Number Theory and Cryptography

Chapter 4

Solving Congruence's

Section 4.4

Section Summary

- Linear Congruences
- The Chinese Remainder Theorem
- Computer Arithmetic with Large Integers (*not currently included in slides, see text*)
- Fermat's Little Theorem
- Pseudoprimes
- Primitive Roots and Discrete Logarithms

Linear Congruence

Definition: A congruence of the form

$$ax \equiv b (\bmod m),$$

where **m** is a positive integer,
a* and *b are integers, and
x is a variable,
is called a **linear congruence**.

- The solutions to a linear congruence $ax \equiv b(\bmod m)$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\bmod m)$ is said to be **an inverse of a modulo m.**

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$

- One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists.
- Although we can not divide both sides of the congruence by a, we can **multiply** by $\bar{a}$ to solve for x.

Inverse of *a* modulo *m*

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists.

Proof:
From **BÉZOUT'S THEOREM**, If a and m are positive integers, then there exist integers s and t such that gcd(a, m) = sa + tm.

Since $\gcd(a,m) = 1$,so, sa + tm = 1.
Hence, $sa + tm \equiv 1 \pmod{m}$.
Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
Consequently, s is an inverse of a modulo m.

The uniqueness of the inverse is Exercise 7. ◁

Finding Inverses

The **Euclidean algorithm** and **Bézout coefficients** gives us a systematic approaches to finding inverses.

Example: Find an inverse of 3 modulo 7.

Solution:

Because **gcd(3,7) = 1**, by **Theorem 1**, an inverse of 3 modulo 7 exists.

– Using the Euclidian algorithm:

$7 = 2 \times 3 + 1$.

Or $-2 \times 3 + 1 \cdot 7 = 1$, $(sa + tm = 1)$

– See that -2 and 1 are **Bézout coefficients** of 3 and 7.

– Hence, $\mathbf{-2}$ is an inverse of 3 modulo 7.

– **General solution:** $-2+7\mathbb{Z}$ (every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7 i.e., 5, -9, 12, etc.)

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

Working Backwards:

$$
\begin{aligned}
4620 &= 45\cdot 101 + 75\\
101 &= 1\cdot 75 + 26\\
75 &= 2\cdot 26 + 23\\
26 &= 1\cdot 23 + 3\\
23 &= 7\cdot 3 + 2\\
3 &= 1\cdot 2 + 1\\
2 &= 2\cdot 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1\cdot 2\\
1 &= 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3\\
1 &= -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23\\
1 &= 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75\\
1 &= 26\cdot(101 - 1\cdot 75) - 9\cdot 75\\
&= 26\cdot 101 - 35\cdot 75\\
1 &= 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)\\
&= -35\cdot 4620 + 1601\cdot 101
\end{aligned}
$$

- Since the last nonzero, remainder is 1, gcd(101,4260) = 1
- **Bézout coefficients** : − 35 and 1601
- **1601** is an inverse of 101 modulo 42620

Using Inverses to Solve Congruence

- We can solve the congruence $ax \equiv b(\bmod m)$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

Solution: We found that **-2 is an inverse of 3 modulo 7 (two slides back)**. We multiply both sides of the congruence by -2 giving

$$-2 \times 3x \equiv -2 \times 4(\bmod 7)$$

$$\text{or } -6x \equiv -8 (\bmod 7)$$

$$\text{or } -6x \bmod 7 = -8 \bmod 7$$

$$\text{or } ((-6 \bmod 7)(x \bmod 7) \bmod 7) = -8(\bmod 7)$$

$$\text{or } x \bmod 7 = -8 \bmod 7$$

$$\therefore x \equiv -8 (\bmod 7)$$

Generally we say, $x \equiv b \times -2 \ (\bmod 7)$

The Chinese Remainder Theorem

- In the first century, the Chinese mathematician **Sun-Tsu** asked:

  There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?

- This puzzle can be translated into the solution of the system of congruences:

  $x \equiv 2 \pmod{3}$,

  $x \equiv 3 \pmod{5}$,

  $x \equiv 2 \pmod{7}$?

- The **Chinese Remainder Theorem** can be used to solve Sun-Tsu's problem.

