




# Prime number theory in $\mathbb{F}_q[t]$

Paul Pollack

University of Georgia

July 2013

# The story of the prime number theorem



Let $\pi(x) = \#\{p \leq x : p \text{ prime}\}$. For example, $\pi(2.9) = 1$, $\pi(3) = 2$, and $\pi(100) = 25$.

Interest in the behavior of $\pi(x)$ goes back at least to Euclid, ca. 300 BCE, who knew $\pi(x) \to \infty$ as $x \to \infty$.

# The story of the prime number theorem



Let $\pi(x) = \#\{p \leq x : p \text{ prime}\}$. For example, $\pi(2.9) = 1$, $\pi(3) = 2$, and $\pi(100) = 25$.

Interest in the behavior of $\pi(x)$ goes back at least to Euclid, ca. 300 BCE, who knew $\pi(x) \to \infty$ as $x \to \infty$.

The prime numbers also attracted the attention of a young Gauss. Towards the end of his life, Gauss wrote a letter describing these early investigations.

> *In 1792 or 1793 . . . one of my first projects was to direct my attention to the decreasing frequency of prime numbers, to which end I counted them up in several chiliads and recorded the results . . . I have very often employed a spare quarter of an hour in order to count up a chiliad here and there.*

# The story of the prime number theorem

When Gauss talks about **counting up a chiliad**, he is speaking of computing $\pi(x+1000)-\pi(x)$.

Gauss then looked at the ratios

$$\frac{\pi(x+1000)-\pi(x)}{1000},$$

which is just the proportion of primes $(x, x+1000]$. Studying several values of $x$, he noticed that this ratio was generally decreasing, and seems to resemble $1/\log x$.

This suggests that the "density" of primes near $x$ is $1/\log x$.

# The story of the prime number theorem



To obtain the value of $\pi(x)$, we should integrate the density. This suggests that the number of primes $p \in [a, b]$ should be approximately

$$\int_a^b \frac{\mathrm{d}t}{\log t}.$$

In particular we expect that

$$\pi(x) \approx \int_2^x \frac{\mathrm{d}t}{\log t}.$$

The right-hand side here is called the **logarithmic integral** and denoted $\mathrm{li}(x)$.

Let's see how Gauss's guess that $\pi(x) \approx \mathrm{li}(x)$ looks numerically.

# The counts of primes up to $x$, for $x = 10^k$



| $x$ | $\pi(x)$ | $\mathrm{li}(x)$ |
|---|---|---|
| $10^3$ | 168 | 177 |
| $10^4$ | 1,229 | 1,245 |
| $10^5$ | 9,592 | 9,629 |
| $10^6$ | 78,498 | 78,627 |
| $10^7$ | 664,579 | 664,917 |
| $10^8$ | 5,761,455 | 5,762,208 |
| $10^9$ | 50,847534 | 50,849,234 |
| $10^{10}$ | 455,052,511 | 455,055,614 |
| $10^{11}$ | 4,118,054,813 | 4,118,066,400 |
| $10^{12}$ | 37,607,912,018 | 37,607,950,280 |
| $10^{13}$ | 346,065,536,839 | 346,065,645,809 |
| $10^{14}$ | 3,204,941,750,802 | 3,204,942,065,691 |

# The counts of primes up to $x$, for $x = 10^k$



| $x$ | $\pi(x)$ | $\mathrm{li}(x)$ |
|---|---|---|
| $10^3$ | 168 | 177 |
| $10^4$ | 1,229 | 1,245 |
| $10^5$ | 9,592 | 9,629 |
| $10^6$ | 78,498 | 78,627 |
| $10^7$ | 664,579 | 664,917 |
| $10^8$ | 5,761,455 | 5,762,208 |
| $10^9$ | 50,847534 | 50,849,234 |
| $10^{10}$ | 455,052,511 | 455,055,614 |
| $10^{11}$ | 4,118,054,813 | 4,118,066,400 |
| $10^{12}$ | 37,607,912,018 | 37,607,950,280 |
| $10^{13}$ | 346,065,536,839 | 346,065,645,809 |
| $10^{14}$ | 3,204,941,750,802 | 3,204,942,065,691 |

**Not bad!**

# The story of the prime number theorem



Around 1850, Chebyshev showed that for all large $x$, one has

$$0.921 \cdot \mathrm{li}(x) < \pi(x) < 1.106 \cdot \mathrm{li}(x).$$

The constants were improved by later authors (e.g., J.J. Sylvester), but it does not seem possible by this method to push the constants $0.921$ and $1.106$ arbitrarily close to $1$.

The real breakthrough came in 1859, with Riemann's memoir. Riemann studied the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

as a function of a **complex variable** $s$.

# The story of the prime number theorem



Riemann showed that $\zeta(s)$ could be continued analytically to the entire complex plane, apart from a simple pole at $s = 1$, and showed that understanding $\pi(x)$ was in some sense equivalent to understanding the distribution of zeros of $\zeta(s)$.

Riemann's plan was brought to fruition by Hadamard and de la Vallée–Poussin at the end of the $19$th century.

**Theorem (Prime number theorem)**

*As* $x \to \infty$,

$$\pi(x) \sim \mathrm{li}(x).$$

Here $\sim$ means that the ratio of the left and right-hand sides tends to $1$; i.e., the relative error goes to $0$.

# Unfinished business



Unfortunately, not all of Riemann's claims could be substantiated. The most famous of these, still unresolved, is the **Riemann Hypothesis**:

**Conjecture (Riemann Hypothesis)**

*If* $\zeta(s) = 0$, *and* $s = \sigma + it$ *with* $\sigma > 0$, *then* $\sigma = \frac{1}{2}$.

**Conjecture (Riemann Hypothesis, von Koch's form)**

*Let* $\epsilon > 0$. *For all* $x \geq 2$ *and a certain constant* $C$,

$$|\pi(x) - \mathrm{li}(x)| < Cx^{\frac{1}{2}} \log x.$$

# Unfinished business



Unfortunately, not all of Riemann's claims could be substantiated. The most famous of these, still unresolved, is the **Riemann Hypothesis**:

**Conjecture (Riemann Hypothesis)**

*If* $\zeta(s) = 0$, *and* $s = \sigma + it$ *with* $\sigma > 0$, *then* $\sigma = \frac{1}{2}$.

**Conjecture (Riemann Hypothesis, von Koch's form)**

*Let* $\epsilon > 0$. *For all* $x \geq 2$ *and a certain constant* $C$,

$$|\pi(x) - \mathrm{li}(x)| < Cx^{\frac{1}{2}} \log x.$$

We cannot even prove that $|\pi(x) - \mathrm{li}(x)| < x^{0.99999}$.

