The covering congruences of Paul Erdős

Carl Pomerance

Dartmouth College

Conjecture (Erdős, 1950): *For each number B, one can cover $\mathbb{Z}$ with finitely many congruences to distinct moduli all $> B$.*

Erdős (1995):

"Perhaps this is my favorite problem."

Early origins

Are there infinitely many primes of the form $2^n - 1$?

Euclid: *n must be prime, but this is not sufficient.*

For example, $2^2 - 1,\ 2^3 - 1,\ 2^5 - 1,\ 2^7 - 1$ are prime, but $2^{11} - 1 = 23 \times 89$.

Euclid: *If* $2^n - 1$ *is prime, then* $2^{n-1}(2^n - 1)$ *is* **perfect**. (That is, it is equal to the sum of its proper divisors.)

Euler: *All even perfect numbers are in Euclid's form.*

Primes of the form $2^n - 1$ are called Mersenne primes. There are 44 of them known, the largest being

$$2^{32\,582\,657} - 1.$$

See `www.mersenne.org` .

Early origins, cont'd

Are there infinitely many primes of the form $2^n + 1$?

Fermat: *A necessary condition is that n is a power of 2.* He conjectured this is also sufficient.

For example,

$2^1+1,\ 2^2+1,\ 2^4+1,\ 2^8+1,\ 2^{16}+1$

are all prime.

Euler: $2^{32}+1 = 641 \times 6\,700\,417.$

No other Fermat primes are known; $2^{2^k}+1$ is composite for $k = 5, 6, \ldots, 32$ and for many higher, sporadic values of k.

Gauss, Wantzel: *A regular n-gon is constructible with straight-edge and compass if and only if n is a power of 2 times a product of distinct Fermat primes.*

A mathematician's credo:

If you can't solve it, generalize!

For each odd number k, are there infinitely many primes of the form $2^n + k$?

OK, way too hard! Lets try:

For each odd number k, there is at least one prime of the form $2^n + k$.

(conjectured by de Polignac in 1849)

$61 + 2 = 63, \quad \{3, 7\}.$

Mod 3, the powers of 2 are $2, 1, 2, 1, \ldots$ (period 2).

So,

$n \equiv 1 \pmod 2 \Rightarrow 61 + 2^n \equiv 0 \pmod 3.$

Mod 7, the powers of 2 are $2, 4, 1, 2, 4, 1, \ldots$ (period 3).

So,

$n \equiv 1 \pmod 3 \Rightarrow 61 + 2^n \equiv 0 \pmod 7$.

Also

$61 + 2^2 = 65, \quad \{5, 13\}.$

Mod 5, powers of 2 are $2, 4, 3, 1, \ldots$
(period 4).

So,

$n \equiv 2 \pmod 4 \Rightarrow 61 + 2^n \equiv 0 \pmod 5.$

Conclude:

$61 + 2^n$ is composite for

$$n \equiv 1 \pmod 2,$$
$$n \equiv 1 \pmod 3,$$
$$n \equiv 2 \pmod 4.$$

$n \equiv 1 \pmod 2$:

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$

$n \equiv 1 \pmod 3$:

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$

$n \equiv 2 \pmod 4$:

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$

$n \equiv 1 \pmod 2, n \equiv 1 \pmod 3$, or

$n \equiv 2 \pmod 4$:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \ldots$$

And, $61 + 2^8 = 317$, a prime.

So de Polignac is still safe, but not for long.

Lets automate the idea:

p	period of powers of 2
3	2
5	4
7	3
13	12
17	8
241	24

We can use the moduli 2, 4, 3, 12, 8, 24 to **cover** $\mathbb{Z}$:

Every $n \in \mathbb{Z}$ is either

$$\begin{array}{llll} 1 & (\text{mod } 2), & 2 & (\text{mod } 4), \\ 1 & (\text{mod } 3), & 8 & (\text{mod } 12), \\ 4 & (\text{mod } 8), & 0 & (\text{mod } 24). \end{array}$$

So, if k **simultaneously** is

$$\begin{aligned} -2^1 &\pmod 3, & -2^2 &\pmod 5, \\ -2^1 &\pmod 7, & -2^8 &\pmod{13}, \\ -2^4 &\pmod{17}, & -2^0 &\pmod{241}, \end{aligned}$$

then $\gcd(2^n + k, 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241) > 1$ for all n.

We also ask for k to be odd. By the magic of the Chinese Remainder Theorem, we can find an infinite arithmetic progression of such numbers k:

$$k \equiv 9\,262\,111 \pmod{11\,184\,810}.$$

In particular, $2^n + 9\,262\,111$ is composite for all n.

Erdős (1950): *de Polignac's conjecture is false.*

Note, the same calculations show that $k \cdot 2^n + 1$ is composite for all n for the same values of k. Sierpiński had a short paper about such k in 1960.

An odd number k with $k \cdot 2^n + 1$ composite for all n is now known as a **Sierpiński number**. They are useful in finding factors of large Fermat numbers.

Conjecture (Selfridge): *The least Sierpiński number is* $k = 78\,557$.

In 2002, for all but 17 values of $k < 78\,557$, a prime had been found of the form $k \cdot 2^n + 1$. Thus began the website `www.seventeenorbust.com` (Helm and Norris). Now there are just 6 remaining values of k for which no prime is known:

10223, 21181, 22699, 24737, 55459, 67607.