The Chinese Remainder Theorem

Theorem 2: (The Chinese Remainder Theorem)

Let $\mathbf{m}_1,\mathbf{m}_2,\ldots,\mathbf{m}_n$ be pairwise relatively prime positive integers greater than one and $\boldsymbol{a}_1,\boldsymbol{a}_2,\ldots,\boldsymbol{a}_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdot$$
$$\cdot$$
$$x \equiv a_n \pmod{m_n}$$

Let $\mathbf{M_k=m/m_k}$ for $k = 1,2,\ldots,n$ and there is an integer $\boldsymbol{y_k}$, an inverse of M_k modulo m_k,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

is a unique solution modulo $m = m_1 m_2 \cdots m_n$.

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

The Chinese Remainder Theorem

Proof:

$M_k = m/m_k$ for k = 1,2,...,n and **m =** $m_1 m_2 \cdots m_n$.

$\gcd(m_k, M_k) = 1$, **by Theorem 1**, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k\, y_k \equiv 1 \pmod{m_k}$.

if $j \neq k$, then m_k divides $M_{k\,,}$ therefore

$$a_j\, M_j\, y_j \equiv 0 \pmod{m_k} \text{ when } j \neq k$$

Let, the solution is

$x = a_1\, M_1\, y_1 + a_2\, M_2\, y_2 + \cdots + a_n\, M_n\, y_n$

$x \bmod m_1 = (a_1\, M_1\, y_1 + a_2\, M_2\, y_2 + \cdots + a_n\, M_n\, y_n) \bmod m_1$

$x \bmod m_1 = (a_1\, M_1\, y_1 \bmod m_1 + 0 + \cdots + 0) \bmod m_1$ $[a_j\, M_j\, y_j \equiv 0 \pmod{m_k}$ when $j \neq k]$

$x \bmod m_1 = a_1\, M_1\, y_1 \bmod m_1$

$x \bmod m_1 = ((a_1 \bmod m_1)(M_1\, y_1 \bmod m_1)) \bmod m_1$

$x \bmod m_1 = a_1 \pmod{m_1}$ $[\text{Since } M_k\, y_k \equiv 1 \pmod{m_k}]$

$x \equiv a_1 \pmod{m_1}$

So $x \equiv a_k \pmod{m_k}$

The Chinese Remainder Theorem

Proof (Continue):

If z is any other solution of the system, then for each k = 1,2,3 … , n

$z \equiv a_k \ (mod\ m_k)$ and $x \equiv a_k \ (mod\ m_k)$

Therefore some $q_1,\ q_2 \in \mathbb{Z}$

$$z = a_k + q_1 m_k$$

$$x = a_k + q_2 m_k$$

Thus

$z - x = 1 + (q_1 - q_1)\, m_k$

This implies m_k divides (z-x), for each i. Hence $m_1 m_2 \cdots m_n$ divides (z-x)

? – Wait it will be proved later

$\boldsymbol{z \equiv x \ (mod\ m_1 m_2 \cdots m_n)}$

Conversely , if $\boldsymbol{z \equiv x \ (mod\ m_1 m_2 \cdots m_n)}$ then $m_1 m_2 \cdots m_n$ divides (z-x). Consequently, since $m_1, m_2, \cdots m_n$ are relatively prime numbers, so m_i divides (z-x), for each i. hence $\boldsymbol{z \equiv x \ (mod\ m_k)}$

And $x \equiv a_k \ (mod\ m_k)$

So $z \equiv a_k \ (mod\ m_k)$

Therefore z is a solution of given system

The Chinese Remainder Theorem

Example: Consider the 3 congruence's from Sun-Tsu's problem:

$$x \equiv 2 \ (\bmod 3),$$
$$x \equiv 3 \ (\bmod 5),$$
$$x \equiv 2 \ (\bmod 7).$$

- Let $m = 3\cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_3 = m/5 = 21$, $M_3 = m/7 = 15$.
- $35y_1 \equiv 1 \ (\text{mod } 3)$,
  - $35 = 3\times11+2$
  - $3 = 2\times 1 +1$
  - $35 = 3\times11+(3\text{-}2) = 3\times12\text{-}1$ or $-35 + 3\times12 = 1$
  - $y_1 = -1 + 3\mathbb{Z}$ (i.e. 2,-1,-4 etc)
- $21y_2 \equiv 1 \ (\text{mod } 5)$, $y_2 = 1 + 5\mathbb{Z}$ (i.e. 1, 6 , -4 etc)
- $15y_3 \equiv 1 \ (\text{mod } 7)$, $y_3 = 1 + 7\mathbb{Z}$ (i.e. 1, 8 , -6 etc)
- $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$
  $= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

- $x \equiv 233 \ (\text{mod } 105)$ or $x \equiv 23 \ (\text{mod } 105)$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

Back Substitution

Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{6}$, and $x \equiv 3 \pmod{7}$.

