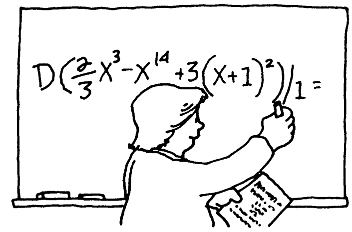
CLASSROOM CAPSULES

EDITOR

Frank Flanigan
Department of Mathematics
and Computer Science
San Jose State University
San Jose, CA 95192



A Classroom Capsule is a short article that contains a new insight on a topic taught in the earlier years of undergraduate mathematics. Please submit manuscripts prepared according to the guidelines on the inside front cover to Frank Flanigan.

Strings of Strongly Composite Integers and Invisible Lattice Points

Peter Schumer, Middlebury College, Middlebury, VT

Many of us are familiar with the result that there are arbitrarily large gaps between successive primes. The proof runs as follows: For any positive integer n, consider the sequence of n consecutive numbers $(n+1)!+2$, $(n+1)!+3, \ldots, (n+1)!+(n+1)$. Since $j \mid (n+1)!+j$ for each $j = 2, \ldots, n+1$, we have constructed a string of n composite numbers. But is this sequence the best one we can construct?

In our sequence above, some of the numbers may be just barely composite, i.e., a product of two distinct primes or the square of a prime. Also, the construction does not preclude the possibility of another string of n composites made up of smaller positive integers. Recently I discovered a construction that generates arbitrarily long strings of strongly composite numbers; that is, each number has at least a prescribed number of prime divisors. Furthermore, if the primes are specified, the method ensures that the numbers generated are as small as possible. Let us state the result formally:

Theorem 1. *For any given n and k there is a string of n consecutive composite numbers each divisible by at least k distinct primes.*

The proof relies on the Chinese remainder theorem, which I now state for reference:

Chinese Remainder Theorem. *Suppose that the positive integers $m_1, \ldots, m_n$ are pairwise relatively prime and let $b_1, \ldots, b_n$ be arbitrary integers. Then the linear congruences*

$$\begin{gathered} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_n \pmod{m_n} \end{gathered}$$

have a simultaneous solution. Moreover, the solution is unique modulo $m_1 \cdots m_n$.

Recall that $x \equiv b_i \pmod{m_i}$ means that $m_i | x - b_i$ or equivalently that x and b_i have the same remainder on division by m_i. The uniqueness condition means that if x and y are two solutions to the system of congruences then $x \equiv y \pmod{m_1 \cdots m_n}$. Now to the proof of the theorem:

Proof of Theorem 1. Let p_r denote the rth prime number. So $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Let $m_1 = p_1 \cdots p_k$, $m_2 = p_{k+1} \cdots p_{2k}$, and in general $m_i = p_{(i-1)k+1} \cdots p_{ik}$ for $i = 1, \ldots, n$. Now consider the system of linear congruences

$$\begin{aligned} x &\equiv -1 \pmod{m_1} \\ x &\equiv -2 \pmod{m_2} \\ &\vdots \\ x &\equiv -n \pmod{m_n}. \end{aligned}$$

Since the moduli are pairwise relatively prime, the Chinese remainder theorem guarantees a solution for x. But then $m_1 | (x+1)$, $m_2 | (x+2), \ldots,$ and $m_n | (x+n)$. Hence $x+1, x+2, \ldots, x+n$ is a string of n consecutive composite numbers each divisible by at least k distinct primes. This completes our proof.

If we replace $-1, -2, \ldots, -n$ in the linear congruences by the numbers in another arithmetic progression with common difference d, then we see there is an arbitrarily long string of strongly composite numbers with common difference d. Similarly we can construct strings of strongly composite numbers whose successive differences form a geometric progression, a Fibonacci sequence, or any other favorite string of numbers. (For example, see solution 345 in the March 1989 issue of *The College Mathematics Journal*.)

The following example shows how to construct the string guaranteed by Theorem 1.

Example. We will find five consecutive integers with the ith integer divisible by the ith prime for $1 \le i \le 5$ (so $n = 5$ and $k = 1$). We need to solve

$$\begin{aligned} x &\equiv -1 \pmod{2} \\ x &\equiv -2 \pmod{3} \\ x &\equiv -3 \pmod{5} \\ x &\equiv -4 \pmod{7} \\ x &\equiv -5 \pmod{11}. \end{aligned}$$

We seek a solution of the form $x = -1c_1 - 2c_2 - 3c_3 - 4c_4 - 5c_5$ where for each i, $c_i \equiv 1 \pmod{p_i}$ and $c_i \equiv 0 \pmod{p_j}$ for $j \neq i$. For example, we want $c_3 \equiv 0 \pmod{2}$, $c_3 \equiv 0 \pmod{3}$, $c_3 \equiv 1 \pmod{5}$, $c_3 \equiv 0 \pmod{7}$, and $c_3 \equiv 0 \pmod{11}$. So $462 | c_3$ since $462 = 2 \times 3 \times 7 \times 11$ and $c_3 \equiv 1 \pmod{5}$. Simply take multiples of 462 until one is congruent to 1 (mod 5). We readily see that $c_3 = 3 \times 462 = 1386$ works. (Alternatively, since 5 and 462 are relatively prime, Euclid's algorithm produces integers $a = 185$ and $b = 2$ such that $5a - 462b = 1$. Then $c_3 = -462b = 1 - 5a = -924$ also works.) Similarly we obtain $c_1 = 1155$, $c_2 = -770$, $c_4 = 330$, and $c_5 = 210$.

