Integers and Polynomials: Parallel Universes

Paul Pollack

August 14, 2006

CAST OF CHARACTERS

The Rational Integers:

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Let F be a finite field, say $F = \mathbf{F}_q$. **The ring of (univariate) polynomials over F is:**

$\mathbf{F}_q[T] =$
$\{a_0 + a_1 T + \cdots + a_n T^n : n \geq 0, \text{ each } a_i \in \mathbf{F}_q\}.$

Division Algorithm

Theorem. *If $a, b \in \mathbf{Z}$ and $b \neq 0$, then there exist $q, r \in \mathbf{Z}$ with $a = bq + r$ and $0 \leq r < b$.*

Theorem. *If $a, b \in \mathbf{F}_q[T]$ and $b \neq 0$, then there exist $q, r \in \mathbf{F}_q[T]$ with $a = bq + r$ satisfying either $r = 0$ or $\deg r < \deg b$.*

Euclidean Domain $\Longrightarrow$ PID $\Longrightarrow$ UFD

Infinitely Many Primes
Euclid's Proof Made Difficult

Recall the definition of the *Jacobson Radical* of a commutative ring R:

$$J(R) = \bigcap_{M \text{ maximal}} M.$$

Theorem. *Let R be a commutative ring. Then*

$$J(R) = \{x : 1 - xy \text{ is invertible for all } y \in R\}.$$

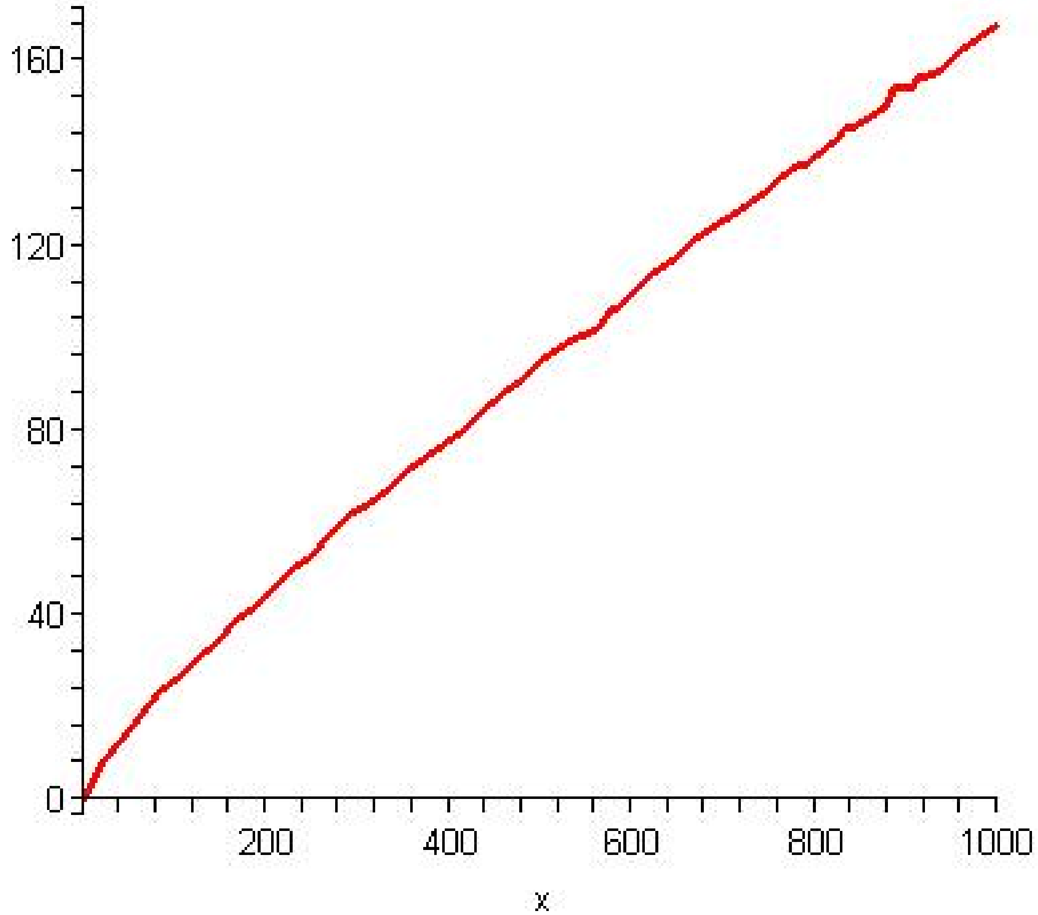
Corollary. *If $R = \mathbf{Z}$ or $R = \mathbf{F}_q[T]$, then the Jacobson radical $J(R) = \{0\}$.*