Solution: Note: $x \equiv 1 \pmod{5}$, $5 \mid x - 1$
$x \equiv 1 \pmod{5}$, according theorem, $x - 1 = 5t$ or $x = 5t + 1$

$x \equiv 2 \pmod{6}$ or $5t+1 \equiv 2 \pmod{6}$
Or $5t \equiv 1 \pmod{6}$
Or $5t \equiv 1+6 \pmod{6}$
Or $5t \equiv 7 \pmod{6}$
Or $5t \equiv 13 \pmod{6}$
Or $5t \equiv 19 \pmod{6}$
Or $5t \equiv 25 \pmod{6}$
Or $t \equiv 5 \pmod{6}$ Since $\gcd(5,6) = 1$
$t \equiv 5 \pmod{6}$, according to theorem, $t = 6u+5$

$x = 5(6u+5) + 1 = 30u+26$

$x \equiv 3 \pmod{7}$ or $30u+26 \equiv 3 \pmod{7}$
Or $30u \equiv -23 \pmod{7}$
Or $30u \equiv 180 \pmod{7}$
Or $u \equiv 6 \pmod{7}$ Since $\gcd(30,7) = 1$

$u = 7v+6$,

$x=30(7v+6)+26 = 210v+206$
$x-206 = 210v$ so $x \equiv 206 \pmod{210}$

Computer Arithmetic with Large Integers

- Use the Chinese remainder theorem to show that an integer a , with $0 \le a < m = m_1 . m_2 \cdots m_n$, where the positive integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, can be represented uniquely by the n-tuple ($a \bmod m_1$, $a \bmod m_2, \ldots, a \bmod m_n$).

Proof: suppose there **exists** distinct integers a and b, where $0 \le a,b < m$ and the **n-tuples** for a and b are identical. i.e. $\forall_I, 1 \le i \le n$, $a \equiv b \pmod{m_i}$

Since the m_i are relatively prime, by Chinese remainder theorem, we get that

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

From definition

$$m \mid (a-b)$$

Since $0 \le a,b < m$, so $-m \le a-b < m$

Hence a-b is divisiable by m iff (a-b)=0 which is a condradiction (i.e. a =b)

So there **does not** exist distinct integers a and b where $0 \le a,b < m$ and the n-tuples for a and b are identical

Computer Arithmetic with Large Integers

- **Example**: What are the pairs used to represent the nonnegative integers less than **12** (3x4) when they are represented by the ordered pair where the first component is the remainder of the integer upon division by 3 and the second component is the remainder of the integer upon division by 4? There pairs are unique.

Solution: a= {0,1,2,3,4,5,6,7,8,9,,10,11}

0 = (0 mod 3, 0 mod 4) = (0,0)   4 = {4 mod 3, 4 mod 4) = (3,1)   8= {4 mod 3, 4 mod 4)=(2,0)

1 = (1 mod 3, 1 mod 4) = (1,1)   5 = {5 mod 3, 5 mod 4) = (2,1)   9= {9 mod 3, 9 mod 4)=(0,1)

2 = (2 mod 3, 2 mod 4) = (2,2)   6 = {6 mod 3, 6 mod 4) = (0,2)   11={11 mod 3, 11 mod 4)=(2,3)

3 = (3 mod 3, 3 mod 4) = (0,3)   7 = {7 mod 3, 7 mod 4) = (1,3)

These pair are unique. i.e. (0,0) is unique.

Computer Arithmetic with Large Integers

- Consider four moduli 99,98,97,95 those are less than 100

By the Chinese remainder theorem, every nonnegative integer less than $99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$ can be represented uniquely by its remainders when divided by these four moduli.

