# Recent Advances in Covering Problems

by Michael Filaseta
University of South Carolina

---

**Background:**

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}, \qquad j = 1, 2, \dots, r,$$

with $a_j$ and $m_j$ integral and with $m_j \geq 1$, such that every integer satisfies at least one of the congruences.

---

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}, \qquad j = 1, 2, \dots, r,$$

with $a_j$ and $m_j$ integral and with $m_j \geq 1$, such that every integer satisfies at least one of the congruences.

$$\boxed{\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 3 \pmod{12} \end{aligned}}$$

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{8} \\ x &\equiv 7 \pmod{12} \\ x &\equiv 23 \pmod{24} \end{aligned}$$

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

---

Classical Result: If the moduli in a covering are distinct and $> 1$, then the sum of the reciprocals of the moduli exceeds 1.

$$x \equiv a_j \pmod{m_j} \qquad (1 \leq j \leq r)$$

$$\begin{aligned} \frac{1}{1-z} &= \sum_{j=1}^{r} \left( z^{a_j} + z^{a_j+m_j} + z^{a_j+2m_j} + \dots \right) \\ &= \sum_{j=1}^{r} \frac{z^{a_j}}{1 - z^{m_j}} \end{aligned}$$

Version 1: Let $z$ approach $\zeta_{\max\{m_j\}}$.

---

Question: Given $c > 0$, is there a covering using only distinct moduli $\geq c$?

Question: Does there exist a covering consisting of distinct odd moduli $> 1$?

Theorem (W. Sierpinski): *A positive proportion of odd positive integers $k$ satisfy $k \times 2^n + 1$ is composite for all positive integers $n$.*

---

Theorem (W. Sierpinski): *A positive proportion of odd positive integers $k$ satisfy $k \times 2^n + 1$ is composite for all positive integers $n$.*

Sierpinski's Argument:

Covering

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 4 \pmod{8} \\ x &\equiv 8 \pmod{16} \\ x &\equiv 16 \pmod{32} \\ x &\equiv 32 \pmod{64} \end{aligned}$$

---

Theorem (W. Sierpinski): *A positive proportion of odd positive integers $k$ satisfy $k \times 2^n + 1$ is composite for all positive integers $n$.*

Sierpinski's Argument:

| Covering | Apply the Chinese Remainder Theorem |
|---|---|
| $x \equiv 1 \pmod{2}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{3}$ |
| $x \equiv 2 \pmod{4}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{5}$ |
| $x \equiv 4 \pmod{8}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{17}$ |
| $x \equiv 8 \pmod{16}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{257}$ |
| $x \equiv 16 \pmod{32}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{65537}$ |
| $x \equiv 32 \pmod{64}$ $\longleftrightarrow$ | $k \equiv 1 \pmod{641}$ |
| $x \equiv 0 \pmod{64}$ $\longleftrightarrow$ | $k \equiv -1 \pmod{6700417}$ |

---

Theorem (W. Sierpinski): *A positive proportion of odd positive integers $k$ satisfy $k \times 2^n + 1$ is composite for all positive integers $n$.*

Sierpinski (1960): $k = 15511380746462593381$

Definition: A *Sierpinski number* is an odd positive integer $k$ with the property that $k \times 2^n + 1$ is composite for all nonnegative integers $n$.

---

Sierpinski (1960): $k = 15511380746462593381$

Selfridge (1962): $k = 78557$

Selfridge's Argument:

$k$ an odd positive integer, $k \times 2^n + 1$ composite $\forall n$

| | |
|---|---|
| $n \equiv 0 \pmod{2}$ | $k \equiv 2 \pmod{3}$ |
| $n \equiv 1 \pmod{4}$ | $k \equiv 2 \pmod{5}$ |
| $n \equiv 3 \pmod{36}$ | $k \equiv 9 \pmod{73}$ |
| $n \equiv 15 \pmod{36}$ | $k \equiv 11 \pmod{19}$ |
| $n \equiv 27 \pmod{36}$ | $k \equiv 6 \pmod{37}$ |
| $n \equiv 7 \pmod{12}$ | $k \equiv 3 \pmod{7}$ |
| $n \equiv 11 \pmod{12}$ | $k \equiv 11 \pmod{13}$ |

Sierpinski (1960): $k = 15511380746462593381$

Selfridge (1962): $k = 78557$

$k$ an odd positive integer, $k \times 2^n + 1$ composite $\forall n$

Why odd?

