Discrete mathematics

Petr Kovář & Tereza Kovářová
petr.kovar@vsb.cz

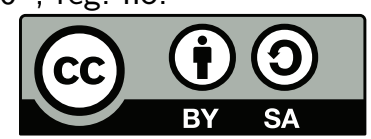
VŠB – Technical University of Ostrava

Winter Term 2022/2023
DiM 470-2301/02, 470-2301/04, 470-2301/06

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

The translation was co-financed by the European Union and the Ministry of Education, Youth and Sports from the Operational Programme Research, Development and Education, project "Technology for the Future 2.0", reg. no. CZ.02.2.69/0.0/0.0/18_058/0010212.



About this file

This file is meant to be a guideline for the lecturer. Many important pieces of information are not in this file, they are to be delivered in the lecture: said, shown or drawn on board. The file is made available with the hope students will easier catch up with lectures they missed.

For study the following resources are better suitable:

- Meyer: Lecture notes and readings for an http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-fall-2005/readings/" (weeks 1-5, 8-10, 12-13), MIT, 2005.
- Diestel: Graph theory http://diestel-graph-theory.com/ (chapters 1-6), Springer, 2010.

See also http://homel.vsb.cz/~kov16/predmety_dm.php

Lecture overview

Chapter 6. Congruences and modular arithmetics

- motivation
- division and divisibility
- congruence relation
- modular arithmetics
- linear congruences in one variable
- methods of solving
- examples and applications

6. Congruences and modular arithmetics

Modern electronic communication makes use of coding theory and cryptography.

- coding – storing or transfer of data with possible loss or disruption of the data; we require to minimize the possible loss
- cryptography – storing or transfer of data, which has to stay hidden from or unreadable for third parties

Using results of Number Theory and Grout Theory.

Exampkles

- CD storage format, mp3
- digital phone calls
- bar codes, ISBN
- RSA cryptosystem

Now follows a brief introduction to Number Theory used in later sections. We will be mostly using integers on a limited set (8, 16, 32 bits . . .).

Motivation examples

First we show/recall counting "mod n" and we learn to answer following questions:

Example

A devise read a UPC bar code. Is 041331021641 a valid UPC bar code?

Example

We wrote an ISBN book number 0-03-001559-5. Is this a valid ISBN code?

Later we show *some* errors can be detected and some can be corrected.

Example

We know the fourth digit of the UPC bar code 041331021641 is wrong, what is the correct digit?

Example

We know the ISBN book code 0-03-001559-5 is wrong. We know we often swap adjacent digits while writing. Can you derive the correct ISBN code?

Divisibility

Let a, b be two integers. We say a divides b, if there exists an integer k, such that $a \cdot k = b$, we write $a \mid b$.
If not, we say a does not divide b, we write $a \nmid b$.
Integer a is the divisor of b and b is a multiple of a.

Example

It holds $3 \mid 6, \quad 3 \mid 15$.
Also it holds $2 \mid -6, \quad 5 \mid -5 \quad$ a $\quad 7 \mid 0$.
However $6 \nmid 3, \quad 2 \nmid 5, \quad 4 \nmid -6, \quad 0 \nmid 1$.
It holds that $0 \mid 0$, while $0 = k0$, for an arbitrary $k \in \mathbb{Z}$.
We can't divide by zero, but zero can be a divisor, however a divisor of zero only.

Operation vs. relation

Division is an operation $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$.
The result of the division of an arbitrary number by a nonzero number is the resulting (third) number.

Example

It holds $18 : 3 = 6, \quad 0 : 7 = 0, \quad 18 : 4 = \frac{9}{2}$.

Divisibility is a relation $|\subset \mathbb{Z} \times \mathbb{Z}$.
Two number (in the given order) are or are not related – one is the divisor of the second or not.

Example

3 divides 18.
7 divides 0.
4 does not divide 18.

