Classroom

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Covering the Integers

B Sury
Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560 059 India.
Email: sury@isibang.ac.in

For an arithmetic function f, we discuss a kind of uncertainty principle which shows that both f and its Möbius transform cannot have finite support simultaneously. This idea not only proves the infinitude of primes but is of interest in the context of 'covering congruences'. For integers $a_1, \cdots, a_k$ and positive integers $n_1, \cdots, n_k$, the set of congruences $x \equiv a_i \pmod{n_i}$ $(i = 1, \cdots, k)$ is called a set of *covering congruences* if $\mathbf{Z} = \bigcup_{i=1}^{k}(a_i + n_i\mathbf{Z})$. We discuss some nice properties and conjectures on covering congruences and, finally, a beautiful application due to Erdös which originally motivated the study of covering congruences. This is the result that there are infinitely many odd integers which are not expressible as the sum of a prime and a power of 2.

Keywords
Möbius transform, covering system of congruences.

Let $f : \mathbf{N} \to \mathbf{C}$ be an arithmetic function. Then, f can be recovered from the function (its Möbius transform)

An arithmetical function and its Möbius transform cannot have finite support simultaneously. The infinitude of primes is a consequence of this 'uncertainty principle'.

$\widehat{f}(n) = \sum_{d|n} f(d)$ by the Möbius inversion formula

$$f(n) = \sum_{d|n} \mu(d)\widehat{f}(n/d)\,,$$

where the Möbius function is defined $\mu(n) = 1$ if $n = 1$, $\mu(n) = (-1)^r$ if $n = p_1 p_2 \cdots p_r$ for distinct primes $p_1, \cdots, p_r$ and $\mu(n) = 0$ if not. Here is an elementary observation (in the spirit of the uncertainty principle as made by Paul Pollack [1]):

Lemma. *Let f be any non-zero arithmetic function such that the support*

$$\{n : \widehat{f}(n) \neq 0\}$$

is a finite set. Then, the support

$$\{n : f(n) \neq 0\}$$

of f is infinite.

Proof. Suppose f is non-zero and that $\{n : f(n) \neq 0\}$ is finite. Then, $F(z) := \sum_{n\geq 1} \widehat{f}(n) z^n$ is a non-zero polynomial. But, if $M = \max(|\widehat{f}(n)| : n \geq 1)$, then for $|z| < 1$, we have

$$\begin{aligned} |F(z)| &= |\sum_n (\sum_{d|n} f(d)) z^n| \leq \sum_n \sum_{d|n} |f(d)||z|^n \\ &\leq \sum_n (\sum_{d|n} M)|z|^n \leq M \sum_n n|z|^n = \tfrac{m|z|}{1-|z|^2} < \infty. \end{aligned}$$

Therefore, we can interchange the summations to obtain

$$F(z) = \sum_r \sum_{d|n} f(d) z^{rd} = \sum_r \sum_{d|n} f(d) \frac{z^d}{1-z^d}\,.$$

Now, if $N = \max(n : f(n) \neq 0)$, then $F(z)$ clearly has a pole at $z = e^{2i\pi/N}$ which contradicts the fact that F is an entire function. □

A finite set of congruences is a 'covering system' if every integer satisfies at least one of the congruences.

This gives a proof of the infinitude of primes as follows.

Note that $\widehat{\mu}(n) = \sum_{d|n} \mu(d) = 0$ for $n > 1$. So, $\widehat{\mu}$ has finite support. So, if there were only finitely many primes, μ would have finite support contradicting the 'uncertainty' result proved above. □

The above type of argument has interesting applications to what are known as covering congruences. These can be described as follows.

Just as every natural number is either odd or even, we see that for any k, the congruences

$$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 4, \quad \ldots,$$
$$x \equiv 2^{k-1} \pmod{2^k}, \quad x \equiv 0 \pmod{2^k}$$

cover the set of all integers. In other words, every integer satisfies at least one of these congruences. Similarly, for any positive integer N, the set of congruences $x \equiv i \pmod N$ for $i = 0, 1, \cdots, N-1$ covers the integers.

