Primes

19CSE311 Computer Security

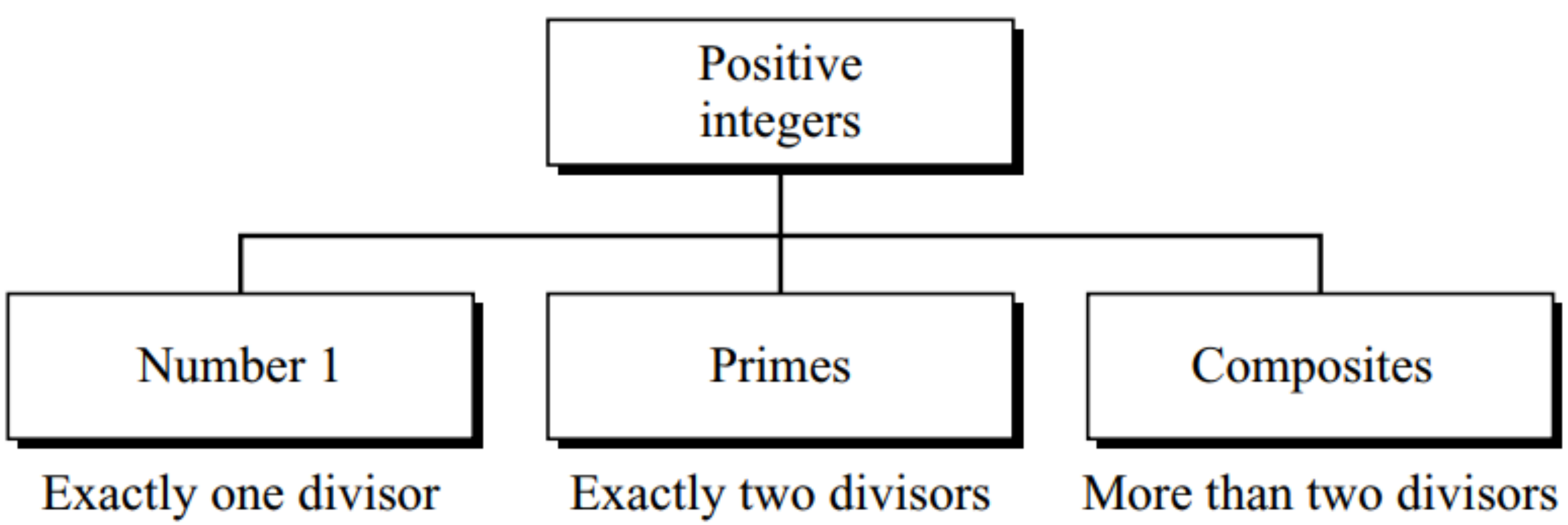
Jevitha KP
Department of CSE

Primes

- Prime numbers play a critical role in number theory
- Asymmetric-key cryptography uses primes extensively.
- The **positive integers** can be divided into three groups: **the number 1, primes, and composites**

Primes

- A **positive integer is a prime** if and only if it is **exactly divisible by two integers**, 1 and itself.
- A composite is a positive integer with more than two divisors.



Primes

- The smallest prime is 2, which is divisible by 2 (itself) and 1.
- Integer 1 is not a prime according to the definition, **because a prime must be divisible by two different integers**, no more, no less.
- The integer 1 is divisible only by itself; it is not a prime.

Primes

- Four primes less than 10: 2, 3, 5, and 7
- Percentage of primes in the range 1 to 10 is 40%.
- The percentage decreases as the range increases

Fundamental Theorem of Arithmetic

- Any integer $a > 1$ can be factored in a unique way as $a = p_1^{a1} * p_2^{a2} * \ldots * p_t^{at}$, where $p_1, p_2 \ldots\ldots p_t$ are prime numbers and a_i is a positive integer
- This is known as the **fundamental theorem of arithmetic**

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

Fundamental Theorem of Arithmetic

- If P is the set of all prime numbers, then any positive integer a can be written uniquely in the following form :

$$a = \prod_{p \in \mathrm{P}} p^{a_p} \quad \text{where each } a_p \geq 0$$

- Multiplication of two numbers is equivalent to adding the corresponding exponents.

a | b

- Any integer of the form p^n can be divided only by an integer that is of a lesser or equal power of the same prime number, p^j , j <= n.

$$a = \prod_{p \in P} p^{a_p},\ b = \prod_{p \in P} p^{b_p}$$

If $a \mid b$, then $a_p \leq b_p$ for all p.

$a = 12; b = 36; 12 \mid 36$

$12 = 2^2 \times 3; 36 = 2^2 \times 3^2$

$a_2 = 2 = b_2$

$a_3 = 1 \leq 2 = b_3$

Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers.

