A covering of the integers is a system of congruences

\[ x \equiv a_j \pmod{m_j}, \quad j = 1, 2, \ldots, r, \]

with \( a_j \) and \( m_j \) integral and with \( m_j \geq 1 \), such that every integer satisfies at least one of the congruences. We only consider \( r \) finite.

\[
\begin{align*}
    x &\equiv 0 \pmod{2} & x &\equiv 0 \pmod{2} \\
    x &\equiv 0 \pmod{3} & x &\equiv 1 \pmod{4} \\
    x &\equiv 1 \pmod{4} & x &\equiv 3 \pmod{8} \\
    x &\equiv 1 \pmod{6} & x &\equiv 7 \pmod{12} \\
    x &\equiv 3 \pmod{12} & x &\equiv 23 \pmod{24}
\end{align*}
\]

Open Problem: What are $\lim \inf_{x \to \infty} \rho(x)$ and $\lim \sup_{x \to \infty} \rho(x)$?

$R(x) = \#\{n \leq x : n \in \mathbb{Z}^+, n \text{ odd,}\}$

$$\exists k \in \mathbb{Z}^+, \exists p \text{ prime with } n = 2^k + p$$

$$\rho(x) = \frac{R(x)}{\lfloor x/2 \rfloor}$$

Open Problem: What are $\lim \inf_{x \to \infty} \rho(x)$ and $\lim \sup_{x \to \infty} \rho(x)$?

$$\lim \inf_{x \to \infty} \rho(x) \geq 0.1873 \quad (\text{Pintz, 2006})$$

$$\lim \sup_{x \to \infty} \rho(x) \leq 0.9819 \quad (\text{Habsieger & Roblot, 2006})$$

$$\lim_{x \to \infty} \rho(x) \approx 0.868 \quad (\text{heuristics by Romani, 1983})$$

Zhi-Wei Sun (1999): If

$$k \equiv 47867742232066880047611079 \pmod{66483034025018711639862527490},$$

then $k$ is not of the form $\pm p^a \pm q^b$ where $p$ and $q$ are primes and $a$ and $b$ are nonnegative integers.

Open Problem: What is the least positive integer not expressible in this form?

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

Comment: For an “exact” covering where every integer satisfies exactly one congruence in a finite system of congruences, it is known that the largest modulus must be used at least twice. Looking at the density of integers covered by a congruence, the above result follows.

Question: If the moduli are distinct and $> 1$, how close to 1 can the sum of the reciprocals of the moduli be?
\begin{align*}
x &\equiv 1 \pmod{2} \\
x &\equiv 2 \pmod{4} \\
x &\equiv 4 \pmod{8} \\
x &\equiv 8 \pmod{16} \\
\vdots \quad \vdots \\
x &\equiv 2^{100} \pmod{2^{101}} \\
x &\equiv 0 \pmod{2^{101}} \\
x &\equiv 0 \cdot 2^{101} \pmod{2^{101} \cdot 3} \\
x &\equiv 1 \cdot 2^{101} \pmod{2^{101} \cdot 3} \\
x &\equiv 2 \cdot 2^{101} \pmod{2^{101} \cdot 3} \\
x &\equiv 0 \cdot 2^{101} \pmod{2^{99} \cdot 3} \\
x &\equiv 1 \cdot 2^{101} \pmod{2^{100} \cdot 3} \\
x &\equiv 2 \cdot 2^{101} \pmod{2^{101} \cdot 3}
\end{align*}

Conclusion: In a covering system, the moduli can be distinct and $> 1$ and the sum of the reciprocals of the moduli can be arbitrarily close to 1, if the minimum modulus is 2.

Further examples show that the moduli can also be distinct and $\geq 4$ and the sum of the reciprocals of the moduli can be arbitrarily close to 1.

Open Problem: If the moduli are distinct and if the minimum modulus is 5, can the sum of the reciprocals of the moduli be arbitrarily close to 1?

