

ISA 666

Internet Security Protocols

Number Theory

Public Key Cryptography

ISA 666 1

Number Theory Outline

- Number Theory
- Prime Numbers
- Division
- Common Divisors
- Euclid's GCD Algorithm
- Modular Arithmetic
- Euler's Totient Function
- Euler's Theorem
- Modular Exponentiation

ISE at George Mason University ISA 666 2

What is Number Theory?

- Branch of pure mathematics dealing with integer properties.
- Mathematics is about finding patterns, bringing order to the chaos.
- One of the greatest challenge to all pattern researchers is prime numbers.
- Some topics in elementary number theory include:
 - Euclidean algorithm to compute GCD
 - factorization of integers into prime numbers
 - Euler's theorem (Euler's $\phi(n)$)
 - Chinese remainder theorem

ISE at George Mason University ISA 666 3

Beauty of Mathematics

Demonstration

Pick a number from 10 to 99

At the 2 digits, for example:

If you chose 51, you would add $5+1=6$

Then subtract the result from the original number

So $51-6=45$

(Demonstration shown in class)

ISE at George Mason University ISA 666 4

Prime Numbers (I)



x	Percentage	Percentage	$x(\ln x - 1)$	Percentage
1,000	168	16.8%	169	16.9%
10,000	1,229	12.3%	1,218	12.2%
100,000	9,592	9.6%	9,512	9.5%
1,000,000	78,498	7.8%	78,030	7.8%
10,000,000	664,579	6.6%	661,459	6.6%
100,000,000	5,761,455	5.8%	5,740,304	5.7%
1,000,000,000	50,847,534	5.1%	50,701,542	5.1%
10,000,000,000	455,052,511	4.6%	454,011,971	4.5%

- Prime numbers "thin out" as the numbers get larger
- There are 25 primes <100, so density is 1 in 4.
- Ten digit number, density is 1 in 23.
- Hundred digit number, density is 1 in 230.

ISE at George Mason University ISA 666 5

Prime Numbers (II)

- Carl Friedrich Gauss
 - Is a German mathematician & scientist
 - Sometimes known as "the prince of mathematics"
 - Introduced modular arithmetic in 1801.
 - At 15, he tried to find a pattern to prime numbers
 - His observed the following:
 - 1 in 4 chance a number between 1 and 100 is prime.
 - 1 in 6 chance a number between 1 and 1,000 is prime.
 - 1 in 8 chance a number between 1 and 10,000 is prime.
 - And so on.
 - His student Bernhard Riemann, came up with the "zeta-hypothesis" also called the Riemann hypothesis
 - He found an exact formula for the number of primes.
 - Since this is one of the most important problems in contemporary mathematics, \$1,000,000 is being offered by the Clay Mathematics Institute for a proof.

ISE at George Mason University ISA 666 6

Prime Numbers (II)

- Largest prime found so far is by Central Missouri State University on December 15th, 2005.
 - The number is $2^{30,402,457}$ which is 9,152,052 digits long.
 - You can order a poster:
 - <http://www.perfsci.com/souvenirs.htm>
- The Electronic Frontier Foundation (EFF) is offering a \$100,000 reward to the first individual or group who discovers a prime number with at least 10,000,000 decimal digits.
 - <http://www.eff.org/awards/coop.php>

Division (I)

Definition: The set of integers is:

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

Definition: The set of natural numbers is:

$$\mathbb{N} = \{ 0, 1, 2, \dots \} \text{ (also called counting numbers)}$$

Definition: Let d and a be integers. We say that d divides a if there exists an integer k such that $a = kd$. In this case, we also say that d is a divisor of a and that a is a multiple of d . The notation $d \mid a$ is used to denote that d divides a .

Convention: Every integer divides 0.

Division (II)

Observation: If $d \mid a$, then so does $(-d) \mid a$.

Convention: In writing $d \mid a$, we assume that d is positive.

Observation: A divisor of a is at least 1 and at most $|a|$.

Example: The divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

Observation: Every integer a is divisible by the two trivial divisors 1 and $|a|$.