The common belief is that Fermat numbers $2^{2^n} + 1$ are composite for all $n \geq 5$.

It follows that $k \times 2^n + 1$ is likely composite for every positive integer $n$ when $k = 2^{16} = 65536$.

---

Sierpinski (1960): $k = 15511380746462593381$

Selfridge (1962): $k = 78557$

$k$ an odd positive integer, $k \times 2^n + 1$ composite $\forall n$

What's the smallest *odd* $k$?

The "belief" is that it is 78557.

Work has been done and continues to be done to establish this.

Idea: For each positive odd integer $< 78557$, find a positive integer $n$ for which $k \times 2^n + 1$ is prime.

---

Idea: For each positive odd integer $< 78557$, find a positive integer $n$ for which $k \times 2^n + 1$ is prime.

As of December 30, 2004, there are 10 values of $k < 78557$ for which a prime of the form $k \times 2^n + 1$ is not known.

$$4847,\ 10223,\ 19249,\ 21181,\ 22699,$$
$$24737,\ 27653,\ 33661,\ 55459,\ 67607$$

Theorem (M. F. Proth, 1878): *Let* $N = k \times 2^n + 1$ *with* $2^n > k$. *If there is an integer* $a$ *such that* $a^{(N-1)/2} \equiv -1 \pmod{N}$, *then* $N$ *is prime.*

---

```
> d:=product(ithprime(j),j=1..7):
> for n from 1 to 100 do
    lprint(n,gcd(4847*2^n+1,d)):
  od:
1, 35
2, 3
3, 17
4, 21
5, 5
6, 3
7, 7
8, 33
9, 5
10, 21
11, 221
12, 3
13, 35
```

---

```
> d:=product(ithprime(j),j=1..7):
> for n from 1 to 100 do
    if gcd(4847*2^n+1,d)=1 then lprint(n): fi:
  od:
15
39
63
87
```

---

```
> d:=product(ithprime(j),j=1..1000):
> for n from 0 to 30 do
    if gcd(4847*2^(24*n+15)+1,d) = 1 then
      lprint(n):
    fi:
  od:
2
3
4
8
12
13
14
17
19
24
```

---

```
> ifactor(4847*2^63+1);
          (13299816775727)(416579)(8069)
> ifactor(4847*2^87+1);
     (97089101)(326883732123650549)(23633)
> ifactor(4847*2^111+1);
  (831141357131)(15140061709955081291592547)
> order(2,831141357131);
                 831141357130
```

---

Unsolved Problems in Number Theory
by Richard Guy (Edition 2, Section F13)

> *Erdős conjectures that all sequences of the form $d \cdot 2^k + 1$ $(k = 1, 2, \ldots)$, $d$ fixed and odd, which contain no primes can be obtained from covering congruences .... Equivalently, the least prime factors of members of such sequences are bounded.*

---

Probable Counterexample:
Due to Anatoly Izotov, 1995.

| Sierpinski's Congruences | Counterexample |
|---|---|
| $k \equiv 1 \pmod{3}$ | $\ell \equiv 1 \pmod{3}$ |
| $k \equiv 1 \pmod{5}$ | |
| $k \equiv 1 \pmod{17}$ | $\ell \equiv 1 \pmod{17}$ |
| $k \equiv 1 \pmod{257}$ | $\ell \equiv 1 \pmod{257}$ |
| $k \equiv 1 \pmod{65537}$ | $\ell \equiv 1 \pmod{65537}$ |
| $k \equiv 1 \pmod{641}$ | $\ell \equiv 1 \pmod{641}$ |
| $k \equiv -1 \pmod{6700417}$ | $\ell \equiv 2^8 \pmod{6700417}$ |