Properties of divisibility

Theorem

Let b, c be integers and let a be a nonzero integer. Platí

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- If $a \mid b$ then $a \mid bc$ for all integer c.
- If $a \mid b$ and $b \mid c$, then $a \mid c$.

Examples

Because $3 \mid 12$, then $3 \mid 12c$ for every integer c.
(notice, not only $12c$, but also $12c + 3$, $12c + 6$, and $12c + 9$)

Corollary

Let b, c be integers and let a be a nonzero integer. If $a \mid b$ and $a \mid c$, then $a \mid rb + sc$ for arbitrary integers r, s.

The Quotient Remainder Theorem

For very integer a and every natural number b there exist unique integers q and r, such that $a = qb + r$, where $0 \leq r < b$.

Integer q is the quotient and non negative integer r is the remainder when dividing a by b.

Example

For $a = 111$ and $b = 9$ holds:

$$\begin{aligned} 111 &= 11 \cdot 9 + 12 \\ 111 &= 12 \cdot 9 + 3 \quad \text{must hold } 0 \leq r < 9 \\ 111 &= 13 \cdot 9 - 6 \end{aligned}$$

Example

It holds $7 \mid 21$, therefore $21 = 3 \cdot 7 + 0$, remainder is $r = 0$.
Since $8 \nmid 21$, therefore $21 = 2 \cdot 8 + 5$, remainder is $r = 5 \neq 0$.

Integer division with a remainder

By the Quotient Remainder Theorem we can to each pair of integers a, b ($b > 0$) assign an integer quotient and a remainder after integer division.

Operation integer division with a remainder

Let a, b be two integers.
In the equality $a = q \cdot b + r$ given gy the Quotient Remainder Theorem is a the dividend, b is the divisor, q is the integer quotient and r is the remainder after integer division of a by b.
The following notation is used to denote the two integer operations of quotient and remainder.

$$q = a \operatorname{div} b, \quad r = a \bmod b$$

Example

For $a = 111$ and $b = 9$ from the previous example holds:

$$111 \operatorname{div} 9 = 12, \qquad 11 \bmod 9 = 3$$

Notice, "mod" written inside a parenthesis has a different meaning (later).

Congruences

Let a, b be integers, let m be a positive integer. We say a, b are congruent modulo m, if both yield the same remainder after dividing by m. We write

$$a \equiv b \pmod{m}.$$

Otherwise we write

$$a \not\equiv b \pmod{m}.$$

Using the "mod" operation introduced earlier we can write

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \bmod m = b \bmod m.$$

Example

It holds $7 \equiv 1 \pmod{2}$, since 7 is odd.
It holds $12 \equiv 0 \pmod{2}$, since 12 is even.
It holds $61\,725 \equiv 0 \pmod{3}$, since 61 725 is a multiple of 3.

Equivalent formulations for congruence of two numbers

Lemma

Let a, b be integers, let m be a positive integer. Then $a \equiv b \pmod{m}$ if an only if $m \mid (b - a)$.

Example

It holds $8\,298 \equiv 8\,228 \pmod{7}$, because the difference $8\,298 - 8\,228 = 70$ is a multiple of 7.

Lemma

Let a, b be integers, let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if there exists an integer k such that $b = a + km$.

Example

Evaluate $748\,549 \bmod 7$ (the remainder after dividing 748 549 by 7).

It holds $748\,549 = 700\,000 + 48\,549 \equiv 48\,549 = 49\,000 - 451 \equiv -451 = -490 + 39 \equiv 39 = 35 + 4 \equiv 4 \pmod{7}$.

Properties of congruences

Congruences with the same modulus can be summed and multiplied.

Theorem

Let a, b, c, d be integers, let m be a positive integer.
If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then also $a + c \equiv b + d \pmod{m}$, $ac \equiv bd \pmod{m}$.

Example

Because $7 \equiv 12 \pmod{5}$ a $-7 \equiv 3 \pmod{5}$, then also
$7 - 7 \equiv 12 + 3 \pmod{5}$ a $7 \cdot (-7) \equiv 12 \cdot 3 \pmod{5}$.