Open Problem: If the moduli are distinct and if the minimum modulus is 6, can the sum of the reciprocals of the moduli be arbitrarily close to 1?

Known (Ford, Konyagin, Pomerance, Yu, F., 2007): If the set of moduli $\mathcal{M}$ consists of distinct integers $\geq N$, where $N$ is sufficiently large, then

$$\sum_{m \in \mathcal{M}} \frac{1}{m} > \frac{\log N \log \log \log N}{4 \log \log N}.$$ 

Known (Sun Kim): There is an $\varepsilon > 0$ such that if the moduli are distinct and $\geq 10^{34}$ (approx.), then the sum of the reciprocals of the moduli is $> 1 + \varepsilon$.

Open Problem (Erdős, $1000$): For every $N$, does there exist a finite covering with distinct moduli all $\geq N$?
Known (Ford, Konyagin, Pomerance, Yu, F., 2007): If the set of moduli $\mathcal{M}$ consists of distinct integers $\geq N$, where $N$ is sufficiently large, then
\[
\sum_{m \in \mathcal{M}} \frac{1}{m} > \frac{\log N \log \log \log N}{4 \log N}.
\]

Open Problem (Erdős, $1000$): For every $N$, does there exist a finite covering with distinct moduli all $\geq N$?

Pace Nielsen (2009): There exists a finite covering with distinct moduli all $\geq 40$.

Erdős: This is perhaps my favourite problem.

Theorem (Riesel, 1956): A positive proportion of odd positive integers $k$ satisfy $k \cdot 2^n - 1$ is composite for all integers $n \geq 1$.

Such $k$ are known as Riesel numbers. They have not received as much attention as the Sierpiński numbers which we will talk about shortly, even though Riesel’s result predates that of Sierpiński. The reason for this may be that Riesel numbers are basically the same as those numbers constructed by Erdős in his 1950 paper mentioned earlier. To find positive odd integers $k$ that are not the sum of a prime and a power of 2, Erdős constructed $k$ for which $k - 2^n$ has a prime factor from the set $\{3, 5, 7, 13, 17, 241\}$.

Proposition: Let $\mathcal{P}$ be a finite set of odd primes, and let $k$ be an integer. Suppose that for every sufficiently large integer $n$ there is a $p \in \mathcal{P}$ for which
\[
(*) \quad k \cdot 2^n - 1 \equiv 0 \pmod{p}.
\]
Then for every integer $n$ there is a $p \in \mathcal{P}$ for which
\[
(**) \quad k - 2^n \equiv 0 \pmod{p}.
\]
Similarly, if for every sufficiently large $n$ there is a $p \in \mathcal{P}$ satisfying $(* *)$, then for every integer $n$ there is a $p \in \mathcal{P}$ satisfying $(* *)$.

Conclusion: Any covering argument for producing Riesel numbers also produces integers that are not the sum of a power of 2 and a prime, and vice-versa.
**The Riesel Problem: Definition and Status**

In 1956 Hans Riesel proved the following interesting result.

**Theorem.** There exist infinitely many odd integers $k$ such that $k2^n - 1$ is composite for every $n \geq 1$.

Actually, Riesel showed that $k_0 = 509203$ has this property, and also the multipliers $k_r = k_0 + 11184810r$ for $r = 1, 2, 3, \ldots$ Such numbers are now called Riesel numbers because of their similarity with the Sierpinski numbers. The Riesel problem consists in determining the smallest Riesel number.

**Conjecture.** The integer $k = 509203$ is the smallest Riesel number.

**Open Problem:** Is 509203 the least Riesel number?

**Open Problem:** Is 2293 a Riesel number?

**Note:** There is no prime of the form $2293 \cdot 2^n - 1$ for $1 \leq n \leq 2^{21} = 2097152$.

**Comments:**

- The smallest known Riesel number is 509203 and appears in Riesel’s 1956 paper on the problem.
- Work is being done to eliminate $k < 509203$ as Riesel numbers, see:
  
  [http://www.prothsearch.net/rieselprob.html](http://www.prothsearch.net/rieselprob.html)

Other Comments:

- The smallest known Riesel number is 509203 and appears in Riesel’s 1956 paper on the problem.
- Work is being done to eliminate $k < 509203$ as Riesel numbers, see:
  
  [http://www.prothsearch.net/rieselprob.html](http://www.prothsearch.net/rieselprob.html)

There are 64 numbers $< 509203$ which have not yet been eliminated as being Riesel numbers.