# The story of the prime number theorem



One often sees the prime number theorem stated in an equivalent but slightly simpler form. An integration by parts shows that

$$\mathrm{li}(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

In particular, as $x \to \infty$,

$$\mathrm{li}(x) \sim \frac{x}{\log x}.$$

Thus, the prime number theorem is equivalent to the statement that $\pi(x) \sim \frac{x}{\log x}$.

So one can approximate $\pi(x)$ with either $\mathrm{li}(x)$ or $x/\log x$, and the **relative error** goes to zero either way. But $\mathrm{li}(x)$ is superior from the standpoint of the **absolute error**.

# A polynomial prime number theorem?



We define the **polynomial prime counting function** (recall our notation $A = \mathbb{F}_q[T]$)

$$\pi(q;n) = \#\{P \in A : P \text{ monic, irreducible, deg } n\}.$$

Notice that we only count monic polynomials (in analogy with only counting positive primes), and we are segregating irreducibles by degree.

What is the asymptotic behavior of $\pi(q;n)$?

# A polynomial prime number theorem?



In Michel Waldschmidt's course, you saw an **exact formula** for $\pi(q;n)$. Recall the definition of the Möbius function:

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not squarefree,} \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes.} \end{cases}$$

**Theorem (Gauss's polynomial prime number theorem)**

*We have*

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

This formula (in the case $q = p$) appears in an unpublished section 8 of the *Disquisitiones Arithmeticae*.

# Gauss's prime number theorem, ctd.



**Theorem (Gauss's polynomial prime number theorem)**

*We have*

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

We're calling this the "polynomial prime number theorem", but is it actually analogous to what we usually think of as the prime number theorem?

If we want an asymptotic result, we can isolate the main (largest) term, corresponding to $d = n$; this is just $q^n/n$.

# Gauss's prime number theorem, ctd.



Isolating the main term suggests that

$$\pi(q;n) \approx \frac{q^n}{n}.$$

There's an error here which we'll bound later, but for now, let's assume that this approximation really is a good one.

**Rephrasing:** If we pick a monic polynomial of degree $n$ at random, the probability that it is irreducible is about $1$ in $n$.

# Gauss's prime number theorem, ctd.



Isolating the main term suggests that

$$\pi(q;n) \approx \frac{q^n}{n}.$$

There's an error here which we'll bound later, but for now, let's assume that this approximation really is a good one.

**Rephrasing:** If we pick a monic polynomial of degree $n$ at random, the probability that it is irreducible is about $1$ in $n$.

Now every polynomial of degree $n$ has norm $X := q^n$. So the number of monic irreducibles of norm $X$ is approximately $q^n/n = X/\log_q X$. This looks an awful lot like the prime number theorem, except that the log is now base $q$ instead of a natural logarithm!

# The error term



OK, we've been working so far with the approximation $\pi(q;n) \approx q^n/n$, ignoring the error.

How close is $\pi(q;n)$ to $q^n/n$? By Gauss's formula,

$$\begin{aligned}\left|\pi(q;n) - \frac{q^n}{n}\right| &= \frac{1}{n}\left|\sum_{d|n,\ d<n} q^d \mu(n/d)\right| \\ &\le \frac{1}{n}(q^{n/2} + q^{n/2-1} + q^{n/2-2} + \dots) \\ &= \frac{q^{n/2}}{n}\left(1 + \frac{1}{q} + \frac{1}{q^2} + \dots\right) < \frac{2}{n}q^{n/2}.\end{aligned}$$

If $X = q^n$, then this is a square root error term, in analogy with what von Koch says should be true for rational primes.

# Proving Gauss's prime number theorem



There are several proofs of Gauss's prime number theorem available. Perhaps the most insightful (and important for the development of the theory) is the proof via zeta functions, mimicking Riemann's approach to the classical prime number theorem.

Assume to begin with that $s > 1$. Let's define

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s}.$$

Unlike in the case of the Riemann zeta function $\zeta(s)$, it's easy to understand $\zeta_A(s)$:

$$\zeta_A(s) = \sum_{d=1}^{\infty} \frac{1}{q^{ds}} \cdot q^d = \frac{1}{1 - q^{1-s}}.$$

# Proving Gauss's prime number theorem

There is also an Euler product for $\zeta_A(s)$, namely

$$\zeta_A(s) = \prod_P \frac{1}{1 - \frac{1}{|P|^s}},$$

where $P$ runs over monic irreducibles. (Also valid for $s > 1$.)

Reorganizing the product according to the degree $d$ of the irreducibles, we get that

$$\prod_{d=1}^{\infty} (1 - q^{-ds})^{-\pi(q;d)} = \zeta_A(s) = \frac{1}{1 - q^{1-s}}.$$

In other words, letting $u = q^{-s}$,

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

# Proving Gauss's prime number theorem, ctd.



We now take the logarithmic derivative of both sides to find that

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

Now we expand both sides into power series in $u$. Clearly,

$$\frac{qu}{1-qu} = qu(1+qu+q^2u^2+\dots) = \sum_{n=1}^{\infty} q^n u^n.$$

On the other hand, the left hand side is equal to

$$\sum_{d\geq 1} d\pi(q;d)(u^d+u^{2d}+u^{3d}+\dots) = \sum_{n\geq 1}\left(\sum_{d|n} d\pi(q;d)\right)u^n.$$

# Proving Gauss's prime number theorem, ctd.



We now compare coefficients of $u$ (takes some justification). This gives that

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

By Möbius inversion,

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

Dividing by $n$ gives Gauss's result:

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

Q.E.D.

# Where do we go from here?



At this point, if we're developing the theory parallel to how it's done in $\mathbb{Z}$, the next step is to investigate how irreducibles are distributed in residue classes mod $M$, for $M \in A$.

In particular, one could hope to prove the analogue of Dirichlet's theorem that for every invertible residue class modulo $M$ contains infinitely many monic irreducibles. Following Dirichlet, this would lead one to introduce $L$-functions

$$L(s,\chi) := \sum_{\substack{f \in A \\ \text{monic}}} \frac{\chi(f)}{|f|^s},$$

corresponding to characters $\chi$ of $A/(m)$, and investigate their nonvanishing at $s = 1$.

# Primes in progressions



**Theorem (Kornblum, 1914)**

*Let $M$ be a nonzero element of $A = \mathbb{F}_q[T]$. Every invertible residue class modulo $M$ contains infinitely many monic irreducibles $P$.*

**Example**

There are infinitely many monic irreducibles of the form

$$(\text{terms of degree} \geq 100) + T + 1,$$

as we see by considering the residue class $T + 1 \bmod T^{100}$.

# Primes in progressions



**Theorem (Kornblum, 1914)**

*Let $M$ be a nonzero element of $A = \mathbb{F}_q[T]$. Every invertible residue class modulo $M$ contains infinitely many monic irreducibles $P$.*

**Example**

There are infinitely many monic irreducibles of the form

$$(\text{terms of degree} \geq 100) + T + 1,$$

as we see by considering the residue class $T + 1 \bmod T^{100}$.