Notice, the reverse implication does not hold!

Example

It holds $3 + 6 \equiv 7 + 5 \pmod{3}$, but $3 \not\equiv 7 \pmod{3}$ nor $6 \not\equiv 5 \pmod{3}$.
Similarly $10 \cdot 6 \equiv 4 \cdot 15 \pmod{5}$, but $10 \not\equiv 4 \pmod{5}$ nor $6 \not\equiv 15 \pmod{5}$.

Modular arithmetics

We can sum and multiply remainders, when dividing by the same divisor (or modulus). The result is expressed again as a remainder modulo m.

Definition

Let a, b be integers. We introduce operations "$+_m$" and "$\cdot_m$" using the usual sum and product and the "mod" operation.

$$a +_m b = (a + b) \bmod m, \qquad a \cdot_m b = (a \cdot b) \bmod m.$$

This can also be introduces as counting with congruence classes modulo m.

Example

Counting on the clock: $9 +_{12} 5 = 2, \quad (9 + 5) \bmod 12 = 2.$

Example

The sum of two even integers or the sum of odd two integers is an even integer.

$$a +_m b = (a + b) \bmod 2.$$

Modular arithmetics - continued

Such operations have "nice" properties. They are

- closed on the set $\{0, 1 \ldots, m-1\}$ (under operation modulo m),
- commutative, $a +_m b = b +_m a, \qquad a \cdot_m b = b \cdot_m a,$
- asociative,

$$a +_m (b +_m c) = (a +_m b) +_m c, \qquad a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c,$$

- and distributive with respect to addition,

$$a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c,$$

- there exist opposite numbers $-a = m - a$.
- However inverses might not exist!

Greatest common divisor and least common multiple

A prime is such positive integer that has *two* positive divisors: one and itself.

Definition

Let a, b be two integers. Greatest common divisor of a, b is such a positive common divisor m of a, b, which is divisible by each other common divisor. We denote it $\mathrm{GCD}(a, b)$ or simply (a, b). Moreover, if $\mathrm{GCD}(a, b) = 1$, we say a, b are coprime.

Examples

Numbers 91 and 77 are not coprime, $\mathrm{GCD}(91, 77) = 7$.
Numbers 92 and 77 are coprime, $\mathrm{GCD}(92, 77) = 1$.

We can have a set of mutually coprime numbers.

Finding a prime factorization, or verifying that a certain integer is a prime, is a difficult task.

Euclid's algorithm

IS an efficient way to find the GCD of two positive integers a, b.

- easy to implement,
- no need for prime factorization.

Euklidův algoritmus

Let a, b be two positive integers. We divide a by b in modular arithmetic with a remainder (using the Quotient Remainder Theorem) and proceed repeating this process, until the remainder is zero.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

The last non-zero remainder r_n is the greatest common divisor.

Example

Find the greatest common divisor of 414 ans 662.

We denote $a = 414$, $b = 662$. (It is better to denote $a = 662$, $b = 414$.)

Proceed by the Euclid's algorithm:

$$\begin{aligned} 414 &= 662 \cdot 0 + 414 \\ 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

The greatest common divisor $(414, 662) = 2$.

Euclid's algorithm – implementation

Input are two positive integers a, b. Repeatedly we divide in modular arithmetic with a remainder.

Euclid's algorithm

```
int a,b;              // positive integers
x = a;                // dividend
y = b;                // divisor
while (y<>0) {
   r = x mod y;       // evaluate the remainder r
   x = y;             // the divisor becomes the dividend
   y = r;             // the remainder becomes the divisor
}
return x;             // (a,b) last non-zero remainder
```

Variable `x` holds the last *non-zero* remainder, which is the greatest common divisor of a, b.

Further use of Euclid's algorithm

Euclid's algorithm work not only for integers but on any set with two (nice) operations.

