Distinct Solution to a Linear Congruence

Donald G. Adams *Vadim Ponomarenko*[†]
Arizona State University *San Diego State University*

† Corresponding author.

1 Linear Congruence

Given $n, k \in \mathbb{N}$ and $a_1, a_2, \ldots, a_k \in \mathbb{Z}_n$, it is known classically (e.g. [4, 5]) that the linear congruence

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1 \quad (\text{in } \mathbb{Z}_n) \tag{$*$}$$

has a solution if and only if $\gcd(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_n^\times$, the group of units of $\mathbb{Z}_n$. We ask when such a solution exists with *distinct* $x_i \in \mathbb{Z}_n$, a question that appears to have been overlooked in the literature. In general, some additional conditions are necessary; for example, $1x_1 + 1x_2 + 1x_3 = 1$ does not have a solution with distinct $x_i \in \mathbb{Z}_3$.

Our partial solution has a stronger coefficient condition, and another restriction involving $\phi(n)$, the Euler totient. The general case remains open.

Theorem 1. *If $k \leq \phi(n)$ and $a_i \in \mathbb{Z}_n^\times$ $(1 \leq i \leq k)$, then there exist distinct $x_i \in \mathbb{Z}_n$ satisfying $(*)$.*

Proof. We first construct $y_1, y_2, \ldots y_k$ iteratively, as will be explained. For notational convenience, for $i < j$ we set $y_{i,j} = y_i(1 - a_{i+1}y_{i+1})(1 - a_{i+2}y_{i+2}) \cdots (1 - a_{j-1}y_{j-1})$ (note that $y_{i,i+1} = y_i$). We set $y_1 = a_1^{-1}$; for $j > 1$ we let y_j be any element chosen from $S_j \setminus T_j$, where $S_j = \{y \in \mathbb{Z}_n : 1 - a_jy \in \mathbb{Z}_n^\times\}$, and $T_j = \{y \in \mathbb{Z}_n : y(1 + a_jy_{i,j}) = y_{i,j}, \text{ for some } i \text{ with } 1 \leq i < j\}$. Note that the defining property of S_j ensures that $1 - a_jy_j$ is invertible, and that T_j ensures that $y_j \neq y_{i,j}(1 - a_jy_j) = y_{i,j+1}$ for all $i < j$.

Now, set $x_i = y_{i,k+1}$, for $1 \leq i \leq k$. Note that $a_1x_1 + a_2x_2 + \cdots + a_kx_k$ conveniently telescopes to 1, because $a_1y_1 = 1$. Suppose that $x_i = x_j$ (for $i < j$). Then $y_{i,k+1} = y_{j,k+1}$. We may cancel the common terms, because they were constructed to be invertible, to get $y_{i,j+1} = y_{j,j+1} = y_j$, which contradicts our construction of y_j. Hence the x_i are distinct, and a solution to $(*)$.

It remains to prove that $S_j \setminus T_j$ is nonempty. We first prove that $|S_j| = |\mathbb{Z}_n^\times| = \phi(n)$, by showing that $f(y) = 1 - a_jy$ is a bijection on $\mathbb{Z}_n$, and thus $f(S_j) = \mathbb{Z}_n^\times$. If $f(y) = f(y')$, then $1 - a_jy = 1 - a_jy'$ and $a_j(y - y') = 0$, but a_j is invertible, hence $y = y'$. So f is injective on a finite set and hence bijective. Finally, we prove that $|T_j| \leq j - 1 \leq k - 1 < k \leq \phi(n)$, by showing that

$y(1 + a_j y_{i,j}) = y_{i,j}$ has at most one solution y. If $(1 + a_j y_{i,j})$ is invertible, then $y = (1 + a_j y_{i,j})^{-1} y_{i,j}$ is unique. If not, then there is some $m > 1$ with $m|n$ and $m|(1 + a_j y_{i,j})$. If there is a solution y then also $m|y_{i,j}$, so $m|(1 + a_j y_{i,j}) - a_j y_{i,j} = 1$, a contradiction.

□

If n is prime, we can do better, solving the problem completely. Clearly it is necessary that $k \leq n$, and that not all a_i are zero, i.e. $\gcd(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_n^\times$.

