Patterns That May Not Last

Keith Conrad
Univ. of Connecticut

Certitude is not the test of certainty. We have been cocksure of many things that were not so.

Oliver Wendell Holmes

Numerical Evidence Led To...

Goldbach's Conjecture (1742)

Waring's Problem (1770)

Prime Number Theorem (Legendre, 1796)

Class Number Problem (Gauss, 1801)

Chebyshev's Bias (1853)

Birch and Swinnerton-Dyer Conjecture (1962)

Cohen-Lenstra Heuristics (1983)

Evidence for Goldbach

Conjecture: *Every even integer $n > 2$ is a sum of two primes.*

n	Sum of Two Primes
4	$2 + 2$
6	$3 + 3$
8	$3 + 5$
10	$3 + 7 = 5 + 5$
12	$5 + 7$
14	$3 + 11 = 7 + 7$
16	$3 + 13 = 5 + 11$
18	$5 + 13 = 7 + 11$
20	$3 + 17 = 7 + 13$
22	$3 + 19 = 5 + 17 = 11 + 11$
24	$5 + 19 = 7 + 17 = 11 + 13$

Regions From Circles

Let R_n be the largest number of regions in a circle formed by connecting n points on the circle with straight lines.

n	R_n
1	1
2	2
3	4
4	8
5	16
6	31

Theorem. *For* $n \geq 1$, $R_n = 1 + \binom{n}{2} + \binom{n}{4}$. *Equivalently,*

$$R_n = \frac{n^4 - 6n^3 + 23n^2 - 18n + 24}{24}.$$

So $R_7 = 57$ (not 64) and $R_8 = 99$ (not 128).

Powers of 2 and Primes

Fermat conjectured $2^{2^m}+1$ is prime for all $m \geq 0$.

m	0	1	2	3	4
$2^{2^m}+1$	3	5	17	257	65537

But $2^{32}+1 = 641 \cdot 6700417$ (Euler). No new primes of this form are known.

If $2^n \equiv 2 \bmod n$ and $n < 300$ then n is prime. (Chinese primality test)

But also true at $n = 341 = 11 \cdot 31$. Next: $561 = 3 \cdot 11 \cdot 17$.

Powers of 2 and Primes (Cont.)

While $2^n + 1$ appears to be prime only for $n = 1, 2, 4, 8, 16$, what about $2^n + k$ for odd $k > 1$? Does it take a prime value *at least once* (for $n = 1, 2, 3, \dots$)?

Certainly having k odd is a *necessary* condition for $2^n + k$ to have a prime value. Is it *sufficient?*

k	Least $n \geq 1$ with $2^n + k$ prime
1	1
3	1
5	1
7	2
$\vdots$	$\vdots$
47	5
$\vdots$	$\vdots$
61	8
$\vdots$	$\vdots$
83	7

For $k \leq 100$, least n is at most 3, unless $k = 47, 61$, or 83.

May need to wait: $2^n + 773$ is first prime for $n = 955$.

Powers of 2 and Primes (Cont.)

Theorem. *For every $n \geq 1$, $2^n + 78557$ is composite.*

Proof. If $n = 2m$ then $2^n + 78557 \equiv 4^m + 2 \equiv 0 \bmod 3$.

p	3	5	7	13	19	37	73
Order of 2 mod p	2	4	3	12	18	36	9
78557 mod p	2	2	3	11	11	6	9

If $n \equiv 3 \bmod 4$, $2^n + 78557 \equiv 8 + 2 \equiv 0 \bmod 5$.

If $n \equiv 2 \bmod 3$, $2^n + 78557 \equiv 4 + 3 \equiv 0 \bmod 7$.

If $n \equiv 1 \bmod 12$, $2^n + 78557 \equiv 2 + 11 \equiv 0 \bmod 13$.

If $n \equiv 3 \bmod 18$, $2^n + 78557 \equiv 8 + 11 \equiv 0 \bmod 19$.

If $n \equiv 9 \bmod 36$, $2^n + 78557 \equiv 31 + 6 \equiv 0 \bmod 37$.

If $n \equiv 6 \bmod 9$, $2^n + 78557 \equiv 64 + 9 \equiv 0 \bmod 73$.