GCD

- It is easy to determine the greatest common divisor of two positive integers if we express each integer as the product of primes.
- If k = gcd(a, b), then kp = min(ap, bp) for all p.
- Determining the prime factors of a large number is not easy
- Not a practical method of calculating the greatest common divisor for large numbers

$$
\begin{aligned}
300 &= 2^2 \times 3^1 \times 5^2 \\
18 &= 2^1 \times 3^2 \\
\gcd(18,300) &= 2^1 \times 3^1 \times 5^0 = 6
\end{aligned}
$$

CoPrimes

- Two positive integers, a and b, are **relatively prime, or coprime**, if gcd (a, b) = 1.
- Number 1 is relatively prime with any integer.
- If p is a prime, then all integers 1 to $p - 1$ are relatively prime to p (Z_p^*)

Cardinality of Primes

- Is there a finite number of primes or is the list infinite?
- The number of primes is **infinite**.
- Given a number n, how many primes are smaller than or equal to n?
- A function called $\pi(n)$ is defined that finds the number of primes smaller than or equal to n.
- $\pi(1) = 0$; $\pi(2) = 1$; $\pi(3) = 2$; $\pi(10) = 4$
  $\pi(20) = 8$; $\pi(50) = 15$; $\pi(100) = 25$

$\pi(n)$

- But if n is very large, we can only use approximation:

- **$[n / (\ln n)] < \pi(n) < [n / (\ln n - 1.08366)]$**

- Gauss discovered the upper limit; Lagrange discovered the lower limit.
- **$\pi(100) = [100 / 4.605] < \pi(100) < [100 / (4.605 - 1.08366)]$**
- **$22 < \pi(100) < 28$**

Example 1

- Find the number of primes less than 1,000,000
- **$[n / (\ln n)] < \pi(n) < [n / (\ln n - 1.08366)]$**
- $1000000/13.8155 < \pi(1{,}000{,}000) < [1000000/(13.8155 - 1.08366)]$
- $1000000/13.8155 < \pi(1{,}000{,}000) < [1000000/12.73184]$
- $72383 < \pi(1{,}000{,}000) < 78543$

Example 2

- Find the number of primes less than 5,000,000
- **$[n / (\ln n)] < \pi(n) < [n / (\ln n - 1.08366)]$**

Example 2

- Find the number of primes less than 5,000,000
- **$[n / (\ln n)] < \pi(n) < [n / (\ln n - 1.08366)]$**
- $5000000/15.4249 < \pi(5{,}000{,}000) < [5000000/(15.4249 - 1.08366)]$
- $5000000/13.8155 < \pi(5{,}000{,}000) < [5000000/14.3412]$
- $361912 < \pi(5{,}000{,}000) < 348646$

Checking for Primeness

- Given a number n, how can we determine if n is a prime?
- We need to see if the number **n is divisible by all primes** less than $\sqrt{n}$.

Examples

- Is 97 a prime?
- Is 301 a prime?

Example 1

- Is 97 a prime?
- The floor of $\sqrt{97}$ = 9.
- The primes less than 9 are 2, 3, 5, and 7.
- 97 is not divisible by any of these numbers.
- So 97 is a prime

Example 2

- Is 301 a prime?
- The floor of $\sqrt{301}$ = 17.
- The primes less than 17 are 2, 3, 5,7,11,13,17.
- 301 is divisible by 7.
- So 301 is not a prime

Sieve of Eratosthenes

- The Greek mathematician Eratosthenes devised a method to find all primes less than n.
- The method is called the sieve of Eratosthenes.
- Suppose we want to find all prime less than n.
- We write down all the numbers between 2 and n.
- Find all primes less than sqrt(n). The numbers not divisible by any of these numbers are primes.

Sieve of Eratosthenes

- Eg: Primes less than 100
- Sqrt(100) = 10
- Primes < 10 = (2,3,5,7)
- The numbers which are not divisible by these numbers are the primes

Sieve of Eratosthenes

Table 9.1 *Sieve of Eratosthenes*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Euler's Phi-Function φ(n)

- **Euler's phi-function or Euler's totient function** φ(n), finds the number of integers that are both **smaller than n and relatively prime to n.**
- Set Zn* contains the numbers that are smaller than n and relatively prime to n.
- The function φ(n) calculates the **number of elements in this set**.