**Theorem (Artin, 1923)**

*As $n \to \infty$, the number of monic irreducibles of degree $n$ in a fixed invertible residue class mod $M$ is asymptotically $\frac{1}{\phi(M)} \frac{q^n}{n}$.*

# A bit of mathematical philosophy



**Metatheorem**

*Anything fact that can be proved about primes in $\mathbb{Z}$ has a proof of equal or lesser difficulty in $\mathbb{F}_q[T]$.*

In fact, the proofs can be considerably easier in the polynomial setting. The distribution of **self-reciprocal irreducible polynomials** provides a good example.

**Definition**

If $f$ is a monic polynomial in $A$ of degree $n$, the **reciprocal polynomial** of $f$ is the polynomial $f^*(t) := t^n f(1/t)$. We say $f$ is **self-reciprocal** if $f = f^*$.

# I LOVE ME, VOL. I



Notice that

$$(t^n + a_{n-1}t^{n-1} + \cdots + a_0)^* = a_0t^n + a_1t^{n-1} + \cdots + 1.$$

Thus, $f$ is self-reciprocal precisely when its list of coefficients leads the same forwards and backwards.

# I LOVE ME, VOL. I



Notice that

$$(t^n + a_{n-1}t^{n-1} + \cdots + a_0)^* = a_0t^n + a_1t^{n-1} + \cdots + 1.$$

Thus, $f$ is self-reciprocal precisely when its list of coefficients leads the same forwards and backwards.

**Question**

*Can we understand the distribution of monic, irreducible self-reciprocal polynomials?*

# I LOVE ME, VOL. I



Notice that

$$(t^n + a_{n-1}t^{n-1} + \cdots + a_0)^* = a_0t^n + a_1t^{n-1} + \cdots + 1.$$

Thus, $f$ is self-reciprocal precisely when its list of coefficients leads the same forwards and backwards.

**Question**

*Can we understand the distribution of monic, irreducible self-reciprocal polynomials?*

This question has an obvious integer analogue:

**Question**

*Say the prime $p$ is* **palindromic** *if the sequence of its decimal digits reads the same forwards and backwards. Can we understand the distribution of palindromic primes?*

# Two theorems of S. Col (2009)



**Theorem**

*The proportion of palindromes in $[1, x]$ that are prime is $\ll \frac{1}{\log x}$ for large $x$.*

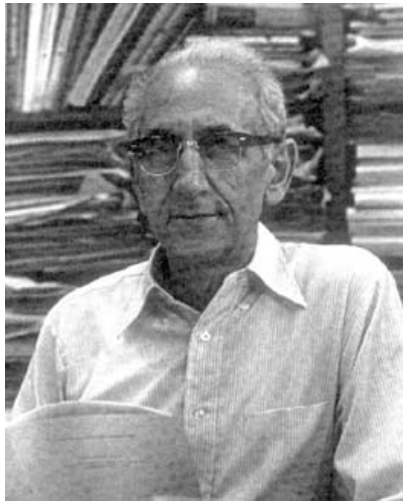
**Theorem**

*Infinitely many palindromes have at most $372$ prime factors.*

We do not know if there are infinitely many palindromic primes.

As we shall soon see, the situation is much better for self-reciprocal irreducible polynomials!

# Counting self-reciprocal irreducibles, d'après Carlitz



We assume throughout that $q$ is odd.

**Goal:** Count the number of self-reciprocal irreducibles of degree $n$ in $A = \mathbb{F}_q[t]$.

We assume $n > 1$.

If $f$ is self-reciprocal of odd degree $n$, then $f(-1) = f^*(-1) = (-1)^n f(-1) = -f(-1)$, so $f(-1) = 0$. So $f$ is divisible by $t+1$ and so is not irreducible.

**Observation**

*It suffices to study the case* $\deg f = 2n$, *where* $n > 1$.

# Calibrating our expectations



What might we expect? There are $q^n$ monic self-reciprocal polynomials of degree $2n$ (since the coefficients of $t$, $t^2$, ..., $t^n$ can be arbitrarily prescribed, and then the rest are determined).

Since a random degree $2n$ polynomial is prime with probability about $\frac{1}{2n}$, maybe we should expect $\approx \frac{q^n}{2n}$ monic self-reciprocal irreducibles of degree $2n$.

This is what Carlitz proves. In fact, Carlitz gets an exact formula for the number of such polynomials, with main term $\frac{q^n}{2n}$.

# A proof of Meyn and Götz



An elegant derivation of Carlitz's formula was given by Meyn and Götz in 1989.

To motivate it, we recall the proof of Gauss's formula for $\pi(q;n)$ seen in Professor Waldschmidt's lectures.

**Proposition**

*The polynomial $t^{q^n} - t$ factors in $\mathbb{F}_q[t]$ as folows:*

$$t^{q^n} - t = \prod_{d|n} \prod_{P \in E_q(d)} P,$$

*where $E_q(d)$ is the set of monic irred. of degree $d$ over $\mathbb{F}_q$.*

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

# A proof of Meyn and Götz, ctd.



## Proposition

*Let $H_{q,n}(t) := t^{q^n+1} - 1 \in A$. Then:*

1. *$H_{q,n}(t)$ has no repeated irreducible factors.*
2. *The only monic linear factors of $H_{q,n}(t)$ are $t \pm 1$.*
3. *If $P$ is a self-reciprocal irreducible of degree $2d$, where $d \mid n$ and $n/d$ is odd, then $P \mid H_{q,n}$.*
4. *Each irreducible factor of degree at least 2 of $H_{q,n}$ is a self-reciprocal irreducible polynomial of degree $2d$, where $d$ divides $n$ and $n/d$ is odd.*

## Corollary

*$H_{q,n}$ factors as $(t-1)(t+1)$ times the product of the distinct self-reciprocal irreducibles of degree $2d$, where $n/d$ is odd.*

# A small example



Over $\mathbb{F}_3$,

$$t^{3^3+1} - 1 = (t+1)(t-1)(t^2+1)(t^6+t^5+t^3+t+1)\cdot$$
$$(t^6+t^5+t^4+t^3+t^2+t+1)(t^6-t^5-t^3-t+1)(t^6-t^5+t^4-t^3+t^2-t+1)$$

This is the product of $(t+1)(t-1)$ with all the self-reciprocal irreducibles of degree $2$ and $6$.

Here $2$ and $6$ are the numbers of the form $2d$, where $d \mid 3$ and $3/d$ is odd.

# Proofs

(1) $H_{q,n}(t)$ has no repeated irreducible factors.