Now $x = -1c_1 - 2c_2 - 3c_3 - 4c_4 - 5c_5 = -6143$ is one solution of the system of congruences. Since all solutions are congruent modulo $2 \times 3 \times 5 \times 7 \times 11 = 2310$, the smallest positive solution is $x = -6143 + 3 \times 2310 = 787$. So 788, 789, 790, 791, and 792 are the smallest five consecutive numbers divisible by 2, 3, 5, 7, and 11, respectively. (However, they are not the smallest five consecutive composite numbers. That distinction belongs to 24, 25, 26, 27, and 28.) We could obtain infinitely many such sequences by simply adding multiples of 2310 to each member of our sequence.

We now turn our attention to a nice variation of this method to lattice points, which appears in Apostol's book [*Introduction to Analytic Number Theory*, Springer-Verlag, 1976, 119–120]. A lattice point in the plane is a point (a, b) where a and b are integers. An observer at the origin will not be able to see some lattice points; for example, (4, 6) is hidden behind (2, 3). In fact, a lattice point is visible from the origin if and only if a and b are relatively prime.

Theorem 2. *The set of lattice points in the plane visible from the origin contains arbitrarily large square gaps. That is, given any $k > 0$ there is a lattice point (a, b) such that none of the lattice points $(a + r, b + s)$, $1 \le r \le k$, $1 \le s \le k$, is visible from the origin.*

We will construct such an invisible square for $k = 3$ that gives the full flavor of the proof in Apostol's book. In fact the proof could easily be extended to lattice points in three or more dimensions. Our construction is also instructive in showing the disparity between a neat theoretical solution and the messy details inherent in working out a concrete example.

Example. Let $k = 3$. Consider the 3×3 matrix M whose entries are the first nine primes:

$$M = \begin{bmatrix} 2 & 3 & 5 \\ 7 & 11 & 13 \\ 17 & 19 & 23 \end{bmatrix}.$$

Let a_i be the product of all primes in the ith row and let b_i be the product of all primes in the ith column. So $a_1 = 30$, $a_2 = 1001$, $a_3 = 7429$, $b_1 = 238$, $b_2 = 627$, and $b_3 = 1495$. The numbers a_i are pairwise relatively prime, as are the b_i. Note that $a_1 a_2 a_3 = b_1 b_2 b_3 = 223092870$.

Next consider the system of congruences

$$a \equiv -1 \pmod{a_1}$$
$$a \equiv -2 \pmod{a_2}$$
$$a \equiv -3 \pmod{a_3}.$$

By the Chinese remainder theorem this system has a solution that is unique modulo 223092870. Proceeding as in the previous example and with some computer assistance, we obtain the least positive solution $a = 119740619$. Thus $30 \mid 119740620$, $1001 \mid 119740621$, and $7429 \mid 119740622$.

Similarly, the system

$$b \equiv -1 \pmod{b_1}$$
$$b \equiv -2 \pmod{b_2}$$
$$b \equiv -3 \pmod{b_3}$$

leads to the least positive solution $b = 121379047$. Hence $238 \mid 121379048$, $627 \mid 121379049$, and $1495 \mid 121379050$.

Now consider the 3×3 square with opposite vertices at $(a+1, b+1)$ and $(a+3, b+3)$. None of the points in the square is visible from the origin. Since $a \equiv -r \pmod{a_r}$ and $b \equiv -s \pmod{b_s}$ for $1 \le r \le 3$, $1 \le s \le 3$, the prime in row r and column s of M divides both $a+r$ and $b+s$. Hence $a+r$ and $b+s$ are not relatively prime, and thus the lattice point $(a+r, b+s)$ is not visible from the origin.

This particular 3×3 square of invisible lattice points is far from the origin. Perhaps we can find another 3×3 square of invisible lattice points that is closer by selecting different primes, or the same primes in a different order, for the entries of M.

If we use the first sixteen primes to construct a 4×4 square of invisible lattice points, we would have to make calculations modulo $2 \times 3 \times \cdots \times 53 = 32589158477190044730$. Such a project is beyond the courage of this author!

Exploring the Volume-Surface Area Relationship

Keith A. Struss (student), Rose-Hulman Institute of Technology, Terre Haute, IN

At first glance it appears to be a coincidence that the surface area of a sphere may be found by taking the derivative of its volume function. However, as we shall see, a particular mathematical relationship often holds between the volume of an object and its surface area—namely,

$$dV = A\,d\tau, \tag{1}$$

where dV is the increase in volume of the solid that would result from coating it with a uniform layer of thickness $d\tau$, and A is the surface area of the solid. Of course, dV and $d\tau$ are infinitesimals. To see that this is reasonable, recall from elementary calculus that the volume of some solids may be computed by using cross-sectional areas as follows

$$V(x) = \int_a^x A(u)\,du. \tag{2}$$

Now, let $A(\tau)$ denote the surface area of the solid when it is uniformly coated by a coating of thickness τ. A natural analogue of (2) is

$$V(\tau) = \int_0^\tau A(u)\,du \tag{3}$$

where $V(\tau)$ is the additional volume arising from coating the solid; therefore differentiating and evaluating the expression at $\tau = 0$ yields

$$\left.\frac{dV}{d\tau}\right|_{\tau=0} = A(0), \tag{4}$$

which is just another way of expressing (1).

Let's verify this for the sphere. Since $V = (4/3)\pi r^3$, we know that

$$dV = \frac{dV}{dr}dr = 4\pi r^2 dr. \tag{5}$$