Number Theory 2

APPLICATION TO ENCRYPTION

Linear congruence equations

- Consider special congruence equation
  $ax \equiv 1 \pmod{m}$ where $a \neq 0 \pmod{m}$.
- It's solution is given by following theorem.
- Theorem 11.25. If a and m are coprime, then $ax \equiv 1 \pmod{m}$ has a unique solution, otherwise it has no solution.
- Example. Consider $6x \equiv 1 \pmod{33}$, then $\gcd(6,33)=3$. Thus the equation has no solution.
- Example. Consider $7x \equiv 1 \pmod{9}$. $\text{Gcd}(7,9) = 1$, so has unique solution. Test the numbers 0,1,2,…8.

Linear congruence equations

- We consider the more general equation.
- $ax \equiv b \pmod{m}$ where $a \neq 0 \pmod{m}$. Suppose a and m are coprime.
- Theorem 11.26. Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. And if s is the unique solution to $ax \equiv 1 \pmod{m}$, then $x = bs$ is the unique solution to $ax \equiv b \pmod{m}$.
- Example. Consider $3x \equiv 5 \pmod{8}$. Since 3 & 8 are coprime, it has a unique solution. Testing integers $0,1,\ldots 7$, we find $3(7) = 21 \equiv 5 \pmod{8}$.

Linear congruence equations

- Theorem 11.27. Consider equation $ax \equiv b \pmod{m}$ where $d = \gcd(a,m)$.
- (i) Suppose d does not divide b. Then $ax \equiv b \pmod{m}$ has no solution.
- (ii) Suppose $d \mid b$. Then there are exactly d incongruent solutions modulo m, given by $x = x_0 + k(m/d)$, where x_0 is a particular solution of the Diophantine equation $ax + my = b$ and $k = 0,1,\ldots,d-1$.
- Example. $21x \equiv 9 \pmod{30}$. Then $x \equiv 9 \pmod{30}$ is a solution. Find the other 2 solutions.

Modular Inverse of a 2x2 matrix

Given a 2 x 2 matrix

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ Its inverse matrix is $A^{-1} = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

The determinant is det = ad –bc. The determinant must be nonzero for the inverse to exist. In general the inverse matrix will have non-integers if det is not equal to 1.

For the modular inverse we must have **only integer values** in the inverse matrix. The modular inverse of A is X so that

$AX \equiv I \pmod{n}$ where I is the identity matrix. This is similar to the modular inverse for a simple number.

Example.

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

Example.

Show that the modular inverse (mod 5) of $A = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$ is $A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

The determinant is 3*2 – 1*2 = 4. Solve $4x \equiv 1 (\text{mod } 5)$, get x = 4. So inverse is

$$A^{-1} = 4\begin{bmatrix} 2 & -1 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 8 & -4 \\ -8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} \bmod 5$$

Compute $A*A^{-1}$ to check:

$$A * A^{-1} = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix}$$ and taking mod 5 of all elements,

We get $\begin{bmatrix} 11 & 5 \\ 10 & 6 \end{bmatrix} \bmod 5 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

We use encryption matrix E = A, and decryption matrix D = A^{-1}.

Example.

Find the modular inverse of $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ mod 5 and show that $A*A^{-1} \equiv I(\text{mod } 5)$.

The same idea applies for higher order square matrices, i.e. of size n x n.

Modular Inverse – Matrix

- The determinant is the term: $a*d - b*c = det$
- For modular inverse, we cannot use $1/det$ as it's not an integer usually. So we solve:
- $det*x \equiv 1 \pmod{n}$. Now x is modular inverse of det.
- Also negative numbers are replaced by positive congruent (mod n) numbers.
- From these we get the modular inverse of A.

Example 1: Show that the modular inverse mod 7 of

$$E = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \text{ is } D = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Hence show how to encrypt the string "ACAB" using E as the encryption matrix, and fnd the encrypted string. Assume letters A to Z are represented by 1 to 26, and '*' represents 0.

1) Compute the determinant of E. Here it is,

$$3*3-2*2=5$$

So, we need the modular inverse of 5 (mod 7).

Solve $5x=1 \pmod 7$

So $x=3$ is the solution.

2) Then the inverse is given by :

$$D=3\begin{pmatrix} 3 & -2 \\ -2 & 3 \end{pmatrix}=\begin{pmatrix} 9 & -6 \\ -6 & 9 \end{pmatrix} \bmod 7$$

$$=\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

3) The string "AC" = 13, and "AB" = 12

Then the encrypted string is :

$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 3 \end{pmatrix}=\begin{pmatrix} 9 \\ 11 \end{pmatrix} \bmod 7 \quad =\begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix}=\begin{pmatrix} 7 \\ 8 \end{pmatrix} \bmod 7 \quad =\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

This gives "BD" and "*A" so the full string is

$$"BD*A"$$

Example 2: Show that the modular inverse mod 7 of

$$E = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix} \text{ is } D = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}.$$

Hence show how to encrypt the string "ABBA" using E as the encryption matrix, and fnd the encrypted string. Assume letters A to Z are represented by 1 to 26, and '*' represents 0.