**Proof.**

$H'_{q,n} = (q^n+1)t^{q^n} = t^{q^n}$ has no common roots with $H_{q,n} = t^{q^n+1} - 1$.

(2) The only monic linear factors of $H_{q,n}(t)$ are $t \pm 1$.

**Proof.**

If $t-a$ is a linear factor, where $a \in \mathbb{F}_q$, then
$0 = H_{q,n}(a) = a^{q^n+1} - 1 = a^{q^n} \cdot a - 1 = a^2 - 1 = (a-1)(a+1)$.

# Proofs



(3) If $P$ is a self-reciprocal irreducible of degree $2d$, where $d \mid n$ and $n/d$ is odd, then $P \mid H_{q,n}$.

**Proof.**

Since $d \mid n$ and $n/d$ is odd, it follows that

$$q^d + 1 \mid q^n + 1; \quad \text{thus} \quad H_{q,d} = t^{q^d+1} - 1 \mid t^{q^n+1} - 1 = H_{q,n}.$$

So it's enough to prove that $P$ divides $H_{q,d}$.
Let $\alpha$ be a root of $P$ in an algebraic closure of $\mathbb{F}_q$. Then all of the roots of $P$ are $\alpha, \alpha^q, \ldots, \alpha^{q^{2d-1}}$. Since $P$ is self-reciprocal, $\alpha^{-1}$ is a root of $P$, and so $\alpha^{q^j} = \alpha^{-1}$ for some $0 \le j \le 2d-1$.
In other words, $H_{q,j}(\alpha) = \alpha^{q^j+1} - 1 = 0$.

## Proof, ctd.

In other words, $H_{q,j}(\alpha) = \alpha^{q^j+1} - 1 = 0$. Thus, $P \mid H_{q,j}$.
On the other hand,

$$H_{q,j} = t^{q^j+1} - 1 \mid t^{q^{2j}-1} - 1 \mid t^{q^{2j}} - t.$$

So $P \mid t^{q^{2j}} - t$. This implies that the degree of $P$ is a divisor of $2j$.

But the degree of $P$ is $2d$. Since $2d \mid 2j$, we get $d \mid j$.
On the other hand, $0 \leq j < 2d$, so $d = j$.

Thus, $P$ divides $H_{q,d}$, as desired!

# Proofs



(4) Each irreducible factor of degree at least 2 of $H_{q,n}$ is a self-reciprocal irreducible polynomial of degree $2d$, where $d$ divides $n$ and $n/d$ is odd.

**Proof:** Suppose $P \mid H_{q,n}$, and let $\alpha$ be a root of $P$. Then $\alpha^{q^n} = \alpha^{-1}$, which implies that $\alpha^{-1}$ is also a root of $P$. Thus, the roots of $P$ come in pairs. Hence $\deg P = 2d$ for some $d$ and the constant term of $P$ is 1. Since $P^*(t) = t^{2d}P(1/t)$ and $P(t)$ have the same roots, the same degree, and the same leading oefficient, we must have $P^* = P$. That is, $P$ is self-reciprocal.

Since

$$P \mid t^{q^n+1} - 1 \mid t^{q^{2n}-1} - 1 \mid t^{q^{2n}} - t,$$

we see $2d \mid 2n$, so $d \mid n$.

# Proofs



It remains to show that $n/d$ is odd.

Since $P$ is irreducible and self-reciprocal of degree $2d$, our work in (3) shows that $P \mid H_{q,d}$. Since $P \mid H_{q,n}$, we see that

$$\begin{aligned} P \mid \gcd(H_{q,d}, H_{q,n}) &= \gcd(t^{q^d+1} - 1, t^{q^n+1} - 1) \\ &= t^{\gcd(q^d+1, q^n+1)} - 1. \end{aligned}$$

Suppose for a contradiction that $n/d$ is even. Let $\ell = \gcd(q^d + 1, q^n + 1)$. Then $q^d \equiv -1 \pmod{l}$ and $q^n \equiv -1 \pmod{\ell}$. Now

$$-1 \equiv q^n = (q^d)^{n/d} \equiv (-1)^{n/d} \equiv 1 \pmod{\ell},$$

and so $\ell \mid 2$. Thus, $\ell = 2$ and $P \mid t^2 - 1$, which is impossible.

# Carlitz's formula



## Corollary

*$H_{q,n}$ factors as $(t-1)(t+1)$ times the product of the distinct self-reciprocal irreducibles of degree $2d$, where $n/d$ is odd.*

In particular, if $\pi'(q;d)$ is the number of self-reciprocal irreducible polynomials of degree $d$, then comparing the degree of $H_{q,n}$ with the sum of the degrees of its irreducible factors, we get

$$q^n + 1 = 2 + \sum_{\substack{d|n \\ n/d \text{ odd}}} 2d \cdot \pi'(q;d).$$

Thus,

$$\frac{q^n - 1}{2} = \sum_{\substack{d|n \\ n/d \text{ odd}}} d\pi'(q;d).$$

# Carlitz's formula



Inverting the formula

$$\frac{q^n - 1}{2} = \sum_{\substack{d|n \\ n/d \text{ odd}}} d\pi(q; d),$$

we find that the number of self-reciprocal irreducibles of degree $2n$ is given by

$$\begin{cases} \frac{1}{2n}(q^n - 1) & \text{if } n = 2^s, \\ \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d} & \text{otherwise.} \end{cases}$$

Hence, the count is always $\frac{q^n}{2n}$ up to a small (square-root) error.

# Twins

## Definition

If $p$ and $p+2$ are rational primes that differ by $2$, then we call $\{p, p+2\}$ a **twin prime pair** in $\mathbb{Z}$.

For example, $11$ and $13$ are a twin prime pair.

## Conjecture (Twin prime conjecture)

*There are infinitely many twin prime pairs.*

## Theorem (Chen, 1973)

*There are infinitely many pairs $p$, $p+2$ where $p$ is prime and $p+2$ is prime or the product of two distinct primes.*

# More on twins

Building on (already revolutionary) work of Goldston, Pintz, and Yildirim, Yitang Zhang recently proved the following spectacular theorem:

**Theorem (Zhang, 2013)**

$\liminf p_{n+1} - p_n < \infty$.

In fact, the $\liminf$ is smaller than $12500$.

What could we mean by a pair of **twin prime polynomials**?

**Definition**

If $P, P+1 \in A$ are both monic and irreducible, we say that $P, P+1$ form a **twin prime pair** in $A$.

# Twin prime polynomials



In $\mathbb{F}_2$, it is easy to see $T, T+1$ are the only twin prime pair.

When $q > 2$, there seem to be lots of twin prime pairs!

In fact, for fixed $q$, the number of twin prime pairs of degree $n$ appears to grow like a constant multiple of $q^n/n^2$, as $n$ gets large. Some data on related questions was collected by Effinger, Hicks, and Mullen (2002).