Euler's Phi-Function $\varphi(n)$

- $\varphi(1) = 0$.
- $\varphi(p) = p - 1$ if p is a prime.
- $\varphi(m \times n) = \varphi(m) \times \varphi(n)$ if m and n are relatively prime.
- $\varphi(p^e) = p^e - p^{e-1}$ if p is a prime.
- If $n = p_1^{e1} * p_2^{e2} * \ldots * p_k^{ek}$,
  $\varphi(n) = (p_1^{e1} - p_1^{e1-1}) \times (p_2^{e2} - p_2^{e2-1}) \times \ldots \times (p_k^{ek} - p_k^{ek-1})$

Examples

- Find $\varphi(13)$, $\varphi(10)$, $\varphi(240)$, $\varphi(49)$,$\varphi(100)$

Examples

- Find $\varphi(13)$, $\varphi(10)$, $\varphi(240)$, $\varphi(49)$,$\varphi(100)$
- $\varphi(13) = 13-1 = 12$
- $\varphi(10) = \varphi(2*5)=\varphi(2) * \varphi(5) = 1 * 4 = 4$
- $\varphi(240) = \varphi(3*2^4 *5)= \varphi(3)*\varphi(5)* \varphi(2^4) = 2 * 4 * (2^4 - 2^3) = 2*4*8= 64$
- $\varphi(100) = \varphi(5^2 * 2^2) = (5^2 - 5^1)* (2^2 - 2) = 40$

Examples

- Observation:
- If $n > 2$, the value of $\varphi(n)$ is even.
- What is number of elements in Z_{14}^*?

Examples

- What is number of elements in Z_{14}^*?
- $\varphi(14) = \varphi(7) \times \varphi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

- Fact:
- If $n > 2$, the value of $\varphi(n)$ is even.

Fermat's Little Theorem

- Two Versions:
- **First Version:**
- If p is a prime and a is positive integer not divisible by p, then

$$\mathbf{a^{p-1} \equiv 1 \bmod p}$$

- **Second Version:**
- If p is a prime and a is an integer, then

$$\mathbf{a^{p} \equiv a \bmod p}$$

Examples

- Verify Fermats Theorem for
- p = 19, a = 7
- p = 5, a = 3
- p = 5, a = 10
- Find the value of using Fermat’s theorem
- 6^{10} mod 11
- 3^{12} mod 11

Examples

- a = 7, p = 19
- Since a is positive integer not divisible by p we can check both

$$\mathbf{a^{p-1} \equiv 1 \bmod p \;;\; a^{p} \equiv a \bmod p}$$

- To check $7^{18} \equiv 1 \bmod 19$

$$\begin{aligned}
&a = 7, p = 19 \\
&7^2 = 49 \equiv 11 \pmod{19} \\
&7^4 \equiv 121 \equiv 7 \pmod{19} \\
&7^8 \equiv 49 \equiv 11 \pmod{19} \\
&7^{16} \equiv 121 \equiv 7 \pmod{19} \\
&a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}
\end{aligned}$$

- To check $7^{19} \equiv 7 \bmod 19$
- $7^{19} \equiv 7 \bmod 19 = 7^{18} * 7^{1} = 1*7 \bmod 19 = 7 \bmod 19$

Examples

- $p = 5$, $a = 3$
- Since a is positive integer not divisible by p we can check both

$$\mathbf{a^{p-1} \equiv 1 \bmod p \; ; \; a^{p} \equiv a \bmod p}$$

- $3^{5-1} \equiv 1 \bmod 5$
- $3^4 \bmod 5 = 81 \bmod 5 = 1 \bmod 5$
- $3^5 \equiv 3 \bmod 5$
- $3^4 * 3^1 \bmod 5 = 1 * 3 \bmod 5 = 3 \bmod 5$

Examples

- $p = 5$, $a = 10$
- Since a is divisible by p we can check only

  $$\mathbf{a^p \equiv a \bmod p}$$

- $10^5 \equiv 10 \bmod 5$
- $100000 \bmod 5 = 0 \bmod 5 = 10 \bmod 5$

Examples

- Find the value of using Fermat's theorem
- 6^{10} mod 11
- Since a is not divisible by p, we have
- **$a^{p-1} \equiv 1$ mod p**
- 6^{10} mod 11 = 1 mod 11
- Verify -
- 6^2 mod 11 = 3 mod 11
- 6^4 mod 11 = 9 mod 11
- 6^8 mod 11 = 9*9 mod 11 = 4 mod 11
- 6^{10} mod 11 = $6^8 * 6^2$ mod 11 = 4 * 3 mod 11 = 12 mod 11 = 1 mod 11.

Examples

- Find the value of using Fermat's theorem
- 3^{12} mod 11
- Since a is not divisible by p, we have
- **$a^{p-1} \equiv 1 \bmod p$**
- 3^{12} mod 11 = $3^{10} * 3^{2}$ mod 11 = 1 * 9 mod 11 = 9 mod 11.
- Verify -
- 3^{2} mod 11 = 9 mod 11
- 3^{4} mod 11 = 9*9 mod 11 = 4 mod 11
- 3^{8} mod 11 = 4*4 mod 11 = 5 mod 11
- 3^{12} mod 11 = $3^{8} * 3^{4}$ mod 11 = 5 * 4 mod 11 = 20 mod 11 = 9 mod 11.