They've only been looking for primes $k \cdot 2^n + 1$ with $n > 0$, so my contribution:

k	n	k	n
10223	$-$ 19	21181	$-$ 28
22699	$-$ 26	24737	$-$ 17
55459	$-$ 14	67607	$-$ 16389

Seventeen or bust? Busted!

Unsolved:

Erdős: If k is a Sierpiński number, must the sequence of least prime factors of $k \cdot 2^n + 1$ be bounded?

Filaseta, Finch, Kozek: Is the sequence of least prime factors of $5 \cdot 2^n + 1$ unbounded?

Erdős: Lets forget about powers of 2 and just look for congruences that cover $\mathbb{Z}$.

For example: 0 (mod 1)

Another example: 0 (mod 2), 1 (mod 2)

Too easy!

Insist that the moduli be distinct and > 1.

Example: $0 \pmod 2$, $0 \pmod 3$,

$1 \pmod 4$, $1 \pmod 6$, $11 \pmod{12}$

What about least modulus > 2?, > 3?, ...

Conjecture (Erdős, 1950): *For each number B, one can cover $\mathbb{Z}$ with finitely many congruences to distinct moduli all $> B$.*

Erdős (1995):

"Perhaps this is my favorite problem."

Records:

least modulus	discovered by
9	Churchhouse (1968)
18	Krukenberg (1971)
20	Choi (1971)
24	Morikawa (1981)
25	Gibson (2006)
36	Nielsen (2007)

Erdős, Selfridge: Is there a covering of $\mathbb{Z}$ with distinct odd moduli > 1?

Erdős: Yes.

Selfridge: No.

Note: 0 (mod 2), 1 (mod 2) *exactly* covers $\mathbb{Z}$ in that each n satisfies exactly one congruence.

Erdős: Can one exactly cover $\mathbb{Z}$ with distinct moduli > 1?

Mirsky, Newman, Znam: *No.*

Say $\{a_i \pmod{b_i}\}$, $i \leq k$, exactly covers $\mathbb{Z}$.

Numbers $\equiv a \pmod{b}$ are represented by

$$z^a + z^{a+b} + z^{a+2b} + \cdots = \frac{z^a}{1 - z^b}.$$

So,

$$\sum_{i=1}^{k} \frac{z^{a_i}}{1 - z^{b_i}} = \frac{1}{1 - z},$$

and the largest b_i is 1 or is repeated.

Note: A covering $\{a_i \pmod{b_i}\}$ is exact iff $\sum 1/b_i = 1$.

Can one have a covering with distinct moduli $b_i > 1$ and $\sum 1/b_i$ arbitrarily close to 1?

Yes, take progressions $2^{i-1} \pmod{2^i}$ for $i = 1, 2, \ldots, 1000$, say. This covers everything except $0 \pmod{2^{1000}}$. Cover this with $0 \pmod{2 \cdot 2^{1000}}$, $0 \pmod{3 \cdot 2^{1000}}$, etc., where we are copying over the 0 (mod 2), 0 (mod 3), etc. covering from before.

Similarly, one can find coverings with distinct moduli with least modulus 3, and with least modulus 4, with the moduli reciprocal sum arbitrarily close to 1.

What about least modulus 5, or larger?

Conjecture (Erdős, Selfridge). *For each* N *there is a* B*: if* $\{a_i \pmod{b_i}\}$ *is a covering with distinct moduli* $> B$*, then* $\sum 1/b_i > N$.

Theorem. *Yes.*

(Filaseta, Ford, Konyagin, P, Yu 2007).

Corollary. *For each $K > 1$, there is some B_0 so that for $B \geq B_0$ there is no covering with distinct moduli from $[B, KB]$.*

Conjecture (Erdős, Graham). *For each $K > 1$, there are $d_K > 0, B_0$ such that for $B \geq B_0$ and for any congruences with distinct moduli from $[B, KB]$, at least density d_K of $\mathbb{Z}$ remains uncovered.*

Theorem. *Yes.*

(Filaseta, Ford, Konyagin, P, Yu 2007).

In fact, any d_K with $0 < d_K < 1/K$ works.

For example, if B is large, at most $1/2 + \epsilon$ of $\mathbb{Z}$ can be covered with congruences with distinct moduli from $[B, 2B]$.

In analogy to the Lovász local lemma:

Suppose we have moduli $b_1, \ldots, b_t$. *Let*

$$\alpha = \prod\left(1 - \frac{1}{b_i}\right), \quad \beta = \sum_{\substack{i<j \\ \gcd(b_i,b_j)>1}} \frac{1}{b_i b_j}.$$

Then no matter the choice of residues, at least $\alpha - \beta$ *of* $\mathbb{Z}$ *remains uncovered.*

R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, 2nd ed., Springer, 2005.

M. Filaseta, K. Ford, S. Konyagin, C. Pomerance, and G. Yu, Sieving by large integers and covering systems of congruences, *J. Amer. Math. Soc.*, **20** (2007), 496–517.

M. Filaseta, C. Finch, and M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers, and Polignac's conjecture, *J. Number Theory*, to appear.

D. Gibson, Covering systems, Doctoral diss. UIUC, 2006.

R. Guy, *Unsolved problems in number theory*, 3rd ed., Springer, 2004.

P. Nielsen, A covering system whose smallest modulus is large, preprint, 2007.