For now, we will take a more qualitative (instead of quantitative) perspective.

**Theorem (Cherly, 1978)**

*Let $q > 2$. There are infinitely many monic $f \in A$ for which $f, f+1$ have at most $4$ prime factors.*

# A pleasant surprise

**Theorem (Hall, 2002)**

*Let $q > 3$. Then there are infinitely many twin prime pairs.*

As we will see a bit later, one can even prove this when $q = 3$ (P. and Effinger, independently).

Remarkably, the proofs are completely elementary.

The main idea is to exploit a **non**-analogy between integers and polynomials. This is orthogonal to all earlier approaches.

# You win some, you lose some

In the 17th century, Fermat made the following ill-fated conjecture.

**Conjecture (Fermat)**

*Every one of the numbers*

$$F_n := 2^{2^n} + 1$$

*is prime, for* $n = 0, 1, 2, \ldots$.

As Fermat knew, the numbers $F_n$ **are** prime for $n = 0, 1, 2, 3, 4$.

**Observation (Euler)**

$F_5 = 641 \cdot 6700417$. *So* $F_5$ *is not prime.*

Today, we know that $F_n$ is composite for $5 \leq n \leq 32$.

# There's being wrong, and there's being **wrong**



**Conjecture (Folklore)**

*There are no prime Fermat numbers with $n \geq 5$. In other words, Fermat was as wrong as he possibly could have been, given what he knew!*

There are probabilistic reasons for believing this. Indeed, a "random number" in the neighborhood of $2^{2^n}$ is prime with probability $\approx \frac{1}{\log(2^{2^n})} \asymp \frac{1}{2^n}$, and

$$\sum \frac{1}{2^n} < \infty.$$

So we expect to see only finitely many Fermat primes (in analogy with the Borel-Cantelli lemma). Moreover, the number we expect to see past $n = 32$ is pretty small.

# The polynomial non-analogy and the vindication of Fermat



Let's temporarily fix $q = 7$, so that $A = \mathbb{F}_7[t]$. The following conjecture is analogous to Fermat's ill-fated guess.

## Conjecture

*For every nonnegative integer $n$,*

$$H_n := t^{3^n} - 2$$

*is irreducible in $A$.*

Again, probabilistic reasoning suggests this is surely false. A degree $3^n$ polynomial is irreducible with probability $\approx 3^{-n}$, and $\sum 3^{-n} < \infty$.

**But in fact, the conjecture is true!**

# Classification of irreducible binomials



**Theorem (Capelli)**

*Let $F$ be any field. Then $t^m - a$, with $a \in F$, is irreducible unless one of the following holds:*

1. *there is a prime $\ell \mid m$ for which $a$ is an $\ell$th power in $F$,*
2. *$4$ divides $m$ and $a = -4b^4$ for some $b$ in $F$.*

This is an if and only if statement. To see the relevance of condition (2), notice that $X^4 + 4Y^4 = (X^2 + 2Y^2)^2 - (2XY)^2$.

By definition, $H_n = t^{3^n} - 2 \in \mathbb{F}_7[t]$. Clearly $4 \nmid 3^n$, so (2) is irrelevant. For (1) to hold, one would need $2$ to be a cube in $\mathbb{F}_7$. But the cubes in $\mathbb{F}_7$ are $0, \pm 1$.

Thus, every $H_n$ is irreducible.

# Back to twin prime polynomials



We have just seen that for every $n$, the polynomial

$$t^{3^n} - 2 \in \mathbb{F}_7[t]$$

is irreducible; all that turned out to be important was that $2$ was not a cube. In $\mathbb{F}_7$, the element $3$ is also not a cube. Hence,

$$t^{3^n} - 3 \in \mathbb{F}_7[t]$$

is also always irreducible.

Hence,

$$t^{3^n} - 2, \quad t^{3^n} - 3$$

is a twin prime pair for every $n$.

This proves Hall's result in the case when $q = 7$.

# What should we do if $q \neq 7$?



Let $q > 3$ be a prime power. Let's suppose $q - 1$ is not a power of 2. Thus, there is an odd prime $\ell \mid q - 1$.

Suppose we can find two neighboring elements of $\mathbb{F}_q$, say $\alpha$ and $\alpha + 1$, neither of which is an $\ell$th power in $\mathbb{F}_q$. Then for every $n$,

$$t^{\ell^n} - \alpha, \quad t^{\ell^n} - (\alpha + 1)$$

is a twin prime pair, by Capelli's theorem.

# What should we do if $q \neq 7$?



Let $q > 3$ be a prime power. Let's suppose $q - 1$ is not a power of 2. Thus, there is an odd prime $\ell \mid q - 1$.

Suppose we can find two neighboring elements of $\mathbb{F}_q$, say $\alpha$ and $\alpha + 1$, neither of which is an $\ell$th power in $\mathbb{F}_q$. Then for every $n$,

$$t^{\ell^n} - \alpha, \quad t^{\ell^n} - (\alpha + 1)$$

is a twin prime pair, by Capelli's theorem.

Suppose we **can't** find such an $\alpha$. Then every element of $\mathbb{F}_q$ is either a $q$th power of next to a $q$th power, and so

$$\mathbb{F}_q \subset \mathbb{F}_q^\ell \cup (\mathbb{F}_q^\ell + 1).$$

Comparing cardinalities, $q \leq 2 \cdot \#\mathbb{F}_q^\ell$, so $\#\mathbb{F}_q^\ell \geq \frac{q}{2}$.

# What should we do if $q \neq 7$, ctd.



We just saw that $\#\mathbb{F}_q^\ell \geq \frac{q}{2}$. But since the multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$, and $\ell \mid q-1$, we in fact have that

$$\mathbb{F}_q^\ell = \frac{q-1}{\ell} + 1 \leq \frac{q+2}{3}.$$

This contradicts the lower bound $\#\mathbb{F}_q^\ell \geq \frac{q}{2}$ unless $q = 4$ and $\ell = 3$. But when $q = 4$ and $\ell = 3$, we can find two neighboring noncubes "by hand". (Exercise!)

# What should we do if $q \neq 7$, ctd.



We just saw that $\#\mathbb{F}_q^\ell \geq \frac{q}{2}$. But since the multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$, and $\ell \mid q-1$, we in fact have that

$$\mathbb{F}_q^\ell = \frac{q-1}{\ell} + 1 \leq \frac{q+2}{3}.$$

This contradicts the lower bound $\#\mathbb{F}_q^\ell \geq \frac{q}{2}$ unless $q = 4$ and $\ell = 3$. But when $q = 4$ and $\ell = 3$, we can find two neighboring noncubes "by hand". (Exercise!)