Thus, these are called sets of 'covering congruences'. The general definition is the following. Let $a_1, \cdots, a_k$ be integers and let $n_1, \cdots, n_k$ be positive integers. The set of congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, \cdots, k$ is called a set of *covering congruences* if $\mathbf{Z} = \bigcup_{i=1}^{k} (a_i + n_i \mathbf{Z})$. We write the set in short as $a_1(n_1), a_2(n_2), \cdots, a_k(n_k)$.

Note that in both the cases above, the moduli $n_1, \cdots, n_k$ of the congruences have the property that $\sum_{i=1}^{k} \frac{1}{n_i} = 1$.

A set of covering congruences $a_1(n_1), \cdots, a_k(n_k)$ is called a *disjoint covering system* if every integer satisfies exactly one of the congruences $x \equiv a_i \pmod{n_i}$.

Note that the two sets of covering congruences above,

viz.,

$$1(2), \quad 2(2^2), \quad 2^2(2^3), \quad \ldots, \quad 2^{k-1}(2^k), \quad 0(2^k)$$

and

$$0(N), \quad 1(N), \quad 2(N), \quad \ldots, \quad N-1(N)$$

are disjoint covering systems. Note also that at least two of the moduli are the same. That this must always be true is the assertion of the following proposition whose proof follows the method we started the article with. There are several interesting properties and open questions on covering congruences (see [2 ,3, 4]).

The sum of the reciprocals of the moduli of a disjoint covering system, equals 1.

Proposition. *Let $a_1(n_1), a_2(n_2), \cdots, a_k(n_k)$ be a disjoint system of covering congruences where $n_1 \leq n_2 \leq \cdots \leq n_k$. Then, $n_{k-1} = n_k$. Moreover $\sum_{j=1}^{k} \frac{1}{n_j} = 1$.*

Proof. We may assume without loss of generality that $0 \leq a_j < n_j$ for each $j \leq k$. By the hypothesis, we have for $|z| < 1$,

$$\sum_{j=1}^{k} \frac{z^{a_j}}{1-z^{n_j}} = \sum_{j=1}^{k} \sum_{r=0}^{\infty} z^{a_j + r n_j} = \sum_{n \geq 0} z^n = \frac{1}{1-z}\,.$$

Thus, this function has a pole at the point $z = 0$. But, if $n_i < n_k$ for all $i < k$, then this function has a pole at $z = e^{2i\pi/n_k}$, a contradiction. This proves the first assertion.

Let $n = \text{lcm}\,(n_1, \cdots, n_k)$. Then, we have

$$1 - z^n = \prod_{j=1}^{k} (1 - e^{2i\pi a_j/n_j} z^{n/n_j})\,,$$

as each n-th root of unity is a simple root of the polynomial on the left-hand side. This can be rewritten as

$$1 - z^n = \sum_{I \subset \{1,\cdots,k\}} (-1)^{|I|} z^{\sum_{j \in S} n/n_j} e^{2i\pi \sum_{j \in I} a_j/n_j}\,.$$

There are infinitely many odd integers which are not expressible as the sum of a prime and a power of 2.

Comparison of degrees gives us $\sum_{j=1}^{k} \frac{n}{n_j} = n$, which is the second assertion. □

This leaves the question of the existence of a covering system (necessarily not disjoint by the above proposition) with distinct moduli. The first set of covering congruences for which the moduli are distinct was given by A Schinzel [5, 6]. This is the set

$$0(2), \quad 0(3), \quad 1(4), \quad 5(6), \quad 7(12).$$

Here are two famous conjectures [7] due to Erdős and others which are still open.

Conjecture 1 (Erdős–Selfridge). *There is no finite system of covering congruences where all the moduli are distinct and odd.*

Conjecture 2 (Erdős). *For any $M > 0$, there exists a system of covering congruences where all the moduli are distinct and greater than M.*

Erdős mentioned in 1995 that this last conjecture is perhaps his favourite problem!

We finish with a number-theoretic application which originally motivated the study of covering congruences. This is the following beautiful result due to (who else but!) Erdős.

Theorem (Erdős, 1950). *There are infinitely many odd integers which are not expressible as the sum of a prime and a power of* 2.

