. A similar computation shows that

$$\begin{aligned} &\operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(H(T) - A(T) - u) \\ &\quad = \operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(-\beta T^n + (h_{n-1} - a_{n-1})T^n + \cdots + (h_1 - a_1)T - a_0 - u) \\ &\qquad = \beta^{3(n-1)(n-2)} Z((a_1 - h_1)\beta^{-1}, \ldots, (a_{n-1} - h_{n-1})\beta^{-1}), \end{aligned}$$

which implies that (7.10) also holds for all but $O(n^2q^{n-2})$ choices of $h_1, \ldots, h_{n-1}$.

Condition (7.11) requires more care. The left hand side of (7.11) defines a polynomial in $h_1, \ldots, h_{n-1}$ of total degree at most $4n^2$ over $\mathbf{F}_q$. Indeed, viewing the inner T-discriminants as determinants of $(2n-1) \times (2n-1)$ Sylvester matrices, we see each argument of the u-resultant has total degree at most $(2n-1)$ in $T_1, \ldots, T_{n-1}$. Now view the resultant as the determinant of a $(2n-2) \times (2n-2)$ Sylvester matrix to bound the degree by $(2n-1)(2n-2) \leq 4n^2$. So the desired bound on the number of exceptions to (7.11) will follow from Lemma 5.4.1 once we check that this polynomial is not identically zero.

Suppose for the sake of contradiction that it is identically zero; then for every field F containing $\mathbf{F}_q$ and every choice of $h_1, \ldots, h_{n-1} \in F$, the polynomials

$$\mathrm{disc}_T^n(\alpha T^n + h_{n-1}T^{n-1} + \cdots + h_1 T - u) \tag{7.12}$$

and

$$\mathrm{disc}_T^n(-\beta T^n + (h_{n-1} - a_{n-1})T^n + \cdots + (h_1 - a_1)T - a_0 - u) \tag{7.13}$$

share a root from the algebraic closure of F. With $v \in F$ to be chosen, define $h_i = \alpha\binom{n}{i}v^i$ (for $1 \leq i < n$). With this choice of the h_i,

$$\alpha T^n + h_{n-1}T^{n-1} + \cdots + h_1 T - u = \alpha(T+v)^n - (u + \alpha v^n),$$

which forces the discriminant (7.12) to vanish only at $u = -\alpha v^n$. Thus (7.13) must also vanish at $u = -\alpha v^n$; in other words, we must have

$$\mathrm{disc}_T^n(\alpha(T+v)^n - A(T)) = 0. \tag{7.14}$$

We show that this fails if we choose $F = \overline{\mathbf{F}}_q(v)$, where v is transcendental over $\overline{\mathbf{F}}_q$. Let m be the largest divisor of n with the property that $A(T)$ is an mth power in $\overline{\mathbf{F}}_q[T]$; say $A(T) = \tilde{A}(T)^m$. Let $\alpha^{1/m}$ denote a fixed mth root of α from $\overline{\mathbf{F}}_q$. Then we can write

$$A(T) - \alpha(T+v)^n = \prod_{\zeta^m=1}\left(\tilde{A}(T) - \zeta\alpha^{1/m}(T+v)^{n/m}\right). \tag{7.15}$$

The m factors in the right-hand product are all coprime: By considering the difference of any two, we see that $-v$ is the only possible common root over the algebraic closure of F; but none of these factors can vanish at $-v$ since v is transcendental over $\overline{\mathbf{F}}_q$.