$123{,}684 = (33, 8, 9, 89)$, because $123{,}684 \bmod 99 = 33$ and so on.
Similarly, we represent, $413{,}456 = (32, 92, 42, 16)$.

To find the sum of 123,684 and 413,456, we work with these 4-tuples instead of these two integers directly.

$$\begin{aligned} 537{,}140 &= (33, 8, 9, 89) + (32, 92, 42, 16) \\ &= (65 \bmod 99,\ 100 \bmod 98,\ 51 \bmod 97,\ 105 \bmod 95) \\ &= (65, 2, 51, 10). \end{aligned}$$

We solve the follwing system of congruences

$$\begin{aligned} x &\equiv 65 \pmod{99}, \\ x &\equiv 2 \pmod{98}, \\ x &\equiv 51 \pmod{97}, \\ x &\equiv 10 \pmod{95}. \end{aligned}$$

The solution is 537140.**(Home Task)**

Fermat’s Little Theorem

Fermat’s Little Theorem: If p is prime and a is an integer not divisible by p, then

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

Proof: Given p is prime and $p \nmid a$.

Every integer is congruent to one of 0,1,2,3…., p-1(mod p)

Note: $a \equiv b \pmod{p}$, $a \in \mathbb{Z}$, and one of {0,1,2,3 …. p-1}

Only **focus** on nonzero congruence class, we ignore 0 (because $p \nmid a$)

Multiply all these by a: a, 2a, 3a, … , (p-1)a

Show: **a, 2a, 3a, … , a(p-1)** is a rearrangement of **1,2,3, …, p-1**

Case 1: None of **a, 2a, 3a, … , a(p-1)** are congruence of 0

Suppose $r.a \equiv 0 \pmod{p}$, then $p \mid r.a$,

This is impossible since $p \nmid a$ and $r < p$

Fermat's Little Theorem

Fermat's Little Theorem: If *p* is prime and *a* is an integer not divisible by *p*, then

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

Proof (continue):

Case 2: a, 2a, 3a, … , a(p-1) are distinct; no two are congruent to each other.
Pick two values: r.a and s.a

$$0<r<p$$
$$0<s<p$$

Suppose $ra \equiv sa \pmod{p}$ then $p \mid a(r-s)$
But $p \nmid a$,

$$-p<-s<0$$
$$\text{So } -p<r-s<p$$

$p \nmid (r-s)$ if $r-s \neq 0$, but it is assumed that r ans s are distinct.
So $ra \not\equiv sa \pmod{p}$

From case 1 and case 2, **a, 2a, 3a, … , a(p-1)** is a rearrangement of **1,2,3, …, p-1**

Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p, then

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

Proof (continue):

$$a, 2a, 3a, \ldots, a(p-1) = 1, 2, 3, \ldots, p-1 \pmod{p}$$
$$(p-1)!\, a^{p-1} = (p-1)! \pmod{p}$$
$$a^{p-1} = 1 \pmod{p}$$

Fermat’s Little Theorem

Fermat’s little theorem is useful in computing the remainders modulo *p* of large powers of integers.

Example: Find 7^{222} **mod** 11.

By Fermat’s little theorem, we know that $7^{10} \equiv 1 \pmod{11}$,

so $7^{10} \bmod 11 = 1$,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2$$

$$\begin{aligned} 7^{222} \bmod 11 &= (7^{10})^{22} 7^2 \bmod 11 \\ &= 1.\,49 \bmod 11 \\ &= 5 \end{aligned}$$

Hence, 7^{222} **mod** $11 = 5$.

Use Fermat’s little theorem to compute 5^{2003} **mod** 7, 5^{2003} **mod** 11, and 5^{2003} **mod** 13.

Pseudoprimes

- By Fermat's little theorem $n > 2$ is prime, where
  $$2^{n-1} \equiv 1 \pmod{n}.$$
- But if this congruence holds, n may not be prime. Composite integers n such that $2^{n-1} \equiv 1 \pmod{n}$ are called **pseudo-primes** to the base 2.

Example: The integer 341 is a pseudo-prime to the base 2.

$341 = 11 \cdot 31$

$2^{340} \equiv 1 \pmod{341}$ (*see in Exercise* 37)

- **We can replace 2 by any integer $b \geq 2$.**

Definition: Let $\boldsymbol{b}$ be a positive integer. If n is a composite integer, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called a **pseudo-prime** *to the base b*.

