Conclusion This method of enumerating sets certainly does not displace Cantor's classic technique, but it does show another, more concrete way to accomplish the task. Though we applied it only to $\mathbb{Q}$ and $\mathbb{A}$, the method presented here can, in theory, be used to count any set X such that $\mathbb{N} \subseteq X$ (so that we may apply inclusion) for which a sufficiently clever function from X into $\mathbb{N}_{(n)}$ for some n can be found.

Acknowledgment. This work was supported by the Paul K. and Evalyn E. Cook Richter Memorial Trust, while the author was simultaneously pursuing a B.S. and M.S. in mathematics at Yale University.

REFERENCES

1. Georg Cantor, Ueber eine Eigenschaft des Inbergriffs aller reellen algebraischen Zahlen, *J. f. Math.* **77** (1874), 258–262.
2. I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, New York, 1975, 214–219.

Covering Systems of Congruences

J. FABRYKOWSKI
T. SMOTZER
Youngstown State University
Youngstown, Ohio 44555
jfabryk@math.ysu.edu
tsmotzer@math.ysu.edu

Let us consider the following problem, which is a variant of problem 9 from the 2002 American Invitational Mathematics Examination (AIME):

PROBLEM. Harold, Tanya, and Ulysses paint a very long fence. Harold starts with the first picket and paints every hth picket; Tanya starts with the second picket and paints every tth picket; and Ulysses starts with the third picket and paints every uth picket. If every picket gets painted exactly once, find all possible triples (h, t, u).

Solution: Label the pickets 1, 2, 3, and so on. Ulysses cannot paint picket 4 or else Ulysses paints all the pickets thereafter. Suppose Harold paints picket 4. Then Ulysses cannot paint picket 5, or else Harold and Ulysses both paint picket 7, so Tanya paints picket 5. Ulysses paints picket 6 and $(h, t, u) = (3, 3, 3)$. On the other hand, suppose Tanya paints picket 4. Then Ulysses cannot paint picket 5, or else there is nothing left for Harold to paint, so Harold paints picket 5. Hence Ulysses paints picket 7 and $(h, t, u) = (4, 2, 4)$.

This problem really asks about how one can partition the set of integers into three arithmetic progressions. The second triple $(4, 2, 4)$ is a bit more interesting than the first, since not all the differences are equal. In elementary number theory, arithmetic progressions are equivalently called residue classes of various moduli. In such a setting, the arithmetic progression $a + km$, $k \in \mathbb{Z}$ is denoted by $a \pmod{m}$.

One can generalize the AIME problem and ask whether there exists a finite set of congruences, with all moduli distinct and greater than or equal to 2, that forms a partition of the set of integers. This turns out to be impossible [**4**]. Relaxing the assumption about *partitioning* the integers, one can look for finite sets of congruences such that every integer belongs to *at least one* of them.

Our purpose in this note is to survey this topic and provide an elementary proof of the relationship between two well-known conjectures.

Erdős's covering systems In 1849, A. de Polignac conjectured that any odd integer $n \geq 3$ can be expressed in the form $2^k + p$, where k is a nonnegative integer and p is either a prime or the integer 1 [**6**]. In 1950, Erdős refuted this by proving that there exists an arithmetic progression, no term of which has the given form.

To prove his assertion, Erdős developed the concept of *covering systems of congruences*. A family of residue classes $a_i \pmod{n_i}$ with $2 \leq n_1 \leq \cdots \leq n_r$ is called a covering system of congruences if every integer belongs to at least one of the residue classes, that is, every integer satisfies at least one of the congruences $x = a_i \pmod{n_i}$.

This is how Erdős's proof worked: Consider the system of congruences (which can be shown to be a covering system): $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $3 \pmod 8$, $7 \pmod{12}$, and $23 \pmod{24}$ [**2, 3**]. Each of these congruences implies a corresponding congruence for certain powers of 2. For example, the congruence $k \equiv 1 \pmod 4$ together with $2^4 \equiv 1 \pmod 5$ imply that $2^k \equiv 2 \pmod 5$. To see this, let $k = 4n + 1$ and observe that

$$2^k \equiv 2^{4n+1} \equiv 2(2^4)^n \equiv 2 \pmod 5.$$

By similar reasoning, if k is a nonnegative integer, then at least one of the following congruences holds: $2^k \equiv 1 \pmod 3$, $2^k \equiv 1 \pmod 7$, $2^k \equiv 2 \pmod 5$, $2^k \equiv 8 \pmod{17}$, $2^k \equiv 2^7 \pmod{13}$, or $2^k \equiv 2^{23} \pmod{241}$.