$$\mathcal{P} = \{3, 17, 257, 65537, 641, 6700417\}$$

$$\ell^4 \equiv k \pmod{p}, \quad \forall p \in \mathcal{P}$$

$$
\begin{array}{ll}
k \equiv 1 \pmod{3} & \ell \equiv 1 \pmod{3} \\
k \equiv 1 \pmod{5} & \\
k \equiv 1 \pmod{17} & \ell \equiv 1 \pmod{17} \\
k \equiv 1 \pmod{257} & \ell \equiv 1 \pmod{257} \\
k \equiv 1 \pmod{65537} & \ell \equiv 1 \pmod{65537} \\
k \equiv 1 \pmod{641} & \ell \equiv 1 \pmod{641} \\
k \equiv -1 \pmod{6700417} & \ell \equiv 2^8 \pmod{6700417}
\end{array}
$$

$$\mathcal{P} = \{3, 17, 257, 65537, 641, 6700417\}$$

$$\ell^4 \equiv k \pmod{p}, \quad \forall p \in \mathcal{P}$$

$$\ell^4 \cdot 2^n + 1 \equiv k \cdot 2^n + 1 \pmod{p}, \quad \forall p \in \mathcal{P}$$

some $p \in \mathcal{P}$ divides $\ell^4 \cdot 2^n + 1$ unless

---

$$
\begin{array}{ll}
k \equiv 1 \pmod{3} & \ell \equiv 1 \pmod{3} \\
k \equiv 1 \pmod{5} & \\
k \equiv 1 \pmod{17} & \ell \equiv 1 \pmod{17} \\
k \equiv 1 \pmod{257} & \ell \equiv 1 \pmod{257} \\
k \equiv 1 \pmod{65537} & \ell \equiv 1 \pmod{65537} \\
k \equiv 1 \pmod{641} & \ell \equiv 1 \pmod{641} \\
k \equiv -1 \pmod{6700417} & \ell \equiv 2^8 \pmod{6700417}
\end{array}
$$

$$\mathcal{P} = \{3, 17, 257, 65537, 641, 6700417\}$$

$$\ell^4 \equiv k \pmod{p}, \quad \forall p \in \mathcal{P}$$

$$\ell^4 \cdot 2^n + 1 \equiv k \cdot 2^n + 1 \pmod{p}, \quad \forall p \in \mathcal{P}$$

some $p \in \mathcal{P}$ divides $\ell^4 \cdot 2^n + 1$ unless $n \equiv 2 \pmod 4$

$$n \equiv 2 \pmod 4 \implies \ell^4 \cdot 2^n + 1 = 4x^4 + 1$$

$$4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$$

---

$$
\begin{array}{ll}
k \equiv 1 \pmod{3} & \ell \equiv 1 \pmod{3} \\
k \equiv 1 \pmod{5} & \\
k \equiv 1 \pmod{17} & \ell \equiv 1 \pmod{17} \\
k \equiv 1 \pmod{257} & \ell \equiv 1 \pmod{257} \\
k \equiv 1 \pmod{65537} & \ell \equiv 1 \pmod{65537} \\
k \equiv 1 \pmod{641} & \ell \equiv 1 \pmod{641} \\
k \equiv -1 \pmod{6700417} & \ell \equiv 2^8 \pmod{6700417}
\end{array}
$$

$\ell^4 \cdot 2^n + 1$ is composite for all positive integers $n$

Chinese Remainder Theorem implies
$\ell \equiv 3479268342425187502$
$\bmod (3 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417)$

---

$$
\begin{array}{ll}
k \equiv 1 \pmod{3} & \ell \equiv 1 \pmod{3} \\
k \equiv 1 \pmod{5} & \\
k \equiv 1 \pmod{17} & \ell \equiv 1 \pmod{17} \\
k \equiv 1 \pmod{257} & \ell \equiv 1 \pmod{257} \\
k \equiv 1 \pmod{65537} & \ell \equiv 1 \pmod{65537} \\
k \equiv 1 \pmod{641} & \ell \equiv 1 \pmod{641} \\
k \equiv -1 \pmod{6700417} & \ell \equiv 2^8 \pmod{6700417}
\end{array}
$$

$\ell^4 \cdot 2^n + 1$ is composite for all positive integers $n$

Chinese Remainder Theorem implies
$\ell \equiv 716861715716709782 5$
$\bmod (3 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417)$

