Checkbooks, Cookbooks, and Matchbooks

Vadim Ponomarenko

Department of Mathematics and Statistics
San Diego State University

Sam Houston State University August 24, 2011

http://www-rohan.sdsu.edu/~vadim/checkbooks.pdf

Shameless advertising

Please encourage your students to apply to the

San Diego State University Mathematics REU.

`http://www.sci.sdsu.edu/math-reu/index.html`

This work was done jointly with undergraduate Ryan Rosenbaum, graduate students Donald Adams and Andreas Philipp, and postdoc David Grynkiewicz.

Ground Rules

This talk is all natural: $\{0, 1, 2, \ldots\}$.

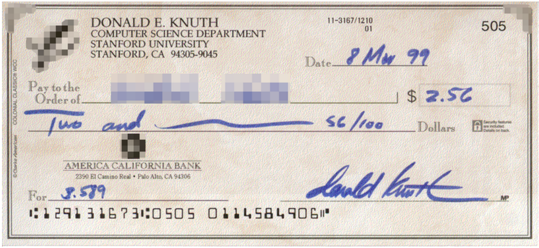
Congruences: $a \equiv b \pmod{n}$ means $n > 0$ and $n|(a - b)$.

Ground Rules

This talk is all natural: $\{0, 1, 2, \ldots\}$.

Congruences: $a \equiv b \pmod{n}$ means $n > 0$ and $n | (a - b)$.

Routing Numbers

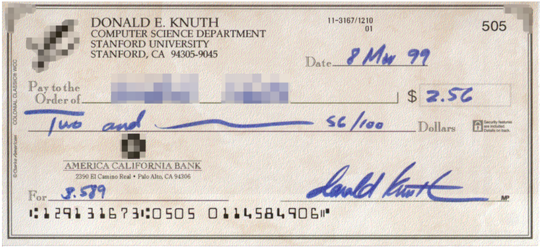


Routing number: 129131673

$x_1 = 1, x_2 = 2, x_3 = 9, \ldots, x_9 = 3$ satisfy:

$3x_1 + 7x_2 + x_3 + 3x_4 + 7x_5 + x_6 + 3x_7 + 7x_8 + x_9 \equiv 0 \pmod{10}$

Routing Numbers



Routing number: 129131673

$x_1 = 1, x_2 = 2, x_3 = 9, \ldots, x_9 = 3$ satisfy:

$3x_1 + 7x_2 + x_3 + 3x_4 + 7x_5 + x_6 + 3x_7 + 7x_8 + x_9 \equiv 0 \pmod{10}$

ISBN codes

ISBN 3-12-675495-3

90000

9 783126 754958

ISBN10: 3126754953

ISBN13: 9783126754958

ISBN10 satisfies
$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10} \equiv 0 \pmod{11}$$

ISBN13 satisfies $x_1 + 3x_2 + x_3 + 3x_4 + \cdots + 3x_{10} + x_{11} \equiv 0 \pmod{10}$

ISBN codes

ISBN10: 3126754953
ISBN13: 9783126754958

ISBN10 satisfies
$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10} \equiv 0 \pmod{11}$

ISBN13 satisfies $x_1 + 3x_2 + x_3 + 3x_4 + \cdots + 3x_{10} + x_{11} \equiv 0 \pmod{10}$

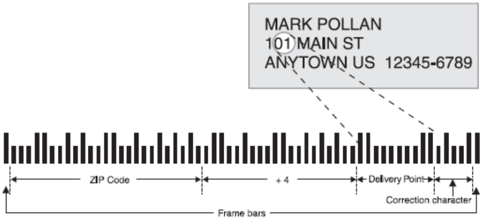
UPC Numbers

6 39382 00039 3

UPC number: 639382000393

Satisfies $3x_1 + x_2 + 3x_3 + 1x_4 + \cdots + 3x_{11} + x_{12} \equiv 0 \pmod{10}$

