CNT4406/5412 Network Security

Basic Number Theory

Zhi Wang

Florida State University

Fall 2014

Remainder

Definition

Remainder ($m \mod n = r$): smallest non-negative number r that differs from m by a multiple of n, that is $m = qn + r (0 r < n)$. q is the quotient; r is the reminder.

- E.g., 13 mod 10 = ??, -3 mod 10 = ??

Remainder

Definition

Remainder ($m \mod n = r$): smallest non-negative number r that differs from m by a multiple of n, that is $m = qn + r(0r < n)$. q is the quotient; r is the reminder.

- E.g., 13 mod 10 = 3, -3 mod 10 = 7
- If $r = 0$, q (or n) is called a factor (or divisor) of m
  ➠ e.g., the factors of 24 =1, 3, 4, 6, 8, 24

Remainder

Definition

Remainder ($m \mod n = r$): smallest non-negative number r that differs from m by a multiple of n, that is $m = qn + r(0r < n)$. q is the quotient; r is the reminder.

- E.g., 13 mod 10 $=$ 3, -3 mod 10 $=$ 7
- If $r = 0$, q (or n) is called a factor (or divisor) of m
  ➠ e.g., the factors of 24 $=$1, 3, 4, 6, 8, 24
- Two integers a and b are equivalent for mod n if $(a - b) = qn$
  ➠ e.g., 3, 13, -7 are equivalent when mod 10

Addition and Multiplication

Modular Addition

- $(a + b) \mod n = a \mod n + b \mod n$

Addition and Multiplication

Modular Addition

- $(a + b) \mod n = a \mod n + b \mod n$
- a is b 's additive inverse if $a + b = 0 \mod n$
  ➠ $-a$ is a 's additive inverse

Addition and Multiplication

Modular Addition

- $(a + b) \mod n = a \mod n + b \mod n$
- a is b 's additive inverse if $a + b = 0 \mod n$

  ➠ $-a$ is a 's additive inverse

Modular Multiplication

- $a \times b \mod n = a \mod n \times b \mod n$

  ➠ $a \times b = (a' + kn)(b' + ln) = a'b' + (a'l + b'k + kln)n = a'b' \mod n$

Addition and Multiplication

Modular Addition

- $(a + b) \mod n = a \mod n + b \mod n$
- a is b's additive inverse if $a + b = 0 \mod n$
  - ➠ $-a$ is a's additive inverse

Modular Multiplication

- $a \times b \mod n = a \mod n \times b \mod n$
  - ➠ $a \times b = (a' + kn)(b' + ln) = a'b' + (a'l + b'k + kln)n = a'b' \mod n$
- a is b's multiplicative inverse if $ab = 1 \mod n$
  - ➠ e.g., $1^{-1} = 1, 3^{-1} = 7, 9^{-1} = 9$ for $\mod 10$
  - ➠ Euclid's algorithm can be used to compute multiplicative inverse

Prime

Definition

Prime: a number that has no non-trivial factors, that is, it can only be evenly divided by 1 and itself

Prime

Definition

Prime: a number that has no non-trivial factors, that is, it can only be evenly divided by 1 and itself

- There are infinite primes, but they thin out as numbers get bigger
  - ➠ 1 in 4 of numbers < 100 are prime
  - ➠ 1 in 23 for ten-digit numbers
  - ➠ 1 in 230 for hundred-digit numbers

Greatest Common Divisor (GCD)

Definition

GCD of two integers is the largest integer that evenly divides both of them

➠ e.g., $gcd(12, 14) = ??, gcd(12, 25) = ??, gcd(0, x) = ??$

Greatest Common Divisor (GCD)

Definition

GCD of two integers is the largest integer that evenly divides both of them

➠ e.g., $gcd(12, 14) = 2, gcd(12, 25) = 1, gcd(0, x) = x$

- $gcd(x, y) = gcd(y, x)$
- a and b are relatively prime iff $gcd(a, b) = 1$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ (why??)

