

involve

a journal of mathematics

Distinct solution to a linear congruence

Donald Adams and Vadim Ponomarenko

 mathematical sciences publishers

Distinct solution to a linear congruence

Donald Adams and Vadim Ponomarenko

(Communicated by Scott Chapman)

Given $n, k \in \mathbb{N}$ and $a_1, a_2, \dots, a_k \in \mathbb{Z}_n$, we give conditions for the equation $a_1x_1 + a_2x_2 + \dots + a_kx_k = 1$ in \mathbb{Z}_n to admit solutions with all the x_i distinct.

A sufficient condition is that $k \leq \phi(n)$ and a_i be invertible in \mathbb{Z}_n for all i .

If $n > 2$ is prime, the following conditions together are necessary and sufficient: $k \leq n$, each a_i is nonzero, and either $k < n$ or not all of the a_i are equal.

1. Linear congruence

Given $n, k \in \mathbb{N}$ and $a_1, a_2, \dots, a_k \in \mathbb{Z}_n$, it is known classically [Uspensky and Heaslet 1939; Vandiver 1924] that the linear congruence

$$a_1x_1 + a_2x_2 + \dots + a_kx_k = 1 \pmod{n} \quad (1)$$

has a solution if and only if $\gcd(a_1, a_2, \dots, a_k) \in \mathbb{Z}_n^\times$, 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 (1).*

Proof. We first construct y_1, y_2, \dots, y_k iteratively, as will be explained. For notational convenience, for $i < j$ we set

$$y_{i,j} = y_i(1 - a_{i+1}y_{i+1})(1 - a_{i+2}y_{i+2}) \cdots (1 - a_{j-1}y_{j-1})$$

MSC2000: 11B50, 11D79.

Keywords: linear congruence, minimal zero-sum sequence, property B.

(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

$$S_j = \{y \in \mathbb{Z}_n : 1 - a_j y \in \mathbb{Z}_n^\times\},$$

$$T_j = \{y \in \mathbb{Z}_n : y(1 + a_j y_{i,j}) = y_{i,j} \text{ for some } i \text{ with } 1 \leq i < j\}.$$

Note that the defining property of S_j ensures that $1 - a_j y_j$ is invertible, and that T_j ensures that $y_j \neq y_{i,j}(1 - a_j y_j) = y_{i,j+1}$, for all $i < j$.

Now, set $x_i = y_{i,k+1}$ for $1 \leq i \leq k$. Note that $a_1 x_1 + a_2 x_2 + \dots + a_k x_k$ conveniently telescopes to 1, because $a_1 y_1 = 1$. 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 (1).

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 $f(y) = 1 - a_j y$ is a bijection on \mathbb{Z}_n , and thus $f(S_j) = \mathbb{Z}_n^\times$. If $f(y) = f(y')$, then $1 - a_j y = 1 - a_j y'$ 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. \square

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, that is, $\gcd(a_1, a_2, \dots, a_k) \in \mathbb{Z}_n^\times$.

Theorem 2. *Let n be an odd prime, $k \leq n$, and $\gcd(a_1, a_2, \dots, a_k) \in \mathbb{Z}_n^\times$. Then there exist distinct $x_i \in \mathbb{Z}_n$ satisfying (1), 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 $a_1 = \dots = a_k = t$, then there is only one possible solution, and it fails because $t(0 + 1 + \dots + n) = tn(n + 1)/2 = 0$ 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 $a'_1x_1 + \dots + a'_nx_n = 1$. But now we have

$$\begin{aligned} a_1x_1 + \dots + a_nx_n &= (a'_1 + a_1)x_1 + \dots + (a'_n + a_1)x_n \\ &= (a'_1x_1 + \dots + a'_nx_n) + a_1(x_1 + \dots + x_n) \\ &= 1 + a_1(0 + 1 + \dots + n) \\ &= 1 + a_1n(n + 1/2) = 1 \quad \text{in } \mathbb{Z}_n. \end{aligned} \quad \square$$

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 (1).

Conjecture 3. Let $k < n$ and $\gcd(a_1, a_2, \dots, a_k) \in \mathbb{Z}_n^\times$. Then there exist distinct $x_i \in \mathbb{Z}_n$ satisfying (1).

2. Application

Fix the finite abelian group $\mathbb{Z}_n \times \mathbb{Z}_n$. We consider multisets¹ of elements such that their sum is zero; we call these zero-sum multisets. They have a rich literature and history [Geroldinger and Halter-Koch 2006], 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 [Gao et al. 2010] that any zero-sum multiset of this size contains some element of multiplicity $n - 1$. In [Gao and Geroldinger 2003] it was shown that the remaining multiplicities a_1, a_2, \dots, a_k (where $a_1 + a_2 + \dots + a_k = n$) must admit a solution to (1) in distinct elements of \mathbb{Z}_n , leaving open the question of when this occurs.

Corollary 4. *Let*

$$n > 0, \quad k \leq \phi(n) \quad \text{and} \quad a_i \in \mathbb{N}, \quad \text{with} \quad \begin{cases} a_1 + \dots + a_k = n, \\ \gcd(a_i, n) = 1. \end{cases}$$

Then there is an irreducible zero-sum multiset in $\mathbb{Z}_n \times \mathbb{Z}_n$ whose elements have multiplicities $n - 1, a_1, a_2, \dots, a_k$.