Corollary. *In both $R = \mathbf{Z}$ and $R = \mathbf{F}_q[T]$, there are infinitely many primes.*

Proof (Porubsky). If $p_1, \ldots, p_k$ are all the primes, then the principal ideals $p_1R, \ldots, p_kR$ are all the maximal ideals, and $0 \neq p_1 \ldots p_k \in J(R)$. $\square$

More on the Distribution of Primes

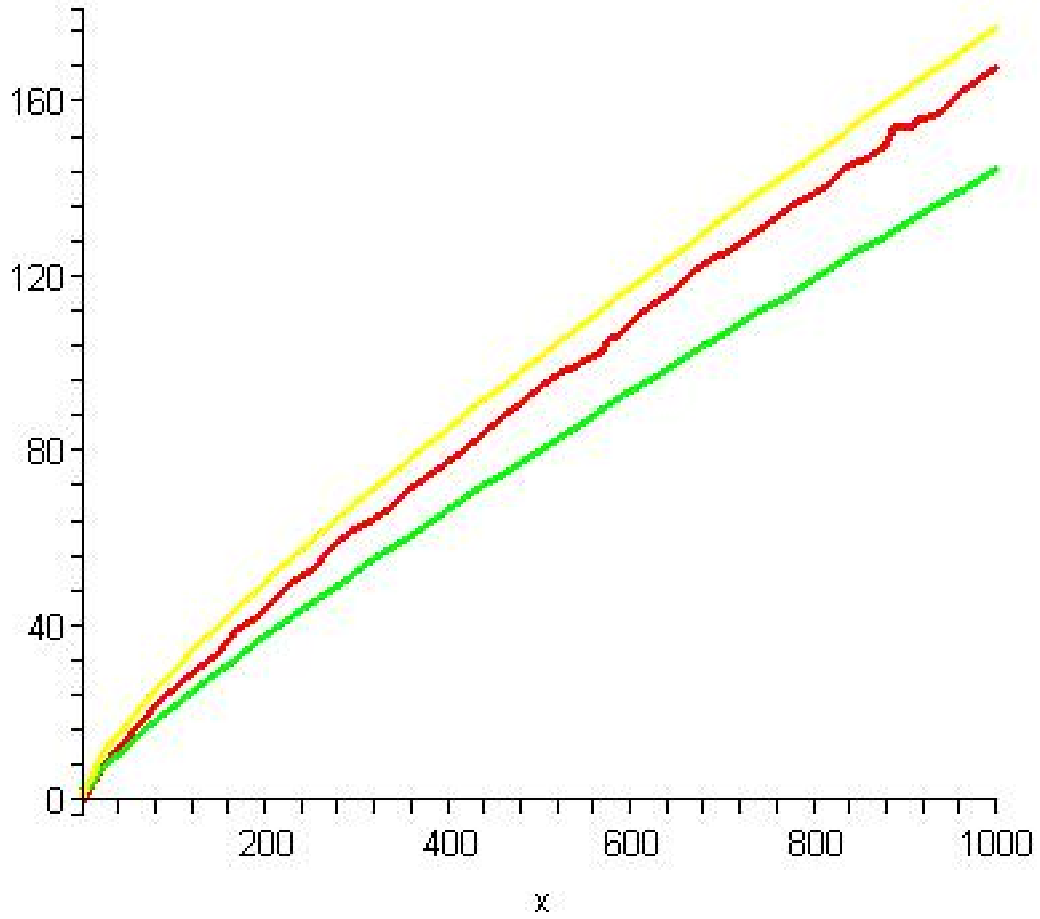
Let $\pi(x)$ be the number of positive primes (in $\mathbf{Z}$) not exceeding x.