**Theorem (Sierpiński, 1960):** A positive proportion of odd positive integers $k$ are such that $k \cdot 2^n + 1$ is composite for all integers $n \geq 1$.

**Comments:**

- These $k$ are called Sierpiński numbers.
- Schinzel has pointed out that there is a one-to-one correspondence between Sierpiński numbers and numbers not expressible in the form $2^n + p$ (though the connection is not as direct as Riesel numbers).

**Selfridge (1962) showed that 78557 is a Sierpiński number (the smallest known).**

**Schinzel has pointed out that there is a one-to-one correspondence between Sierpiński numbers and numbers not expressible in the form $2^n + p$ (though the connection is not as direct as Riesel numbers).**
Selfridge (1962) showed that 78557 is a Sierpiński number (the smallest known).

In March of 2002 when there were 17 numbers < 78557 which were not yet eliminated as being Sierpiński numbers. Helm and Norris began the Seventeen or Bust project to eliminate these 17 possibilities:

http://www.seventeenorbust.com

Selfridge (1962) showed that 78557 is a Sierpiński number (the smallest known).

In March of 2002 when there were 17 numbers < 78557 which were not yet eliminated as being Sierpiński numbers. Helm and Norris began the Seventeen or Bust project to eliminate these 17 possibilities:

http://www.seventeenorbust.com

There are 6 numbers left to eliminate:

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

Open Problem: Is 78557 the smallest Sierpiński number?

Unsolved Problems in Number Theory by Richard Guy (Edition 3, Section F13)

Unsolved Problems in Number Theory

by Richard Guy

Problem Books in Mathematics

Springer

Third Edition

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 (see B21 for examples). Equivalently, the least prime factors of members of such sequences are bounded.

Sketch: Suppose there is an infinite set of congruences...
Open Problem (Erdős): For a Sierpiński number $k$, is the least prime factor of $k \cdot 2^n + 1$ bounded as $n$ tends to infinity?

A. Izotov (1995) gave a convincing argument that the answer to this question is probably, “No.” He used a partial covering to find a $k = \ell^4$ such that if $n \not\equiv 2 \pmod{4}$, then $k \cdot 2^n + 1$ has a small prime factor. For $n \equiv 2 \pmod{4}$, he notes that

$$k \cdot 2^n + 1 = \ell^4 \cdot 2^{4m+2} + 1$$

$$= (2^{2m+1} \ell^2 + 2^{m+1} \ell + 1)(2^{2m+1} \ell^2 - 2^{m+1} \ell + 1).$$

Open Problem (Erdős): For a Sierpiński number $k$, is the least prime factor of $k \cdot 2^n + 1$ bounded as $n$ tends to infinity?

Finch, Kozek, F.: $k = 44745755^4$ is a Sierpiński number and a likely example where the least prime divisor of $k \cdot 2^n + 1$ is unbounded. This is the smallest known number constructed from Izotov’s trick.

Open Problem: Is $k = 44745755^4$ the smallest Sierpiński number with the least prime divisor of $k \cdot 2^n + 1$ unbounded?

Open Problem: For a Sierpiński number $k$ not of the form $\ell^r$ with $r \geq 2$, is the least prime factor of $k \cdot 2^n + 1$ bounded as $n$ tends to infinity?

Open Problem: Is $k = 44745755^4$ the smallest Sierpiński number with the least prime divisor of $k \cdot 2^n + 1$ unbounded?