Moreover, each of these factors is irreducible in $F[T] = \overline{\mathbf{F}}_q(v)[T]$. To see this, note that by Gauss's lemma, it is enough to verify irreducibility in $\overline{\mathbf{F}}_q[v][T] = \overline{\mathbf{F}}_q[T][v]$. Now there is an automorphism of $\overline{\mathbf{F}}_q[T][v]$ fixing $\overline{\mathbf{F}}_q[T]$ and sending $v \mapsto v - T$; this implies that $\tilde{A}(T) - \zeta\alpha^{1/m}(T+v)^{n/m}$ is irreducible in $\overline{\mathbf{F}}_q[T][v]$ if and only if the same is true for $\tilde{A}(T) - \zeta\alpha^{1/m}v^{n/m}$. We finally appeal to Capelli's theorem (Theorem 1.3.11): the choice of m guarantees that this polynomial is irreducible over $\mathbf{F}_q(T)$ and, being primitive in T, also over $\mathbf{F}_q[T]$.

Since each of these m irreducibles has degree prime to q, they are all separable over F. Moreover, since the m factors are relatively prime, it follows that their product $A(T) - \alpha(T+v)^n$ also has distinct roots in the algebraic closure of F. This contradicts (7.14).

It remains to prove that conditions (7.9)-(7.11) imply (i)-(iii). Let $\bar{K}_1 = \overline{\mathbf{F}}_q K_1$ be the splitting field of $H(T) - u$ over $\overline{\mathbf{F}}_q(u)$ and $\bar{K}_2 = \overline{\mathbf{F}}_q K_2$ be the splitting field of $H(T) - A(T) - u$ over $\overline{\mathbf{F}}_q(u)$. From (7.9) and (7.10), we deduce by means of the Birch and Swinnerton-Dyer criterion (p. 133) that $\bar{K}_1/\overline{\mathbf{F}}_q(u)$ and $\bar{K}_2/\overline{\mathbf{F}}_q(u)$ are Galois with the full symmetric group on n letters as their Galois group, and similarly for $K_1/\mathbf{F}_q(u)$ and $K_2/\mathbf{F}_q(u)$. In particular, we have (i).

To obtain (ii), we first show that $\bar{K}_1$ and $\bar{K}_2$ are linearly disjoint over $\overline{\mathbf{F}}_q(u)$. Notice that (7.11) together with Kummer's theorem (p. 94) implies that the only prime of $\overline{\mathbf{F}}_q(u)$ that can possibly ramify in $\bar{K}_1 \cap \bar{K}_2$ is P_∞. Moreover, from Lemma 5.4.4 and our assumption that $\gcd(q, 2n) = 1$, we see that P_∞ is tamely ramified in both $\bar{K}_1$ and $\bar{K}_2$, and so certainly in their intersection. Lemma 4.2.1 now implies that $\bar{K}_1$ and $\bar{K}_2$ intersect precisely in $\overline{\mathbf{F}}_q(u)$, giving the stated linear disjointness. The proof of part (ii) now follows the proof of Lemma 4.4.4: we have a commutative square

$$\begin{tikzcd}
\mathrm{Gal}(\bar{L}/\overline{\mathbf{F}}_q(u)) \arrow[r, "\sigma\mapsto(\sigma|_{\bar{K}_1},\sigma|_{\bar{K}_2})"] \arrow[d, "\sigma\mapsto\sigma|_L"'] & \mathrm{Gal}(\bar{K}_1/\overline{\mathbf{F}}_q(u)) \times \mathrm{Gal}(\bar{K}_2/\overline{\mathbf{F}}_q(u)) \arrow[d, "(\tau_1,\tau_2)\mapsto(\tau_1|_{K_1},\tau_2|_{K_2})"'] \\
\mathrm{Gal}(L/\mathbf{F}_q(u)) \arrow[r, "\sigma\mapsto(\sigma|_{K_1},\sigma|_{K_2})"] & \mathrm{Gal}(K_1/\mathbf{F}_q(u)) \times \mathrm{Gal}(K_2/\mathbf{F}_q(u))
\end{tikzcd} , \qquad (7.16)$$

where each map except the one we are interested in is known to be an isomorphism. So that map must be an isomorphism as well. Moreover, if $\alpha \in L$ is algebraic over $\mathbf{F}_q$, then the left vertical isomorphism forces α to be fixed by every element of $\mathrm{Gal}(L/\mathbf{F}_q(u))$. So $\alpha \in \overline{\mathbf{F}}_q \cap \mathbf{F}_q(u) = \mathbf{F}_q$. Thus $L/\mathbf{F}_q(u)$ is geometric.

