Chinese Remainder Theorem

Discrete Mathematics

Andrei Bulatov

Previous Lecture

- Residues and arithmetic operations
- Caesar cipher
- Pseudorandom generators

Divisors of Zero

- It is not hard to see that the operation tables of addition looks similar for all m
- It is not the case for multiplication. Consider

$\cdot$	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 divisor of 0 modulo m is a residue a such that there is $b \not\equiv 0 \pmod{m}$ with $a \cdot b \equiv 0 \pmod{m}$. $\mathbb{Z}_4$ has a proper divisor of zero. $\mathbb{Z}_5$ 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}
- 3 is the inverse of 2 modulo 5
- 2 does not have an inverse modulo 4
- **Theorem**

  Let a be residue modulo m. The following conditions 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) $\Rightarrow$ (ii) By contraposition.

  Suppose $a \cdot b \equiv 0 \pmod{m}$ for some b.

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

  $b \equiv 1 \cdot b \equiv 0 \pmod{m}$

  (ii) $\Rightarrow$ (iii) By contraposition.

  Suppose $\gcd(a,m) = d$ and $a = ld$, $m = kd$. Note that $k \not\equiv 0 \pmod{m}$

  Then $ak \equiv kld \equiv lm \equiv 0 \pmod{m}$. Thus a is a proper divisor of 0.

  (iii) $\Rightarrow$ (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.

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

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

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

- Find the inverse of 3 modulo 7
- Solve the linear congruence $3x \equiv 4 \pmod{7}$

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

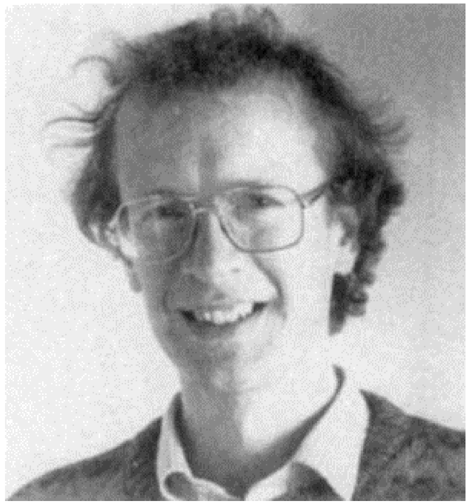
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

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



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.

$\mathbb{Z}_5$

$\cdot$	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 $\varphi(m)$ denotes the Euler totient function, the number of numbers $0 < k < m$ relatively prime with m

- Example: $\mathbb{Z}_8$

Public Key Cryptography

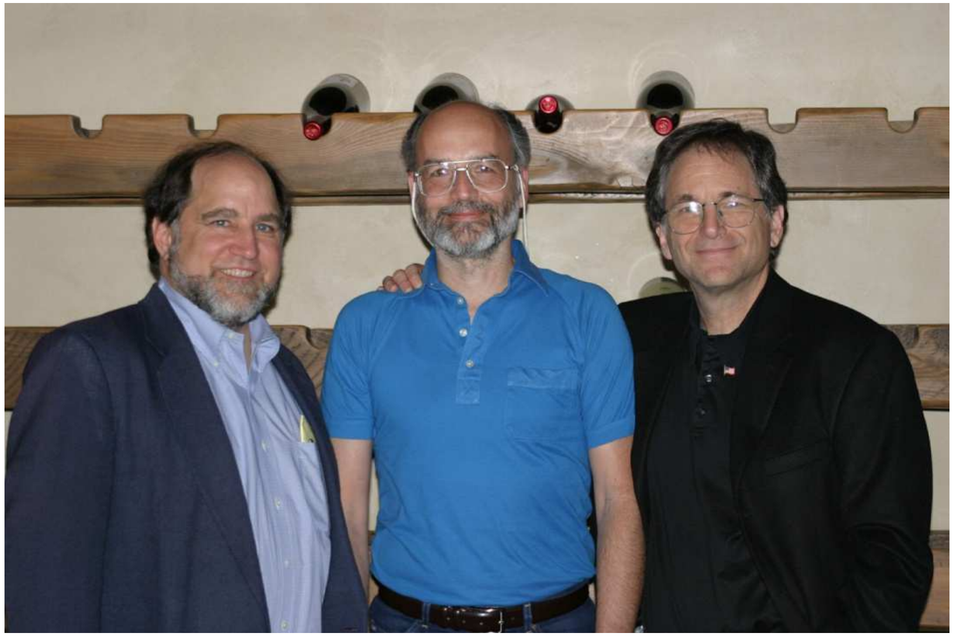
- Earlier we considered Caesar cipher. To encrypt and decrypt messages using this cipher one needs to know the key
- Caesar cipher uses the same key for encryption and decryption; it is secret, and if one knows the key he knows everything.
- Public key cryptosystems use a different approach
- Such a system uses different keys for encryption and decryption:

