The Chinese Remainder Theorem

Discrete Mathematics

Courtesy of Andrei Bulatov

Previous Lecture

- *Congruence modulo m*
  - $a \equiv b \pmod{m}$ *if* $m \mid (a - b)$
- *Residues modulo m*
  - *Remainder* $0 \leq r < m$ *when dividing by m*
- *Integers modulo m*
  - $\mathbb{Z}_m = \{0,1,\ldots,m-1\}$
- *Modular arithmetic*
  - *Addition, subtraction, and multiplication as operations on* $\mathbb{Z}_m$

+	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

Divisors of Zero

- *Modular addition just rotates/shifts/cycles the numbers*
  - *In particular, it* **is injective as a function** $f(x) = x + a \pmod m$
- *Multiplication however is not injective over* $\mathbb{Z}_4$

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

- *A proper 0 divisor modulo m is a residue* $a \not\equiv 0 \pmod m$ *such that there exists* $b \not\equiv 0 \pmod m$ *with* $a \cdot b \equiv 0 \pmod m$.
- $\mathbb{Z}_4$ *has a proper 0 divisor.* $\mathbb{Z}_5$ *does not.*

Inverse

- *A residue b modulo m is called an inverse of a residue a if* $a \cdot b \equiv 1 \pmod{m}$, *denoted* a^{-1}

- *What is...*
  - *The inverse of 2 modulo 5?* 3
  - *The inverse of 2 modulo 4?*

- **Theorem**

  Let a be residue modulo m. The following are equivalent:

  (i) a has an inverse;

  (ii) a is not a proper divisor of 0;

  (iii) a is relatively prime with m.

Inverse (cntd)

- **Proof**.

  (i) ⇒ (ii) By contradiction.

  Suppose $a \cdot b \equiv 0 \pmod m$ *for some* b *not equal to 0.*

  Then $a^{-1} \cdot a \cdot b \equiv a^{-1} \cdot 0 \pmod m$

  $b \equiv 1 \cdot b \equiv 0 \pmod m$, *a contradiction*

  (ii) ⇒ (iii) By contraposition.

  Suppose $\gcd(a,m) = d$ *and* $a = ld$, $m = kd$.

  Then $ak \equiv kld \equiv lm \equiv 0 \pmod m$.

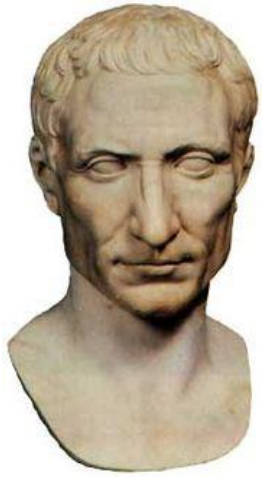
  Thus a *is a proper divisor of* 0.

  (iii) ⇒ (i)

  Suppose $\gcd(a,m) = 1$. *Then there are* u, v *with* $au + mv = 1$.

  Thus $au \equiv 1 \pmod m$; a *has an inverse.*

Applications: Cryptography



- *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 26 to every letter.*
- *Finally, replace numbers with corresponding letters*
- *To decrypt a message, perform all the actions above in the reverse order*

Applications: Cryptography (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 Z

18 4 13 3 12 14 17 4 12 4 13 0 13 3 12 20 13 8 19 8 14 13 25

21 7 16 6 15 17 20 7 15 7 16 3 16 6 15 23 16 11 22 11 17 16 2

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

Question: can the receiver ever decrypt a different message than the one that was sent? I.e. is decryption unambiguous?

Applications: Cryptography (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 Z

18 4 13 3 12 14 17 4 12 4 13 0 13 3 12 20 13 8 19 8 14 13 25

10 4 24 10 4 24 10 4

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

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

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 $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$*
- *We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by repeatedly using the congruence*

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

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

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 often need to solve linear congruences for x*
- *If a is relatively prime with m, then it has the inverse a^{-1}. Then*

$$a^{-1} \cdot ax \equiv a^{-1} \cdot b \pmod{m}$$

$$x \equiv a^{-1} \cdot b \pmod{m}$$

- *Example:*
  Solve the linear congruence $3x \equiv 4 \pmod{7}$

$3^{-1} = 5$ ✓

$x \equiv 4 \cdot 5 \bmod 7 \equiv 6 \bmod 7$

Systems of congruences

- *Sometimes an unknown x is defined by multiple linear congruences, called a system of congruences*
- *(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 (i.e. values of x satisfying) the system of congruences*

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

The Chinese Remainder Theorem

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 $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

That is, there is a solution x *with* $0 \leq x < m$, *and all other solutions are congruent modulo* m *to this solution.*

Alternatively, the solutions have the form $c + dm$

The Chinese Remainder Theorem (cntd)

- *Proof (Existence)*

Set $M_i = \frac{m}{m_i}$ for $i = 1,2,\ldots,k$ --- i.e. $M_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$

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

So, M_i has an inverse M_i^{-1} mod m_i, i.e. $M_i M_i^{-1} \equiv 1 \pmod{m_i}$

Now set $x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_k M_k M_k^{-1}$.