Lemma 5.5.3 gives a bound of $O(nn!)$ for the genus of both $\bar{K}_1$ and $\bar{K}_2$; feeding these bounds into the Castelnuovo-Severi inequality (p. 103) shows that the genus of $\bar{K}_1\bar{K}_2 = \bar{L}$ is $O(nn!^2)$. Since L and $\bar{L} = \overline{\mathbf{F}}_q L$ have the same genus, (iii) follows. □

Proof of Theorem 7.1.4. For each polynomial $H(T)$ of the form (7.8), we count the number of $a \in \mathbf{F}_q$ for which both $H(T) - a$ and $H(T) - A(T) - a$ are irreducible. Each such a gives rise to a decomposition

$$A(T) = (H(T) - a) + (A(T) - H(T) + a)$$

of $A(T)$ as a sum of degree-n irreducibles with respective leading coefficients α and β. Conversely, each such decomposition comes from a unique $H(T)$ and a.

Suppose $H(T)$ has the shape (7.8) and is such that (i)-(iii) of Lemma 7.3.1 hold. Suppose moreover that

$$\mathrm{disc}_T\,(H(T) - a) \neq 0 \quad \text{and} \quad \mathrm{disc}_T\,(H(T) - A(T) - a) \neq 0;$$

each of these conditions specifies that a lie outside the zero-set of a degree $(n-1)$-polynomial, and so together they exclude at most $2n - 2$ values of $a \in \mathbf{F}_q$. Lemma 4.3.2 shows that for these a, the polynomials $H(T) - a$ and $H(T) - A(T) - a$ are simultaneously irreducible if and only if $(K_1/\mathbf{F}_q(u), P_a)$ and $(K_2/\mathbf{F}_q(u), P_a)$ both correspond to the conjugacy class of n-cycles in the symmetric group on n letters. From part (ii) of Lemma 7.3.1, we see this is equivalent to requiring that the Frobenius $(L/\mathbf{F}_q(u), P_a)$ coincide with a conjugacy class of size $(n-1)!^2$ in $\mathrm{Gal}(L/\mathbf{F}_q(u))$. So by the explicit form of the Chebotarev density theorem given in Chapter 4 (p. 96), the number of a for which $H(T) - a$ and $H(T) - A(T) - a$ are simultaneously irreducible is

$$q\frac{(n-1)!^2}{n!^2} + O\left(\frac{1}{n^2} n n!^2 q^{1/2}\right) + O(n) = \frac{q}{n^2} + O(n!(n-1)!q^{1/2}).$$

Let X be the number of polynomials $H(T)$ of the form (7.8) for which the conclusions (i)-(iii) of Lemma 7.3.1 hold, so that

$$q^{n-1} - Cn^2q^{n-2} \leq X \leq q^{n-1}$$

for some absolute constant C. Taking into account all possible values of H, we find that

$$\begin{aligned} R(A) &= X\frac{q}{n^2} + O(Xn!(n-1)!q^{1/2}) + O((q^{n-1} - X)q) \\ &= \frac{q^n}{n^2} + O(q^{n-1}) + O(n!(n-1)!q^{n-1/2}) + O(n^2q^{n-1}) \\ &= \frac{q^n}{n^2} + O(n!(n-1)!q^{n-1/2}), \end{aligned}$$

as was to be proved. □

Bibliography

[1] G. E. Andrews, *Number theory*, Dover Publications Inc., New York, 1994, Corrected reprint of the 1971 original [Dover, New York; MR0309838 (46 #8943)].

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. I and II*, Math. Z. **19** (1924), no. 1, 153–246.

[3] ———, *Quadratische Körper über Polynombereichen Galois'scher Felder und ihre Zetafunktionen*, Abh. Math. Sem. Univ. Hamburg **70** (2000), 3–30.