So the only remaining cases with $q > 3$ are those $q$ where $q - 1$ is a power of $2$.

Note in that in these cases, $4 \mid q - 1$.

# What should we do if $q \neq 7$, ctd.



So the only remaining cases with $q > 3$ are those $q$ where $q - 1$ is a power of 2. Note that in these cases, $4 \mid q - 1$.

In this case, we look for twin prime pairs of the form

$$t^{2^n} - \alpha, \quad t^{2^n} - (\alpha + 1).$$

By Capelli again, it is enough to find $\alpha \in \mathbb{F}_q$ so that $\alpha, \alpha + 1$ are both nonsquares in $\mathbb{F}_q$.

Here, rather than using a counting argument, we work explicitly. If $q = 9$, we can find $\alpha$ by hand. (Again, exercise!)

If $q > 9$, then $q$ has to be prime. Otherwise, $q - 1$ (a power of 2) and $q$ are consecutive powers. But 9 is the only proper prime power of the form $2^j + 1$.

# What should we do if $q \neq 7$, ctd.



The only remaining case is that $q > 3$ is prime and $q - 1$ is a power of $2$. In this case, an elementary argument shows that

$$q = 2^{2^m} + 1 \quad \text{for some } m > 0.$$

(Fermat again!)

One can use this to show that

$$q \equiv 1 \pmod 8,\ q \equiv 2 \pmod 5,\ q \equiv 2 \pmod 3,$$

and now Gauss's law of quadratic reciprocity implies that $5$ and $6$ are a pair of consecutive nonsquares modulo $q$.

Phew!

# Dealing with $q = 3$



There's no way to choose $\ell$ and $\alpha$ which will make $t^{\ell^n} - \alpha$ and $t^{\ell^n} - (\alpha + 1)$ form a twin prime pair for every $n$.

But all is not lost!

Instead of applying Capelli's theorem directly, we use the following consequence.

**Theorem**

*Let $F$ be an arbitrary field field. Suppose $f(t) \in F[t]$ is irreducible over $F$, and let $\xi$ be a root of $f$ in a splitting field. With $\ell$ an odd prime, suppose that $\xi$ is not an $\ell$th power in $F(\xi)$. Then $f(t^{\ell^n})$ is irreducible over $F$ for every nonnegative integer $n$.*

# Another prime-producing theorem



**Theorem**

*Let $F$ be an arbitrary field field. Suppose $f(t) \in F[t]$ is irreducible over $F$, and let $\xi$ be a root of $f$ in an appropriate splitting field.*
*With $\ell$ an odd prime, suppose that $\xi$ is not an $\ell$th power in $F(\xi)$. Then $f(t^{\ell^n})$ is irreducible over $F$ for every nonnegative integer $n$.*

Proof: Say $f$ has degree $d$.

It suffices to show that if $\rho$ is a root of $f(t^{\ell^n})$, then $[F(\rho) : F] = d\ell^n$. Now $F(\rho)$ contains $\rho^{\ell^n}$, which is a root of $f$. Say $\xi = \rho^{\ell^n}$. Then

$$[F(\rho) : F] = [F(\rho) : F(\xi)][F(\xi) : F] = [F(\rho) : F(\xi)] \cdot d.$$

# Another prime-producing theorem, ctd.

It suffices to show that if $\rho$ is a root of $f(t^{\ell^n})$, then $[F(\rho) : F] = d\ell^n$. Now $F(\rho)$ contains $\rho^{\ell^n}$, which is a root of $f$. Say $\xi = \rho^{\ell^n}$. Then

$$[F(\rho) : F] = [F(\rho) : F(\xi)][F(\xi) : F] = [F(\rho) : F(\xi)] \cdot d.$$

So we want to show $[F(\rho) : F(\xi)] = \ell^n$.

Equivalently, we have to show that $\rho$ is algebraic over $F(\xi)$ of degree $\ell^n$. But by definition, $\rho$ is a root of

$$t^{\ell^n} - \xi,$$

which is a polynomial over $F(\xi)$. We are assuming $\xi$ is not an $\ell$th power in $F(\xi)$, and so this polynomial is irreducible. QED.

# Back to $q = 3$

**Proof that there are infinitely many twin prime polynomials over $\mathbb{F}_3$** (Effinger/P.):

We search for a twin prime pair over $\mathbb{F}_3$ by hand and find

$$t^3 - t + 1, \quad t^3 - t + 2.$$

The roots of these polynomials live in $\mathbb{F}_{27}$.

Neither polynomial has roots which are $13$th powers in $\mathbb{F}_{27}$. (Note that $0, \pm 1$ are the only $13$th powers!)

So by the theorem we just proved,

$$t^{3 \cdot 13^n} - t^{13^n} + 1, \quad t^{3 \cdot 13^n} - t^{13^n} + 2$$

form a twin prime pair for every nonnegative integer $n$.

# We've proved the twin prime conjecture. Why aren't we happy?



1. We solved one problem. Is there an actual **method** here that can be used to solve others?

# We've proved the twin prime conjecture. Why aren't we happy?



1. We solved one problem. Is there an actual **method** here that can be used to solve others?
2. One might argue this is the wrong proof, or that we have been asking the wrong question. Sure, we get infinitely many "twin primes", but the proof gives terribly weak quantitative lower bounds.

# We've proved the twin prime conjecture. Why aren't we happy?



1. We solved one problem. Is there an actual **method** here that can be used to solve others?
2. One might argue this is the wrong proof, or that we have been asking the wrong question. Sure, we get infinitely many "twin primes", but the proof gives terribly weak quantitative lower bounds.
3. We didn't prove **any** theorem for $q = 2$, and our method seems incapable of doing so. Here a natural version of the twin prime conjecture is the infinitude of twin prime pairs $P, P + (t^2 + t)$ in $\mathbb{F}_2[t]$.

# An observation of Effinger



We cannot resist mentioning a beautiful observation of Effinger.

**Theorem**

*If $P_k(t) = t^k + t^3 + t^2 + t + 1$ is irreducible over $\mathbb{F}_2$, then so is $P_k(t) + (t^2 + t) = t^k + t^3 + 1$.*

Effinger also shows that the converse holds when $k$ is odd.

To prove the theorem, one shows that if $\alpha$ is a root of $t^k + t^3 + 1$, then $\alpha^3$ is a root of $P_k(t)$. This follows from

$$P_k(t^3) = (t^k + t^3 + 1)(t^{2k} + t^{k+3} + t^k + t^6 + 1).$$

Unfortunately, it is far from clear how to show that $P_k(t)$ is irreducible infinitely often.

# Generalizations



To generalize our argument, we combine our previous ideas with some estimates for character sums that are consequences of Weil's Riemann Hypothesis.