Postnet Barcodes



Postnet number: 123456789014

Satisfies $x_1 + x_2 + x_3 + \cdots + x_{12} \equiv 0 \pmod{10}$

VIN codes

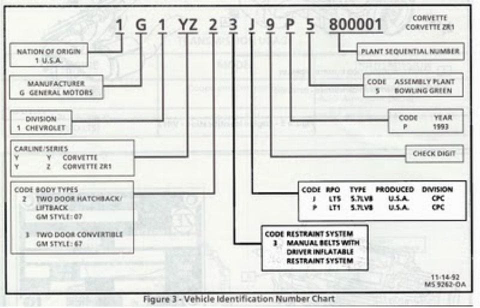


Figure 3 - Vehicle Identification Number Chart

VIN (translated): 17189231975800001

Satisfies
$8x_1 + 7x_2 + 6x_3 + 5x_4 + 4x_5 + 3x_6 + 2x_7 + 10x_8 + 10x_9 + 9x_{10} + 8x_{11} + 7x_{12} + 6x_{13} + 5x_{14} + 4x_{15} + 3x_{16} + 2x_{17} \equiv 0 \pmod{11}$

San Diego State University

Okay, enough examples already!

A multilinear modular equation consists of constants $\{r, a_i, b, n\}$ and variables $\{x_i\}$, where

$$a_1x_1 + a_2x_2 + \cdots + a_rx_r \equiv b \pmod{n}$$

Question 1: Does it have a solution?

Question 2: Does it have a distinct solution?

Note: A solution is distinct if $x_i \not\equiv x_j \pmod{n}$ for all $i \neq j$.

Okay, enough examples already!

A multilinear modular equation consists of constants $\{r, a_i, b, n\}$ and variables $\{x_i\}$, where

$$a_1x_1 + a_2x_2 + \cdots + a_rx_r \equiv b \pmod{n}$$

Question 1: Does it have a solution?

Question 2: Does it have a distinct solution?

Note: A solution is distinct if $x_i \not\equiv x_j \pmod{n}$ for all $i \neq j$.

Two Simple Examples

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod{6}$

LHS is $2(2x_1 + x_2 + x_3)$, even. RHS is odd. LHS-RHS is odd, so 6 cannot divide.

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod{5}$

No problem: $x_1 = 0, x_2 = 1, x_3 = 2$ works.

Two Simple Examples

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod 6$

LHS is $2(2x_1 + x_2 + x_3)$, even. RHS is odd. LHS-RHS is odd, so 6 cannot divide.

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod 5$

No problem: $x_1 = 0, x_2 = 1, x_3 = 2$ works.

Two Simple Examples

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod 6$

LHS is $2(2x_1 + x_2 + x_3)$, even. RHS is odd. LHS-RHS is odd, so 6 cannot divide.

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod 5$

No problem: $x_1 = 0, x_2 = 1, x_3 = 2$ works.

Two Simple Examples

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod{6}$
LHS is $2(2x_1 + x_2 + x_3)$, even. RHS is odd. LHS-RHS is odd, so 6 cannot divide.

$4x_1 + 2x_2 + 2x_3 \equiv 1 \pmod{5}$
No problem: $x_1 = 0, x_2 = 1, x_3 = 2$ works.

What's The Problem?

If $\gcd(a_1, a_2, \ldots, a_r, n)$ does not divide b, no solution.

We call this the Subgroup Obstacle.

If each a_i lies in some subgroup of $\mathbb{Z}/n\mathbb{Z}$, then every linear combination does too.

e.g. $2(\mathbb{Z}/6\mathbb{Z}) = \{0, 2, 4\} \leq (\mathbb{Z}/6\mathbb{Z})$

What's The Problem?

If $\gcd(a_1, a_2, \ldots, a_r, n)$ does not divide b, no solution.

We call this the Subgroup Obstacle.