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

$gcd(408, 595 \mod 408) = gcd(408, 187)$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

$gcd(408, 595 \mod 408) = gcd(408, 187)$

$gcd(187, 408 \mod 187) = gcd(187, 34)$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

$gcd(408, 595 \mod 408) = gcd(408, 187)$

$gcd(187, 408 \mod 187) = gcd(187, 34)$

$gcd(34, 187 \mod 34) = gcd(34, 17)$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

$gcd(408, 595 \mod 408) = gcd(408, 187)$

$gcd(187, 408 \mod 187) = gcd(187, 34)$

$gcd(34, 187 \mod 34) = gcd(34, 17)$

$gcd(17, 34 \mod 17) = gcd(17, 0)$

Euclid's Algorithm

Euclid's algorithm is a method to compute $gcd(x, y)$

- Observation: $gcd(x, y) = gcd(x - y, y)$
  $x = kd, y = ld, x - y = (k - l)d$
- Method: repeatedly replace $gcd(x, y)$ with $gcd(y, x \mod y)$ until one number becomes 0, the other number is the $gcd(x, y)$ ($gcd(0, x) =?$)

Example

$gcd(595, 408)$

$gcd(408, 595 \mod 408) = gcd(408, 187)$

$gcd(187, 408 \mod 187) = gcd(187, 34)$

$gcd(34, 187 \mod 34) = gcd(34, 17)$

$gcd(17, 34 \mod 17) = gcd(17, 0)$

What is the first step for $gcd(408, 595)$?

Euclid's Algorithm

- Pseudo-code for Euclid's algorithm:

$r_{-2} = x, r_{-1} = y, n = 0$

loop until $r_{n-1} == 0$:

$\quad r_n = r_{n-2} \mod r_{n-1}$

$\quad n = n + 1$

output r_{n-2}

Euclid's Algorithm

- Pseudo-code for Euclid's algorithm:

$r_{-2} = x, r_{-1} = y, n = 0$	$u_{-2} = 1, v_{-2} = 0, u_{-1} = 0, v_{-1} = 1$
loop until $r_{n-1} == 0$:	
$\quad r_n = r_{n-2} \mod r_{n-1}$	$u_n = u_{n-2} - q_n u_{n-1},$
$\quad n = n + 1$	$v_n = v_{n-2} - q_n v_{n-1}$
output r_{n-2}	$gcd(x, y) = u_{n-2}x + v_{n-2}y$

- We can extend it to keep track of u_n, v_n, so $r_n = u_n x + v_n y$
  - ➠ Exercise: show why $r_n = u_n x + v_n y$
  - ➠ $gcd(x, y) = ux + vy$

Euclid's Algorithm

- In each step: $r_n = r_{n-2} \mod r_{n-1}$, $u_n = u_{n-2} - q_n u_{n-1}$, and $v_n = v_{n-2} - q_n v_{n-1}$

n	q_n	r_n	u_n	v_n
-2		408	1	0
-1		595	0	1

Euclid's Algorithm

- In each step: $r_n = r_{n-2} \mod r_{n-1}$, $u_n = u_{n-2} - q_n u_{n-1}$, and $v_n = v_{n-2} - q_n v_{n-1}$
  - ➠ Note: how step 0 swaps x and y when $x < y$

n	q_n	r_n	u_n	v_n
-2		408	1	0
-1		595	0	1
0	0	408	1	0

Euclid's Algorithm

- In each step: $r_n = r_{n-2} \mod r_{n-1}$, $u_n = u_{n-2} - q_n u_{n-1}$, and $v_n = v_{n-2} - q_n v_{n-1}$
  - Note: how step 0 swaps x and y when $x < y$
  - $gcd(x, y) = r_3 = u_3 x + u_3 y = -16 \times 408 + 11 \times 595$

n	q_n	r_n	u_n	v_n
-2		408	1	0
-1		595	0	1
0	0	408	1	0
1	1	187	-1	1
2	2	34	3	-2
3	5	17	-16	11
4	2	0	35	-24

Multiplicative Inverse

- **Multiplicative inverse**: $um = 1 \mod n$, or $um + vn = 1$

*This is not a mod operation!

Multiplicative Inverse

- **Multiplicative inverse**: $um = 1 \mod n$, or $um + vn = 1$
- m 's multiplicative inverse exists iff $gcd(m, n) = 1$
  - ➠ $gcd(m, n) = 1 \rightsquigarrow um + vn = 1$ (Eulcid's algorithm)
    $\rightsquigarrow u$ is m 's multiplicative inverse.

---
*This is not a mod operation!

