Indecomposable Numbers: 10589

Tim Keller; GCHQ Problem Solving Group

The American Mathematical Monthly, Vol. 106, No. 5. (May, 1999), p. 473.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28199905%29106%3A5%3C473%3AIN1%3E2.0.CO%3B2-S

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/maa.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

http://www.jstor.org
Sat Dec 22 05:26:35 2007

Indecomposable Numbers

10589 [1997, 362]. *Proposed by Tim Keller, Fair Oaks, CA.* Fix $n \geq 3$, and let S be the set of positive integers congruent to 1 modulo n. A number $m \in S$ is called *indecomposable* if it is not the product of two smaller numbers in S. Problem 2 from the 1977 International Mathematical Olympiad asks for a number that can be expressed as the product of indecomposable numbers in more than one way. Show that the least such number is the product of two numbers each of the form $k(k+n)$.

Solution by the GCHQ Problems Group, Cheltenham, U. K. Define a *clone* to be a number expressible as a product of indecomposable factors in two different ways. Let m be the smallest clone. By the minimality of m, no indecomposable factor can appear in both expressions. Let $an+1$ be the smallest indecomposable factor in either expression, and let $bn+1 = m/(an+1)$. Let $cn+1$ be an indecomposable factor in the other expression, and let $dn+1 = m/(cn+1)$. Thus $m = (an+1)(bn+1) = (cn+1)(dn+1)$.

Since $cn+1$ is indecomposable, $an+1$ does not divide it. Also $an+1$ does not divide $dn+1$, since otherwise $dn+1$ is a smaller clone than m. Therefore $an+1$ is not prime and factors as pq, where $p|(cn+1)$ and $q|(dn+1)$. Both p and q are coprime to n.

Now $p|(an+1)$ and $p|(cn+1)$, so $p|(c-a)n$. Since p is coprime to n, we have $p|(c-a)$, so $c = rp+a$, where $r \geq 1$ since $c > a$. Hence $cn+1 = rpn+an+1 = rpn+pq = p(rn+q)$. Similarly, $q|(d-a)n$ leads to $dn+1 = q(sn+p)$, where $s \geq 1$. Thus $m = p(rn+q)q(sn+p)$.

Finally, we show that $r = s = 1$. Let $t = p(n+q)q(n+p)$. If $r > 1$ or $s > 1$, then $t < m$, so t must not be a clone. Since $t = pq \times (n+p)(n+q)$ and pq is indecomposable, pq must divide one of the two factors in the factorization $t = p(n+q) \times q(n+p)$. But if $pq|p(n+q)$, then $pq|pn$, and $q|n$, a contradiction since q is coprime to n. An identical argument shows that pq cannot divide $q(n+p)$.

With $r = s = 1$, we have $m = p(n+p) \times q(n+q)$, as desired.

Editorial comment. The proposer and the NCCU Problems Group both noted that pq is not necessarily the smallest composite congruent to 1 modulo n, giving the example $n = 336$, where $336k+1$ is prime for $1 \leq k \leq 3$, $336 \cdot 4 + 1 = 5 \cdot 269$, and $336 \cdot 5 + 1 = 41 \cdot 41$, but $5 \cdot 269(5+336)(269+336) > 41 \cdot 41(41+336)(41+336)$.

Solved also by X. Wang, NCCU Problems Group, and the proposer.

Negatively Correlated Vectors of Signs

10593 [1997, 456]. *Proposed by Donald E. Knuth, Stanford University, Stanford, CA.* A certain matrix has m rows and $n = 1+k^2$ columns. All entries of the matrix are ± 1, and the dot product of any two columns is less than or equal to 0. Prove that the total number of positive entries in the matrix is at most $\frac{1}{2}m(n+k)$, and construct a matrix that achieves this upper bound.

Solution by GCHQ Problem Solving Group, Cheltenham, U. K. Consider the sum S of the dot products of all pairs of columns. Since each dot product is nonpositive, so is S. If row i has r_i positive entries, then its contribution to the sum is $\binom{r_i}{2} + \binom{n-r_i}{2} - r_i(n-r_i)$, which equals $\left((2r_i - n)^2 - n\right) / 2$.

Substituting $r_i = (n+k+b_i)/2$ leads to

$$S = \frac{1}{2}\sum_{i=1}^{m}\left((k+b_i)^2 - n\right) = \frac{1}{2}\sum_{i=1}^{m}\left((k+b_i)^2 - \left(1+k^2\right)\right) = \frac{1}{2}\sum_{i=1}^{m}\left(2kb_i + b_i^2 - 1\right).$$

Since $S \leq 0$, we obtain

$$\sum_{i=1}^{m} b_i \leq \frac{1}{2k}\sum_{i=1}^{m}(1-b_i^2).$$