---

Remarks: *Let $\ell \equiv 7168617157167097825$ modulo*

$$2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417.$$

*Then $\ell^4 \times 2^n + 1$ is composite for all positive $n \in \mathbb{Z}^+$. Furthermore, the least prime divisor of $\ell^4 \times 2^n + 1$ "appears" to be unbounded as $n \to \infty$.*

---

Remarks: *Let $\ell \equiv 7168617157167097825$ modulo*

$$2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417.$$

*Then $\ell^4 \times 2^n + 1$ is composite for all positive $n \in \mathbb{Z}^+$. Furthermore, the least prime divisor of $\ell^4 \times 2^n + 1$ "appears" to be unbounded as $n \to \infty$.*

---

Remarks: *Let $\ell \equiv 856437595$ modulo*

$$2 \cdot 3 \cdot 5 \cdot 17 \cdot 97 \cdot 241 \cdot 257 \cdot 673.$$

*Then $\ell^4 \times 2^n + 1$ is composite for all positive $n \in \mathbb{Z}^+$. Furthermore, the least prime divisor of $\ell^4 \times 2^n + 1$ "appears" to be unbounded as $n \to \infty$.*

---

```
> d:=product(ithprime(j),j=1..1000):
> ell:=856437595^4:
> for n from 0 to 100 do
    if gcd(ell*2^(4*n+2)+1,d)=1 then
      lprint(n):
    fi:
  od:
0
3
7
9
25
27
33
53
54
66
```

---

```
> ifactor(ell*2^394 + 1):
(7098991021)(3883605819146153)
(37937215288639472482907054298118055687 2...4297)
(20754102888892871830241569611095660593 3...2341)
```

## Miscellaneous Remarks and Questions

Question: Is 78557 the smallest Sierpinski number?

Question: Is 4847 a Sierpinski number?

Question: Is $856437595^4$ the smallest example of a Sierpinski number that "likely" cannot be obtained from coverings?

Remark: This Sierpinski number has interesting heuristics associated with it. As $856437595^4 \cdot 2^n + 1$ is of the form $4x^4 + 1$ for $n \equiv 2 \pmod 4$, it is likely that for such $n$ the number of prime factors of $856437595^4 \cdot 2^n + 1$ tends to infinity with $n$. The analogous heuristic does not hold for Sierpinski numbers constucted by coverings.

## Miscellaneous Remarks and Questions

Remark: The number 271129 is the second smallest known Sierpinski number. It is a prime.

Question: Is 271129 the smallest prime that is a Sierpinski number?

Question: Are there any prime Sierpinski numbers that cannot be obtained from coverings? In other words, if $p$ is a prime and $p \cdot 2^n + 1$ is composite for all positive integers $n$, then is it the case that the smallest prime factor of $p \cdot 2^n + 1$ is bounded as $n$ tends to infinity?

## Miscellaneous Remarks and Questions

Definition: A *Riesel number* is an odd positive integer $k$ for which $k \cdot 2^n - 1$ is composite for all positive integers $n$.

Question: Is 509203 the smallest Riesel number?

Question: Is 2293 a Riesel number?

Definition: A *Brier number* is an odd positive integer $k$ for which $k \cdot 2^n \pm 1$ is composite for all positive integers $n$. In other words, a Brier number is an odd positive integer for which $k \cdot 2^n$ is not adjacent to a prime for every positive integer $n$.

Question: Is 878503122374924101526292469 the least Brier number?

## Miscellaneous Remarks and Questions

Remark: An example of a Riesel number that "likely" does not come from coverings is:

$$7202057536340330005772745051833205761872129947928766 7^2$$

Calling this example $\ell^2$, we see that $\ell^2 2^n - 1$ is composite whenever $n$ is even. For odd $n$, a covering is used with the 20 moduli

$$7,\ 17,\ 31,\ 41,\ 71,\ 97,\ 113,\ 127,\ 151,\ 241,\ 257,\ 281,\ 337,\ 641,\ 673,\ 1321,\ 14449,\ 29191,\ 65537,\ 6700417.$$

## Miscellaneous Remarks and Questions

Question: What's the smallest Riesel number that is likely not obtainable from coverings?

Question: Are there examples of Brier numbers that cannot be obtained from coverings?