By a multiplicative character $\chi$ of $\mathbb{F}_q$, we mean a homomorphism from $\mathbb{F}_q^\times$ to the complex unit circle $\{z : |z| = 1\} \subset \mathbb{C}^\times$. We extend $\chi$ to all of $\mathbb{F}_q$ by setting $\chi(0) = 0$.

The multiplicative characters of $\mathbb{F}_q$ form a group under pointwise multiplication, with the identity corresponding to the trivial homomorphism.

In fact, this group is isomorphic to $\mathbb{F}_q^\times$, so cyclic of order $q - 1$.

# What does RH have to do with this?



The image of $\chi$, after zero is excluded, is a finite subgroup of $\{z : |z| = 1\}$, and so is the $d$th roots of unity for some $d$.

**Exercise**

*Show that if the order of $\chi$ in the character group is $d$, then the image of $\chi$ consists precisely of the $d$th roots of unity.*

Let $q$ be odd. Since the group of characters of $\mathbb{F}_q$ is cyclic of order $q-1$, there is a character $\epsilon$ of order 2 on $\mathbb{F}_q$. Since the image of $\epsilon$ is $\{\pm 1\}$, the kernel of $\chi$ is the subgroup of nonzero squares in $\mathbb{F}_q$. Thus,

$$\epsilon(a) = \begin{cases} 0 & \text{if a=0,} \\ 1 & \text{if } a \text{ is a nonzero square,} \\ -1 & \text{if } a \text{ is not a square.} \end{cases}$$

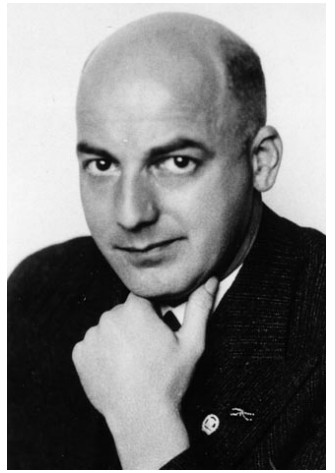
# What does RH have to do with this?

Suppose $q$ is odd, and let $f(t) = t^3 + at + b \in \mathbb{F}_q[t]$ have distinct roots. We saw in Professor Schoof's lectures that

$$|\sum_{x \in \mathbb{F}_q} \epsilon(f(x))| \leq 2\sqrt{q}.$$

In fact, the sum here measures the deviation from $q+1$ of the number of $\mathbb{F}_q$-points on the elliptic curve $y^2 = x^3 + ax + b$.

So RH for curves $\Rightarrow$ estimates for character sums with polynomial arguments.
This phenomenon (noted by Davenport and Hasse) is very useful in analytic number theory.



# A general character sum estimate



Using RH for curves, one can prove the following generalization of the inequality we saw on the previous slide.

## Theorem

*Let $f_1(t), \dots, f_n(t)$ be $n$ monic pairwise relatively prime polynomials in $\mathbb{F}_q[t]$ whose largest squarefree divisors have degrees $d_1, \dots, d_n$. Let $\chi_1, \dots, \chi_n$ be nontrivial multiplicative characters of $\mathbb{F}_q$. Assume that for some $1 \le i \le n$, the polynomial $f_i(t)$ is not of the form $g(t)^{\mathrm{ord}(\chi_i)}$ in $\mathbb{F}_q[t]$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi_1(f_1(x)) \cdots \chi_n(f_n(x)) \right| \le (\sum_{i=1}^{n} d_i - 1)\sqrt{q}.$$

# Generalizing our twin prime proof



Euler and Goldbach were interested in the question of whether there are infinitely many primes of the form $n^2+1$, such as $2006^2+1 = 4024037$.

This question is still open.

**Conjecture (Bunyakovsky)**

*Let $f$ be a polynomial with integer coefficients and positive leading coefficient. Suppose $f$ is irreducible over $\mathbb{Z}$ and that there is no prime $p$ dividing all the values of $f(n)$. Then $f(n)$ is prime infinitely often.*

The local condition rules out polynomials like $f(t) = t^2+t+2$, which assumes only even values.

# Generalizations



OK, what about in $A$? Again, let's ask about irreducibles of the form $f^2+1$. If $-1=i^2$ with $i \in \mathbb{F}_q$, then $f^2+1=(f-i)(f+i)$ is not irreducible. To avoid this, let's assume that $q \equiv 3 \pmod 4$.

**Theorem (P.)**

*Assume that $q \equiv 3 \pmod 4$. There are infinitely many monic $f \in A$ for which $f^2+1$ is irreducible over $\mathbb{F}_q$.*

We use the lemma:

**Lemma**

*Let $G(t) \in F[t]$ be irreducible over $F$, and let $\xi$ be a root of $G$ in a splitting field. With $\ell$ an odd prime, suppose $\xi$ is not an $\ell$th power in $F(\xi)$. Then $G(t^{\ell^n})$ is irred. over $F$ for every $n \geq 0$.*

# Irreducibles of the form $f^2 + 1$



**Lemma**

*Let $G(t) \in F[t]$ be irreducible over $F$, and let $\xi$ be a root of $G$ in a splitting field. With $\ell$ an odd prime, suppose $\xi$ is not an $\ell$th power in $F(\xi)$. Then $G(t^{\ell^n})$ is irred. over $F$ for every $n \geq 0$.*

We attempt to apply the lemma with $G(t) = (t - \beta)^2 + 1$, where both $\beta \in \mathbb{F}_q$ and the odd prime $\ell$ are to be chosen suitably.

If the lemma applies, then every $f_n(t) = t^{\ell^n} - \beta$ has $f_n^2 + 1$ irreducible, so we're done!

One root of $g$ is $\beta + i$, which lives in $\mathbb{F}_q(i) = \mathbb{F}_{q^2}$. So we need to choose $\beta \in \mathbb{F}_q$ and an odd prime $\ell$ so that $\beta + i$ is **not** an $\ell$th power in $\mathbb{F}_{q^2}$.

# Irreducibles of the form $f^2 + 1$



OK, so we need an odd prime $\ell$ and a $\beta \in \mathbb{F}_q$ so that $\beta + i$ is not an $\ell$th power in $\mathbb{F}_q(i) = \mathbb{F}_{q^2}$.

Let's choose any odd prime $\ell \mid q - 1$. Since $q \equiv -1 \pmod 4$, we have $\frac{q-1}{2}$ odd. So we take for $\ell$ an odd prime factor of $\frac{q-1}{2}$. If $q = 3$, we can't do this, so we come back to this later.

# Irreducibles of the form $f^2 + 1$



OK, so we need an odd prime $\ell$ and a $\beta \in \mathbb{F}_q$ so that $\beta + i$ is not an $\ell$th power in $\mathbb{F}_q(i) = \mathbb{F}_{q^2}$.