Every positive integer n fits one of these seven congruence conditions. $\square$

Rational points on $y^2 = x^3 - 25x$

x	y
0	0
-4	6
$25/4$	$75/8$
$-5/9$	$100/27$
$1681/144$	$62279/1728$
$-3600/41^2$	$455700/41^3$
$12005/31^2$	$1205400/31^3$
$-4805/49^2$	$-762600/49^3$

Are the denominators always a square and a cube?

Rational points on $y^2 = x^3 - 25x$

Theorem. *Any rational solution to* $y^2 = x^3 - 25x$ *has* $x = a/c^2$ and $y = b/c^3$.

Proof: Write

$$x = \frac{a}{k}, \quad y = \frac{b}{\ell}$$

in reduced form. Then

$$\frac{b^2}{\ell^2} = \frac{a^3}{k^3} - 25\frac{a}{k},$$

so clearing denominators gives

$$b^2k^3 = a^3\ell^2 - 25ak^2\ell^2 = \ell^2(a^3 - ak^2).$$

Thus $\ell^2 | k^3$ and $k^3 | \ell^2$, so $k^3 = \ell^2$. By unique factorization, $k = c^2$ and $\ell = c^3$. $\square$

PODASIP: Let $f(T)$ and $g(T)$ be in $\mathbf{Z}[T]$ with degrees m and n, respectively. If $f(a/k) = g(b/\ell)$ then $k = c^n$ and $\ell = c^m$.

Now *you* decide which way things go!

Coefficients of Polynomials

Factor $X^n - 1$ as much as possible in $\mathbf{Z}[X]$.

n	$X^n - 1$
1	$X - 1$
2	$(X+1)(X-1)$
3	$(X^2+X+1)(X-1)$
4	$(X^2+1)(X+1)(X-1)$
5	$(X^4+X^3+X^2+X+1)(X-1)$
6	$(X^2-X+1)(X-1)$

For all $n \leq 100$, every factor has coefficients 0, 1, or -1.

Coefficients of Polynomials (Cont.)

Consider coefficients of $(1-X)(1-X^2)(1-X^3)(1-X^4)\cdots$

n	nth product
1	$1-X$
2	$1-X-X^2+X^3$
3	$1-X-X^2+X^4+X^5-X^6$
4	$1-X-X^2+2X^5-X^8-X^9+X^{10}$
5	$1-X-X^2+X^5+X^6+X^7-X^8$
	$-X^9-X^{10}+X^{13}+X^{14}-X^{15}$

Each term in degree ≤ 100 *eventually* becomes 0, 1, or -1.

Coefficients of Polynomials (Cont.)

Let c_n be constant term of $(x+1+1/x)^n$.

Example. $c_2 = 3$ since

$$\left(x+1+\frac{1}{x}\right)^2 = x^2+2x+3+\frac{2}{x}+\frac{1}{x^2}.$$

n	1	2	3	4	5	6	7	8
c_n	1	3	7	19	51	141	393	1107

There is no evident formula for c_n. Euler observed a pattern in $d_n = 3c_n - c_{n+1}$.

n	2	3	4	5	6	7	8
d_n	2	2	6	12	30	72	182
	$\mathbf{1}\cdot 2$	$\mathbf{1}\cdot 2$	$\mathbf{2}\cdot 3$	$\mathbf{3}\cdot 4$	$\mathbf{5}\cdot 6$	$\mathbf{8}\cdot 9$	$\mathbf{13}\cdot 14$

A partitioning of Z?

n	$[n\sqrt{2}]$	$2n + [n\sqrt{2}]$
1	1	3
2	2	6
3	4	10
4	5	13
5	7	17
6	8	20
7	9	23
8	11	27
9	12	30
10	14	34

Squares Inside Themselves

We know $5^2 = 25$ ends in 5 and $6^2 = 36$ ends in 6. Also $25^2 = 625$ ends in 25. While $36^2 = 1296$ doesn't end in 36, $76^2 = 5776$ ends in 76. Let's continue...