## Miscellaneous Remarks and Questions

Polignac's Conjecture: *For every sufficiently large odd positive integer $k$, there is a prime $p$ and an integer $n$ such that $k = 2^n + p$.*

Examples of odd $k$ not as above are:

$$127,\ 149,\ 251,\ 331,\ 337,\ 373,\ 509$$

The first composite $k > 1$ as above is 905.

## Miscellaneous Remarks and Questions

Polignac's Conjecture: *For every sufficiently large odd positive integer $k$, there is a prime $p$ and an integer $n$ such that $k = 2^n + p$.*

Erdős gave a construction of infinitely many such $k$ (not satisfying the conjecture above) by taking

$$k \equiv 1 \pmod 2,\quad k \equiv 1 \pmod 3,\quad k \equiv 2 \pmod 5,$$
$$k \equiv 1 \pmod 7,\quad k \equiv 11 \pmod{13},$$
$$k \equiv 8 \pmod{17},\quad k \equiv 121 \pmod{241}.$$

## Miscellaneous Remarks and Questions

Unsolved Problems in Number Theory
by Richard Guy (Edition 1, Section F13)

> *Erdős also formulates the following conjecture. Consider all the arithmetic progressions of odd numbers, no term of which is of the form $2^k + p$. Is it true that all these progressions can be obtained from covering congruences? Are there infinitely many integers, not of the form $2^k + p$, which are not in such progressions?*

Note: Switching notation, we want $k$ with $k - 2^n$ not prime for all positive integers $n$.

## Miscellaneous Remarks and Questions

Note: Switching notation, we want $k$ with $k - 2^n$ not prime for all positive integers $n$.

Idea: To get an example that is not derived from a covering, take $k = \ell^2$ and note that when $n \equiv 0 \pmod 2$ the number $k - 2^n$ factors.

Claim: The example of the Riesel number $\ell^2$ is a likely counterexample for the $2^{\text{nd}}$ Erdős conjecture.

Miscellaneous Remarks and Questions

Claim: The example of the Riesel number $\ell^2$ is a likely counterexample for the 2nd Erdős conjecture.

Proof: If $n$ is even, both $\ell^2 2^n - 1$ and $\ell^2 - 2^n$ factor (one needs to check that each has two factors $> 1$). For each odd $n$, the number $\ell^2 2^n - 1$ is divisible by a prime from a fixed finite set $\mathcal{S}$. Let $P$ be the product of the primes in $\mathcal{S}$, and let $m$ be a positive odd integer for which $2^m \equiv 2^{-1} \pmod{P}$ (one can take $m = \phi(P) - 1$). Let $n$ be an arbitrary odd number. There is a prime $p \in \mathcal{S}$ such that $p$ divides $\ell^2 2^{nm} - 1$. Then $p$ divides

$$\ell^2 2^{nm+n} - 2^n \equiv \ell^2 - 2^n \pmod{p}. \quad \blacksquare$$

Miscellaneous Remarks and Questions

Seemingly, we have infinitely many numbers not of the from $2^n + p$ which do not lie in an arithmetic progression arising from coverings. These are given by $\ell^2$ where

$$\ell \equiv 7202057536340330005772745051833205761872129947928766 7 \pmod{27947898258323881972182646521842901866274453744090525 62}.$$

Question: What is the smallest example of a number of the form $2^n + p$ which does not lie in an arithmetic progression arising from coverings?

Question: Are there proofs that these apparent counterexamples are in fact counterexamples?

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Chen established that such $k$ exist if $r$ is odd or both $r \equiv 2 \pmod{4}$ and $3 \nmid r$.

Carrie Finch and Mark Kozek were given the task of resolving the conjecture by possibly making use of "partial coverings" (which Chen had not done). We were able to resolve the conjecture, in the end without using partial coverings.

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Some of what was involved:

- We may suppose that $r$ is big.

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Some of what was involved:

- We may suppose that $r$ is big.

Chen's Conjecture: *For each positive integer $r$, there are infinitely many positive odd integers $k$ such that $k^r 2^n + 1$ has at least two distinct prime divisors for all positive integers $n$.*

Some of what was involved:

- We may suppose that $r$ is big.
- At least two distinct prime divisors follows from any covering argument.

- At least two distinct prime divisors follows from any covering argument.