1) Compute the determinant of E. Here it is,

$$3*2-1*2=3$$

So, we need the modular inverse of 3 (mod 7).

Solve $\quad 3x=1(\text{mod } 7)$

So $\qquad x=5 \qquad$ is the solution.

2) Then the inverse is given by :

$$D=5\begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix}=\begin{pmatrix} 10 & -5 \\ -10 & 15 \end{pmatrix}\text{mod } 7$$

$$=\begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}$$

3) The string "AB"=1 2, and "BA"= 21

Then the encrypted string is :

$$\begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix}=\begin{pmatrix} 5 \\ 6 \end{pmatrix}\text{mod } 7 \quad =\begin{pmatrix} 5 \\ 6 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}=\begin{pmatrix} 7 \\ 6 \end{pmatrix}\text{mod } 7 \quad =\begin{pmatrix} 0 \\ 6 \end{pmatrix}$$

This gives "EF" and "*F" so the full string is

$$"EF\ *F"$$

Modular exponentiation

We often need to compute $a^b \pmod{m}$, with a, b, m possibly large.

Example. Compute $5^3 \pmod{7}$.

- $5 \bmod 7 = 5$,
- $5^2 \bmod 7 = 4$,
- $5^3 \bmod 7 = 125 \bmod 7 = 6$,

or use $(5^2 * 5) \bmod 7 = 4*5 \pmod{7} = 6$

- So $5^4 \bmod 7 = 6*5 \pmod{7} = 2$, etc.

We use these computations in public-key encryption algorithms.

- Exercise: Compute $3^{10} \bmod 7$, without a calculator.

Modular exponentiation

- Example. Compute 5^{40} mod 7.

Use rules of modular multiplication. Don't need to find 5^{40} on a calculator.

  - $5^1 \bmod 7 = 5$
  - $5^2 \bmod 7 = 4$
  - $5^4 \bmod 7 = 4^2 \bmod 7 = 2$
  - $5^8 \bmod 7 = 2^2 \bmod 7 = 4$
  - $5^{16} \bmod 7 = 4^2 \bmod 7 = 2$
  - $5^{32} \bmod 7 = 2^2 \bmod 7 = 4$
  - $5^{40} \bmod 7 = 5^{32}\, 5^8 \pmod 7 \equiv (4*4) \bmod 7 = 2$

- We can also use a 'Fast Algorithm' on computer to do this!

Modular exponentiation

- **Algorithm.** Need binary form of exponent
- **function** modular_pow (base, exponent, modulus)

```
result := 1
while exponent > 0
    if (exponent % 2 = 1)
        result = (result * base) mod modulus
    exponent := exponent / 2
    base = (base * base) mod modulus
return result
```

Chinese remainder theorem

- An Ancient riddle (theorem) on congruences posed by Chinese mathematician Sun Tsu (3rd-5th century):
- Is there a positive integer x such that when x is divided by 3 it gives remainder 2, when x is divided by 5 it given remainder 4, when divided by 7 it gives a remainder 6?
- So we seek a solution of the following 3 congruence equations $x \equiv 2 \pmod 3$

  $x \equiv 4 \pmod 5$

  $x \equiv 6 \pmod 7$
- Note: that the moduli 3, 5, 7 are pairwise coprime.
- Also all solutions x of this system are congruent modulo $N = 3*5*7$

Chinese remainder theorem

- Chinese remainder theorem: Given the system
- $x \equiv r_1 \pmod{n_1}$
- $x \equiv r_2 \pmod{n_2}$ (1)
- ...
- $x \equiv r_k \pmod{n_k}$

where the n_i are pairwise relatively prime. Then the system has a unique solution modulo $N = n_1 n_2 \ldots n_k$.

There is an explicit formula for the solution of this system (1), which we state as following.

Let $N_1 = N/n_1$, $N_2 = N/n_2$, ..., $N_k = N/n_k$. Then each pair N_i and n_i are coprime. Let $s_1, s_2, \ldots, s_k$ be the solutions of the congruence equations:

Chinese remainder theorem

- Let $s_1, s_2, \dots, s_k$ be the solutions of the congruence equations:
- $N_1 x \equiv 1 \pmod{n_1}$
- $N_2 x \equiv 1 \pmod{n_2}$ (2)
- ...
- $N_k x \equiv 1 \pmod{n_k}$
- Then $X_0 = N_1 s_1 r_1 + N_2 s_2 r_2 + \dots + N_k s_k r_1$ is a solution of the system (1).
- Note that $N_k s_k \equiv 1 \pmod{n_k}$ for each k.
- Let's solve the Chinese congruence problem.

Chinese remainder theorem

- First apply the theorem to 1st 2 equations.
- $x \equiv 2 \pmod{3}$ (a)

  $x \equiv 4 \pmod{5}$ (b)

Theorem says there is a unique solution modulo $N = 3*5=15$.

From 2nd one, adding multiples of the modulus $n = 5$ we obtain 3 solutions less than 15.