5	6
25	76
625	376
625	9376
90625	9376
890625	109376
2890625	7109376
12890625	87109376
212890625	787109376
8212890625	1787109376

1 mod 4 **vs.** 3 mod 4

$p \equiv 1 \bmod 4 : 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, \ldots$

$p \equiv 3 \bmod 4 : 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, \ldots$

Here are three places the dichotomy *seems* to appear:

1) $x^2 - py^2 = -1$ solvable: $2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89$

2) $\mathbf{Z}[\sqrt{p}]$ has unique fact$^{\mathrm{n}}$: $2, 3, 7, 11, 19, 23, 31, 43, 47, 59, 67$

3) Let $C(p) = \#\{(x, y) \bmod p : x^2 + y^2 \equiv 1 \bmod p\}$.

p	$C(p)$	p	$C(p)$
3	4	5	4
7	8	13	12
11	12	17	16
19	20	29	28
23	24	37	36
31	32	41	40
43	44	53	52
47	48	61	60

Races

Set

$$\mu(n) = \begin{cases} (-1)^r, & \text{if } n = p_1 \cdots p_r \text{ with distinct } p_i, \\ 0, & \text{otherwise } (n \text{ div. by square factor}). \end{cases}$$

So $\mu(12) = 0$, $\mu(15) = 1$. Let $M(x) = \sum_{n \leq x} \mu(n)$.

x	$M(x)$
1	1
2	0
3	-1
5	-2
6	-1
7	-2
10	-1
11	-2
13	-3
14	-2
15	-1
17	-1

Races (Cont.)

Set $\lambda(p_1^{e_1} \cdots p_r^{e_r}) = (-1)^{e_1+\cdots+e_r}$, *e.g.*, $\lambda(12) = -1$.

Let $L(x) = \sum_{n \le x} \lambda(n)$.

n	1	2	3	4	5	6	7	8	9	10
$\lambda(n)$	1	-1	-1	1	-1	1	-1	-1	1	1
$L(n)$	1	0	-1	0	-1	0	-1	-2	-1	0

x	$L(x)$
10	0
10^2	-2
10^3	-14
10^4	-94
10^5	-288
10^6	-530
10^7	-842
10^8	-3884

Polya's Conjecture (1919): $L(x) \le 0$ for all $x > 1$.

The conjecture holds for all $x \le 10^8$.

Races (Cont.)

Let $\pi_{a,m}(x) = \#\{p \leq x : p \equiv a \bmod m\}$.

Example. $\pi_{3,4}(10) = \#\{3, 7\} = 2$.

x	$\pi_{1,4}(x)$	$\pi_{3,4}(x)$
10	1	2
10^2	11	13
10^3	80	87
10^4	609	619
10^5	4783	4808
10^6	39175	39322
10^7	332180	332398

Chebyshev observes $\pi_{1,4}(x) \leq \pi_{3,4}(x)$ in tables in 1853. Is it always true?

Races (Cont.)

x	$\pi_{1,3}(x)$	$\pi_{2,3}(x)$
10	1	2
10^2	11	13
10^3	80	87
10^4	611	617
10^5	4784	4807
10^6	39231	39266
10^7	332194	332384

For $x \leq 10^{10}$, $\pi_{1,3}(x) \leq \pi_{2,3}(x)$. Is it always so?

Decimal Periods

For $p \neq 2$ or 5, let $n_1(p)$ = period length of $1/p$, $n_2(p)$ = period length of $1/p^2$, $n_k(p)$ = period length of $1/p^k$.

p	$n_1(p)$	$n_2(p)$	$n_3(p)$
3	1	1	3
7	6	$42 = 6 \cdot 7$	$294 = 6 \cdot 7^2$
11	2	$22 = 2 \cdot 11$	$242 = 2 \cdot 11^2$
13	6	$78 = 6 \cdot 13$	$1014 = 6 \cdot 13^2$
17	16	$272 = 16 \cdot 17$	$4624 = 16 \cdot 17^2$
19	18	$342 = 18 \cdot 19$	$6498 = 18 \cdot 19^2$
23	22	$506 = 22 \cdot 23$	$11638 = 22 \cdot 23^2$
29	28	$812 = 28 \cdot 29$	$23548 = 28 \cdot 29^2$
31	15	$465 = 15 \cdot 31$	$14415 = 15 \cdot 31^2$
37	3	$111 = 3 \cdot 37$	$4107 = 3 \cdot 37^2$
41	5	$205 = 5 \cdot 41$	$8405 = 5 \cdot 41^2$
43	21	$903 = 21 \cdot 43$	$38829 = 21 \cdot 43^2$

Is $n_k(p) = n_1(p)p^{k-1}$ for $p \geq 7$?