- dividing polynomials
- for so called Gaussian integers

The following theorem states that the greatest common divisor of a,b can be expressed as a linear combination of a, b.

Bézout's Theorem

Let a, b be positive integers. There exists integers r, s such that $\mathrm{GCD}(a, b) = ra + sb$.

Bézout's Theorem provides a nice tool to solve certain problems expressed by congruences.

Euclid's algorithm can be easily extend to evaluate the coefficients r, s in the Bézout's equality.

Example

We have shown that the greatest common divisor of 414 and 662 is 2. Find the Bézout's coefficients r, s, so that $2 = r \cdot 414 + s \cdot 662$.

Using the Euclid's algorithm we got:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Now from the next-to-the last equation express $\mathrm{GCD}(414, 662)$ and backward substitutions.

$$\begin{aligned} 2 &= 166 - 2 \cdot 82 \\ 2 &= 166 - 2 \cdot (248 - 166 \cdot 1) = (-2) \cdot 248 + 3 \cdot 166 \\ 2 &= (-2) \cdot 248 + 3 \cdot (414 - 248 \cdot 1) = 3 \cdot 414 + (-5) \cdot 248 \\ 2 &= 3 \cdot 414 + (-5) \cdot (662 - 414 \cdot 1) = 8 \cdot 414 + (-5) \cdot 662 \end{aligned}$$

The coefficients are $r = 8$, $s = -5$.

The following statements follow by the Bézout's Theorem

Theorem

Let a, b, c be positive integers. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

In congruences we can cancel by numbers coprime with modulus m.

Theorem

Let a, b, c be integers and m a positive integer. If $ac \equiv bc \pmod{m}$ and $(m, c) = 1$, then $a \equiv b \pmod{m}$.

In congruences we can cancel by common divisors of both sides and the modulus m.

Theorem

Let a, b, c be integers and m a positive integer. If $ac \equiv bc \pmod{cm}$, then $a \equiv b \pmod{m}$.

We use these theorems in the last part of this lecture.

Linear congruences

Definition

Let a, b be integers, let m be a positive integer, and let x be a variable. Congruence

$$ax \equiv b \pmod{m}$$

is a linear congruence in one variable.

To solve a congruence is to find *all* values of x, for which the congruence holds.

Example

Solution of the congruence $x \equiv 1 \pmod{2}$ are (precisely) all odd integers.
Solution of the congruence $x \equiv 4 \pmod{7}$ are integers $x = 7k + 4$, $k \in \mathbb{Z}$.
Solution of the congruence $3x \equiv 0 \pmod{7}$ are integers $x = 7k$, $k \in \mathbb{Z}$.
Solution of the congruence $3x \equiv 4 \pmod{7}$ are integers $x = 7k + 6$, $k \in \mathbb{Z}$.
Congruence $3x \equiv 1 \pmod{6}$ has no solution.

Now we show how to find the solutions, provided it exists.

Solving linear congruences

For solving congruences we use (similarly as for equations) so called inverses modulo m.

Definition

Let a be an integer and let m be a positive integer, where $m > 1$. The integer $\overline{a}$ is the inverse to a modulo m, if $\overline{a} \cdot a \equiv 1 \pmod{m}$.

Example

Number 5 is inverse to 3 modulo 7, because $5 \cdot 3 = 15 \equiv 1 \pmod{7}$.
Number 3 is inverse to itself modulo 8, because $3 \cdot 3 \equiv 1 \pmod{8}$.
Number 7 is inverse to 3 modulo 10, because $7 \cdot 3 \equiv 1 \pmod{10}$.
Number 8 has no inverse modulo 10, since $8 \cdot x$ is even, $8 \cdot x \not\equiv 1 \pmod{10}$.

The following theorem shows, when inverses modulo m exist.

Theorem

Let a be an integer, let m be a positive integer, $m > 1$. If a, m are coprime, then there exists the inverse $\overline{a}$ of a modulo m and is unique modulo m.