$x = 4, 9, 14.$

Testing each of these in equation (a) we find that $x = 14$ is the only solution of both equations. So we get

(c) $x \equiv 14 \pmod{15}$ and

(d) $x \equiv 6 \pmod{7}$

Chinese remainder theorem

- Theorem tells us there is unique solution modulo $N = 15*7 = 105$.
- Adding multiples of modulus $n = 15$ to the solution $x = 14$ of the 1st equation (c) we obtain the solutions that are < 105.
- 14, 29, 44, 59, 74, 89, 104
- Testing each of these solutions in equation (d), we find that 104 is the only solution of both (c) and (d). Thus
- $x = 104$ is the smallest positive integer satisfying all 3 equations.
- Method 2. We find
- $N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = 105/3 = 35$, $N_2 = 105/5 = 21$, $N_3 = 15$

Chinese remainder theorem

- We now solve the congruence equations:
- $35x \equiv 1 \pmod{3}$, $21x \equiv 1 \pmod{5}$, $15x \equiv 1 \pmod{7}$
- Reducing 35 mod 3, 21 mod 5 and 15 mod 7 we get:
- $2x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{7}$
- Solutions of these are respectively:
- $s_1 = 2, s_2 = 1, s_3 = 1$
- We substitute into the formula $x_0 = N_1 s_1 r_1 + N_2 s_2 r_2 + \ldots + N_k s_k r_1$ to get solution of original system.

  $x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$

  Dividing this solution by the modulus $N = 105$, we get $x = 104$, the unique solution between 0 and 105.

CRT Question

- Find the smallest positive solution to the following system of congruences

$$x \equiv 1 \; mod \; 5$$
$$x \equiv 2 \; mod \; 4$$
$$x \equiv 3 \; mod \; 7$$

Fermat's Little Theorem – FLT

- French mathematician Fermat (1601-1665) proved
- Fermat's Little Theorem. If p is prime and a is an integer not divisible by p, then
- $a^{p-1} \equiv 1 \pmod{p}$
- Furthermore, for every integer a we have
- $a^p \equiv a \pmod{p}$
- Example. $4^4 \equiv 1 \pmod{5}$
- Exercise. Show that $2^{340} \equiv 1 \pmod{11}$, using Fermat's Little Theorem. Note that $340 = 10*34$ or $2^{340} = (2^{10})^{34}$

RSA Encryption

- A message is translated into a sequence of integers, e.g. a to z into 0 to 25.
- Group integers together to form larger integers, representing block of letters.
- Transform M, an integer representing plaintext, to C representing the ciphertext (the encrypted message) by
- $C = M^e \bmod n$ (encrypted text)
- Choose primes p, q and $n = pq$. Also choose e so that $\gcd(e,(p-1)*(q-1)) = 1$. And decryption key d so that $de \equiv 1 \bmod((p-1)(q-1))$. Then plaintext can be recovered by
- $C^d \bmod n \equiv M^{de} = M^{1+k(p-1)*(q-1)} \equiv M \pmod{p}$
- $C^d \bmod n \equiv M^{de} = M^{1+k(p-1)*(q-1)} \equiv M \pmod{q}$

A demonstration of the usefulness of the CRT

- CRT is extremely useful for manipulating very large integers in modulo arithmetic. We are talking about integers with over 150 decimal digits (that is, numbers potentially larger than 10^{150}).
- To illustrate the idea as to why CRT is useful for manipulating very large numbers in modulo arithmetic, let's consider an example that can be shown on a slide.

Example: Find the residue, modulo 271, of 5^{29} and hence calculate the residue, modulo 271, of $488(5^{29})$

Solution:

Step 1: Find what powers you need by successive division

2	29	
	14	1
	7	0
	3	1
	1	1
	0	1

i.e. $29_{10} = 11101_2$

$= 2^4 + 2^3 + 2^2 + 2^0$

$= 16 + 8 + 4 + 1$...use these powers to find the overall power of 29.

Step 2: Find $5^{29}\ mod(271)$

$$5^0 \equiv 1\ (mod 271)$$
$$5^1 \equiv 5\ (mod 271)$$
$$5^2 \equiv 25\ (mod 271)$$
$$5^4 \equiv\ 25^2 (mod 271) \equiv 85 (mod 271)$$
$$5^8 \equiv\ 85^2 (mod 271) \equiv 179 (mod 271)$$
$$5^{16} \equiv\ 179^2 (mod 271) \equiv 63 (mod 271)$$

So

$$5^{29} = 5^{16+8+4+1}$$
$$= 5^{16} \cdot 5^8 \cdot 5^4 \cdot 5^1$$
$$\equiv 63 \cdot 179 \cdot 85 \cdot 5\ (mod 271)$$
$$\equiv 11277 \cdot 425\ (mod 271)$$
$$\equiv [11277 (mod 271) \cdot 425 (mod 271)] (mod\ 271)$$

$$\equiv 166 \cdot 154 \ (mod\ 271)$$

$$\equiv 25564 \ (mod\ 271)$$

$\equiv 90 \ (mod\ 271)$…the residue of $5^{29} \ (mod 271)$

Step 3: Use this residue to find the large number

Thus

$488(5^{29})$ (mod 271)$\equiv 488 \cdot 90 \ (mod\ 271)$

$$\equiv 18 \ (mod\ 271)$$