If each a_i lies in some subgroup of $\mathbb{Z}/n\mathbb{Z}$, then every linear combination does too.

e.g. $2(\mathbb{Z}/6\mathbb{Z}) = \{0, 2, 4\} \leq (\mathbb{Z}/6\mathbb{Z})$

Finally, a Theorem

Thm: [folklore]

A multilinear modular equation has a solution if and only if the subgroup obstacle does not hold.

Proof: Suppose that $\gcd(a_1, \dots, a_r, n) | b$. Choose $\{x_i\}$ so that $a_1 x_1 + \cdots + a_r x_r = \gcd(a_1, \dots, a_r)$. Let $c > 0$ with $c \gcd(a_1, \dots, a_r) \equiv \gcd(a_1, \dots, a_r, n) \pmod{n}$.
Let $d > 0$ with $d \gcd(a_1, \dots, a_r, n) = b$. Then $a_1(cdx_1) + a_2(cdx_2) + \cdots + a_r(cdx_r) \equiv b \pmod{n}$.

Finally, a Theorem

Thm: [folklore]

A multilinear modular equation has a solution if and only if the subgroup obstacle does not hold.

Proof: Suppose that $\gcd(a_1, \ldots, a_r, n) | b$. Choose $\{x_i\}$ so that $a_1 x_1 + \cdots + a_r x_r = \gcd(a_1, \ldots, a_r)$. Let $c > 0$ with $c \gcd(a_1, \ldots, a_r) \equiv \gcd(a_1, \ldots, a_r, n) \pmod{n}$.
Let $d > 0$ with $d \gcd(a_1, \ldots, a_r, n) = b$. Then
$a_1(cdx_1) + a_2(cdx_2) + \cdots + a_r(cdx_r) \equiv b \pmod{n}$.

Another Obstacle

We focus henceforth on finding distinct solutions.

$x_1 - x_2 \equiv 0 \pmod{n}$ has no solutions.

We call this the Bivariate Obstacle.

Another Obstacle

We focus henceforth on finding distinct solutions.

$x_1 - x_2 \equiv 0 \pmod{n}$ has no solutions.

We call this the Bivariate Obstacle.

A New Perspective

By taking some $a_i = 0$ if needed, we henceforth assume that $r = n$.

Then $\{x_i\}$ is a permutation of $\{0, 1, \ldots, n-1\}$.

Set $S = x_1 + x_2 + \cdots + x_n = 0 + 1 + \cdots + (n-1) = \frac{(n-1)n}{2}$.
Note that either $S \equiv 0 \pmod{n}$ or $S \equiv \frac{n}{2} \pmod{n}$.

A New Perspective

By taking some $a_i = 0$ if needed, we henceforth assume that $r = n$.

Then $\{x_i\}$ is a permutation of $\{0, 1, \ldots, n-1\}$.

Set $S = x_1 + x_2 + \cdots + x_n = 0 + 1 + \cdots + (n-1) = \frac{(n-1)n}{2}$.
Note that either $S \equiv 0 \pmod{n}$ or $S \equiv \frac{n}{2} \pmod{n}$.

A New Perspective

By taking some $a_i = 0$ if needed, we henceforth assume that $r = n$.

Then $\{x_i\}$ is a permutation of $\{0, 1, \ldots, n-1\}$.

Set $S = x_1 + x_2 + \cdots + x_n = 0 + 1 + \cdots + (n-1) = \frac{(n-1)n}{2}$.
Note that either $S \equiv 0 \pmod{n}$ or $S \equiv \frac{n}{2} \pmod{n}$.

Equivalence for Multilinear Modular Equations

Fix k. Suppose there are a_i', b' with $a_i \equiv a_i' + k \pmod{n}$, $b \equiv b' + kS \pmod{n}$.

$a_1x_1 + \cdots + a_nx_n \equiv (a_1' + k)x_1 + \cdots + (a_n' + k)x_n = k(x_1 + \cdots + x_n) + (a_1'x_1 + \cdots + a_n'x_n) = kS + a_1'x_1 + \cdots + a_n'x_n$.