The proof is constructive, it provides a way to find the inverse $\overline{a}$ to a.

Theorem

Let a be an integer, let m be a positive integer, where $m > 1$. If a, m are coprime, then there exists the inverse $\overline{a}$ of a modulo m and is unique modulo m.

Proof: Since a, m are coprime, then by Bézout's Theorem exist integers r, s, such that

$$r \cdot a + s \cdot m = 1.$$

This implies

$$\begin{aligned} r \cdot a + s \cdot m &\equiv 1 \pmod{m} \\ r \cdot a &\equiv 1 \pmod{m} \end{aligned}$$

Hence, r is the inverse $\overline{a}$ modulo m, thus $\overline{a} = r$.
We wont prove uniqueness here. □

A stronger claim holds also: if $\mathrm{GCD}(a, m) > 1$, then no inverse to a modulo m exists.

Example

Because $(3, 7) = 1$, we can write $1 = 5 \cdot 3 - 2 \cdot 7 \equiv 3 \cdot 5 \pmod 7$.
Number 5 is inverse to 3 modulo 7, thus $\overline{3} = 5$.

Notice, if a is not coprime to modulus m, no inverse can exist!

Example

Take 14, 6. Because $(14, 6) = 2$, by Bézout's Theorem follow
$2 = 1 \cdot 14 - 2 \cdot 6$ and no such smaller integer exist.
Therefore, for no number $\overline{a}$ can hold $14\overline{a} \equiv 1 \pmod 6$.

When solving linear congruences we conclude:

Theorem

Let a, b be integers and let m be a positive integer. There exists a solution of the linear congruence $ax \equiv b \pmod m$ if and only if $GCD(a, m)$ divides b.

Solving linear congruences

Now we can solve linear congruences in one variable analogously to solving linear equations.

Example

Find all solutions of the linear congruence $3x \equiv 4 \pmod 7$.

First we find the inverse to 3 modulo 7. By previous example $\overline{3} = 5$.
We multiply both sides of the congruence by the inverse 5. We get

$$\begin{aligned} 5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\ x &\equiv 20 \pmod 7 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

The solution are all integers, that have remainder 6 when dividing by 7.
The solution is $x = 7k + 6$, where $k \in \mathbb{Z}$.

The most toilsome part is to find the inverse modulo m.

Manipulation and simplification of congruences

Let a, b, c, d be integers and let m be a positive integer.
Let $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ be congruences.

- We can add congruences with the same modulus.

$$a + c \equiv b + d \pmod{m}$$

- We can multiply congruences with the same modulus.

$$ac \equiv bd \pmod{m}$$

- We can multiply both sides of a congruence by the same integer c.

$$ac \equiv bc \pmod{m}$$

- We can cancel in congruences by c coprime with the modulus, thus for $(c, m) = 1$ is

$$ac \equiv bc \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

- We can cancel in congruences by $c = \mathrm{GCD}(a, b, m)$

$$ac \equiv bc \pmod{mc} \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

These manipulations allow to simplify and solve linear congruences.

Example

Find the solution of the congruence $5x \equiv 2 \pmod{13}$ and verify it.

Using $\overline{5} = 8$ we get $x \equiv 16 \pmod{13}$, therefore $x = 13t + 3$, $t \in \mathbb{Z}$.

Another solution: we add modulus 13 to the right side $5x \equiv 2 + 13 \pmod{13}$. Cancelation by 5 yileds $x \equiv 3 \pmod{13}$, thus $x = 13t + 3$, $t \in \mathbb{Z}$.

Verification? Substitute $5(13t + 3) \equiv 5 \cdot 13t + 15 \equiv 0t + 2 \pmod{13}$.

Example

Find the solution of the congruence $3x \equiv 2 \pmod{15}$.

Congruence has no solution, because $(3, 15) = 3$, and can't cancel by 3.