Now consider the congruences $1 \pmod 3$, $1 \pmod 7$, $2 \pmod 5$, $8 \pmod{17}$, $2^7 \pmod{13}$, and $2^{23} \pmod{241}$. Since the moduli are pairwise relatively prime, there are infinitely many integers that satisfy all the congruences, by virtue of the Chinese Remainder Theorem. Now, if an odd integer a satisfies all the congruences, then all the integers of the form $a - 2^k$ are divisible by one of the moduli 3, 7, 5, 17, 13 or 241. It follows that $a - 2^k$ is not prime and therefore a does not have the form $2^k + p$.

Another example of application of covering systems of congruences came from R. L. Graham [**5**]. His result is in a sense opposite to a well-known conjecture stating that the Fibonacci sequence, defined by $f_0 = 0$, $f_1 = 1$, and for $n \geq 0$ $f_{n+2} = f_{n+1} + f_n$, contains infinitely many primes. Graham used covering systems to show that one can choose the initial relatively prime values f_0 and f_1 so that the corresponding sequence contains only composite integers. The smallest known choice is

$$f_0 = 331635635998274737472200656430763$$

and

$$f_1 = 1510028911088401971189590305498785.$$

The major open problem in this topic is a conjecture of Erdős, that for every $c \geq 2$ there is a covering system of congruences with $n_1 \geq c$ and distinct moduli. This is known to be true for some values of c; the current record, held by Choi [**1**], is $c = 20$. If there is a covering system of congruences with distinct moduli, and $n_1 \geq c$ for every $c \geq 2$, then one would obtain the following result about arithmetic progressions: For every positive integer m there exists an arithmetic progression, no term of which is a sum of a power of two and an integer, having at most m prime factors [**4**].

Two other important conjectures are by Selfridge and Schinzel:

SELFRIDGE CONJECTURE. There is no covering system of congruences with distinct odd moduli.

SCHINZEL CONJECTURE. In every covering system $a_i \pmod{n_i}$ with $1 \leq i \leq r$, there exists $i \neq j$ such that $n_i \mid n_j$.

Schinzel has proved that Selfridge's conjecture implies the Schinzel conjecture using the irreduciblity of certain polynomials [7]. We propose to prove this result using only elementary methods.

Main result We begin with a definition. Let $a_s \pmod{n_s}$ with $1 \le s \le r$ be a covering system of congruences. Then it is a *reduced covering system of congruences* if no proper subset of the covering system of congruences is a covering system of congruences.

THEOREM. *The Selfridge conjecture implies the Schinzel conjecture.*

Proof. Let us assume that the Selfridge conjecture holds, but the Schinzel conjecture does not. Then there is a reduced system of covering congruences, $a_s \pmod{m_s}$, such that $m_i \nmid m_j$ for all $i \neq j$. Let $m_i = 2^{\beta_i} O_i$, where O_i is odd for $1 \le i \le r$. Let us also assume that the congruences have been numbered in such a way that if $i < j$ then $\beta_i \le \beta_j$. It follows from the Selfridge conjecture that $\beta_r > 0$. Obviously, all the numbers O_i are different.

Now, if $O_i \ge 3$ for all i, then we would contradict the Selfridge conjecture since if $x \equiv a_i \pmod{2^{\beta_i} O_i}$, and $2^{\beta_i} \mid (2^{\beta_i} O_i)$, then $x \equiv a_i \pmod{O_i}$, and we would have a covering system with all odd moduli. Consequently, if $a_i \pmod{m_i}$ is a covering system of congruences and $n_i | m_i$ for each i, then $a_i \pmod{n_i}$ is also a covering system of congruences. Thus, there exists i_0, such that $O_{i_0} = 1$ and consequently $m_{i_0} = 2^{i_0}$. It follows that $i_0 = r$ or else we would have $m_{i_0} \mid m_{i_0+1}$.

Next, we shift the system of congruences by $-a_r$, that is, change the variable x to $x + a_r$, so that we may assume that the rth congruence has the form $0 \pmod{2^{\beta_r}}$. Consider now integers of the form $x2^{\beta_r} - 1$, with $x \in \mathbb{Z}$. None of these integers is covered by the congruence $0 \pmod{2^{\beta_r}}$, however all of them are covered by the rest of the congruences, since the system is a covering system. Our system now takes the form:

$$x2^{\beta_r} - 1 \equiv a_s \pmod{m_s} \quad 1 \le s \le r - 1. \qquad (*)$$

Note that it may happen that not all of the congruences have solutions; however, whenever a congruence has solutions, we must have

$$\gcd(2^{\beta_r}, m_s) \mid a_s + 1.$$

Since $\gcd(2^{\beta_r}, m_s) = 2^{\beta_s}$, it follows that $2^{\beta_s} \mid a_s + 1$. Let

$$U = \{s : 1 \le s \le r - 1 \quad \text{such that} \quad 2^{\beta_s} \mid a_s + 1\}.$$

