Modular Arithmetic II

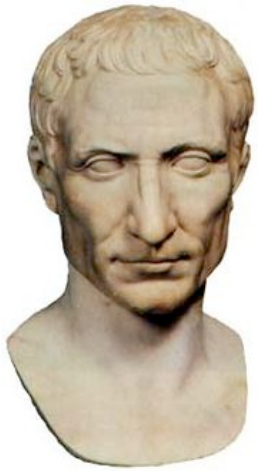
Discrete Mathematics

Andrei Bulatov

Previous Lecture

- Residues, set of residues Z_n
- Arithmetic operations on residues
- Divisors of zero
- Inverse

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 forth 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 $x_{n+1} \equiv ax_n + c \pmod{m}$
- Typical values: $m = 2^{32}$, a = 1664525, b = 1013904223

Linear Congruences

- A congruence of the form

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

  where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.
- We will solve linear congruences
- If a is relatively prime with m, then it has the inverse a^{-1}. Then

  $$a^{-1} \cdot ax \equiv a^{-1} \cdot b \pmod{m}$$
  $$x \equiv a^{-1} b \pmod{m}$$
- Find the inverse of 3 modulo 7
- Solve the linear congruence $3x \equiv 4 \pmod{m}$

The Chinese Remainder Theorem

- A linear congruence is similar to a single linear equation. What about systems of equations
- (Sun Tzu's puzzle, 400 – 460 BC):

  "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things"
- This can be translated into the following question: What are the solutions of the system of congruences

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

The Chinese Remainder Theorem (cntd)

- **Theorem**

  Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_k$ arbitrary integers. Then the system

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

  has a unique solution modulo $m = m_1 \times m_2 \times \cdots \times m_k$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem (cntd)

- Proof.

  We construct a solution to this system

  Set $M_i = \frac{m}{m_i}$ for i = 1,2,…,k. Thus M_i is the product of all the moduli except for m_i

  Since m_i and m_j are relatively prime when $i \neq j$, $\gcd(M_i, m_i) = 1$

  Therefore M_i has the inverse modulo m_i, that is y_i such that

$$M_i y_i \equiv 1 \pmod{m_i}$$

  Let us set $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k$

  Note that $M_j \equiv 0 \pmod{m_i}$ whenever $i \neq j$, all terms except for the *i*th term in this sum are congruent to 0 modulo m_i. As $M_i y_i \equiv 1 \pmod{m_i}$ we have

$$x \equiv a_i M_i y_i \equiv a_i \pmod{m_i}$$

Sun Tzu's Puzzle

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Homework

Exercises from the Book:

No. 1, 5, 9, 12, 20, 23 (page 696)