[4] A. Balog and T. D. Wooley, *On strings of consecutive integers with no large prime factors*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 2, 266–276.

[5] A. S. Bang, *Taltheoretiske undersögelser.*, Tidsskrift for mathematik **5** (1886), 130–137.

[6] G. Bareikis, *The Selberg sieve method in the polynomial set*, Liet. Mat. Rink. **41** (2001), no. Special Issue, 39–44.

[7] ———, *Poisson distribution in the polynomial semigroup*, Liet. Mat. Rink. **44** (2004), no. 4, 429–442.

[8] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.

[9] A. O. Bender and O. Wittenberg, *A potential analogue of Schinzel's hypothesis for polynomials with coefficients in* $\mathbf{F}_q[t]$, Int. Math. Res. Not. **36** (2005), 2237–2248.

[10] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication.

[11] B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. **5** (1959), 417–423.

[12] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, third ed., Contemporary Mathematics, vol. 22, American Mathematical Society, Providence, RI, 2002, updates available at `http://homes.cerias.purdue.edu/~ssw/cun/`.

[13] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ *où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bull. Sci. Math **43** (1919), 100–104, 124–128.

[14] V. Buniakovsky, *Sur les diviseurs numeriques invariables des fonctions rationnelles entieres*, Mem. Acad. Sci. St. Petersburg **6** (1857), 305–329.

[15] M. Car, *Le problème de Goldbach pour l'anneau des polynômes sur un corps fini*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A201–A204.

[16] ———, *Sommes de carrés et d'irréductibles dans* $\mathbf{F}_q[X]$, Ann. Fac. Sci. Toulouse Math. (5) **3** (1981), no. 2, 129–166.

[17] ———, *Le théorème de Chen pour* $\mathbf{F}_q[X]$, Dissertationes Math. (Rozprawy Mat.) **223** (1984), 54.

[18] ———, *Sommes de carrés de polynômes irréductibles dans* $\mathbf{F}_q[X]$, Acta Arith. **44** (1984), no. 4, 307–321.

[19] ———, *Sommes d'un carré et d'un polynôme irréductible dans* $\mathbf{F}_q[X]$, Ann. Fac. Sci. Toulouse Math. (5) **6** (1984), no. 3-4, 185–213 (1985).

[20] ———, *Théorèmes de densité dans* $\mathbf{F}_q[X]$, Acta Arith. **48** (1987), no. 2, 145–165.

[21] ———, *The generalized polynomial Goldbach problem*, J. Number Theory **57** (1996), no. 1, 22–49.

[22] ———, *Distribution des polynômes irréductibles dans* $\mathbf{F}_q[T]$, Acta Arith. **88** (1999), no. 2, 141–153.

[23] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Proc. Nat. Acad. Sci. U. S. A. **17** (1931), 120–122.

[24] A. Cauchy, *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Oeuvres complètes, 2, vol. XIII, Gauthier Villars, Paris, 1932, pp. 171–282.

[25] J. Cherly, *A lower bound theorem in* $F_q[x]$, J. Reine Angew. Math. **303/304** (1978), 253–264.

[26] S. Chowla, *A note on the construction of finite Galois fields* $\mathrm{GF}(p^n)$, J. Math. Anal. Appl. **15** (1966), 53–54.

[27] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271.

[28] ———, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) **6** (1972), 93–102.

[29] ———, *Windmill polynomials over fields of characteristic two*, Monatsh. Math. **107** (1989), no. 4, 291–301.

[30] ———, *Some function field estimates with applications*, Number theory and its applications (Ankara, 1996), Lecture Notes in Pure and Appl. Math., vol. 204, Dekker, New York, 1999, pp. 23–45.

[31] B. Conrad and K. Conrad, *The Möbius function and the residue theorem*, J. Number Theory **110** (2005), no. 1, 22–36.