Proof. Consider a covering system of congruences $a_i(n_i)$ with $1 \leq i \leq k$, where $p_1, \cdots, p_k$ are distinct odd primes and n_i the least positive number satisfying $2^{n_i} \equiv 1 \bmod p_i$.

Erdős constructed such covering systems explicitly; one such is

$$0(2), \quad 0(3), \quad 1(4), \quad 3(8), \quad 7(12), \quad 23(24).$$

Note that the n_i's here (2, 3, 4, 8, 12, 24) are the orders of 2 modulo the primes 3, 7, 5, 17, 13, 241.

Given any such system, the Chinese remainder theorem provides a common solution to the congruences

$$x \equiv 2^{a_i} \pmod{p_i}, \ \ 1 \leq i \leq k, \quad x \equiv 1 \pmod{2}.$$

Such a solution x is unique modulo $2\prod_{i=1}^{k} p_i$. Consider the smallest positive integer solution, say x_0. Now, for each integer r, there exists some i such that $r \equiv a_i \pmod{m_i}$.

So, if $n \equiv n_0 \pmod{2p_1 \cdots p_k}$, then

$$n - 2^r \equiv n_0 - 2^{a_i} \equiv 0 \pmod{p_i}.$$

Thus, if $n - 2^r > p_i$, then it must be composite.

This proves that all n not of the form $2^r + p_i$ for some r and some $i \leq k$ are inexpressible in the form asserted. To dispose of the exceptional cases, we may impose extra congruence conditions.

An example (taking the above covering system 0(2), 0(3), 1(4), 3(8), 7(12), 23(24) of Erdős) gives us:

No integer congruent to 7629217 (mod 1184810) *is a sum of a power of* 2 *and an odd prime.*

Z-W Sun has done substantial work in the subject of covering congruences and revealed connections with zero-sum problems. We finish with a following amazing application completed by Sun [8] of the above work by

Simple questions for integers arising out of covering systems of congruences have many interesting analogues for groups where the congruences are replaced by cosets of subgroups.

Erdős and later work of Cohen and Selfridge [9] on covering congruences.

Consider the 29-digit number

$$M = 66483084961588510124010691590$$
$$= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot$$
$$97 \cdot 109 \cdot 151 \cdot 241 \cdot 257 \cdot 331.$$

Then, the solutions of the congruence

$$x \equiv 47867742232066880047611079 \ mod\ M$$

cannot be expressed as $\pm p^a \pm q^b$ *where* p, q *are primes and* a, b *are non-negative integers.*

As can be readily imagined, simple questions for integers arising out of covering systems of congruences have many interesting analogues for groups where the congruences are replaced by cosets of subgroups. That will be a topic to discuss on another occasion.

Suggested Reading

[1] **P Pollack, The Möbius transform and the infinitude of primes, http://www.math.uiuc.edu/~pppollac**

[2] **T Cochrane and G Myerson, Covering congruences in higher dimensions, *Rocky Mountain J. Math.*, Vol.26, pp.77–81, 1996.**

[3] **R K Guy, *Unsolved Problems in Number Theory* (2nd Ed.), Springer-Verlag, New York, 1994.**

[4] **B Jin and G Myerson, Homogeneous covering congruences and subgroup covers, *Journal of Number Theory*, Vol.110, pp.120–135, 2005.**

[5] **A Schinzel, Reducibility of polynomials and covering systems of congruences, *ACTA Arithmetica*, Vol.13, pp.91–101, 1967.**

[6] **A Schinzel, On homogeneous covering congruences, *Rocky Mountain J. Math.*, Vol.27, pp.335–342, 1997.**

[7] **P Erdõs. On integers of the form $2^k + p$ and some related problems. *Summa Brasiliensis Mathematicae*, Vol.2, pp.113–123, 1950.**

[8] **Z W Sun, On integers not of the form $\pm p^a \pm q^b$, *Proc. Amer. Math. Soc.*, Vol.128, pp.997–1002, 2000.**

[9] **E Cohen and J L Selfridge, Not every number is the sum or difference of two prime powers, *Math.Comput.*, Vol.29, pp.79–81, 1975.**