Example

Find the solution of the congruence $3x \equiv 6 \pmod{15}$.

We cancel both sides and modulus by 3. We get $x \equiv 2 \pmod{5}$.
This conguence tha the solution $x = 5t + 2$, $t \in \mathbb{Z}$, because $(3, 15) = 3$.
We canceled both sides and the modulus by 3.

Restoring an ISBN code

A friend has an excellent book on C language. Its ISBN-10 code is 80-05-001?4-1. Unfortunately, we cannot read the eighth digit. Which digit was it?

We know the ISBN-10 code must satisfy

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

We set up a linear congruence.

$$\begin{aligned} 8 + 0 + 0 + 20 + 0 + 0 + 7 + 8x_8 + 36 + 10 &\equiv 0 \pmod{11} \\ 8x_8 + 81 &\equiv 0 \pmod{11} \\ 8x_8 &\equiv -81 \pmod{11} \\ 8x_8 &\equiv 7 \pmod{11} \\ 7 \cdot 8x_8 &\equiv 7 \cdot 7 \pmod{11} \\ x_8 &\equiv 49 \equiv 5 \pmod{11} \end{aligned}$$

The missing digit of the ISBN-10 code is 5. (We used $\overline{8} = 7$ modulo 11.)
The ISBN-10 code of the book is 80-05-00154-1.

Chinese Remainder Theorem

The following theorem states, that there is a unique solution to a system of congruences with pairwise coprime moduli.

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be coprime positive integers greater than one. Let $a_1, a_2, \ldots, a_n$ be integers. The system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Has a unique solution modulo $m_1 \cdot m_2 \cdots m_n$.

We provide a general method.

Due problems solved in ancient manuscripts is the theorem called "Chinese Remainder Theorem".

The proof of the theorem is constructive, however the solution can be found using manipulations backward substitution of congruences.

Example

Find the solution of the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Based on the theorems above we get the solution of the first congruence

$$x \equiv 1 \pmod 5$$

to be $x = 1 + 5t$, where $t \in \mathbb{Z}$.
This solution we substitute the the second congruence

$$\begin{aligned} 1 + 5t &\equiv 2 \pmod 6 \\ 5t &\equiv 1 \pmod 6 \\ -t &\equiv 1 \pmod 6 \\ t &\equiv -1 = 5 \pmod 6 \end{aligned}$$

The solution of the congruence

$$t \equiv 5 \pmod 6$$

is $t = 6u + 5$, where $u \in \mathbb{Z}$.
Substituting do $x = 1 + 5t$ we get the solution of the first two congruences

$$x = 1 + 5(6u + 5) = 30u + 26, u \in \mathbb{Z},$$

which can be substituted to the third congruence. We get

$$\begin{aligned} 30u + 26 &\equiv 3 \pmod 7 \\ 2u - 2 &\equiv 3 \pmod 7 \\ 4 \cdot 2u &\equiv 4 \cdot 5 \pmod 7 \\ u &\equiv 6 \pmod 7. \end{aligned}$$

The solution is $u = 7v + 6$, where $v \in \mathbb{Z}$, which we substitute to the solution of the first two congruences.

$$x = 30u + 26 = 30(7v + 6) + 26 = 210v + 206, v \in \mathbb{Z}.$$

We get the solution of the system of three congruences.

Application of congruences – hash functions

When storing a large database we can add a new entry x to the end of the database. This is cumbersome or searching the database – we have to search the whole database.
Of there are m entries, we need $O(m)$ steps.

Hash function: We estimate the expected database size m and allocate the corresponding memory. New entry with key k we enter to position $h(k)$, where

$$h(k) = k \bmod m,$$

or the next appropriate free place after $h(k)$.
Instead of searching whole database, we start searching at position $h(k)$.

Example

Students at a university with 15 000 students, key is the social security number.

Possible hash function $h(k) = \mathit{security\_number} \bmod 15\ 000$.
Even better $h(k) = \mathit{security\_number} \bmod 30\ 000$.