Multiplicative Inverse

- **Multiplicative inverse**: $um = 1 \mod n$, or $um + vn = 1$
- m 's multiplicative inverse exists iff $gcd(m, n) = 1$
  - $gcd(m, n) = 1 \rightsquigarrow um + vn = 1$ (Eulcid's algorithm)
    $\rightsquigarrow u$ is m 's multiplicative inverse.
  - assume $gcd(m, n) = a(a > 1) \rightsquigarrow m = ka, n = la$
    $\rightsquigarrow um + vn = a(ku + lv) \neq 1^*$
    $\rightsquigarrow gcd(m, n) = 1$

*This is not a $\mod$ operation!

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

standard representation: $x \mod z_1 z_2 ... z_k$

decomposed representation: $x_1 \mod z_1$, ..., $x_k \mod z_k$

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

standard representation: $x \mod z_1 z_2 ... z_k$

decomposed representation: $x_1 \mod z_1$, ..., $x_k \mod z_k$

➠ standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

standard representation: $x \mod z_1 z_2 ... z_k$

decomposed representation: $x_1 \mod z_1$, ..., $x_k \mod z_k$

- standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$
- decomposed $\rightarrow$standard : (by construction)
  Let $N = z_1 z_2 ... z_k$, and $N_{-i} = \frac{N}{z_i}$

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

standard representation: $x \mod z_1 z_2 ... z_k$

decomposed representation: $x_1 \mod z_1$, ..., $x_k \mod z_k$

- standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$
- decomposed $\rightarrow$standard : (by construction)
  Let $N = z_1 z_2 ... z_k$, and $N_{-i} = \frac{N}{z_i}$
  z_i and N_{-i} are relatively-prime $\rightsquigarrow gcd(z_i, N_{-i}) = 1 \rightsquigarrow u_i z_i + v_i N_{-i} = 1$

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

> **standard representation**: $x \mod z_1 z_2 ... z_k$
>
> **decomposed representation**: $x_1 \mod z_1$, ..., $x_k \mod z_k$

- standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$
- decomposed $\rightarrow$standard : (by construction)
  Let $N = z_1 z_2 ... z_k$, and $N_{-i} = \frac{N}{z_i}$
  z_i and N_{-i} are relatively-prime $\rightsquigarrow gcd(z_i, N_{-i}) = 1 \rightsquigarrow u_i z_i + v_i N_{-i} = 1$
  $\rightsquigarrow v_i N_{-i} = 1 - u_i z_i$
  $\rightsquigarrow v_i N_{-i} \mod z_i = 1$ and $v_i N_{-i} \mod z_j = 0 (j \neq i)$

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

standard representation: $x \mod z_1 z_2 ... z_k$

decomposed representation: $x_1 \mod z_1$, ..., $x_k \mod z_k$

- standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$
- decomposed $\rightarrow$standard : (by construction)
  Let $N = z_1 z_2 ... z_k$, and $N_{-i} = \frac{N}{z_i}$
  z_i and N_{-i} are relatively-prime $\rightsquigarrow gcd(z_i, N_{-i}) = 1 \rightsquigarrow u_i z_i + v_i N_{-i} = 1$
  $\rightsquigarrow v_i N_{-i} = 1 - u_i z_i$
  $\rightsquigarrow v_i N_{-i} \mod z_i = 1$ and $v_i N_{-i} \mod z_j = 0 (j \neq i)$
  then $x = (\sum x_i v_i N_{-i}) \mod N$.

Chinese Remainder Theorem

Theorem

If z_1, z_2, ..., z_k are pair-wise relatively-prime, the following representations are equivalent:

> **standard representation**: $x \mod z_1 z_2 ... z_k$
>
> **decomposed representation**: $x_1 \mod z_1$, ..., $x_k \mod z_k$

- standard $\rightarrow$decomposed: $x_1 = x \mod z_1, ..., x_k = x \mod z_k$
- decomposed $\rightarrow$standard : (by construction)
  Let $N = z_1 z_2 ... z_k$, and $N_{-i} = \frac{N}{z_i}$
  z_i and N_{-i} are relatively-prime $\rightsquigarrow gcd(z_i, N_{-i}) = 1 \rightsquigarrow u_i z_i + v_i N_{-i} = 1$
  $\rightsquigarrow v_i N_{-i} = 1 - u_i z_i$
  $\rightsquigarrow v_i N_{-i} \mod z_i = 1$ and $v_i N_{-i} \mod z_j = 0 (j \neq i)$
  then $x = (\sum x_i v_i N_{-i}) \mod N$. ($x \mod z_i = ??$)

