

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel

# Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Whittier College

December 7, 2010



## About Paul Erdős.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. About Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited



- Hungarian mathematician, 1913-1996.
- Interested in combinatorics, graph theory, number theory, classical analysis, approximation theory, set theory, probability theory...



## More on Paul Erdős.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. About Paul Erdős

Part 2. Erdős and covering systems in research

Erdős problen on covering systems

Part 4: Sierpiński and Riesel revisited

- Wrote/co-wrote over 1400 research papers.
- Erdős number.
- Erdős problems: issued "bounties" for problems that he thought were interesting or for which he wanted to know the solution.

#### Erdős resources:

- The man who loved only numbers, book by Paul Hoffman, 1998, (based on his Atlantic Monthly article from 1989).
- N is a Number: A portrait of Paul Erdős, film by George Csicsery, 1993 (also based on the Atlantic Monthly article).
- And what is your Erdős number?", Caspar Goffman, the American Mathematical Monthly, 1969.



# Erdős and covering systems in research

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abo Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

#### Question: (de Polignac, 1849)

Is it the case that every sufficiently large odd integer > 1 can be written as the sum of a prime number and a power of 2?

- Some small counter examples include: 127, 905.
- (Romanoff) A positive proportion of the integers may be expressed this way.
- (van der Corput) The exceptions form a set of positive density.
- (Erdős) Constructed an arithmetic progression of odd integers not representable in this way.

# Background: (from Number Theory 101)

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

## **Def.: Congruent**

The integers a and b are *congruent* modulo the natural number n > 1 if there exists an integer, z such that

$$a-b=zn$$
.

If so, we write

$$a \equiv b \pmod{n}$$
.

For example,

$$77 \equiv 7 \pmod{10}$$
 $500 \equiv 1700 \pmod{1200}$ 
 $3 \equiv 58 \pmod{5}$ 
 $143 \equiv 0 \pmod{11}$ .

# Background: (from Number Theory 101)

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

#### **Def.: Covering system**

A *covering system* or covering, for short, is a finite system of congruences

$$n \equiv a_i \pmod{m_i}, \quad 1 < i \le t,$$

such that every integer satisfies at least one of the congruences.



# Example of a covering.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős probler on covering systems

Part 4: Sierpiński and Riesel revisited For example, the congruences

$$n \equiv 0 \pmod{2}$$

$$n \equiv 1 \pmod{3}$$

$$n \equiv 3 \pmod{4}$$

$$n \equiv 5 \pmod{6}$$

$$n \equiv 9 \pmod{12}$$

form a covering of the integers.



# More background.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

#### **Def.: Chinese Remainder Theorem**

A system of congruences has a unique solution if the moduli are pairwise relatively prime.

For example: Can we solve for x in the following system?

$$x \equiv 3 \mod 9$$

$$x \equiv 5 \mod 10$$

$$x \equiv 2 \mod 11$$

Yes, because {9,10,11} are pair-wise, relatively prime. We get:

$$x \equiv 255 \mod 990$$

(Note: 
$$990 = 9 \times 10 \times 11$$
)

# Back to de Polignac's question.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

### **Question: (de Polignac, 1849)**

Is it the case that every sufficiently large odd integer > 1 can be written as the sum of a prime number and a power of 2?

de Polignac asked about odd numbers of the form

$$x = p + 2^n$$
.

• Erdős instead thought about writing primes in the form

$$p = x - 2^n$$
,

and changed the question to:

## Question': (Erdős)

Is it possible to find an integer x such that  $x - 2^n$  is not prime for all (non-negative) integers n?

Covering systems: number theory in the spirit of Paul Erdős Mark Kozek

This led to the "sub-question": For which n and for which x would  $x - 2^n$  be divisible by 3?

 $\Leftrightarrow x - 2^n = 3z \Leftrightarrow x - 2^n \equiv 0 \pmod{3} \Leftrightarrow x \equiv 2^n \pmod{3}$ 

Part 1. About Paul Erdős Part 2. Erdős Lativa taka nawara at 2 (mad 2)

systems in research

Part 3. An Erdős proble

and covering

Let us take powers of 2 (mod 3)

Part 3. An Erdős problem on covering systems  $2^{0} \equiv 1 \pmod{3}$   $2^{1} \equiv 2 \pmod{3}$   $2^{2} \equiv 4 \equiv 1 \pmod{3}$  $2^{3} \equiv 8 \equiv 2 \pmod{3}$ 

Part 4: Sierpiński and Riesel revisited

We see that:

- $2^n \not\equiv 0 \pmod{3}$ .
- For even powers of 2,  $2^n \equiv 1 \pmod{3}$ .
- For odd powers of 2,  $2^n \equiv 2 \pmod{3}$ .



Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. About Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited This led to the "sub-question": For which n and for which x would  $x - 2^n$  be divisible by 3?

We have that if,

•  $n \equiv 0 \pmod{2}$  (even) and  $x \equiv 1 \pmod{3}$  then  $x - 2^n$  is divisible by 3.

OR

•  $n \equiv 1 \pmod{2}$  (odd) and  $x \equiv 2 \pmod{3}$  then  $x - 2^n$  is divisible by 3.



Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abo Paul Erdős

Part 2. Erdős and covering systems in research

Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited Erdős' strategy was to continue along these lines and try to find conditions on n and on x that would ensure that  $x - 2^n$  would be divisible by primes from a given set (that would include 3).

He found the following relations:

- $n \equiv 0 \pmod{2}$  and  $x \equiv 1 \pmod{3} \Rightarrow 3|x-2^n|$
- $n \equiv 0 \pmod{3}$  and  $x \equiv 1 \pmod{7} \Rightarrow 7|x-2^n$
- $n \equiv 1 \pmod{4}$  and  $x \equiv 2 \pmod{5} \Rightarrow 5|x-2^n|$
- $n \equiv 3 \pmod{8}$  and  $x \equiv 8 \pmod{17} \Rightarrow 17|x-2^n$
- $n \equiv 7 \pmod{12}$  and  $x \equiv 11 \pmod{13} \Rightarrow 13|x-2^n|$
- $n \equiv 23 \pmod{4}$  and  $x \equiv 121 \pmod{241} \Rightarrow 241 | x 2^n |$



Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Erdős problen on covering systems

Part 4: Sierpiński and Riesel revisited

- $n \equiv 0 \pmod{2}$  and  $x \equiv 1 \pmod{3} \Rightarrow 3|x-2^n|$
- $n \equiv 0 \pmod{3}$  and  $x \equiv 1 \pmod{7} \Rightarrow 7|x-2^n|$
- $n \equiv 1 \pmod{4}$  and  $x \equiv 2 \pmod{5} \Rightarrow 5|x-2^n|$
- $n \equiv 3 \pmod{8}$  and  $x \equiv 8 \pmod{17} \Rightarrow 17|x-2^n|$
- $n \equiv 7 \pmod{12}$  and  $x \equiv 11 \pmod{13} \Rightarrow 13|x-2^n|$
- $n \equiv 23 \pmod{24}$  and  $x \equiv 121 \pmod{241} \Rightarrow 241|x-2^n$

We observe that the set of congruences describing *n* form a covering system.

We observe that the set of congruences describing x can be combined solved using Chinese Remainder Theorem.



# Erdős' arithmetic progression of counterexamples

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited By the Chinese Remainder Theorem, we get

$$x \equiv 7629217 \pmod{11184810},$$

where

$$11184810 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$$

This gives us the Erdős' arithmetic progression of counterexamples to de Polignac's conjecture.

$$k = 7629217 \pm 11184810z$$
, for  $z \in \mathbb{Z}$ .



# Erdős' arithmetic progression of counterexamples

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited There exists an arithmetic progression of odd integers x, that simultaneously satisfy the system of congruences

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

such that  $x - 2^n$  is composite (not prime) for all non-negative integers n because  $x - 2^n$  will be divisible by at least one of the primes from the set  $\{3, 5, 7, 13, 17, 241\}$ .  $\square$ 



## **Question:** What next?

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abo Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős probler on covering systems

Part 4: Sierpiński and Riesel revisited **Answer:** We try to generalize.

Recall, Erdős constructed an arithmetic progression of odd integers x such that  $x - 2^n$  was composite for all non-negative integers n.

### Def.: Sierpiński number

A *Sierpiński number* is a positive odd integer k with the property that  $k \cdot 2^n + 1$  is composite for all positive integers n.



## Sierpiński numbers

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős probler on covering systems

Part 4: Sierpiński and Riesel revisited

## Def.: Sierpiński number

A Sierpiński number is a positive odd integer k with the property that  $k \cdot 2^n + 1$  is composite for all positive integers n.

