Solved and Unsolved Problems in Elementary Number Theory

Paul Pollack
2005 Ross Summer Mathematics Program

Good mathematics consists in solving difficult problems, not in fabricating new theories in search of a problem.

– Harold Davenport

Digit Races and the Thue-Morse Sequence

Let $s(n)$ be the sum of the binary digits of n. Define the sequence $t(n)$ according to the rule

$$t(n) = (-1)^{s(n)}.$$

Examples:

n	expansion	$t(n) = 1$?	$t(n) = -1$?
0	0		
1	1		
2	10		
3	11		
4	100		
5	101		
6	110		
7	111		
8	1000		
9	1001		
10	1010		
11	1011		
12	1100		
13	1101		
14	1110		
15	1111		

The first ($t(n) = 1$) and second ($t(n) = -1$) columns seem evenly matched!

Exercise. *Prove that this race is a tie: No matter what stopping point we pick, no column ever beats any other by more than* 1*, and and the two columns each take the lead infinitely often.*

Let's try something different. Consider $t(3n)$.

$3n$	expansion	$t(3n) = 1$?	$t(3n) = -1$?
0	0		
3	11		
6	110		
9	1001		
12	1100		
15	1111		
18	10010		
21	10101		
24	11000		
27	11011		
30	11110		
33	100001		
36	100100		
39	100111		
42	101010		
45	101101		

Theorem (Newman). *Let $P(3N)$ denote the number of checks in the first column among the integers $n = 0, 3, \ldots, 3N$ and $M(3N)$ denote the checks in the second column.*

Then

$$\frac{P(3N)}{N+1} \to \frac{1}{2} \quad \textit{and} \quad \frac{M(3N)}{N+1} \to 1/2.$$

BUT

$$\frac{1}{20}N^{\alpha} < P(3N) - M(3N) < 5N^{\alpha},$$

where

$$\alpha = \frac{\log 3}{\log 4} = .79248\ldots$$

What about racing primes?

Unsolved Problem. *Are there infinitely many primes p for which $t(p) = 1$? for which $t(p) = -1$?*

Artin's Primitive Root Conjecture

2 is a generator mod p for

$$p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, \ldots$$

It seems unthinkable that this list would stop...

Conjecture (Artin). *Let a be an integer $\neq -1, \neq \blacksquare$. Then a is generator of U_p for infinitely many primes p.*

Actually was quantitative:

Example: 2 should be a primitive root 37.4% of the time.

Known under certain generalizations of the Riemann Hypothesis.

But we don't know a single a for which Artin's conjecture is true!

On the other hand . . .

Theorem (Heath-Brown). *One of* $2, 3$ *and* 5 *is a generator for infinitely many primes* p.

Exercise (Schinzel & Sierpiński). *Show that there are infinitely many primes* p *for which the sequence*

$$2 \mod p, \quad 2^2 \mod p, \quad 2^3 \mod p, \ldots$$

contains the term 3.

This certainly holds if 2 is a generator (and $p > 3$). But there are other examples: e.g., $2^8 \equiv 3 \pmod{23}$.

Generalize!

Sums of Powers

Theorem (Four Squares Theorem). *Every non-negative integer n can be written in the form*

$$n = a^2 + b^2 + c^2 + d^2$$

with integers a, b, c and d. That is, every positive integer is a sum of four squares.

Random example:

$$\begin{aligned} &7103333114129321134514340 7 = \\ &\quad 23811041225657^2 + 11973622964306^2 + \\ &\qquad\qquad\qquad\qquad 11^2 + 1^2. \end{aligned}$$

Every integer is a square or the sum of two, three, or four squares; every integer is a cube or the sum of at most nine cubes; every integer is also the square of a square, or the sum of up to nineteen such, and so forth.

– Edward Waring

Let $g(k)$ be the minimal number of NONNEGATIVE kth powers needed to represent every nonnegative integer additively.

Conjecture (Waring). *We have* $g(2) \leq 4$, $g(3) \leq 9$ *and* $g(4) \leq 19$*; moreover,* $g(k)$ *exists for every* k*.*

Theorem (Hilbert). $g(k)$ *exists for every* k*.*

It's known that $g(3) = 9$, $g(4) = 19$ and probably

$$g(k) = \lfloor (3/2)^k \rfloor + 2^k - 2$$

for every k. (This is known for all but finitely many k.)