[32] B. Conrad, K. Conrad, and R. Gross, *Prime specialization in genus* 0, Transactions of the AMS (to appear), 2006.

[33] K. Conrad, *Irreducible values of polynomials: a non-analogy*, Number fields and function fields—two parallel worlds, Progr. Math., vol. 239, Birkhäuser Boston, Boston, MA, 2005, pp. 71–85.

[34] R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, second ed., Springer, New York, 2005.

[35] N. G. de Bruijn, *Asymptotic methods in analysis*, third ed., Dover Publications Inc., New York, 1981.

[36] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev, *A complete Vinogradov* 3*-primes theorem under the Riemann hypothesis*, Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 99–104 (electronic).

[37] K. Dickman, *On the frequency of numbers containing prime factors of a certain relative magnitude*, Ark. Mat. Astr. Fys. **22** (1930), 1–14.

[38] L. E. Dickson, *Higher irreducible congruences*, Bull. Amer. Math. Soc. **3** (1897), 381–389.

[39] ———, *Linear groups: with an exposition of the Galois field theory*, With an introduction by W. Magnus, Dover Publications Inc., New York, 1958.

[40] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991, Oxford Science Publications.

[41] ———, *A complete solution to the polynomial* 3*-primes problem*, Bull. Amer. Math. Soc. (N.S.) **24** (1991), no. 2, 363–369.

[42] G. W. Effinger, K. Hicks, and G. L. Mullen, *Twin irreducible polynomials over finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111.

[43] P. Erdős, *Problems and results on number theoretic properties of consecutive integers and related questions*, Proceedings of the Fifth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1975), Winnipeg, Man., 1976, pp. 25–44. Congressus Numerantium, No. XVI,Utilitas Math.

[44] P. Erdős and C. Pomerance, *On the largest prime factors of n and $n+1$*, Aequationes Math. **17** (1978), no. 2-3, 311–321.

[45] L. Euler, *Letter to Goldbach (October 28, 1752)*, Available electronically from the Euler archive: `http://www.math.dartmouth.edu/~euler/correspondence/correspondents/Goldbach.html`.

[46] G. Frei, *The unpublished section eight: on the way to function fields over a finite field*, The shaping of arithmetic after C. F. Gauss's *Disquisitiones arithmeticae*, Springer, Berlin, 2007, pp. 159–198.

[47] M. D. Fried and M. Jarden, *Field arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005.

[48] W. Fulton, *Algebraic curves. An introduction to algebraic geometry*, W. A. Benjamin, Inc., New York-Amsterdam, 1969, Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[49] P. X. Gallagher, *On the distribution of primes in short intervals*, Mathematika **23** (1976), no. 1, 4–9.

[50] C. F. Gauss, *Untersuchungen über höhere Arithmetik*, Deutsch herausgegeben von H. Maser, Chelsea Publishing Co., New York, 1965.

[51] X. Gourdon, *Combinatoire, algorithmique et géométrie des polynômes*, Ph.D. thesis, Ecole Polytechnique, 1996.

[52] A. Granville, *Harald Cramér and the distribution of prime numbers*, Scand. Actuar. J. (1995), no. 1, 12–28, Harald Cramér Symposium (Stockholm, 1993).

[53] A. Granville and K. Soundararajan, *A binary additive problem of Erdős and the order of* $2 \bmod p^2$, Ramanujan J. **2** (1998), no. 1-2, 283–298, Paul Erdős (1913–1996).

[54] C. J. Hall, *L-functions of twisted Legendre curves*, Ph.D. thesis, Princeton University, 2003.

[55] ———, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128–147.

[56] G. H. Hardy and J. E. Littlewood, *Some problems of Partitio Numerorum III: on the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[57] ———, *Some problems of Partitio Numerorum V: a further contribution to the study of Goldbach's problem*, J. London Math. Soc. **22** (1923), 46–56.

[58] D. R. Hayes, *A polynomial analog of the Goldbach conjecture*, Bull. Amer. Math. Soc. **69** (1963), 115–116.