Sierpiński (1960) observed the following implications:

```
\implies k \cdot 2^n + 1 \equiv 0 \pmod{3}
n \equiv 1 \pmod{2},
                            k \equiv 1 \pmod{3}
                                                               \implies k \cdot 2^n + 1 \equiv 0 \pmod{5}
n \equiv 2 \pmod{4}.
                            k \equiv 1 \pmod{5}
n \equiv 4 \pmod{8}.
                            k \equiv 1 \pmod{17}
                                                               \implies k \cdot 2^n + 1 \equiv 0 \pmod{17}
n \equiv 8 \pmod{16},
                                                               \implies k \cdot 2^n + 1 \equiv 0 \pmod{257}
                            k \equiv 1 \pmod{257}
                                                               \implies k \cdot 2^n + 1 \equiv 0 \pmod{65537}
n \equiv 16 \pmod{32}.
                            k \equiv 1 \; (\text{mod } 65537)
                                                              \implies k \cdot 2^n + 1 \equiv 0 \pmod{641}
n \equiv 32 \pmod{64}
                            k \equiv 1 \pmod{641}
n \equiv 0 \pmod{64}
                            k \equiv -1 \pmod{6700417}
                                                              \implies k \cdot 2^n + 1 \equiv 0 \pmod{6700417}.
```



# Sierpiński numbers

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problen on covering systems

Part 4: Sierpiński and Riesel The moduli appearing in the congruences involving k are 7 primes, the first (perhaps only) five Fermat primes  $F_n = 2^{2^n} + 1$  for  $0 \le n \le 4$  and the two prime divisors of  $F_5$ .

We add the condition  $k \equiv 1 \pmod{2}$  to ensure that k is odd.

Then the Chinese Remainder Theorem implies that there are infinitely many Sierpiński numbers given by

 $k \equiv 15511380746462593381$ 

 $(\text{mod } 2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417).$ 



# Smallest Sierpiński number

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited In 1962, Selfridge (unpublished) found what is believed to be the smallest Sierpiński number, namely k = 78557.

His argument is based on the following implications:

```
\begin{array}{lll} n\equiv 0\ (\text{mod }2), & k\equiv 2\ (\text{mod }3) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }3)\\ n\equiv 1\ (\text{mod }4), & k\equiv 2\ (\text{mod }5) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }5)\\ n\equiv 3\ (\text{mod }9), & k\equiv 9\ (\text{mod }73) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }73)\\ n\equiv 15\ (\text{mod }18), & k\equiv 11\ (\text{mod }19) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }19)\\ n\equiv 27\ (\text{mod }36), & k\equiv 6\ (\text{mod }37) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }37)\\ n\equiv 11\ (\text{mod }12), & k\equiv 11\ (\text{mod }13) & \Longrightarrow & k\cdot 2^n+1\equiv 0\ (\text{mod }13). \end{array}
```

There have been attempts to prove that 78557 is the smallest Sierpiński number.

In this regard, the web page

http://www.seventeenorbust.com

contains the current up-to-date information.



# Smallest Sierpiński number

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Erdős probler on covering systems

Part 4: Sierpiński and Riesel revisited As of this writing, there remain 6 values of k < 78557 which are unresolved by the Seventeen or Bust project, namely

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

The most recent value of k < 78557 to have been eliminated was 33661, by Sturle Sunde's computer, on October 30, 2007.





# Other generalizations.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abo Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problen on covering systems

Part 4: Sierpiński and Riesel revisited

#### **Def.: Riesel number**

A *Riesel number* is a positive odd integer k with the property that  $k \cdot 2^n - 1$  is composite for all positive integers n.

The smallest known Riesel number is 509203, due to Riesel (1956).

There have been attempts to prove that 509203 is the smallest Riesel number.

http://www.prothsearch.net/rieselprob.html

As of this writing there remain 64 unresolved candidates, of these 2293 is the smallest.



## More generalizations

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abo Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős probler on covering systems

Part 4: Sierpiński and Riesel

#### Conjecture (Chen)

For every positive integer r, there exist infinitely many positive odd integers k such that the number  $k^r 2^n + 1$  has at least two distinct prime factors for each positive integer n.

### Conjecture (Chen)

For every positive integer r, there exist infinitely many positive odd integers k such that the number  $k^r - 2^n$  has at least two distinct prime factors for each positive integer n. (Equivalent to  $k^r 2^n - 1$ .)