Open Problem: Is the least prime divisor of the number $5 \cdot 2^n + 1$ bounded as $n$ tends to infinity?

Open Problem: Is the least prime divisor of the number $11 \cdot 2^n - 1$ bounded as $n$ tends to infinity?
Other Related Problems

Open Problem: *Is 271129 the smallest prime that is a Sierpiński number?*

Open Problem: *Is 143665583045350793098657 the smallest number that is both Riesel and Sierpiński?*

Finch, Kozek, F.: For every $r \in \mathbb{Z}^+$, there is a $k$ for which all of the numbers $k, k^2, k^3, \ldots, k^r$ are simultaneously Sierpiński numbers.

Open Problem: *Is there a positive odd integer $k$ such that each number in the infinite sequence $k, k^2, k^3, \ldots$ is a Sierpiński number?*

Open Problem (Y.-G. Chen): *For every $r \in \mathbb{Z}^+$, is there a $k$ such that $k^r$ is a Riesel number?*

Open Problem: *Is there a Riesel number that is an 8th power?*

Open Problem (Erdős, $25; Selfridge, $2000 sort-of):* Does there exist a finite covering consisting only of distinct “odd” moduli $> 1$?*

Legend: Erdős and Selfridge had different points of view on whether there exists an “odd” covering. After some discussion, Erdős, who believed that there is an odd covering, offered $25 to the first proof that no such covering exists. Selfridge, who believed there is no odd covering, offered $300 for the first explicit construction of an odd covering. The latter offer was eventually raised to $2000. Note that no financial gain is offered for a non-constructive proof that there is an odd covering.

Some Special Coverings

Open Problem (J. Selfridge): *Does there exist a finite covering consisting only of distinct squarefree moduli $\geq 3$?*

C. E. Krukenberg (1971): There is a finite covering using the modulus 2 and distinct squarefree moduli that are $\geq 5$.

Open Problem (Erdős, $25; Selfridge, $2000 sort-of):* Does there exist a finite covering consisting only of distinct “odd” moduli $> 1$?*
Open Problem (Erdős, $25; Selfridge, $2000 sort-of): Does there exist a finite covering consisting only of distinct “odd” moduli > 1?

Open Problem: For each positive integer $M$, does there exist a finite covering consisting only of distinct moduli relatively prime to $M$?

Let $k = k(N)$ denote the least rational number, if it exists, for which there is a covering with all moduli distinct and in $[N, kN]$.

Ford, Konyagin, Pomerance, Yu, F. (2007): If $c < 1/2$, $N$ is sufficiently large and $k(N)$ exists, then

$$k(N) \geq \exp\left(c \log N \log \log \log N / \log \log N\right).$$

Krukenberg (1971) notes that $k(2) = 6$, $k(3) = 12$, $k(4) = 15$ and $k(5) \leq 21.6$.

Open Problem: What is $k(5)$?

Open Problem (O. Trifonov): Is $k(N) \geq N$, $\forall N$?

---

Sierpiński “Polynomials”

Question 1: Is there an $f(x) \in \mathbb{Z}[x]$ satisfying $f(x)x^n + 1$ is reducible for all positive integers $n$ and $f(1) \neq -1$? Don’t Know

Question 2: Is it true that any such $f(x)$ must be associated with a covering of the integers? Yes

Comment: Schinzel has shown that if there is such an $f(x)$, then there is a covering of the integers in which no modulus divides another. It is known that such a covering can only exist if there is a covering consisting of distinct odd moduli > 1.

Sierpiński “Polynomials”

Open Problem (Schinzel, 1967): Does there exist an $f(x) \in \mathbb{Z}[x]$ satisfying $f(x)x^n + 1$ is reducible for all positive integers $n$ and $f(1) \neq -1$?

Question 2: Is it true that any such $f(x)$ must be associated with a covering of the integers? Yes

Comment: Schinzel has shown that if there is such an $f(x)$, then there is a covering of the integers in which no modulus divides another. It is known that such a covering can only exist if there is a covering consisting of distinct odd moduli > 1.
**Open Problem (Schinzel, 1967):** Does there exist an \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x)x^n + 1 \) is reducible for all positive integers \( n \) and \( f(1) \neq -1 \)?