Chinese Remainder Theorem

Example

- $x = 2 \mod 3$, $x = 3 \mod 4$, and $x = 1 \mod 5$

Chinese Remainder Theorem

Example

- $x = 2 \mod 3$, $x = 3 \mod 4$, and $x = 1 \mod 5$
- $x = \sum x_i v_i N_{-i} = 2 \times v_1 \times 20 + 3 \times v_2 \times 15 + 1 \times v_3 \times 12$
  ➠ using Euclid's algorithm, $v_1 = 2, v_2 = 3, v_3 = 3,$
  ➠ $x = 251 \mod (3 \times 4 \times 5) = 11$

Z_n^*

- Z_n: set of integers mod n
  Z_n^*: $x \in Z_n^*$ iff $x \in Z_n$ and $gcd(x, n) = 1$
  ➠ e.g., $Z_{10} = \{0, 1, 2, ..., 9\}$, $Z_{10}^* = \{1, 3, 7, 9\}$

Z_n^*

- Z_n: set of integers mod n
  Z_n^*: $x \in Z_n^*$ iff $x \in Z_n$ and $gcd(x, n) = 1$
  ➠ e.g., $Z_{10} = \{0, 1, 2, ..., 9\}$, $Z_{10}^* = \{1, 3, 7, 9\}$
- Z_n^* is closed under multiplication $\mod n$
  ➠ proof: if $a, b \in Z_n^* \rightsquigarrow u_a a + v_a n = 1, u_b b + v_b n = 1$
  $\rightsquigarrow (u_a u_b)ab + (u_a v_b a + v_a u_b b + v_a v_b n)n = 1 \rightsquigarrow ab \in Z_n^*$

Z_n^*

- Z_n: set of integers mod n
  Z_n^*: $x \in Z_n^*$ iff $x \in Z_n$ and $gcd(x, n) = 1$
  ➠ e.g., $Z_{10} = \{0, 1, 2, ..., 9\}$, $Z_{10}^* = \{1, 3, 7, 9\}$
- Z_n^* is closed under multiplication $\mod n$
  ➠ proof: if $a, b \in Z_n^* \rightsquigarrow u_a a + v_a n = 1, u_b b + v_b n = 1$
  $\rightsquigarrow (u_a u_b)ab + (u_a v_b a + v_a u_b b + v_a v_b n)n = 1 \rightsquigarrow ab \in Z_n^*$
  ➠ e.g., $3 \times 7 = 21 = 1 \mod 10, 7 \times 7 = 9 \mod 10$

Z_n^*

Each row (or column) of the multiplication table for Z_n^* is a rearrange of the elements of Z_n^*

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Z_n^*

Each row (or column) of the multiplication table for Z_n^* is a rearrange of the elements of Z_n^*

- assume $ab = ac \mod n \rightsquigarrow a(b-c) = 0 \mod n$ $\rightsquigarrow a^{-1}a(b-c) = 0 \mod n \rightsquigarrow b - c = 0 \mod n$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Euler's Totient Function

- $\phi(n)$: number of elements in Z_n^*

Euler's Totient Function

- $\phi(n)$: number of elements in Z_n^*
- For two primes p and q: $\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$
  - ➠ exercise: why
  - ➠ e.g., $\phi(2) = 1, \phi(5) = 4$, and $\phi(10) = 1 \times 4 = 4$

Euler's Theorem

Theorem

For all $a \in Z_n^*$, $a^{\phi(n)} = 1 \mod n$

Euler's Theorem

Theorem

For all $a \in Z_n^*$, $a^{\phi(n)} = 1 \mod n$

- proof: Let $x = a_1 a_2 \ldots a_{\phi(n)} \rightsquigarrow a^{\phi(n)} x = (aa_1) \ldots (aa_{\phi(n)}) = x$ (why??) $\rightsquigarrow a^{\phi(n)} = 1 \mod n$