Plot of $\pi(x)$ in the range $[0, 1000]$

Prime Number Theorem for $\mathbf{Z}$. *We have*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$



Red: $\pi(x)$ **Yellow**: $\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t}$ **Green**: $\frac{x}{\log x}$

Prime Number Theorem for $\mathbf{F}_q[T]$

Goal: count number $\nu_q(n)$ of monic irreducibles of degree n over $\mathbf{F}_q$.

Theorem. *In $\mathbf{F}_q[T]$ we have the factorization*

$$T^{q^n} - T = \prod \pi(T),$$

where the product is over all monic irreducibles π of $\mathbf{F}_q[T]$ whose degree divides n.

Compare degrees:

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

An Explicit Formula for $\nu_q(d)$

Invert

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

Obtain

$$\begin{aligned}
\nu_q(1) &= q, \\
\nu_q(2) &= (q^2 - q)/2, \\
\nu_q(3) &= (q^3 - q)/3, \\
&\vdots \\
\nu_q(n) &= \frac{q^n}{n} + \frac{1}{n} \sum_{d|n, d<n} q^d \mu(n/d) \\
&= q^n/n + O(q^{n/2}/n).
\end{aligned}$$

for coefficients $\mu(n/d) \in \{0, -1, 1\}$.

Prime Number Theorem for $\mathbf{F}_q[T]$. *The number of prime polynomials of degree n over $\mathbf{F}_q$ is given by*

$$\begin{aligned}\nu_q(n) &= q^n/n + O(q^{n/2}/n) \\ &= \frac{x}{\log_q x} + O(x^{1/2}/\log_q(x)),\end{aligned}$$

if we set $x = q^n$.

Twin Primes and Twin Prime Polynomials

A pair of primes $p, p+2$ is called a **twin prime pair.**

A pair of monic irreducible polynomials $A, A+1$ over $\mathbf{F}_q$ is called a **twin irreducible pair**.

Conjecture. *There are infinitely many twin prime pairs.*
Conjecture. *Fix $\mathbf{F}_q$ with $q > 2$. Then there are infinitely many twin irreducible pairs.*

Recent Progress

Theorem (C. Hall, 2003). *If $q > 3$, then infinitely often $f, f+1$ are simultaneously prime as f ranges over the monic polynomials over $\mathbf{F}_q[u]$.*

Theorem (P, 2004). *If $q > 2$ and $\alpha \in \mathbf{F}_q^*$, then infinitely often $f, f+\alpha$ are simultaneously prime as f ranges over the monic polynomials of $\mathbf{F}_q[u]$.*

Lemma. *Let $f(T)$ be an irreducible polynomial over $\mathbf{F}_q$ of degree d. Let α be a root of f inside the splitting field $\mathbf{F}_{q^d}$ of f. If l is an odd prime for which α is not an lth power in $\mathbf{F}_{q^d}$, then each of the substitutions*

$$T \mapsto T^{l^k}, \quad k = 1, 2, 3, \ldots$$

preserves the irreducibility of f.

Example: Twin Prime Polynomials over $\mathbf{F}_3$

Begin with the twin prime pair

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

The splitting field of both polynomials is F_{3^3}. Neither polynomial has a root which is a 13th power in F_{3^3}, and so

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

is a twin prime pair for each $k = 1, 2, \ldots$.

Extensions of these Results

Hardy-Littlewood Conjectures. *Any reasonable family of integer polynomials*

$$f_1(u), \ldots, f_k(u) \in \mathbf{Z}[u]$$

simultaneously represent primes infinitely often. Moreover, we have an asymptotic formula predicted by the prime number theorem + local considerations predict.