[59] ———, *Correction to "A polynomial analog of the Goldbach conjecture"*, Bull. Amer. Math. Soc. **69** (1963), 493.

[60] ———, *The distribution of irreducibles in* $\mathrm{GF}[q, x]$, Trans. Amer. Math. Soc. **117** (1965), 101–127.

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

[62] ———, *The Galois group of $x^n + x - t$*, Duke Math. J. **40** (1973), 459–461.

[63] A. J. Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. **95** (1985), no. 4, 517–523.

[64] ———, *On integer sets containing strings of consecutive integers*, Mathematika **36** (1989), no. 1, 60–70.

[65] ———, *Multiplicative properties of consecutive integers*, Analytic number theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser., vol. 247, Cambridge Univ. Press, Cambridge, 1997, pp. 103–117.

[66] C.-N. Hsu, *The distribution of irreducible polynomials in $\mathbf{F}_q[t]$*, J. Number Theory **61** (1996), no. 1, 85–96.

[67] ———, *A large sieve inequality for rational function fields*, J. Number Theory **58** (1996), no. 2, 267–287.

[68] ———, *Applications of the large sieve inequality for $\mathbf{F}_q[T]$*, Finite Fields Appl. **4** (1998), no. 3, 275–281.

[69] G. J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[70] D. Klyve, *Explicit bounds on twin primes and Brun's constant*, Ph.D. thesis, Dartmouth College, 2007.

[71] J. Knopfmacher, *Analytic arithmetic of algebraic function fields*, Lecture Notes in Pure and Applied Mathematics, vol. 50, Marcel Dekker Inc., New York, 1979.

[72] J. Knopfmacher and W.-B. Zhang, *Number theory arising from finite fields: analytic and probabilistic theory*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 241, Marcel Dekker Inc., New York, 2001.

[73] D. E. Knuth and L. Trabb Pardo, *Analysis of a simple factorization algorithm*, Theoret. Comput. Sci. **3** (1976/77), no. 3, 321–348.

[74] H. von Koch, *Sur la distribution des nombres premiers*, Acta Math. **24** (1901), 159–182.

[75] H. Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Zeitschrift **5** (1919), 100–111.

[76] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[77] D. N. Lenskoi, *On the arithmetic of polynomials over a finite field*, Volz. Mat. Sb. **4** (1966), 155–159.

[78] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.

[79] Y.-R. Liu, *A generalization of the Turán theorem and its applications,* and *A generalization of the Erdös-Kac theorem and its applications*, Canad. Math. Bull. **47** (2004), no. 4, 573–606.

[80] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields*, preprint available electronically from the second author's website: `http://www.maths.bristol.ac.uk/~matdw/wpfqt290507.pdf`, 2008.

[81] G. Martin, *An asymptotic formula for the number of smooth values of a polynomial*, J. Number Theory **93** (2002), no. 2, 108–182.

[82] A. Masuda and D. Panario, *Sequences of consecutive smooth polynomials over a finite field*, Proc. Amer. Math. Soc. **135** (2007), no. 5, 1271–1277 (electronic).

[83] T. Nicely, *Counts of twin prime pairs and Brun's constant to* $5e15$, Available at `http://www.trnicely.net/twins/tabpi2.html`.

[84] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Astérisque (1988), no. 161-162, Exp. No. 694, 4, 165–186 (1989), Séminaire Bourbaki, Vol. 1987/88.

[85] M. Omar, D. Panario, B. Richmond, and J. Whitely, *Asymptotics of largest components in combinatorial structures*, Algorithmica **46** (2006), no. 3-4, 493–503.

[86] D. Panario, X. Gourdon, and P. Flajolet, *An analytic approach to smooth polynomials over finite fields*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 226–236.

[87] A. E. Pellet, *Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier p*, C. R. Acad. Sci. Paris. **86** (1878), 1071–1072.