Definition: Non-trivial divisors of a are called factors of a .

Example: The factors of 20 are 2, 4, 5, and 10.

Division (III)

Definition: An integer $p \geq 2$ is called a prime if it is divisible only by 1 and by itself (that is, it has no factors).

Theorem: There are infinitely many primes.

Definition: An integer $a > 1$ that is not a prime is said to be a composite number.

Convention: Integer 1 is said to be a unit (neither a prime nor a composite).

Convention: The negative integers and 0 are considered neither prime nor composite.

Division (IV)

Division Theorem: For any integer a and for any positive integer n , there are two unique integers q and r , such that $0 \leq r < n$ and $a = qn + r$.

Notation: The value q is called the quotient of the division.

Notation: The value r is called the residue or remainder of the division, and we write $r = a \bmod n$.

Definition: For two integers a and b , and for any positive integer n , if $n \mid (a-b)$ (that is, $a \bmod n = b \bmod n$, which means that a and b have the same residue modulo n), then we say that a is congruent to b modulo n , and we write $a \equiv b \pmod{n}$.

Common Divisors (I)

Definition: If d is a divisor of a and d is also a divisor of b , then d is called a common divisor of a and b .

Example: All the common divisors of 24 and 30 are 1, 2, 3, and 6.

Observation: If $d \mid a$ and $d \mid b$, then $d \mid (a+b)$ and $d \mid (a-b)$.

Observation: If $d \mid a$ and $d \mid b$, then $d \mid (ax+by)$ for any integers x and y .

Observation: If $a \mid b$, then either $|a| \leq |b|$ or $b=0$.

Observation: If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

Common Divisors (II)

Definition: The **greatest common divisor** of two integers a and b , not both zero, is the largest of the common divisors of a and b , and it is denoted by $\gcd(a, b)$.

Examples: $\gcd(24, 30) = 6$
 $\gcd(15, 7) = 1$
 $\gcd(0, 9) = 9$

Observation: If a and b are both not zero, then $\gcd(a, b)$ is an integer between 1 and $\min(|a|, |b|)$.

Definition: $\gcd(0, 0) = 0$.

Common Divisors (III)

Observations: $\gcd(a, b) = \gcd(b, a)$
 $\gcd(a, b) = \gcd(-a, b)$
 $\gcd(a, b) = \gcd(|a|, |b|)$
 $\gcd(a, 0) = |a|$
 $\gcd(a, ka) = |a|$ for any k in \mathbb{Z}

Common Divisors (IV)

Theorem: For any integers a, b , and p , if both $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$, then $\gcd(ab, p) = 1$.

Theorem: For all primes p and all integers a and b , if $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both).

Fundamental Theorem of Arithmetic: For all positive integers d, a , and b , if $d \mid ab$ and $\gcd(a, d) = 1$, then $d \mid b$.

Definition: Two integers a and b are **relatively prime** if their only common divisor is 1, that is, if $\gcd(a, b) = 1$.

Example: $\gcd(8, 15) = 1$

Euclid's GCD Algorithm (I)

- Euclid of Alexandria
 - Greek mathematician who lived in Egypt.
 - His algorithm is one of the oldest known.
 - Appeared around 300 BC.
- The Algorithm
 - Given a and b natural numbers
 - assuming a is greater than or equal to b .



function $\gcd(a, b)$
if $b = 0$ **return** a
else return $\gcd(b, a \bmod b)$

Euclid's GCD Algorithm (II)

Observation: Discussion can be restricted to nonnegative integers (since $\gcd(a, b) = \gcd(|a|, |b|)$).

GCD Recursion Theorem: For any nonnegative integer a and b , we have $\gcd(a, b) = \gcd(b, (a \bmod b))$.