Decimal Periods (Cont.)

Set

$$\delta_{11}(x) = \frac{\#\{p \le x : 1/p \text{ has decimal period div. by } 11\}}{\#\{p \le x\}}.$$

Example. $1/23 = \mathbf{.0434782608695652173913}043\ldots$

x	$\delta_{11}(x)$
10^2	.119999
10^3	.089285
10^4	.094385
10^5	.090909
10^6	.091683
10^7	.091250

Does $\delta_{11}(x) \to 1/11 = .090909...$ as $x \to \infty$?

Cube roots of $2 \bmod p$

We count the primes p for which $2 \bmod p$ is a cube:

Example. $2 \equiv 3^3 \bmod 5$.

Example. Modulo 7, the cubes are 0, 1, 6; no 2 occurs.

$$2, 3, 5, 11, 17, 23, 29, 31, 41, 43, 47, 53, 59, 71, 83, 89, \ldots$$

x	$\#\{p \leq x : 2 \equiv \text{cube mod } p\}/\#\{p \leq x\}$
10	.7500
10^2	.6400
10^3	.6666
10^4	.6655
10^5	.6637

Does the proportion tend to $2/3 = .6666\ldots$ as $x \to \infty$?

Generators of Units

p	2 generates U_{p^2}?	2 generates U_{p^3}?
3	Y	Y
5	Y	Y
7	N	N
11	Y	Y
13	Y	Y
17	N	N
19	Y	Y
23	N	N
29	Y	Y
31	N	N
37	Y	Y
41	N	N

For odd primes $p < 10^{22}$, 2 generates U_{p^2} if and only if it generates U_{p^3}. Is this true for all $p > 2$?

Polynomials and Polynomial Values

If $f(X)$ and $g(X)$ are relatively prime in $\mathbf{Z}[X]$, it may or may not be true that $(f(n), g(n)) = 1$ for all $n \in \mathbf{Z}$.

Example. $f(X) = X^2 + 1$, $g(X) = X^2 - 2 = f(X) - 3$. If p divides $f(n)$ and $g(n)$ then $p = 3$, but $n^2 + 1 \equiv 0 \bmod 3$ has no solution. Thus $(f(n), g(n)) = 1$ for all n.

Example. $f(X) = X^2 + 1$, $g(X) = X^3 - 2$. If $n \equiv 3 \bmod 5$, $f(n)$ and $g(n)$ are multiples of 5.

Example. $f(X) = X^{19} + 6$, $g(X) = (X + 1)^{19} + 6$. For $n \leq 10^{50}$, $(f(n), g(n)) = 1$. Is it always so?

Polynomials and Polynomial Values (Cont.)

The polynomials $f(X) = X^{19} + 6$ and $g(X) = (X + 1)^{19} + 6$ have no common factor in $\mathbf{Z}[X]$.

The first n where $(f(n), g(n)) \neq 1$ is the 61-digit number

1578270389554680057141787800241971645032008710129107
338825798,

where the gcd is the 61-digit prime

5299875888670549565548724808121659894902032916925752
559262837.

We should take great care not to accept as true such properties of the numbers which we have discovered by observation and which are supported by [experiment] alone.

Euler

References

A. Granville and G. Martin, "Prime Number Races," Amer. Math. Monthly **113** (2006), 1–33.

R. K. Guy, "The Strong Law of Small Numbers," Amer. Math. Monthly **95** (1988), 697–712.

R. K. Guy, "The Second Strong Law of Small Numbers," Math. Mag. **63** (1990), 3–20.

D. Haimo, "Experimentation and Conjecture are Not Enough," Amer. Math. Monthly **102** (1995), 102–112.