Theorem (Five Cubes Theorem?). *Every integer n can be written in the form*

$$n = a^3 + b^3 + c^3 + d^3 + e^3$$

with integers a, b, c, d and e. That is, every integer is a sum of five cubes.

Proof: We have the polynomial identity

$$(x-1)^3 + (x+1)^3 + (-x)^3 + (-x)^3 = 6x.$$

So every multiple of 6 is a sum of four cubes.

If n is any integer, then $n - n^3$ is a multiple of 6. (Because 6 divides the product of the three consecutive integers $n-1, n, n+1$.) So

$$n - n^3 = a^3 + b^3 + c^3 + d^3$$

for some integers a, b, c and d. And

$$n = a^3 + b^3 + c^3 + d^3 + n^3.$$

Exercise. *Show that not every integer n is a sum of three cubes (look mod 9).*

Unsolved Problem. *Is every n a sum of four cubes?*

Let R be a ring (e.g., $R = \mathbf{Z}$ or $R = \mathbf{Z}_p[x]$).

Let $w(k, R)$ be the smallest number (if it exists) of kth powers needed to represent additively any element of R.

So we showed $w(3, \mathbf{Z}) \leq 5$ and it is not known whether or not $w(3, \mathbf{Z}) = 4$.

Exercise. *Prove that $w(k, \mathbf{Z})$ is finite for every odd integer k.*

Exercise. *Prove that $w(k, \mathrm{C}[x])$ is finite for every positive integer k. In fact, prove that $w(k, \mathrm{C}[x]) \leq k + 1$.*

Ask me about the problem with $R = \mathbf{Z}_p[x]$.

Perfection

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

We say n is *perfect* if $n = \sum_{d|n, d<n} d$, i.e.,

$$2n = \sum_{d|n} d = \sigma(n).$$

Example: $6 = 1 + 2 + 3$.
And $28 = 1 + 2 + 4 + 7 + 14$.

Questions: Can they be described more explicitly? Are there infinitely many?

Theorem (Euclid). *If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is an even perfect number.*

Examples: $p = 2$, then $2^1 \cdot (2^2 - 1) = 6$, and if $p = 3$, then $2^2 \cdot (2^3 - 1) = 28$.

Proof. We have

$$\begin{aligned} &\sigma(2^{p-1}(2^p - 1)) \\ &\qquad = \sigma(2^{p-1})\sigma(2^p - 1) \\ &\qquad = (1 + 2 + \cdots + 2^{p-1})(1 + (2^p - 1)) \\ &\qquad = (2^p - 1)(2^p) = 2 \cdot (2^p - 1)(2^{p-1}). \ \square \end{aligned}$$

Theorem (Euler). *Every even perfect number is of this form.*

EXERCISE!

Unsolved Problem. *Are there any odd perfect numbers?*

Are there infinitely many perfect numbers? What about even perfect numbers?

Unsolved Problem. *Are there infinitely many primes of the form* $2^p - 1$*?*

Unsolved Problem. *Are there infinitely many composite numbers of the form* $2^p - 1$ *where* p *is prime?*

Exercise. *Show that if* $p \equiv 3 \pmod 4$ *and* $q := 2p + 1$ *are both prime, then* $q \mid 2^p - 1$*, and so* $2^p - 1$ *is composite.*

But we don't know whether there are infinitely many of these "prime pairs."

We aren't *completely* ignorant:

Theorem. *If n is an odd perfect number, then*

1. *the prime factorization of n has the shape*

   $$q^{\alpha} p_1^{2e_1} \dots p_k^{2e_k}$$

   where q and the p_i are distinct primes and $q \equiv \alpha \equiv 1 \pmod 4$ (Euler).

2. *$n > 10^{300}$ (Brent, Cohen, teRiele).*

3. *n has at least 8 distinct prime factors (Hagis) and at least 75 prime factors with multiplicity counted (Hare)*

Theorem (Nielsen). *If n is an odd perfect number with k distinct prime factors, then $n < 2^{4^k}$.*

Also there can't be too many odd perfect numbers:

Theorem (Wirsing). *For every k, there are more kth powers than there are odd perfect numbers.*

Prime and Composite Numbers

The primes:

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

The composites:

$$4, 6, 8, 9, 12, 14, 15, 16, \ldots$$

Infinitely many primes. In fact (Euler),

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots$$

doesn't converge! Since

$$\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots < \infty,$$

there are "more primes than squares."

Infinitely many composites.

Fermat's Conjecture. *The integer* $F_n := 2^{2^n} + 1$ *is prime for every positive integer* n.

