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

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

Since $S \leq 0$, we obtain

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

Since $r_i = (1+k+k^2+b_i)/2$ and r_i is an integer, b_i must be odd, and so $1-b_i^2 \le 0$ for all i. Therefore $\sum_{i=1}^m b_i \le 0$. The total number of positive entries in the matrix thus satisfies

$$\sum_{i=1}^m r_i = \sum_{i=1}^m \frac{1}{2}(n+k+b_i) = \frac{m}{2}(n+k) + \frac{1}{2}\sum_{i=1}^m b_i \le \frac{m}{2}(n+k).$$

Achieving the bound requires $\sum_{i=1}^m b_i = 0$, which occurs only when half the rows have $b_i = +1$ and the other half have $b_i = -1$. Thus it is necessary that m be even. One matrix that achieves the bound when $m = 2(n!)$ is formed by taking all $n!$ permutations of a row with $\frac{1}{2}(n+k+1)$ positive entries and all $n!$ permutations of a row with $\frac{1}{2}(n+k-1)$ positive entries. By symmetry, all of the dot products are equal, and their sum is zero; hence each dot product must be zero.

Editorial comment. John H. Lindsey observed that equality in the bound requires m to be divisible by 4. The proposer asked for the smallest number of rows allowing equality to be achieved for a given n. He and Richard Stong independently provided a construction with $m = 2\binom{n-1}{(k+1)k/2}$.

Solved also by R. J. Chapman (U. K.), J. H. Lindsey II, K. McInturff, R. Stong, and the proposer.

n-Tuples Whose Elements Divide Their Sum

10597 [1997, 457]. *Proposed by David Cox, Amherst College, Amherst, MA.* Fix an integer $n \ge 2$, and let $d_1, d_2, \ldots, d_n$ be positive integers with no common divisor greater than 1. Suppose that d_i divides $d_1 + \cdots + d_n$ for $1 \le i \le n$.
(a) Prove that $d_1 d_2 \cdots d_n$ divides $(d_1 + \cdots + d_n)^{n-2}$.
(b) For each $n \ge 3$, give an example to show that the exponent in part **(a)** cannot be made smaller.

Solution by GCHQ Problems Group, Cheltenham, U. K.
(a) Let p be a prime factor of the product $d_1 d_2 \cdots d_n$, and let p^k be the highest power of p dividing any one of the d_i. We have $p^k \mid \sum d_i$, and thus $p^{k(n-2)} \mid \left(\sum d_i\right)^{n-2}$. Since $d_1, \ldots, d_n$ have no common factor greater than 1, some element d_j is not divisible by p. Furthermore, since $p \mid \sum d_i$, at least two summands are not divisible by p. Hence the highest power of p dividing $\prod d_i$ does not exceed $p^{k(n-2)}$. Repeating this for each prime factor shows that $\prod d_i$ divides $(\sum d_i)^{n-2}$.
(b) Let $d_1 = 1$, $d_2 = n-1$, and $d_i = n$ for $3 \le i \le n$. Here $\sum d_i = n(n-1)$, which is divisible by each d_i. Since $d_1 = 1$, the greatest common divisor is 1. We have $\prod d_i = n^{n-2}(n-1)$. Since n and $n-1$ are coprime, the smallest power of $n(n-1)$ divisible by $n^{n-2}(n-1)$ is $(n(n-1))^{n-2}$, and thus the exponent cannot be reduced.

Editorial comment. Other examples submitted for part **(b)** by various solvers included

$$d_1 = 1, d_2 = 2, \text{ and } d_i = 3 \cdot 2^{i-3} \text{ for } 3 \le i \le n$$

and

$$d_1 = 1, d_i = 2 \text{ for } 2 \le i \le n-1, \text{ and } d_n = 2n-3.$$

Using Euclid's sequence 2, 3, 7, 43, 1807, ..., the San Jose State Problem Solving Ring gave an example in which $d_1 d_2 \cdots d_n = (d_1 + \cdots + d_n)^{n-2}$. Another use of Euclid's sequence appears in this MONTHLY in the solution of Problem 10532 [1996, 510; 1998, 775], where references are given.

M. J. Knight and the San Jose State Problem Solving Ring each showed that for given n the set D_n of n-tuples $(d_1, d_2, \ldots, d_n)$ satisfying the conditions of the problem is finite. For example, D_2 contains only the pair (1, 1), and D_3 contains only the triples (1, 1, 1), (1, 1, 2), (1, 2, 3), and their permutations. The finiteness of D_n is equivalent to the finiteness