Reasonable: $\{u, u+2\}$, $\{7u+3\}$, or $\{u^2+1\}$
Unreasonable: $\{u^2\}$, $\{u, u+1\}$ or $\{u^2+u+2\}$.

Sample Results

Theorem (P). *Let $\mathbf{F}_q$ be a finite field with $q \equiv 3 \pmod 4$. Then there are infinitely many irreducible polynomials of the form f^2+1 with f monic.*

Theorem (P). *Fix $n \geq 1$. As $q \to \infty$ through prime powers congruent to* 3 mod 4 *and prime to* $2n$*, the number of monic polynomials f for which f^2+1 is irreducible is asymptotically q^n/n.*

Perfect Numbers and Perfect Polynomials

In the case of the too much, is produced excess, superfluity, exaggerations and abuse; in the case of too little, is produced wanting, defaults, privations and insufficiencies. And in the case of those that are found between the too much and the too little, that is in equality, is produced virtue, just measure, propriety, beauty and things of that sort - of which the most exemplary form is that type of number which is called perfect.
– Nicomachus

The Sum of Divisors Function

For n a positive integer, define

$$\sigma(n) := \sum_{d|n} d$$

as the sum of the (positive) divisors of n.

Examples:

$$\sigma(9) = 1 + 3 + 9 = 13,$$

$$\sigma(125) = 1 + 5 + 25 + 125 = 156.$$

Also,

$$\begin{aligned}\sigma(1125) &= \sigma(9 \cdot 125)\\ &= (1+3+9)(1+5+25+125)\\ &= 2028.\end{aligned}$$

More generally,

$$\sigma(mn) = \sigma(m)\sigma(n) \quad \text{if } m, n \text{ are coprime.}$$

Deficient, Abundant, and Perfect

Deficient: $\sigma(n) < 2n$

> [like animals with] a single eye, ... one armed or one of his hands has less than five fingers, or if he does not have a tongue. . .

Examples: $1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, \ldots$

Abundant: $\sigma(n) > 2n$

Examples: $12, 18, 20, 24, 30, 36, 40, 42, \ldots$

> [like animals with] ten mouths, or nine lips, and provided with three lines of teeth; or with a hundred arms, or having too many fingers on one of its hands . . .

Perfect: $\sigma(n) = 2n$

Theorem (Euclid's Perfect Number Theorem)**.** *If $2^n - 1$ is prime, then*

$$N := 2^{n-1}(2^n - 1)$$

is a perfect number.

Example: $n = 3$, and $N = 2^2 \cdot (2^3 - 1) = 28$.

Proof.

$$\begin{aligned} \sigma(N) &= \sigma(2^{n-1})\sigma(2^n - 1) \\ &= (1 + 2 + \cdots + 2^{n-1})(1 + (2^n - 1)) \\ &= (2^n - 1)(2^n) = 2N. \end{aligned}$$

□

Theorem (Euler's Perfect Number Theorem). *If N is an* even *perfect number, then N comes from Euclid's theorem; in other words*

$$N = 2^{n-1}(2^n - 1)$$

for some n with $2^n - 1$ prime.

p	Digits in M_p	Digits in N_p	Year
2	1	1	
3	1	2	
5	2	3	
7	3	4	
13	4	8	1456
17	6	10	1588
19	6	12	1588
31	10	19	1772
61	19	37	1883
89	27	54	1911
107	33	65	1914
127	39	77	1876
521	157	314	1952
⋮	⋮	⋮	⋮
13466917	4053946	8107892	2001
20996011	6320430	12640858	2003
24036583	7235733	14471465	2004
25964951	7816230	15632458	2005
30402457	9152052	18304103	2005

Two Quotes on Odd Perfect Numbers

I am odd. It is conjectured that I am not perfect. – number theorist Harold N. Shapiro

There are many old problems in arithmetic whose interest is practically nil, e.g., the existence of odd perfect numbers, problems about the iteration of numerical functions, the existence of infinitely many Fermat primes $2^{2^n}+1$, etc. – Enrico Bombieri

Odd Perfect Numbers: A Dossier

- not too common: counting function is $O(x^\epsilon)$,
- have over 300 decimal digits,
- at least 9 distinct prime factors,
- at least 75 total prime factors,
- only finitely many odd perfect numbers with k prime factors for any given k,
- have prime factorization with special properties: e.g., must look like $p^\alpha m^2$, where $p \equiv \alpha \equiv 1 \pmod 4$.