Hence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{n}$ if and only if $a_1'x_1 + \cdots + a_n'x_n \equiv b - kS \equiv b' \pmod{n}$.

We say that $\{a_i, b, n\}$ and $\{a_i', b', n\}$ are equivalent.

Equivalence for Multilinear Modular Equations

Fix k. Suppose there are a'_i, b' with $a_i \equiv a'_i + k \pmod{n}$, $b \equiv b' + kS \pmod{n}$.

$a_1x_1 + \cdots + a_nx_n \equiv (a'_1 + k)x_1 + \cdots + (a'_n + k)x_n = k(x_1 + \cdots + x_n) + (a'_1x_1 + \cdots + a'_nx_n) = kS + a'_1x_1 + \cdots + a'_nx_n$.

Hence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{n}$ if and only if $a'_1x_1 + \cdots + a'_nx_n \equiv b - kS \equiv b' \pmod{n}$.

We say that $\{a_i, b, n\}$ and $\{a'_i, b', n\}$ are equivalent.

Equivalence for Multilinear Modular Equations

Fix k. Suppose there are a'_i, b' with $a_i \equiv a'_i + k \pmod{n}$, $b \equiv b' + kS \pmod{n}$.

$a_1x_1 + \cdots + a_nx_n \equiv (a'_1 + k)x_1 + \cdots + (a'_n + k)x_n = k(x_1 + \cdots + x_n) + (a'_1x_1 + \cdots + a'_nx_n) = kS + a'_1x_1 + \cdots + a'_nx_n$.

Hence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{n}$ if and only if $a'_1x_1 + \cdots + a'_nx_n \equiv b - kS \equiv b' \pmod{n}$.

We say that $\{a_i, b, n\}$ and $\{a'_i, b', n\}$ are equivalent.

Equivalence for Multilinear Modular Equations

Fix k. Suppose there are a_i', b' with $a_i \equiv a_i' + k \pmod{n}$, $b \equiv b' + kS \pmod{n}$.

$a_1x_1 + \cdots + a_nx_n \equiv (a_1' + k)x_1 + \cdots + (a_n' + k)x_n = k(x_1 + \cdots + x_n) + (a_1'x_1 + \cdots + a_n'x_n) = kS + a_1'x_1 + \cdots + a_n'x_n$.

Hence $a_1x_1 + \cdots + a_nx_n \equiv b \pmod{n}$ if and only if $a_1'x_1 + \cdots + a_n'x_n \equiv b - kS \equiv b' \pmod{n}$.

We say that $\{a_i, b, n\}$ and $\{a_i', b', n\}$ are equivalent.

An Example

$$1x_1 + 1x_2 + 1x_3 + 3x_4 + 3x_5 + 5x_6 \equiv 2 \pmod 6$$

$S = 15 \equiv 3 \pmod 6$, so this is equivalent to $0x_1 + 0x_2 + 0x_3 + 2x_4 + 2x_5 + 4x_6 \equiv 5 \pmod 6$, which has no solutions at all by the subgroup obstacle.

Note: $x_1 = 2, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

An Example

$$1x_1 + 1x_2 + 1x_3 + 3x_4 + 3x_5 + 5x_6 \equiv 2 \pmod 6$$

$S = 15 \equiv 3 \pmod 6$, so this is equivalent to $0x_1 + 0x_2 + 0x_3 + 2x_4 + 2x_5 + 4x_6 \equiv 5 \pmod 6$, which has no solutions at all by the subgroup obstacle.

Note: $x_1 = 2, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

An Example

$$1x_1 + 1x_2 + 1x_3 + 3x_4 + 3x_5 + 5x_6 \equiv 2 \pmod 6$$

$S = 15 \equiv 3 \pmod 6$, so this is equivalent to $0x_1 + 0x_2 + 0x_3 + 2x_4 + 2x_5 + 4x_6 \equiv 5 \pmod 6$, which has no solutions at all by the subgroup obstacle.