Euler's Theorem

Theorem

For all $a \in Z_n^*$, $a^{\phi(n)} = 1 \mod n$

- proof: Let $x = a_1 a_2 ... a_{\phi(n)} \rightsquigarrow a^{\phi(n)} x = (aa_1)...(aa_{\phi(n)}) = x$
  $\rightsquigarrow a^{\phi(n)} = 1 \mod n$

  each row of the multiplication table for Z_n^* is a rearrange of elements
  multiplication is closed for Z_n^*
  $\rightsquigarrow aa_1, aa_2, ..., aa_{\phi(n)}$ consist of just the elements of Z_n^*

Euler's Theorem

Theorem

For all $a \in Z_n^*, a^{\phi(n)} = 1 \mod n$

- proof: Let $x = a_1 a_2 ... a_{\phi(n)} \rightsquigarrow a^{\phi(n)} x = (aa_1)...(aa_{\phi(n)}) = x$
  $\rightsquigarrow a^{\phi(n)} = 1 \mod n$

  each row of the multiplication table for Z_n^* is a rearrange of elements
  multiplication is closed for Z_n^*
  $\rightsquigarrow aa_1, aa_2, ..., aa_{\phi(n)}$ consist of just the elements of Z_n^*

Theorem

Euler's theorem variant: for all $a \in Z_n^*, a^{k\phi(n)+1} = a \mod n (k \geq 0)$

Generic Euler's Theorem

Theorem

If p *and* q *are distinct primes and* $n = pq$, $a^{k\phi(n)+1} = a \mod n$ *for all* $a \in Z_n$

Generic Euler's Theorem

Theorem

If p and q are distinct primes and $n = pq$, $a^{k\phi(n)+1} = a \mod n$ for all $a \in Z_n$

➠ proof:

- if a is relatively prime to n, Euler's theorem

Generic Euler's Theorem

Theorem

If p and q are distinct primes and $n = pq$, $a^{k\phi(n)+1} = a \mod n$ for all $a \in Z_n$

➠ proof:

- if a is relatively prime to n, Euler's theorem
- if a is not relatively prime to $n \rightsquigarrow a$ is a multiple of q (or p, why?)

Generic Euler's Theorem

Theorem

If p and q are distinct primes and $n = pq$, $a^{k\phi(n)+1} = a \mod n$ for all $a \in Z_n$

➠ proof:

- if a is relatively prime to n, Euler's theorem
- if a is not relatively prime to $n \rightsquigarrow a$ is a multiple of q (or p, why?) $\rightsquigarrow a \mod q = 0 \rightsquigarrow a^{k\phi(pq)+1} = 0 \mod q = a \mod q$

Generic Euler's Theorem

Theorem

If p and q are distinct primes and $n = pq$, $a^{k\phi(n)+1} = a \mod n$ for all $a \in Z_n$

➠ proof:

- if a is relatively prime to n, Euler's theorem
- if a is not relatively prime to $n \rightsquigarrow a$ is a multiple of q (or p, why?)
  $\rightsquigarrow a \mod q = 0 \rightsquigarrow a^{k\phi(pq)+1} = 0 \mod q = a \mod q$
  $\rightsquigarrow a$ and p are relatively prime $\rightsquigarrow a^{k\phi(p)} = 1$
  $a^{k\phi(p)\phi(q)+1} = a \times (a^{k\phi(p)})^{\phi(q)} = a \mod p$ (Euler's)

Generic Euler's Theorem

Theorem

If p and q are distinct primes and $n = pq$, $a^{k\phi(n)+1} = a \mod n$ for all $a \in Z_n$

➠ proof:

- if a is relatively prime to n, Euler's theorem
- if a is not relatively prime to $n \rightsquigarrow a$ is a multiple of q (or p, why?)
  $\rightsquigarrow a \mod q = 0 \rightsquigarrow a^{k\phi(pq)+1} = 0 \mod q = a \mod q$
  $\rightsquigarrow a$ and p are relatively prime $\rightsquigarrow a^{k\phi(p)} = 1$
  $a^{k\phi(p)\phi(q)+1} = a \times (a^{k\phi(p)})^{\phi(q)} = a \mod p$ (Euler's)
  $\rightsquigarrow a^{k\phi(pq)+1} = aup + avq = a(up + vq) = a \mod n$
  (Chinese remainder theorem and $up + vq = 1$)