Modular Arithmetic

Discrete Mathematics
Andrei Bulatov

Congruences

- In some situations we care only about the remainder of an integer when it is divided by some specified positive number. For instance, when we ask what time it will be 50 hours from now, we care only about the remainder of 50 plus the current hour divided by 24.
- If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.

  We use the notation $a \equiv b \pmod m$ to indicate that a is congruent to b modulo m.

  If a and b are not congruent modulo m, we write $a \not\equiv b \pmod m$
- Integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

  Indeed, if $a - b = km$ and $b = qm + r$, then $a = km + b = (k + q)m + r$

Congruences (cntd)

- Examples:

  $12 \equiv 5 \pmod 7$

  $12 \equiv 6 \pmod 3$

  $12 \equiv -3 \pmod{15}$

  $12 \equiv 0 \pmod{12}$
- For any integers a, b, and m, $a \equiv b \pmod m$ if and only if $a = b + km$ for some integer k.

  By definition, $a \equiv b \pmod m$ if and only if $a - b = km$ for some integer k. Then $a = b + km$

Congruences and Arithmetic Operations

- Addition, subtraction, multiplication behave really well with respect to congruences
- **Theorem**.

  Let m be positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$, and $ac \equiv bd \pmod m$
- Proof

  For multiplication. We have $a = b + km$ and $c = d + lm$ for some k and l.

  Then $ac = (b + km)(d + lm) = bd + blm + dkm + kmlm$
  $= bd + (bl + dk + klm) \cdot m$
- Example: $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$
  $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$
  $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$

Congruences and Arithmetic Operations (cntd)

- Division is not so good:

  Although $8 \equiv 24 \pmod 4$ and $4 \equiv 8 \pmod 4$,

  $$\frac{8}{4} = 2 \not\equiv 3 = \frac{24}{8} \pmod m$$

Residues

- Let us consider the binary relation $\equiv$ modulo m on the set of integers, that is, the relation that contains pair (a,b) such that $a \equiv b \pmod m$
- It is reflexive, symmetric, and transitive. This is an equivalence relation
- Each such relation defines a partition on the set of integers into equivalence classes.
- We choose a representative from each such class

Residues (cntd)

- The residue of an integer a modulo m is such a number b that $a \equiv b \pmod m$ and $0 \le b < m$

  In other words the residue of a modulo m is the remainder of a when divided by m

- Let $\mathbb{Z}_n$ denote the set $\{0,1,2,\ldots,n-1\}$. This is the set of all possible remainders of integers when divided by n

  It is called the set of residues, and its members are called residues

Modular Arithmetic

- We define addition, subtraction, and multiplication of residues:

  Let $a,b \in \mathbb{Z}_n$. Then

  $a + b \pmod n$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a + b \pmod n$

  $a - b \pmod n$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a - b \pmod n$

  $a \cdot b \pmod n$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a \cdot b \pmod n$

- Example. Construct operation tables for $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Applications: Criptography

- One of the oldest cryptosystems is the Caesar cipher. He made messages secret by shifting each letter three letters forward. Thus B becomes E, and X is sent to A
- To express this process mathematically we first replace letters by integers from 0 to 25. For example, A is replaced by 0, K by 10.
- Next, to encrypt a message we add 3 modulo 25 to every letter.
- Finally, replace numbers with corresponding letters
- To decrypt a message, perform all the actions above in the reverse order

Applications: Criptography (cntd)

- Encrypt `SEND MORE MEN AND MUNITION'

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

S E N D M O R E M E N A N D M U N I T I O N

18 4 13 3 12 14 17 4 12 4 13 0 13 3 12 20 13 8 19 8 14 13

21 7 16 6 15 17 20 7 15 7 16 3 16 6 15 23 16 11 22 11 17 16

V H Q G P R U H P H Q D Q G P X Q L W L R Q

Applications: Criptography (cntd)

- Caesar cipher with a key. A key is just a word, e.g. `KEY'
- Replace it with numbers: 10 4 24
- Then the message is encrypted by adding 10 to the first letter, 4 to the second letter, 24 to the third letter, 10 to the fourth letter and so on.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

S E N D M O R E M E N A N D M U N I T I O N

18 4 13 3 12 14 17 4 12 4 13 0 13 3 12 20 13 8 19 8 14 13

10 4 24

2 8 11 13 16 12 1 8 10 8 11 10 17 1 22 24 11 18 23 6 24 17

C I L N Q M B I K I L K R B W Y L S X G Y R

Pseudorandom Generators

- Randomly chosen numbers are often needed for computer simulations. However, truly random numbers are very difficult to obtain.
- This is why people mostly use pseudorandom numbers
- The most commonly used procedure for generating pseudorandom numbers is the linear congruential method
- We choose four numbers: the modulus m, multiplier a, increment c, and seed x_0, with $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n < m$ for all n, by successfully using the congruence

  $$x_{n+1} \equiv a x_n + c \pmod m$$

- Typical values: $m = 2^{32}$, a = 1664525, c = 1013904223

Homework

Exercises from the Book:
No. 1, 5, 9, 12, 20, 23 (page 696)