Theorem 2. *Let n be an odd prime, $k \leq n$, and gcd$(a_1, a_2, \ldots, a_k) \in \mathbb{Z}_n^\times$. Then there exist distinct $x_i \in \mathbb{Z}_n$ satisfying $(*)$, if and only if either (a) $k < n$, or (b) not all of the a_i are equal.*

Proof. The nonzero a_i are in $\mathbb{Z}_n^\times$, and $\phi(n) = n - 1$, so unless there are n nonzero a_i, we can apply Theorem 1, and arbitrarily assign leftover distinct elements from $\mathbb{Z}_n$ to those x_i where $a_i = 0$. If $k = n$ and $a_1 = \cdots = a_k = t$, then there is only one possible solution, and it fails because $t(0 + 1 + \cdots + n) = tn\frac{n+1}{2} = 0$ in $\mathbb{Z}_n$.

Remaining is the case where $k = n$, the a_i are all nonzero and not all equal. Set $a'_i = a_i - a_1$. More than zero, but less than n, of the a'_i are nonzero, so we can find distinct $x_i \in \mathbb{Z}_n$ with $a'_1 x_1 + \cdots a'_n x_n = 1$. But now $a_1 x_1 + \cdots + a_n x_n = (a'_1 + a_1)x_1 + \cdots + (a'_n + a_1)x_n = (a'_1 x_1 + \cdots + a'_n x_1) + a_1(x_1 + \cdots + x_n) = 1 + a_1(0 + 1 + \cdots + n) = 1 + a_1 n\frac{n+1}{2} = 1$ in $\mathbb{Z}_n$. □

In fact, we believe that a similar result holds for composite n; this is supported by preliminary computer calculations. For example, consider $n = 6, k = 5, (a_1, a_2, a_3, a_4, a_5) = (2, 2, 2, 3, 3)$. Neither of the strong conditions of Theorem 1 are met; however $(x_1, x_2, x_3, x_4, x_5) = (2, 4, 5, 0, 1)$ satisfies $(*)$.

Conjecture 3. *Let $k < n$ and gcd$(a_1, a_2, \ldots a_k) \in \mathbb{Z}_n^\times$. Then there exist distinct $x_i \in \mathbb{Z}_n$ satisfying $(*)$.*

2 Application

Fix the finite abelian group $\mathbb{Z}_n \times \mathbb{Z}_n$. We consider multisets[1] of elements such that their sum is zero; we call these zero-sum multisets. They have a rich literature and history (see [3]), arising from fundamental number theoretic questions about nonunique factorization.

It is well-known that the largest minimal (i.e. containing no other nontrivial zero-sum multiset) zero-sum multiset is of size $2n - 1$. Recently it has been shown (see [2]) that any zero-sum multiset of this size contains some element of multiplicity $n - 1$. In [1] it was shown that the remaining multiplicities $a_1, a_2, \ldots a_k$ (where $a_1 + a_2 + \cdots + a_k = n$) must admit a solution to $(*)$ in distinct elements of $\mathbb{Z}_n$, leaving open the question of when this occurs.

[1] For historical reasons these are called sequences in the literature, although the elements are not ordered.

Corollary 4. *Let $n > 0$, $k \leq \phi(n)$, and $a_i \in \mathbb{N}$ with $a_1 + \cdots + a_k = n$ and $gcd(a_i, n) = 1$. Then there is an irreducible zero-sum multiset in $\mathbb{Z}_n \times \mathbb{Z}_n$ whose elements have multiplicities $n-1, a_1, a_2, \ldots, a_k$.*

Corollary 5. *Let $n > 0$ be prime, $k \leq n$, and $a_i \in \mathbb{N}$ with $a_1 + \cdots + a_k = n$ and $gcd(a_1, a_2, \ldots, a_k, n) = 1$. Then there is an irreducible zero-sum multiset in $\mathbb{Z}_n \times \mathbb{Z}_n$ whose elements have multiplicities $n-1, a_1, a_2, \ldots, a_k$ if and only if $1 < k < n$.*

References

[1] Weidong Gao and Alfred Geroldinger. On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. *Integers*, 3:A8, 45 pp. (electronic), 2003.

[2] Weidong Gao, Alfred Geroldinger, and David J. Grynkiewicz. Inverse zero-sum problems. III. *Acta Arith.*, 141(2):103–152, 2010.

[3] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[4] J. V. Uspensky and M. A. Heaslet. *Elementary Number Theory*. McGraw-Hill Book Company, Inc., New York, 1939.

[5] H. S. Vandiver. Questions and Discussions: Discussions: On Algorithms for the Solution of the Linear Congruence. *Amer. Math. Monthly*, 31(3):137–140, 1924.