[88] J. Pintz, *Landau's problems on primes*, preprint available from the author's website at `http://www.renyi.hu/~pintz/pjapr.pdf`.

[89] P. Pollack, *Arithmetic properties of polynomial specializations over finite fields*, submitted.

[90] ———, *An explicit approach to Hypothesis H for polynomials over a finite field*, Proceedings of the Anatomy of Integers Conference, Montréal, March 2006 (to appear).

[91] ———, *A polynomial analogue of the twin prime conjecture*, Proceedings of the AMS (to appear), 2008.

[92] ———, *Simultaneous prime specializations of polynomials over finite fields*, J. London Math. Soc. (to appear), 2008.

[93] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. **118** (2003), no. 2, 353–373.

[94] R. Ree, *Proof of a conjecture of S. Chowla*, J. Number Theory **3** (1971), 210-212; erratum **4** (1972), 223.

[95] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. (Rozprawy Mat.) **95** (1972), 75.

[96] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996.

[97] H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. **21** (1983), no. 1, 46–74.

[98] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919.

[99] P. Roquette, *The Riemann hypothesis in characteristic p, its origin and development. I. The formation of the zeta-functions of Artin and of F. K. Schmidt*,

Mitt. Math. Ges. Hamburg **21** (2002), no. 2, 79–157, Hamburger Beiträge zur Geschichte der Mathematik.

[100] ______, *The Riemann hypothesis in characteristic p, its origin and development. II. The first steps by Davenport and Hasse*, Mitt. Math. Ges. Hamburg **23** (2004), no. 2, 5–74.

[101] ______, *The Riemann hypothesis in characteristic p, its origin and development. III. The elliptic case*, Mitt. Math. Ges. Hamburg **25** (2006), 103–176.

[102] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[103] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum **5** (1958), 259.

[104] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeitschrift (1931), 1–32.

[105] P. Sebah and X. Gourdon, *Introduction to twin primes and Brun's constant computation*, available from the authors' website at the URL `http://numbers.computation.free.fr/Constants/constants.html`.

[106] E. S. Selmer, *En enkel summasjonsmetode i primtallsteorien, og dens anvendelse på "Bruns sum"*, Norsk mat. tiddskr. **24** (1942), 74–81.

[107] J.-A. Serret, *Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible*, Mémoires de l'Académie des sciences de l'Institut Impérial de France **35** (1866), 617–688.

[108] W. Sierpiński, *Elementary theory of numbers*, second ed., North-Holland Mathematical Library, vol. 31, North-Holland Publishing Co., Amsterdam, 1988, Edited and with a preface by Andrzej Schinzel.

[109] V. T. Sós, *Turbulent years: Erdős in his correspondence with Turán from 1934 to 1940*, Paul Erdős and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 85–146.

[110] C. L. Stewart and K. Yu, *On the abc conjecture. II*, Duke Math. J. **108** (2001), no. 1, 169–181.

[111] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[112] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[113] J. J. Sylvester, *On certain inequalities relating to prime numbers*, Nature **XXXVIII** (1888), 259–262.

[114] F. Thorne, *Irregularities in the distributions of primes in function fields*, Journal of Number Theory (to appear), 2008.

[115] J. G. van der Corput, *Sur l'hypothèse de Goldbach pour presque tous les nombre pairs*, Acta Arith. **2** (1937), 266–290.

[116] R. C. Vaughan, *The Hardy-Littlewood method*, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[117] G. D. Villa Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser Boston Inc., Boston, MA, 2006.

[118] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Comptes Rendues (Doklady) de l'Academy des Sciences de l'USSR **15** (1937), 191–294.

[119] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), no. 219, 1195–1212.

[120] W. A. Webb, *On the representation of polynomials over finite fields as sums of powers and irreducibles*, Rocky Mountain J. Math. **3** (1973), 23–29.

[121] ———, *Sieve methods for polynomial rings over finite fields*, J. Number Theory **16** (1983), no. 3, 343–355.

[122] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.