Multiplicative Inverse using Formats Theorem

- Interesting application of Fermat's theorem is in finding some multiplicative inverses quickly **if the modulus is a prime.**
- If p is a prime and a is an integer such that p does not divide a, then

  $$\mathbf{a^{-1} \bmod p = a^{p-2} \bmod p.}$$

- Proof:
- Since a is not divisible by p, we have:
- $\mathbf{a^{p-1} \equiv 1 \bmod p}$
- Multiply both sides by $\mathbf{a^{-1}}$
- $\mathbf{a^{-1} * a^{p-1} \equiv a^{-1} * 1 \bmod p}$
- $\mathbf{\Rightarrow\ a^{p-2} \equiv a^{-1} \bmod p}$

Examples

- Find Multiplicative inverse for the following without using Extended Euclid's algorithm:
- $8^{-1} \bmod 17$
- $5^{-1} \bmod 23$

Examples

- Since a is not divisible by p, we have:

  a^{-1} mod p = a^{p-2} mod p.
- 8^{-1} mod 17
- = 8^{17-2} mod 17
- = 8^{15} mod 17
- = 15 mod 17

Examples

- Since a is not divisible by p, we have:

  a^{-1} mod p = a^{p-2} mod p.
- 5^{-1} mod 23
- = 5^{23-2} mod 17
- = 5^{21} mod 17
- = 14 mod 23

Euler’s Theorem

- Euler’s theorem can be thought of as a generalization of Fermat’s little theorem.
- The modulus in the Fermat theorem is a prime, **the modulus in Euler’s theorem is an integer.**
- There are two versions similar to Fermat’s theorem

Euler’s Theorem

- **First Version**
- The first version of Euler’s theorem is similar to the first version of the Fermat’s little theorem.
- If a and n are coprime, then $\mathbf{a^{\varphi(n)} \equiv 1 \pmod{n}}$
- **Second Version**
- The second version of Euler’s theorem is similar to the second version of Fermat’s little theorem;
- It removes the condition that a and n should be coprime.
- If $n = p \times q$, $a < n$, and k an integer, then
- $\mathbf{a^{k \times \varphi(n) + 1} \equiv a \pmod{n}}$

Examples

- Find the result of
- 6^{24} mod 35,
- 20^{62} mod 77.

Examples

- Find the result of $6^{24} \bmod 35$,
- $6^{24} \bmod 35$
- $\varphi(35) = \varphi(7*5) = \varphi(7)* \varphi(5) = 6*4 = 24$
- $6^{\varphi(35)} \bmod 35 = 1$
- $6^{24} \bmod 35 = 1$

Examples

- Find the result of 20^{62} mod 77.
- $\varphi(77) = \varphi(7*11) = \varphi(7)*\varphi(11) = 6*10 = 60$
- 20^{60} mod 77 = 1 mod 77
- 20^{62} mod 77 = $20^{60} * 20^{2}$ mod 77 = 1 * 400 mod 77 = 15 mod 77.

Multiplicative inverse using Euler's theorem

- Fermat's theorem can be used to find multiplicative inverses **modulo a prime**;
- Euler's theorem can be used to find multiplicative inverses **modulo a composite**
- **If n and a are coprime, then a^{-1} mod n = $a^{\varphi(n)-1}$ mod n**
- Proof:
- Euler's theorem first version , If a and n are coprime, then **$a^{\varphi(n)} \equiv 1 \pmod{n}$**
- Multiply both sides by a^{-1}
- $a^{\varphi(n)} * a^{-1} \equiv a^{-1} \pmod{n}$
- $a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$

Examples

- Find $8^{-1} \bmod 77$,
- Find $7^{-1} \bmod 15$,
- Find $60^{-1} \bmod 187$

Examples

- $8^{-1} \bmod 77$
- n = 77 is composite ; 8 and 77 are co-prime. Hence we can use $a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$
- $\varphi(77) = \varphi(7*11)=\varphi(7)*\varphi(11) = 6*10 = 60$
- $8^{\varphi(77)-1} \bmod 77$
- $= 8^{59} \bmod 77$
- $= 29 \bmod 77$

Examples

- 7^{-1} mod 15
- n=15 is composite ; 7 and 15 are co-prime.Hence we can use $a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$
- $\varphi(15) = \varphi(3*5)=\varphi(3)*\varphi(5) = 2*4= 8$
- $7^{\varphi(15)-1}$ mod 15
- $= 7^7$ mod 15
- = 13 mod 15

Examples

- $60^{-1} \bmod 187$
- n=187 is composite ; 60 and 187 are co-prime.Hence we can use $a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$
- $\varphi(187) = \varphi(17*11)=\varphi(17)*\varphi(11) = 16*10= 160$
- $60^{\varphi(187)-1} \bmod 187$
- $= 60^{159} \bmod 187$
- $= 53 \bmod 187$