Examples:

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537.$

Non-example:

$$F_5 = 641 \cdot 6700417.$$

Is F_n composite for every $n \geq 5$? infinitely many n? Similar questions for $b^{2^n} + 1$ with b even.

Another source of primes:
$n! + 1$ (e.g., $1, 2, 3, 11, \ldots, 6380, \ldots$),
$n! - 1$ (e.g., $3, 4, 6, \ldots, 21840, \ldots$)

Two Exercises in Composite Number Theory

Exercise (Sierpiński). *Prove that one of the sequences* $\{2^{2^n}+1\}$ *and* $\{6^{2^n}+1\}$ *contains infinitely many composite numbers.*

Exercise (Schinzel). *Prove that there are infinitely many composite numbers of the form* $n!+1$ *and infinitely many of the form* $n!-1$. *Do the same with* $n!$ *replaced by* $cn!$, *with* $c>0$ *rational.*

Gaps Between Primes

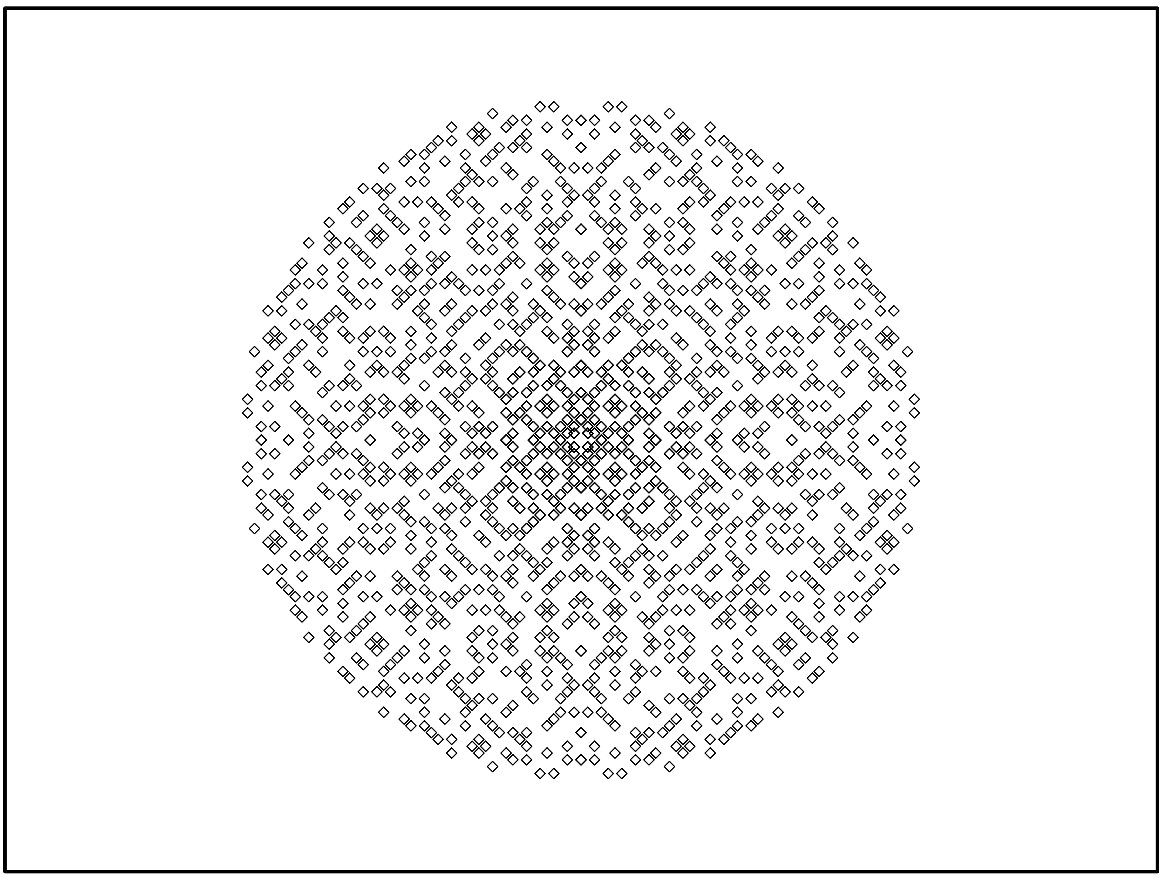
Start at the origin. Is there a number B so that taking steps of length at most B along the real number line, you can walk to infinity only stepping on primes?