  Every person has a key for encryption, and can write an encrypted message

  But this does not help to decrypt the message

RSA Cryptosystem

- RSA stands for the names of the inventors: Rivest, Shamir, Adleman



From left to right:
Ron Rivest
Adi Shamir
Len Adleman

- RSA key: a modulus $n = pq$, where p and q are large prime numbers (current standards are 128, 256, or 512 digits each), n is public while p and q are secret, and

  an exponent e relatively prime with $(p – 1)(q – 1)$

RSA Encryption

- In the RSA method, messages are translated into an integer (a short message) or a sequence of integers
- Let M be the plaintext (the original message). Then the ciphertext is the residue

$$C \equiv M^e \pmod{n}$$

- Example. Encrypt the message STOP using the RSA cryptosystem with $p = 43$ and $q = 59$, so that $n = 43 \cdot 59 = 2537$, and with $e = 13$.

  Note that $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$
- Solution. Translate the letters of STOP into their numerical equivalents and group them into groups of four: 1819 1415

  Encrypt them using $C \equiv M^{13} \pmod{2537}$. We get

  $1819^{13} \equiv 2081 \pmod{2537}$ and $1415^{13} \equiv 2182 \pmod{2537}$

  Thus, the encrypted message is 2081 2182

RSA Decryption

- The decryption key d is the inverse of e modulo $(p – 1)(q – 1)$. It is secret!

  Since $\gcd(e, (p – 1)(q – 1)) = 1$, the inverse exists.

- Indeed, $de \equiv 1 \pmod{(p – 1)(q – 1)}$, therefore there is k such that $de = 1 + k(p – 1)(q – 1)$. Hence

$$C^d \equiv (M^e)^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

Note that $\varphi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = (p – 1)(q – 1)$

By Fermat's Little Theorem, $M^{k(p-1)(q-1)} = (M^{\varphi(n)})^k \equiv 1 \pmod{n}$

Hence, $C^d \equiv M \cdot M^{k(p-1)(q-1)} \equiv M \pmod{n}$

Thus $C^d \equiv M \pmod{n}$

Example

- We receive the encrypted message 0981 0461. What is the plaintext if it was encrypted using the RSA cipher from the previous example.
- Solution

  The encryption keys were $n = 43 \cdot 59$ and $e = 13$.

  It is not hard to see that $d = 937$ is the inverse of 13 modulo $42 \cdot 58 = 2436$.

  Therefore to decrypt a cipher block C, we compute

$$P \equiv C^{937} \pmod{n}$$

  In our case we have

  $0981^{937} \equiv 0704 \pmod{2537}$ and $0461^{937} \equiv 1115 \pmod{2537}$

  Thus the plaintext is 0704 1115, that is HELP

Why RSA Works

- The secrecy comes from the fact that it is incredibly difficult to find an inverse modulo a big number if we do not know it. And we do not know $(p – 1)(q – 1)$, as we do not know the prime decomposition of $n = pq$.

- However, it is also very difficult to find a prime decomposition of a number if its prime factors are big. The most efficient factorization method known requires billions of years of work of the fastest computers to factorize a 400-digit number.

- We need n to be the product of 2 prime numbers, because the method works only if the message is relatively prime with n. Thus n needs to have very few divisors.

Homework

Exercises from the Book:

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