Application of congruences – Pseudorandom numbers

A truly random number is computationally "expensive".
However, pseudorandom numbers we evaluate quickly

$$x_{n+1} = (ax_n + b) \bmod m,$$

where a, b, m are carefully selected integers. The value x_0 is the "seed".

Example

For example for $a = 7$, $b = 4$, $m = 9$, and $x_0 = 1$ we get

$$\begin{aligned} x_1 &= (7x_0 + 4) \bmod 9 = 11 \bmod 9 = 2 \\ x_2 &= (7x_1 + 4) \bmod 9 = 18 \bmod 9 = 0 \\ x_3 &= (7x_0 + 4) \bmod 9 = 4 \bmod 9 = 4 \\ x_4 &= (7x_0 + 4) \bmod 9 = 32 \bmod 9 = 5 \\ &\vdots \end{aligned}$$

This gives the sequence $1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, \ldots$

A commonly used random generator: $a = 7^5$, $b = 0$, $m = 2^{31} - 1$.

Application of congruences – check sums

Parity sums

Let $x_1, x_2, \ldots, x_n$ be an n-bit word.
The sender adds another bit (bits), a parity check digit

$$x_{n+1} = (x_1 + x_2 + \cdots + x_n) \bmod 2.$$

If during the transfer *one* (or an odd number) errors occur, the recipient evaluates

$$x_1 + x_2 + \cdots + x_n + x_{n+1} \not\equiv 0 \pmod 2$$

and can require ask for the message to be sent again.

Using several parity check digits, we can CORRECT certain errors without sending it again.
(example provided later)

Application of congruences – UPC bar codes

UPC bar code (Universal Product Code)

There are many variations on UPC bar codes, most of them make use of check sums.
UPC-A bar code has 12 digits. It satisfies

$$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$$

Example

Is 041331021641 a valid UPC code?

Since $0+4+3+3+9+1+0+2+3+6+12+1 = 44 \equiv 4 \pmod{10}$, therefore the code is invalid.

Application of solving linear congruences

Reconstruction of UPC bar codes

We know the UPC code 041331021641 is not valid. However it seems the fourth digit is damaged. What is the correct UPC code?

We know the digits of the UPC code 041?31021641 must satisfy

$$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$$

We set up a linear congruence.

$$\begin{aligned} 0+4+3+x_4+9+1+0+2+3+6+12+1 &\equiv 0 \pmod{10} \\ x_4+41 &\equiv 0 \pmod{10} \\ x_4 &\equiv -1 \pmod{10} \\ x_4 &\equiv 9 \pmod{10} \end{aligned}$$

The missing digit of the UPC bar code is 9. The code is 041931021641.

It is easy to verify

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} =$$
$$= 0+4+3+9+9+1+0+2+3+6+12+1 = 50 \equiv 0 \pmod{10}.$$

Further application of congruences

- ISBN/ISSN
- social security numbers (rodná čísla)
- banknote numbers
- bank account numbers
- simple ciphers

Application of solving linear congruences

Reconstruction of the social security number (rodné číslo)

An old lady forgot her social security number. She remembers her birthday and the last three digits. Thus, we can reconstruct the following parts of the number: 346509?248. What is the missing digit?

We know that the digits have to satisfy

$$x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 + x_9x_{10} \equiv 0 \pmod{11}.$$

We set up a linear congruence

$$\begin{aligned} 34 + 65 + 9 + (10x + 2) + 48 &\equiv 0 \pmod{11} \\ 1 - 1 - 2 + 10x + 2 + 4 &\equiv 0 \pmod{11} \\ 10x &\equiv -4 \pmod{11} \\ -x &\equiv -4 \pmod{11} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

The missing digit is 4.

Next lecture

Algorithms for discrete structures

- types discrete structures
- implementation of sets
- generating selection and arrangements
- generating random numbers
- combinatorial explosion