Corollary 5. *Let $n > 0$ be prime, $k \leq n$, and $a_i \in \mathbb{N}$ with*

$$a_1 + \dots + a_k = n \quad \text{and} \quad \gcd(a_1, a_2, \dots, a_k, n) = 1.$$

Then there is an irreducible zero-sum multiset in $\mathbb{Z}_n \times \mathbb{Z}_n$ whose elements have multiplicities $n - 1, a_1, a_2, \dots, a_k$ if and only if $1 < k < n$.

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

References

- [Gao and Geroldinger 2003] W. Gao and A. Geroldinger, “On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ ”, *Integers* **3** (2003), A8, 45 pp. MR 2004m:11015
- [Gao et al. 2010] W. Gao, A. Geroldinger, and D. J. Grynkiewicz, “Inverse zero-sum problems. III”, *Acta Arith.* **141**:2 (2010), 103–152. MR 2579841 Zbl 05691756
- [Geroldinger and Halter-Koch 2006] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics (Boca Raton) **278**, Chapman & Hall/CRC, Boca Raton, FL, 2006. MR 2006k:20001 Zbl 1113.11002
- [Uspensky and Heaslet 1939] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill, New York, 1939.
- [Vandiver 1924] H. S. Vandiver, “Discussions: on algorithms for the solution of the linear congruence”, *Amer. Math. Monthly* **31**:3 (1924), 137–140. MR 1520388

Received: 2010-07-07 Revised: 2010-09-29 Accepted: 2010-09-29

DJUNIOR82@gmail.com

*Arizona State University, Tempe, AZ 85287-1804,
United States*

vadim@sciences.sdsu.edu

*San Diego State University, Department of Mathematics and
Statistics, 5500 Campanile Dr., San Diego, CA 92182-7720,
United States*
<http://www-rohan.sdsu.edu/~vadim/>

involve

pjm.math.berkeley.edu/involve

EDITORS

MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhs@wfu.edu

BOARD OF EDITORS

John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
Martin Bohner	Missouri U of Science and Technology, USA bohner@mst.edu	Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
Pietro Cerone	Victoria University, Australia pietro.cerone@vu.edu.au	Frank Morgan	Williams College, USA frank.morgan@williams.edu
Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Ken Ono	University of Wisconsin, USA ono@math.wisc.edu
Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Behrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Yuval Peres	Microsoft Research, USA peres@microsoft.com
Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	Y.-F. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
Andrew Granville	Université Montréal, Canada andrew@dms.umontreal.ca	Robert J. Plemmons	Wake Forest University, USA plemmons@wfu.edu
Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
Sat Gupta	U of North Carolina, Greensboro, USA sgupta@uncg.edu	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	József H. Przytycki	George Washington University, USA przytyck@gwu.edu
Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Filip Saidak	U of North Carolina, Greensboro, USA f.saidak@uncg.edu
Karen Kafadar	University of Colorado, USA karen.kafadar@cudenver.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	Ravi Vakil	Stanford University, USA vakil@math.stanford.edu
David Larson	Texas A&M University, USA larson@math.tamu.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu

PRODUCTION

Silvio Levy, Scientific Editor

Sheila Newbery, Senior Production Editor

Cover design: ©2008 Alex Scorpan

See inside back cover or <http://pjm.math.berkeley.edu/involve> for submission instructions.

The subscription price for 2010 is US \$100/year for the electronic version, and \$120/year (+\$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY
 **mathematical sciences publishers**
<http://www.mathscipub.org>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2010 by Mathematical Sciences Publishers

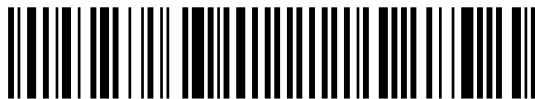
involve

2010

vol. 3

no. 3

Gracefulness of families of spiders	241
PATRICK BAHLS, SARA LAKE AND ANDREW WERTHEIM	
Rational residuacity of primes	249
MARK BUDDEN, ALEX COLLINS, KRISTIN ELLIS LEA AND STEPHEN SAVIOLI	
Coexistence of stable ECM solutions in the Lang–Kobayashi system	259
ERICKA MOCHAN, C. DAVIS BUENGER AND TAMAS WIANDT	
A complex finite calculus	273
JOSEPH SEABORN AND PHILIP MUMMERT	
$\zeta(n)$ via hyperbolic functions	289
JOSEPH D'AVANZO AND NIKOLAI A. KRYLOV	
Infinite family of elliptic curves of rank at least 4	297
BARTOSZ NASKRECKI	
Curvature measures for nonlinear regression models using continuous designs with applications to optimal experimental design	317
TIMOTHY O'BRIEN, SOMSRI JAMROENPINYO AND CHINNAPHONG BUMRUNGSUP	
Numerical semigroups from open intervals	333
VADIM PONOMARENKO AND RYAN ROSENBAUM	
Distinct solution to a linear congruence	341
DONALD ADAMS AND VADIM PONOMARENKO	
A note on nonresidually solvable hyperlinear one-relator groups	345
JON P. BANNON AND NICOLAS NOBLETT	



1944-4176(2010)3:3;1-E