  Fix $r$. A covering produces $k$ and a finite set

  $$\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$$

  of primes such that $k^r 2^n + 1$ is always divisible by some prime from $\mathcal{P}$. The equation

  $$k^r 2^n + 1 = p_j^{e_j}$$

  can be rewritten in the form

  $$ax^r - by^r = 1,$$

  which has finitely many solutions.

Some of what was involved:

- We may suppose that $r$ is big.
- At least two distinct prime divisors follows from any covering argument.
- Find a covering construction.

- Find a covering construction.

$$\begin{aligned} \ell &\equiv 1 \pmod{p_1} \\ \ell &\equiv 1 \pmod{p_2} \\ \ell &\equiv 1 \pmod{p_3} \\ &\vdots \quad \vdots \\ \ell &\equiv 1 \pmod{p_{s-1}} \\ \ell &\equiv 1 \pmod{p_s} \end{aligned}$$

$$\ell = k^r$$

$$p_j | (2^{2^{j-1}} + 1)$$

plus more congruences

"More" congruences are for covering $n \equiv 0 \pmod{2^s}$.

- Find a covering construction.

Lemma: Let $t > 2$. Let $q$ be an odd prime. If $p$ is a primitive prime divisor of $2^{q \cdot 2^t} - 1$, then both

(i) $-1$ is a $2^t$th power modulo $p$

(ii) 2 has order $q \cdot 2^t$ modulo $p$

Idea: Take $q$ so that $q \nmid r$. Imagine $s$ is very large. Let $p'_j$ be a primitive prime divisor of $2^{q \cdot 2^{s+1-j}} - 1$ for $j \in \{1, 2, \ldots, q\}$. Create "more" congruences modulo these $p'_j$'s to cover $n \equiv 0 \pmod{2^s}$.

## Conjectures Concerning a Large Minimum Modulus

Joint Work With: Kevin Ford, Sergei Konyagin, Carl Pomerance and Gang Yu

Question: Given $c > 0$, is there a covering using only distinct moduli $\geq c$?

Erdős: *This is perhaps my favourite problem.*

Question: What conditions can we impose on the moduli that would cause no covering to exist?

Conjecture 1 (Erdős and Selfridge): For any $B$, there is an $N_B$, such that in a covering system with distinct moduli greater than $N_B$, the sum of reciprocals of these moduli is greater than $B$.

Conjecture 2 (Erdős and Graham): For each $K > 1$, there is a positive $d_K$ such that if $N$ is sufficiently large, depending on $K$, and we choose arbitrary integers $r(n)$ for each $n \in (N, KN]$, then the complement in $\mathbb{Z}$ of the union of the residue classes $r(n) \pmod{n}$ has density at least $d_K$.

Conjecture 3 (Erdős and Graham): For any $K > 1$ and $N$ sufficiently large, depending on $K$, there is no covering system using distinct moduli from the interval $(N, KN]$.

Conjecture 1 (Erdős and Selfridge): Fix $B$. If $N$ is sufficiently large and a covering consists of distinct moduli $m_1, m_2, \ldots, m_r$ each exceeding $N$, then

$$\sum_{j=1}^{r} \frac{1}{m_j} > B.$$

Theorem: Let $0 < c < 1/3$ and let $N$ be sufficiently large (depending on $c$). If $S$ is a set of integers $> N$ such that

$$\sum_{n \in S} \frac{1}{n} \leq c \frac{\log N \log\log\log N}{\log\log N},$$

then any system of congruences consisting of distinct moduli from $S$ cannot cover all of $\mathbb{Z}$.

$$x \equiv a_j \pmod{m_j} \qquad (1 \leq j \leq r)$$

Question: What is the density of integers which are not covered by these congruences?

If the moduli are pairwise relatively prime, then the density is

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right).$$

If the moduli are large, then on average the density is $\approx \alpha$. By choosing the $a_j$ carefully, one can always make the density $\leq \alpha$. By choosing the $a_j$ and $m_j$ carefully, one can make the density much smaller than $\alpha$.

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right)$$

Suppose the set of moduli $S = \{m_1, \ldots, m_r\}$ is $(N, KN] \cap \mathbb{Z}$.