Example 1: to find $\gcd(595, 408)$ **Example 3:** to find $\gcd(225, 112)$
 $595 \bmod 408 = 187$ $225 \bmod 112 = 1$
 $408 \bmod 187 = 34$ $112 \bmod 1 = 0$
 $187 \bmod 34 = 17$ so $\gcd(225, 112) = 1$
 $34 \bmod 17 = 0$ We see that 225 & 112
 so $\gcd(595, 408) = 17$ are **Relatively Prime**

Example 2: to find $\gcd(225, 3)$
 $225 \bmod 3 = 0$
 so $\gcd(225, 3) = 3$

Modular Arithmetic (I)

- **Properties**
- **Commutative laws**
 - $(w + x) \bmod n = (x + w) \bmod n$
 - $(w \times x) \bmod n = (x \times w) \bmod n$
- **Associative laws**
 - $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
 - $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
- **Distributive law**
 - $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
- **Identities**
 - $(0 + w) \bmod n = w \bmod n$
 - $(1 \times w) \bmod n = w \bmod n$
- **Additive inverse ($-w$)**
 - For each $w \in \mathbb{Z}_n$, there exists a z such that $w + z = 0 \bmod n$.

Modular Arithmetic (II)

- **Addition Modulo:**
 $(a+b) \pmod n = (a \pmod n) + (b \pmod n)$
- **Subtraction Modulo:**
 $(a-b) \pmod n = (a \pmod n) - (b \pmod n)$
- **Definition:** The additive inverse of element $(a \pmod n)$ is the element $((n-a) \pmod n)$. We denote the additive inverse of a by $-a$.
- **Examples:**
 $(8+3) \pmod 7 = (8 \pmod 7) + (3 \pmod 7) = 4$
 $(15-22) \pmod{10} = (15 \pmod{10}) - (22 \pmod{10}) = 3$
 $-3 \pmod 8 = 5$ & $3 \pmod 8 = 3$

Modular Arithmetic (III)

- **Multiplication Modulo:**
 $(a*b) \pmod n = (a \pmod n) * (b \pmod n)$
- **Subtraction Modulo:**
 $(a/b) \pmod n = (a \pmod n) / (b \pmod n)$
- **Observation:** Multiplication modulo n does not necessarily have an inverse operation (that is: division modulo n).
- **Definition:** Multiplication inverse of an element $(a \pmod n)$ is an element $(b \pmod n)$, such that $(a*b) \pmod n = 1$. The multiplication inverse of a is a^{-1} .
- **Examples:**
 The inverse of $3 \pmod 5$ is 2, because $(2*3) \pmod 5 = 1$
 How about $30^{-1} \pmod{53}$? $\rightarrow 30^{-1} = 23 \pmod{53}$, this can be confirmed by $23*30 \pmod{53} = 1$
 How about the inverse of $3 \pmod{12}$? No inverse! an inverse only exists if $\text{GCD}(n,p) = 1$. If p is prime, then there will be always be an inverse.

Modular Arithmetic (IV)

- Why do we care about modular multiplicative inverse?
 – Will see in RSA...
- Don't always exist
 – Example: There doesn't exist a z such that $6 \times z = 1 \pmod 8$.

Z_8	0	1	2	3	4	5	6	7
$\times 6$	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

- An integer $a \in Z_n$ has a modular multiplicative inverse iff $\text{gcd}(a, n) = 1$.
- In particular, if n is a prime number, then all elements in Z_n have modular multiplicative inverse.

Euler's Totient Function (I)

- **Leonhard Euler**
 – Swiss mathematician and physicist
 – First to use the term function.
 – Lived in the 1700's



Euler's Phi Function: The size of Z_n^* is:

$$\Phi(n) = n \prod_{p|n} (1 - (1/p))$$

(where p runs over all the primes that divide n).