**Open Problem (Schinzel, 1967):** Does there exist a covering of the integers in which no modulus divides another?

**Open Problem:** Does there exist an \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x)x^n + 1 \) is reducible over \( \mathbb{Q} \) for all positive integers \( n \) and \( f(1) \neq -1 \)?

**Modification of an Example due to Schinzel:** \((5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12\) is reducible for all integers \( n \geq 0 \).

**L. Jones, 2008:** For infinitely many \( d \equiv 6 \pmod{12} \), there exists an \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x)x^n + d \) is reducible over \( \mathbb{Q} \) for all positive integers \( n \) and \( f(1) \neq -d \). For \( d = 90 \), such an \( f(x) \) exists.

**L. Jones, 2008:** For infinitely many \( d \equiv 6 \pmod{12} \), there exists an \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x)x^n + d \) is reducible over \( \mathbb{Q} \) for all positive integers \( n \) and \( f(1) \neq -d \). For \( d = 90 \), such an \( f(x) \) exists.

**F., 2002:** If \( d \) is an integer divisible by 4, then there exists an \( f(x) \in \mathbb{Z}[x] \) satisfying \( f(x)x^n + d \) is reducible over \( \mathbb{Q} \) for all positive integers \( n \) and \( f(1) \neq -d \).

**F., 2002:** Does \( f(x) \) exist for \( d = 2 \)?
R. Graham (1964): Define
\[ A_0 = 1786772701928802632268715130455793 \]
\[ A_1 = 1059683225053915111058165141686995 \]
\[ A_n = A_{n-1} + A_{n-2} \quad \text{for} \ n \geq 2. \]
Then \( \gcd(A_0, A_1) = 1 \) and \( A_n \) is composite for all \( n \geq 0 \).

Open Problem: What choices of \( A_0 \) and \( A_1 \) satisfy \( \gcd(A_0, A_1) = 1 \), \( A_n \) is composite for all \( n \geq 0 \) and \( \max\{A_0, A_1\} \) is as small as possible?

M. Vsemirnov (2004): Found the smallest known values of \( A_0 \) and \( A_1 \):
\[ A_0 = 106276436867, \quad A_1 = 35256392432. \]

Question: For \( m \in \mathbb{Z}^+ \), the number
\[ (11 \cdot 13 \cdot 17 \cdot 19 \cdot 10) m + 15. \]
is composite and is such that if you change any one digit, then the number remains composite. Are there numbers coprime to 10 with this property?

Kozek, Nicol, Selfridge, F.: There are infinitely many composite natural numbers \( N \), coprime to 10, with the property that if we replace any digit in the decimal expansion of \( N \) with \( d \in \{0, \ldots, 9\} \), then the number created by this replacement is composite.

Open Problem: Do similar results hold in all bases?

Open Problem: Do there exist infinitely many composite numbers \( N \) satisfying both conditions, that is replacing any one digit or inserting any digit leads to a composite number?

Open Problem: Are there infinitely many primes that are composite for every replacement (or for every insertion) of a digit?

Open Problem: Is there a \( K > 0 \) such that for every integer \( k \geq K \) there is a composite number \( N \) with exactly \( k \) digits that remains composite after any replacement (or insertion) of a digit?
Open Problem: *Do there exist infinitely many composite numbers that remain composite when any two digits (not necessarily consecutive) are changed (or inserted)?*

Various topics we haven’t considered:
- Infinite coverings (infinitely many congruences in the system)
- Exact coverings (every integer satisfies exactly one congruence in the system)
- Gaussian integers (analogs in $\mathbb{Z}[i]$)
- Other generalizations (eg., groups covered with cosets; higher dimensional analogs)
- Things which I’ve forgotten or don’t know (for example, longer recursion relations)