Note: $x_1 = 2, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

Another Example

$$1x_1 + 1x_2 + 1x_3 + 1x_4 + 2x_5 \equiv 3 \pmod 6$$

$S \equiv 3$, so this is equivalent to $x_5 - x_6 \equiv 0 \pmod 6$, which has no distinct solutions by the bivariate obstacle.

Note: $x_1 = 3, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

Another Example

$$1x_1 + 1x_2 + 1x_3 + 1x_4 + 2x_5 \equiv 3 \pmod{6}$$

$S \equiv 3$, so this is equivalent to $x_5 - x_6 \equiv 0 \pmod{6}$, which has no distinct solutions by the bivariate obstacle.

Note: $x_1 = 3, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

Another Example

$$1x_1 + 1x_2 + 1x_3 + 1x_4 + 2x_5 \equiv 3 \pmod 6$$

$S \equiv 3$, so this is equivalent to $x_5 - x_6 \equiv 0 \pmod 6$, which has no distinct solutions by the bivariate obstacle.

Note: $x_1 = 3, x_2 = x_3 = x_4 = x_5 = x_6 = 0$ solves the non-distinct version.

Today's Other Theorem

Thm: [GPP] A multilinear modular equation has a distinct solution if and only if, for all equivalent equations, neither the subgroup nor the bivariate obstacles hold.

Proof Strategy: Replace $\mathbb{Z}/n\mathbb{Z}$ with a general finite abelian group. One more obstacle arises, for Klein 4-group.

Today's Other Theorem

Thm: [GPP] A multilinear modular equation has a distinct solution if and only if, for all equivalent equations, neither the subgroup nor the bivariate obstacles hold.

Proof Strategy: Replace $\mathbb{Z}/n\mathbb{Z}$ with a general finite abelian group. One more obstacle arises, for Klein 4-group.

Concrete Version

Thm: Consider $a_1 x_1 + \cdots + a_n x_n \equiv b \pmod{n}$. This has a distinct solution, unless either:

1. $\gcd(a_2 - a_1, a_3 - a_1, \ldots, a_n - a_1, n)$ does not divide $b - a_1 S$ (subgroup obstacle), or
2. For some c, d, i, j, all of the following hold:
   - For all $k \notin \{i, j\}$, $a_k \equiv c \pmod{n}$
   - $a_i \equiv c + d \pmod{n}$
   - $a_j \equiv c - d \pmod{n}$
   - $b \equiv cS \pmod{n}$
   - $\gcd(d, n) = 1$

   (bivariate obstacle)

Open Problems

Problem: What about distinct solutions to *systems* of multilinear modular equations?

e.g. $1x_1 + 2x_2 + 2x_3 + 1x_4 \equiv 2 \pmod 4$,

$1x_3 + 1x_4 \equiv 3 \pmod 4$.

Easier Problem: What if the systems are decoupled?

e.g. $1x_1 + 2x_2 \equiv 2 \pmod 4, 1x_3 + 1x_4 \equiv 3 \pmod 4$.

Open Problems

Problem: What about distinct solutions to *systems* of multilinear modular equations?

e.g. $1x_1 + 2x_2 + 2x_3 + 1x_4 \equiv 2 \pmod 4$,

$1x_3 + 1x_4 \equiv 3 \pmod 4$.

Easier Problem: What if the systems are decoupled?

e.g. $1x_1 + 2x_2 \equiv 2 \pmod 4, 1x_3 + 1x_4 \equiv 3 \pmod 4$.

For Further Reading

- D. Adams, P
  Distinct Solutions to a Linear Congruence.
  Involve 3 (3), 2010.
- D. Grynkiewicz, A. Philipp, P
  Arithmetic-Progression-Weighted Subsequence Sums.
  To appear in *Israel Math Journal*.
- Preprints available at:
  http://www-rohan.sdsu.edu/~vadim/research.html