- **Totient function $\phi(n)$:** $|Z_n^*|$
 – number of integers less than n and relatively prime to n
 – If n is prime, $\phi(n) = n-1$
 – If $n = p*q$, and p, q are primes, $\phi(n) = (p-1)(q-1)$
 – If p is prime and $k > 0$, $\phi(p^k) = (p-1)p^{k-1}$

Euler's Totient Function (II)

- **Examples:**
 $\phi(7) = 7*(1-(1/7)) = 6$ {1,2,3,4,5,6}
 Or $\phi(7) = 7-1 = 6$, because 7 is prime

 $\phi(10) = 10*(1-(1/2))*(1-(1/5)) = 4$ {1,3,7,9}
 $\phi(18) = 18*(1-(1/2))*(1-(1/3)) = 6$ {1,5,7,11,13,17}

 $\phi(21) = 21*(1-(1/3))*(1-(1/7)) = 12$
 {1,2,4,5,8,10,11,13,16,17,19,20}
 Or $\phi(21) = \phi(3*7) = \phi(3) * \phi(7) = 2*6 = 12$

Euler's Theorem (I)

- For every a and n that are relatively prime, $a^{\phi(n)} \equiv 1 \pmod n$.
- **Examples**
 – $a=3, n=10, \phi(10)=4, 3^{\phi(10)} \pmod{10} = 1$
 – $a=2, n=11, \phi(11)=10, 2^{\phi(11)} \pmod{11} = 1$
- **What if a and n that are NOT relatively prime?**
- **Generalization of Euler's Theorem**
 – if $n=pq$ (p, q are prime numbers) $a^{k\phi(n)+1} \equiv a \pmod n$ for all a in Z_n .

Modular Exponentiation (I)

- If x, n are relative primes, $x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$
- if $y \bmod \phi(n) = 1$ and x is relative prime with n , then $x^y \bmod n = x \bmod n$
- Example:
 $2^{101} \bmod 33 = 2$
 $x=2, n=33, \phi(33)=20, y=10$
 So $2^{101 \bmod 20} \bmod 33 = 2^1 \bmod 33 = 2$

Modular Exponentiation (II)

- To calculate $66^{77} \bmod 119$
 - multiply 66 by itself for 76 times, then mod 119
 - take mod 119 every time multiply 66
 - take advantage of property of modulo operation:
- $x \times y \bmod n = [(x \bmod n) \times (y \bmod n)] \bmod n$
- “Squaring and Multiplication”
 - The number of square and multiplication operations is linear to the number of bits of the exponent 77

Modular Exponentiation (III)

- To calculate $66^{77} \bmod 119$ ($77=1001101$)
 - 1 $66 \bmod 119=66$
 - 10 $66^2 \bmod 119=72$
 - 100 $66^4 \bmod 119=(66^2 \bmod 119)^2 \bmod 119=67$
 - 1000 $66^8 \bmod 119=(66^4 \bmod 119)^2 \bmod 119=86$
 - 1001 $66^9 \bmod 119=[66(66^8 \bmod 119)] \bmod 119=83$
 - 10010 $66^{18} \bmod 119=(66^9 \bmod 119)^2 \bmod 119=106$
 - 10011 $66^{19} \bmod 119=[66(66^{18} \bmod 119)] \bmod 119=94$
 - 100110 $66^{38} \bmod 119=(66^{19} \bmod 119)^2 \bmod 119=30$
 - 1001100 $66^{76} \bmod 119=(66^{38} \bmod 119)^2 \bmod 119=67$
 - 1001100 $66^{77} \bmod 119=[66(66^{76} \bmod 119)] \bmod 119=19$

Modular Exponentiation (IV)

Yet another way to calculate $66^{77} \bmod 119$:

66	^	1	=	66	mod	119	=	66	x	1	=	66
66	^	2	=	4356	mod	119	=	72	x	0	=	0
72	^	2	=	5184	mod	119	=	67	x	1	=	67
67	^	2	=	4489	mod	119	=	86	x	1	=	86
86	^	2	=	7396	mod	119	=	18	x	0	=	0
18	^	2	=	324	mod	119	=	86	x	0	=	0
86	^	2	=	7396	mod	119	=	18	x	1	=	18

Note: The blue column represents 77 in binary 1001101

Now calculate $(66 \times 67 \times 86 \times 18) \bmod 119 = 19$

How about: $204^{994} \bmod 287$?

204	^	1	=	204	mod	287	=	204	x	0	=	0
204	^	2	=	41616	mod	287	=	1	x	1	=	1

1 raised to any power is still 1, so the result is $1 \bmod 287 = 1$