For every $s \in U$, the congruence (*) takes the form $x2^{\beta_r - \beta_s} \equiv (a_s + 1)/2^{\beta_s} \pmod{O_s}$ or $x \equiv c_s \pmod{O_s}$ for some integers c_s. This new system of congruences is a covering system of congruences with all distinct odd moduli, contradicting the Selfridge conjecture. ■

REFERENCES

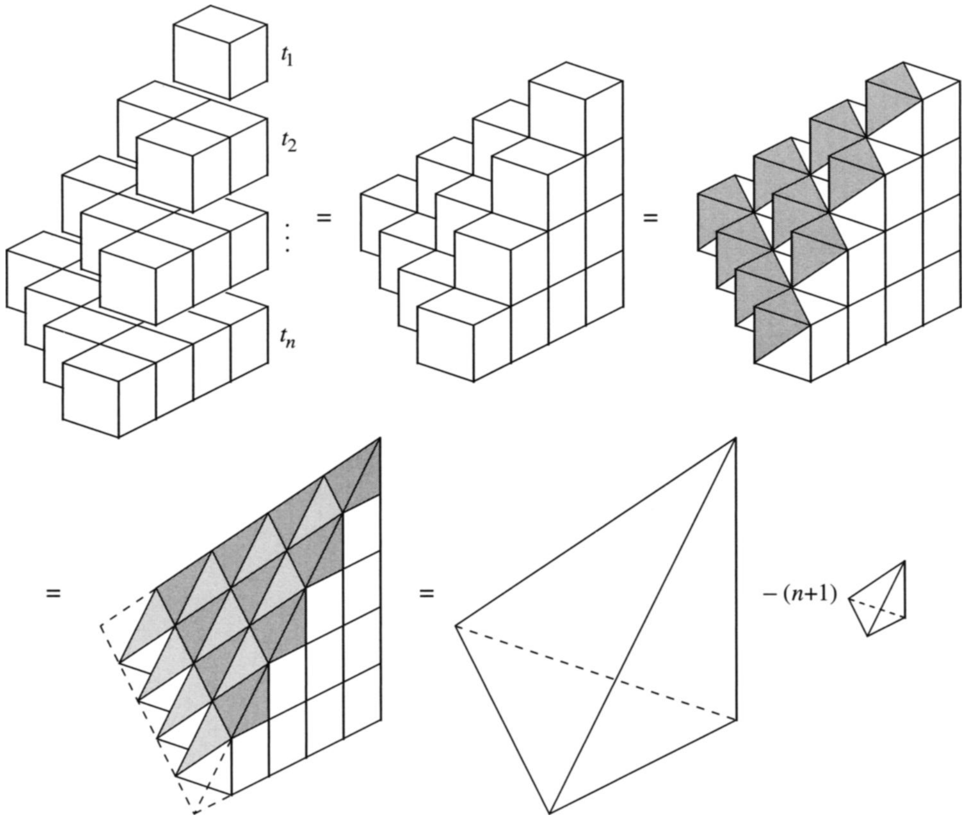
1. S. Choi, Covering the set of integers by congruence classes of distinct moduli, *Math. Comp.* **25** (1971), 885–895.
2. P. Erdős, On integers of the form $2^n + p$ and some related problems, *Summa Brasil Math.* **11** (1950), 1–11.
3. ———, On a problem concerning congruence systems, *Mat. Lapok* **3** (1952), 122–128.
4. P. Erdős and R. L. Graham, Old and new problems and results in combinatorial number theory, *Monogr. Enseign Math.* **28**, L'Enseignement Mathématique, Geneva, 1980.
5. R. L. Graham, A Fibonacci-like sequence of composite numbers, this MAGAZINE **37** (1964), 322–324.

6. A. de Polignac, Six propositions arithmologiques déduites du crible d'Eratosthene, *Nouv. Ann. Math.* **8** (1849), 423–429.

7. A. Schinzel, Reducibility of polynomials and covering systems of congruences, *Acta Aritm.* **13** (1967), 91–101.

Proof Without Words: Sums of Triangular Numbers

$$t_n = 1 + 2 + \cdots + n \Rightarrow t_1 + t_2 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$$



$$t_1 + t_2 + \cdots + t_n = \frac{1}{6}(n+1)^3 - (n+1)\cdot\frac{1}{6} = \frac{n(n+1)(n+2)}{6}$$

——ROGER B. NELSEN
LEWIS & CLARK COLLEGE
PORTLAND OR 97219