Since $M_j \equiv 0 \pmod{m_i}$ when $i \neq j$, we see that x is a solution:

$$x = a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_k M_k M_k^{-1} \equiv a_i M_i M_i^{-1} \pmod{m_i}$$
$$\equiv a_i \pmod{m_i}$$

The Chinese Remainder Theorem (cntd)

- *Proof (Uniqueness)*

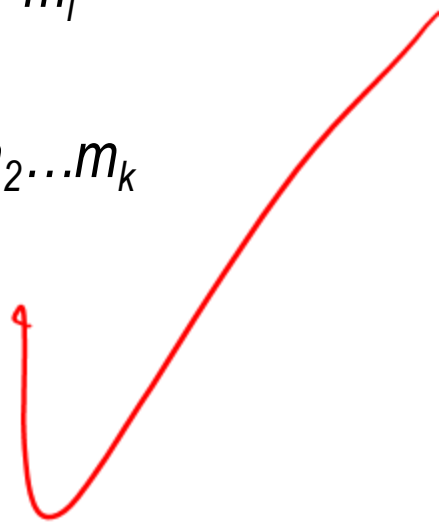
Assume x and y are solutions to the system of congruences

Then $x \equiv y \pmod{m_i}$ *for each i*

But this means that (x-y) is a multiple of m_i *for every* m_i

Hence (x-y) is a multiple of $m=LCM(m_1,\ldots,m_k)=m_1m_2\ldots m_k$

Hence $x \equiv y \pmod{m}$



Sun Tzu's Puzzle

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

Diophantine equations

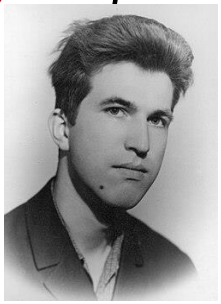
- *Systems of linear congruences are examples of a larger class of equations or massive importance in mathematics: Diophantine equations*
- *Diophantine equations are equations of the form*

  $$ax^n + by^m + cz^p + \ldots = d$$

  where x, y, z, … are unknown integers to be solved for
- *Linear congruences are Diophantine equations of the form*

  $$x = y + mz$$
- *Hilbert's tenth problem*

  Devise an algorithm which can solve any Diophantine equation
- *Hilbert's tenth problem was closed in 1970 by Yuri Matiyasevich, who showed no such algorithm can exist*

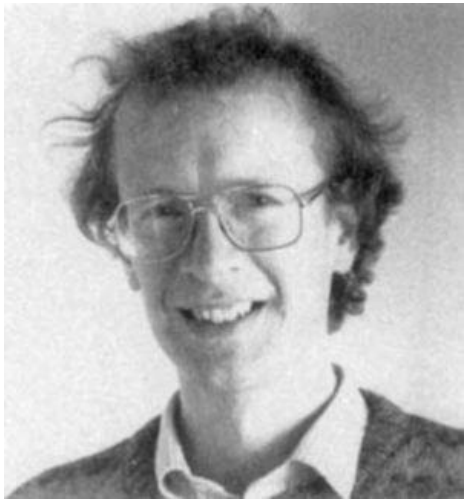


Fermat's Theorem

- **Fermat's Great (Last) Theorem**.
  For any $n > 2$, the equation $x^n + y^n = z^n$ does not have integer solutions $x,y,z > 0$

- *It had remained unproven for 358 years (posed in 1637, proved in 1995)*

- *Andrew Wiles proved it in 1995 with a 100 page proof using group theory, Galois theory, and tools from algebraic geometry*



Fermat's Little Theorem

- **Fermat's Little Theorem.**

  If p is prime and a is an integer not divisible by p, then

  $$a^{p-1} \equiv 1 \pmod{p}$$

- *Clearly, it suffices to consider only residues modulo p.*

$\mathbb{Z}_5$

·	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

Fermat's Little Theorem (cntd)

- *Fermat's Little Theorem was improved by Euler*
- **Fermat's Little Theorem improved**

  For any integers m and a such that they are relatively prime

  $$a^{\varphi(m)} \equiv 1 \pmod{m}$$

  where φ(m) denotes the Euler totient function, the number of numbers 0 < k < m relatively prime with m

- *Example:* $\mathbb{Z}_8$

Practice

Exercises from the Book:

7th edition: 17, 20, 31, 33, 35 (page 284 – 285)

8th edition: 17, 20, 31, 33, 35 (page 301)