NO. There are arbitrarily large gaps between primes: If $n > 1$, then

$$n! + 2, n! + 3, \ldots, n! + n$$

are all composite.

Unsolved Problem. *What about the corresponding problem for Gaussian primes?*



Famous Unsolved Prime Problems

Goldbach's Conjecture: Every even $n \geq 4$ is a sum of two primes.

Theorem (Schnirelmann)**.** *There is a fixed number N with the following property: every integer $n > 1$ is the sum of at most N primes.*

Theorem (Vinogradov)**.** *Every large enough odd integer (i.e., every odd integer from some point on) is a sum of three primes.*

Theorem (Chen)**.** *Every large enough even integer can be written in the form $p + p'$, where p is prime and p' is either prime or a product of two primes.*

Twin Prime Conjecture:

For infinitely many primes p, the number $p + 2$ is also prime.

$$\{3,5\},\{5,7\},\{11,13\},\{17,19\},\ldots,$$

$$\{33218925{\cdot}2^{169690}-1, 33218925{\cdot}2^{169690}+1\},\ldots$$

Theorem (Brun). *If there are infinitely many twin primes, they are sparse. In fact,*

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\ldots,$$

where in the denominator we only take those primes which occur in a twin prime pair, DOES converge.

Theorem (Chen). *There are infinitely many primes p for which $p+2$ is either prime or a product of two primes.*

The Situation for Polynomials

Primes have other homes!

Theorem (C. Hall). *Let p be an odd prime. Then there are infinitely many pairs of primes $f, f+1$ in $\mathbf{Z}_p[x]$.*

But is the Goldbach conjecture true?

Unsolved Problem. *That is, let p be an odd prime. Is every element of $\mathbf{Z}_p[x]$ a sum of two prime polynomials?*

Theorem (Hayes). *Goldbach's conjecture is true in $\mathbf{Z}[x]$: Every polynomial of degree $n \geq 1$ with integer coefficients is the sum of two irreducible polynomials of degree n.*

More on the Distribution of Primes

Let $\pi(N)$ be the number of primes not exceeding N; e.g., $\pi(2) = 1$, and $\pi(10) = 4$.

Let

$$\mathrm{li}(N) = \int_2^N \frac{dt}{\log t}.$$

If this bothers you, think of

$$\frac{1}{\log 2} + \frac{1}{\log 3} + \cdots + \frac{1}{\log N}.$$

N	$\pi(N)$	$\mathrm{li}(N)$
10^3	168	177
10^4	1,229	1245
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	50,847,534	50,849,234
10^{10}	455,052,512	455,055,614
10^{11}	4,118,054,813	4,118,066,400
10^{12}	37,607,912,018	37,607,950,280

N	$\pi(N)$	$\mathrm{li}(N) - \pi(N)$
10^3	168	9
10^4	1,229	16
10^5	9,592	37
10^6	78,498	129
10^7	664,579	338
10^8	5,761,455	753
10^9	50,847,534	1700
10^{10}	455,052,512	3103
10^{11}	4,118,054,813	11587
10^{12}	37,607,912,018	38263

These tables suggest several conjectures.

Two Conjectures

Conjecture. *We always have* li$(N) > \pi(N)$.

This is badly false. Littlewood showed that the difference

$$\mathrm{li}(N) - \pi(N)$$

changes sign infinitely often. It even gets big in both directions.

Skewes (1955) showed the first sign change has to appear before

$$10^{10^{10^{10^3}}}.$$

But the first sign change is now known to occur before $2 \cdot 10^{316}$.

Conjecture. *The percentage error made in approximating* $\pi(N)$ *by* $\mathrm{li}(N)$ *tends to* 0*. In technical terms,*

$$\lim_{N\to\infty} \frac{\pi(N)}{\mathrm{li}(N)} = 1.$$

This is true: it's known as the **Prime Number Theorem**.

The Riemann Hypothesis

The Riemann Hypothesis is (equivalent to) a statement about the error term in the prime number theorem:

Riemann Hypothesis. *For every* $N \geq 3$,

$$|\pi(N) - \mathrm{li}(N)| < \sqrt{N} \log N.$$

The elementary theory of numbers . . . is unique among the mathematical sciences in its appeal to natural human curiosity. – G.H. Hardy

Book Recommendations

Unsolved Problems in Number Theory (3rd Edition), by Richard Guy

Elementary Theory of Numbers (2nd Edition), by W. Sierpiński (edited by A. Schinzel)