Let's choose any odd prime $\ell \mid q-1$. Since $q \equiv -1 \pmod 4$, we have $\frac{q-1}{2}$ odd. So we take for $\ell$ an odd prime factor of $\frac{q-1}{2}$. If $q = 3$, we can't do this, so we come back to this later.

We have our $\ell$, now we need our $\beta$. Let $\chi$ be an order $\ell$ character of $\mathbb{F}_{q^2}^\times$. (This exists since $\ell \mid q-1 \mid q^2-1$.) Since $\chi$ has order $\ell$, the kernel of $\chi$ has index $\ell$ and so consists of the nonzero $\ell$th powers in $\mathbb{F}_{q^2}$.

Thus, it is enough to show that

$$\Big|\sum_{\beta \in \mathbb{F}_q} \chi(\beta + i)\Big| < q.$$

# An estimate for incomplete character sums



The following character sum estimate was shown by Lenstra to be a consequence of Weil's RH:

**Lemma (Lenstra)**

*Let $\chi$ be a nontrivial character of the multiplicative group of $\mathbb{F}_{q^n}$ (extended to vanish $0$). Suppose $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$, where $\gamma \in \mathbb{F}_{q^n}$. Then*

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

This lemma applies immediately in our case ($n = 2$, $\gamma = i$). We get a bound of $\sqrt{q}$ on the character sum that we needed to be bounded by $q$.

# An estimate for incomplete character sums



The following character sum estimate was shown by Lenstra to be a consequence of Weil's RH:

**Lemma (Lenstra)**

*Let $\chi$ be a nontrivial character of the multiplicative group of $\mathbb{F}_{q^n}$ (extended to vanish $0$). Suppose $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$, where $\gamma \in \mathbb{F}_{q^n}$. Then*

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

This lemma applies immediately in our case ($n = 2$, $\gamma = i$). We get a bound of $\sqrt{q}$ on the character sum that we needed to be bounded by $q$.

We win! If $q = 3$, take $\ell = 2$.

# A more general character sum estimate



In fact, Lenstra's method proves the following:

**Lemma**

*Let $f_1(t), \dots, f_s(t)$ be nonassociate irreducible polynomials over $\mathbb{F}_q$. Fix roots $\alpha_1, \dots \alpha_s$ of $f_1, \dots, f_s$, respectively, lying in an algebraic closure of $\mathbb{F}_q$. Suppose that for every $1 \le i \le s$ we are given a multiplicative character $\chi_i$ of $\mathbb{F}_q(\alpha_i)$ and that at least one of these $\chi_i$ is nontrivial. Then*

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

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

# Does the prime number theorem have a twin?



Let

$$\pi_2(x) = \#\{p \le x : p, p+2 \text{ both prime}\}.$$

We cannot even prove that $\pi_2(x) \to \infty$. Nevertheless, we believe that it does, and we can make a very precise conjecture concerning how quickly it does so!

If we pick two random numbers both of size $\approx x$, independently, the prime number theorem leads us to expect that both are prime with probability about $1/(\log x)^2$. So our first guess might be that

$$\pi_2(x) \sim \frac{x}{(\log x)^2} \quad \text{or perhaps} \quad \int_2^x \frac{\mathrm{d}t}{(\log t)^2}.$$

# Does the prime number theorem have a twin?



This guess doesn't look so good; we seem to be off by a constant. In other words, it appears that

$$\pi_2(x) \sim C \frac{x}{(\log x)^2}$$

for some positive constant $C \neq 1$. Where does this constant come from?

# Does the prime number theorem have a twin?



This guess doesn't look so good; we seem to be off by a constant. In other words, it appears that

$$\pi_2(x) \sim C \frac{x}{(\log x)^2}$$

for some positive constant $C \neq 1$. Where does this constant come from?

**Our heuristic is flawed:**
If we pick a random prime $p$ near $x$, it is not the case that $p+2$ behaves like a random integer near $x$. For example, $p+2$ is automatically odd, whereas a random integer of size near $x$ is odd with probability $1/2$. So starting with a prime $p$ gives $p+2$ an **advantage** in being prime, by a factor of

$$\frac{1}{1/2} = 2.$$

# Does the prime number theorem have a twin, ctd.



Let's look at $3$. A prime $p > 3$ is either $1$ or $2$ mod $3$, and both cases occur with probability $\frac{1}{2}$. So $p+2$ is nondivisible by $3$ with probability $1/2$, whereas a typical integer is nondivisible by $3$ with probability $2/3$. So we are at a **disadvantage** for primality, by a factor of

$$\frac{1/2}{2/3} = \frac{3}{4}.$$

## Exercise

*Show that for every odd prime $\ell$, the expression $p+2$ is at a disadvantage for being nondivisible by $\ell$, by a factor of*

$$\frac{1 - \frac{1}{\ell-1}}{1 - \frac{1}{\ell}} = 1 - \frac{1}{(\ell-1)^2}.$$

# Does the prime number theorem have a twin, ctd.



We collect all the local factors appearing in the previous analysis by defining $C = 2\prod_{\ell>2}\left(1-\frac{1}{(\ell-1)^2}\right)$. We have $C = 1.3203236\ldots$.

**Conjecture (Twin prime conjecture, quantitative form)**

*As* $x \to \infty$,

$$\pi_2(x) \sim C\frac{x}{(\log x)^2} \quad \textit{or equivalently} \quad C\int_2^x \frac{\mathrm{d}t}{(\log t)^2}.$$

This looks pretty good numerically. For example,

$$\pi_2(10^{11}) = 224376048$$

and the integral approximation is about $224368865$.

# Back to polynomials



One can propose an analogous statement for polynomials. Let $\pi_2(q;n)$ count the number of monic prime pairs $P, P+1$ of degree $n$ over $\mathbb{F}_q$. A completely analogous heuristic argument suggests that

$$\pi_2(q;n) \sim C_q \frac{q^n}{n^2}, \quad \text{with} \quad C_q = \prod_P \left(1 - \frac{1}{(|P|-1)^2}\right).$$

Here the approximation is supposed to be good whenever $q$ is large **or** $n$ is large (i.e., whenever $q^n \to \infty$).

# A polynomial twin prime theorem



For fixed $q$, we do not know how to prove the asymptotic. In fact, we cannot even prove $\pi_2(q;n) \to \infty$ as $n \to \infty$.

**Theorem**

*The proposed asymptotic holds if $n$ is fixed and $q \to \infty$ through odd prime powers.*

This is due to Bender & P. (in preparation) and independently to Lior Bary-Soroker. There are analogues results for more general twins $f, f+A$, and also for irreducibles of the form $f^2+1$.

The key tool in all of these proof is a form of the Chebotarev density theorem for function fields with an explicit error term (using RH).



# Maraming salamat!