Then

$$\alpha = \prod_{m=N+1}^{KN} \left(1 - \frac{1}{m}\right) = \prod_{m=N+1}^{KN} \left(\frac{m-1}{m}\right) = \frac{1}{K}.$$

Conjecture 2 (Erdős and Graham): For each $K > 1$, there is a positive $d_K$ such that if $N$ is sufficiently large, depending on $K$, and we choose arbitrary integers $r(n)$ for each $n \in (N, KN]$, then the complement in $\mathbb{Z}$ of the union of the residue classes $r(n) \pmod{n}$ has density at least $d_K$.

Theorem: For any numbers $c$ with $0 < c < 1/2$, $N \geq 20$, and $K$ with

$$1 < K \leq \exp(c \log N \log\log\log N / \log\log N),$$

if $S$ is a set of integers contained in $(N, KN]$, then the minimal density of integers not covered when using distinct moduli from $S$ is $(1 + o(1))\alpha(S)$ as $N \to \infty$.

Theorem: For any numbers $c$ with $0 < c < 1/2$, $N \geq 20$, and $K$ with

$$1 < K \leq \exp(c \log N \log\log\log N / \log\log N),$$

if $S$ is a set of integers contained in $(N, KN]$, then the minimal density of integers not covered when using distinct moduli from $S$ is $(1 + o(1))\alpha(S)$ as $N \to \infty$.

Notation:

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right) \qquad \beta = \sum_{\substack{i<j \\ \gcd(m_i, m_j) > 1}} \frac{1}{m_i m_j}$$

Notation:

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right) \qquad \beta = \sum_{\substack{i<j \\ \gcd(m_i, m_j) > 1}} \frac{1}{m_i m_j}$$

Rough Ideas:

- Recall we can make the density $\delta \leq \alpha$.
- We show $\delta \geq \alpha - \beta$.

$$\alpha \geq \text{minimal density } \delta \geq \alpha - \beta$$

Comment: The quantities $\alpha$ and $\beta$ are so difficult to estimate when we consider the moduli to be square-free integers with each prime divisor in an interval

$$(e^{\sqrt{N}\log N}, N].$$

This can be used to give the following improvement of a result of J. A. Haight (1979):

Theorem: There is an infinite set of positive integers $H$ such that for any residue system $C$ with distinct moduli from $\{d : d > 1,\ d \mid H\}$, the density of integers not covered is at least $(1+o(1))\alpha(C)$ and

$$\sigma(H)/H = (\log\log H)^{1/2} + O(\log\log\log H).$$

Notation:

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right) \qquad \beta = \sum_{\substack{i<j \\ \gcd(m_i, m_j) > 1}} \frac{1}{m_i m_j}$$

Rough Ideas:

- Recall we can make the density $\delta \leq \alpha$.
- We show $\delta \geq \alpha - \beta$.
- Split up the contribution from small primes dividing the moduli and large primes.

Lemma: Let $C$ be an arbitrary residue system. Let $P$ be an arbitrary finite set of primes, and set

$$M = \prod_{p \in P} p^{\nu(p)},$$

where $\nu(p)$ is the exponent of $p$ in the factorization of $\operatorname{lcm}\{m : m \text{ a modulus}\}$. For $0 \leq h \leq M - 1$, let $C_h$ be the multiset of pairs

$$\left(\frac{m}{\gcd(m, M)}, a\right)$$

where $(m, a) \in C$, $a \equiv h \pmod{\gcd(m, M)}$. Then

$$\delta(C) = \frac{1}{M} \sum_{h=0}^{M-1} \delta(C_h).$$

Notation:

$$\alpha = \prod_{j=1}^{r} \left(1 - \frac{1}{m_j}\right) \qquad \beta = \sum_{\substack{i<j \\ \gcd(m_i, m_j) > 1}} \frac{1}{m_i m_j}$$

Rough Ideas:

- Recall we can make the density $\delta \leq \alpha$.
- We show $\delta \geq \alpha - \beta$.
- Split up the contribution from small primes dividing the moduli and large primes.
- Use $\delta(C_h) \geq \alpha(C_h) - \beta(C_h)$ and estimates for $\alpha(C_h)$ and $\beta(C_h)$.

# The End