Perfect Polynomials

We work over $\mathbf{F}_2$, the field with two elements. Define

$$\sigma(A) = \sum_{D|A} D.$$

Examples:

$$\sigma(T^2+1) = \sigma((T+1)^2) = \\ 1 + (T+1) + (T+1)^2 = T^2 + T + 1.$$

$$\sigma(T^2+T) = \sigma(T(T+1)) = \\ 1 + T + (T+1) + (T^2+T) = T^2 + T.$$

As over $\mathbf{Z}$, we have

$$\sigma(MN) = \sigma(M)\sigma(N) \quad \text{if } M, N \text{ are coprime.}$$

Theorem (Canaday). *If A splits over $\mathbf{F}_2$, then A is perfect if and only if $A = (T(T+1))^{2^n-1}$ for some positive integer n.*

Example: $T(T+1)$.

Proof of sufficiency. Use the multiplicativity of σ. Check that

$$\sigma(T^{2^n-1}) = 1 + T + \cdots + T^{2^n-1} = (1+T)^{2^n-1}$$

over $\mathbf{F}_2$. □

Table of Non-splitting Perfect Polynomials (due to E.F. Canaday)

Degree	Factorization into Irreducibles
5	$T(T+1)^2(T^2+T+1)$
	$T^2(T+1)(T^2+T+1)$
11	$T(T+1)^2(T^2+T+1)^2(T^4+T+1)$
	$T^2(T+1)(T^2+T+1)^2(T^4+T+1)$
	$T^3(T+1)^4(T^4+T^3+1)$
	$T^4(T+1)^3(T^4+T^3+T^2+T+1)$
15	$T^3(T+1)^6(T^3+T+1)(T^3+T^2+1)$
	$T^6(T+1)^3(T^3+T+1)(T^3+T^2+1)$

Degree 16:

$$T^4(T+1)^4(T^4+T^3+1)(T^4+T^3+T^2+T+1)$$

Degree 20:

$$T^6(T+1)^4(T^3+T+1)(T^3+T^2+1)(T^4+T^3+1),$$

$$T^4(T+1)^6(T^3+T+1)(T^3+T^2+1)(T^4+T^3+T^2+T+1).$$

Let $R = \mathbf{F}_2[T]$. Call an element A of R *even* if A is divisible by some prime π in $\mathbf{F}_2[T]$ with $R/\pi R \cong \mathbf{Z}/2\mathbf{Z}$, otherwise call A *odd*.

Conjecture (Canaday)**.** *There are no odd perfect polynomials: if A is perfect, then A is divisible by either T or $T+1$. (Equivalently, A has a root over $\mathbf{F}_2$.)*

A Profile of Odd Perfect Polynomials

For $A \in \mathbf{F}_q[T]$, let $|A| := q^{\deg A}$. We know:

- odd perfect polynomials have at least 10 prime factors, counted with multiplicity,

- their counting function is $O(x^{1/10+\epsilon})$.

If there's a single odd perfect polynomial with k prime factors, then *probably* there are infinitely many odd perfect polynomials with k distinct prime factors.

In fact, there are probably lots of them!

Why Finite Fields?

Theorem. *100% of polynomials over $\mathbf{Q}$ (or over $\mathbf{Z}$) are irreducible. In fact,* 100% *of degree n polynomials over $\mathbf{Q}$ (or over $\mathbf{Z}$) have S_n as their Galois group.*

So it's not so surprising one can obtain results like . . .

Theorem (Goldbach's Conjecture for Integer Polynomials)**.** *Every nonconstant monic polynomial in $\mathbf{Z}[T]$ can be written as the sum of two monic irreducibles.*

Proof. Exercise: use the Eisenstein irreducibility criterion. □