## Chen's conjectures.

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problen on covering systems

Part 4: Sierpiński and Riesel revisited Chen (2002) resolves each conjecture in the case that r is odd and in the case that r is twice an odd number and  $3 \nmid r$ . As he notes, the least r for which his arguments do not apply are r = 4 and r = 6.

Conjecture 1 is true in general and that Conjecture 2 holds in the special cases r = 4 and r = 6.

#### Theorem (Filaseta, Finch, K., 2008)

For every positive integer R, there exist infinitely many positive odd numbers k such that each of the numbers

$$k2^{n} + 1, k^{2}2^{n} + 1, k^{3}2^{n} + 1, \dots, k^{R}2^{n} + 1$$

has at least two distinct prime factors for each positive integer n.



## The minimum modulus problem

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel

## Open problem: (Erdős, \$1000)

For every natural number N > 1 does there exist a covering system with distinct moduli all  $\geq N$ ?

### Personal attempts:

Summer 2008, with Kelly Bickell, Michael Firrisa, Juan Pablo Ortiz, and Kristen Pueschel.

We made it to N = 14.

Summer 2009, with Tobit Raff.

We made it to N = 11.



## The minimum modulus problem: results

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

## Open problem: (Erdős, \$1000)

For every natural number N > 1 does there exist a covering system with distinct moduli all  $\geq N$ ?

#### Early results:

- N = 3: Erdős.
- *N* = 9: Churchhouse, 1968.
- N = 14: Selfridge.
- *N* = 18: Krukenburg (Ph.D. Thesis), 1971.
- *N* = 20: Choi, 1971.
- N = 24: Morikawa, 1981.
- *N* = 25: Gibson (Ph.D. Thesis) 2008.
- *N* = 36, 40: Nielsen, 2009.



# The minimum modulus problem: techniques

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel For small *N*, examples can be worked out by hand, but quickly computers come into play.

Churchouse's result (N=9) came from using computers and a greedy algorithm. The LCM of the moduli was

$$604,800 = 2^7 3^3 5^2 7.$$

Krukenburg and Choi's results did not use computers. The LCM of Krukenburg's moduli was

$$475,371,719,222,400 = 2^73^35^27^211^213^217^219.$$



## Gibson's techniques

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abor Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited

#### Gibson uses:

- a greedy algorithm (like Churchhouse)
- the notion of an "almost covering" (like Morikawa who in turned used ideas of Krukenburg)
- "random covering" (like Erdős)
- extensive computing.

The LCM of the moduli used primes up to 2017.



## Nielsen's techniques

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdő: and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited Nielsen uses a graph theoretic approach, representing covering systems as trees, and introducing new primes, as necessary to "plug" holes.

The LCM of the moduli uses primes up to 103.

Initially, he used the primes in order.

However, the referee noted that sometimes it was more efficient to use certain primes out of order. This allowed for the improvement from N = 36 to N = 40.

There was very little wiggle room, and thus, fears a "negative solution" for the minimum modulus problem.



## Sierpiński + Riesel?

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős probler on covering systems

Part 4: Sierpiński and Riesel revisited **Question:** Do here exist numbers that are simultaneously Sierpiński and Riesel numbers?

**Answer:** Yes. (Cohen and Selfridge, 1975).

k = 47867742232066880047611079



## Sierpiński + Riesel?

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problen on covering systems

Part 4: Sierpiński and Riesel revisited However, folks (computer scientists) didn't read their paper. So they offered their results.

- Brier (1998) k = 29364695660123543278115025405114452910889
- Gallot (2000) k = 623506356601958507977841221247
- Gallot (2000) k = 3872639446526560168555701047
- Gallot (2000) k = 878503122374924101526292469
- E. Vantieghem (2010) k = 47867742232066880047611079
- Filaseta, Finch and K. (2008) k = 143665583045350793098657

For more information on this problem, visit:

http://www.primepuzzles.net/problems/prob\_029.htm



# Thank you

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

Part 2. Erdős and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited Any Questions?



## In Memoriam

Covering systems: number theory in the spirit of Paul Erdős

Mark Kozek

Part 1. Abou Paul Erdős

and covering systems in research

Part 3. An Erdős problem on covering systems

Part 4: Sierpiński and Riesel revisited



John L. Selfridge 1927-2010