Robert Carmichael
(1879-1967)

Carmichael Numbers

Definition: A composite integer **n** that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $\mathbf{gcd(}b,n\mathbf{) = 1}$ is called a **Carmichael number**.

Example: The integer 561 is a Carmichael number.

To see this:

–561 is composite, since $561 = 3 \cdot 11 \cdot 17$.

–If $\mathbf{gcd(}b\mathbf{, 561) = 1}$, then $\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$.

–Using Fermat's Little Theorem: $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$.

–Then

$$b^{560} = (b^2)^{280} \equiv 1 \pmod{3},$$

$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$

$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

–It follows that $\mathbf{b^{560} \equiv 1 \pmod{561}}$ for all positive integers b with $\gcd(b, 561) = 1$. **Hence, 561 is a Carmichael number**.

Primitive Roots

Definition: A primitive root modulo a prime p is an integer r in $\mathbf{Z}_p$ such that every nonzero element of $\mathbf{Z}_p$ ={ 1 2 3 , … , p-1} is a power of r.

Example: Since every element of $\mathbf{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

Powers of 2 modulo 11: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$.

2,4,8,5,10,9,7,3,6,1 → Unique

Example: Since not all elements of $\mathbf{Z}_{11}$ are powers of 3, 3 is not a primitive root of 11.

Powers of 3 modulo 11: $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, and the pattern repeats for higher powers.

Important Fact: There is a primitive root modulo p for every prime number p.

Primitive Roots

Primitive root of modulo 5

	a^1 mod 5	a^2 mod 5	a^3 mod 5	a^4 mod 5	Is primitive root
1	1	1	1	1	×
2	2	4	3	1	√
3	3	4	2	1	√
4	4	1	4	1	×

Discrete Logarithms

Suppose

- p is prime
- r is a primitive root modulo p.
- $a \in \mathbf{Z}_p = \{1, 2, \ldots, p-1\}$,
- there is a unique exponent e such that $r^e = a$ in $\mathbf{Z}_p$,
- $r^e \bmod p = a$.

Example:

A prime, p=11,

A primitive root, r = 2,

An integer, a= 2 $\in \mathbf{Z}_p$,

$$r^e = a \Rightarrow 2^1 = 2$$

e = 1,

$2^1 \bmod 11 = a$

Discrete Logarithms

Definition:

Suppose that

p is prime,
r is a primitive root modulo p, and
a is an integer between 1 and $p-1$, inclusive. If $r^e \bmod p = a$ and $1 \leq e \leq p-1$,

we say that

e* is the *discrete logarithm* of *a* modulo *p* to the base *r

and we write

$\log_r a = \mathrm{e}$ (where the prime p is understood).

Discrete Logarithms

Example 1: Find the discrete logarithms of 3 modulo 11 to the base 2.

Suppose that

p =11

r = 2 (base)

a =3 is an integer between 1 and 10, inclusive.

a mod 5 → a↓	a^1	a^2	a3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
2	2	4	8	5	10	9	7	3	6	1

e=8

$\mathbf{log}_r\, \boldsymbol{a} = \mathbf{e}$

$\rightarrow \mathbf{log}_2\, \mathbf{3 = 8}$

Discrete Logarithms

Example 1: Find the discrete logarithms of 5 modulo 11 to the base 2.

Suppose that

p =11

r = 2 (base)

a =5 is an integer between 1 and 10, inclusive.

a mod 5 → a↓	a^1	a^2	a3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
2	2	4	8	5	10	9	7	3	6	1

e=4

$\mathbf{log}_r\, \boldsymbol{a} = \mathbf{e}$

$\rightarrow \mathbf{log}_2\, \mathbf{5 = 4}$

Query???

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4....}}}}$$

$$\exists_{x\in\Re}\exists_{y\in\Re}(\,x = y\,) = ?$$

$$\sum_{x=1}^{\infty} x = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$

$$\forall_{x}(\,\Re \mid x\,) = ?$$

$$\exists_{x\in\Re}\exists_{y\in\Re}(\,x = y\,) = ?$$

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4....}}}} = ?$$

$$1-1+1-1+1......... = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$