Information & System Security

Lecture 23

VIT-AP
UNIVERSITY

Mathematics Related to Public Key Cryptography

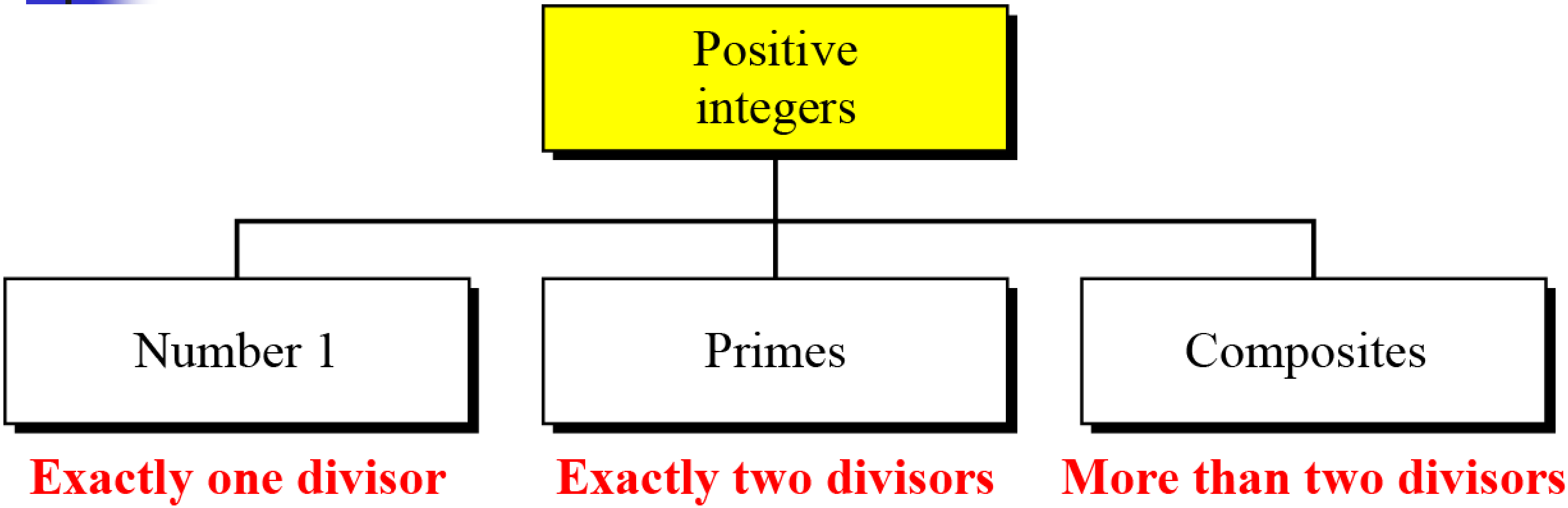
9-1 PRIMES

- ***Asymmetric-key cryptography uses primes extensively.***
- ***This section discusses only a few concepts and facts to pave the way for Chapter 10.***

Topics discussed in this section:

9.1.1 Definition
9.1.2 Cardinality of Primes
9.1.3 Checking for Primness

9.1.1 Definition



Three groups of positive integers

Note

A prime is divisible only by itself and 1.

Example

What is the smallest prime?

Solution

The smallest prime is 2, which is divisible by 2 (itself) and 1.

Example

List the primes smaller than 10.

Solution

There are four primes less than 10: 2, 3, 5, and 7.

Note: It is interesting that the percentage of primes in the range 1 to 10 is 40%. The percentage decreases as the range increases.

An integer p > 1 is a prime number if and only if its only divisors are ± 1 and ±p.

Any integer a > 1 can be factored in a unique way as:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$$

where $p_1 < p_2 < \ldots < p_n$ are prime numbers and each a_i is a positive integer. This is known as the fundamental theorem of arithmetic.

- **If P is the set of all prime numbers, then any positive integer k can be written uniquely in the following form:** $$k = \prod_{p \in P} p^{k_p}$$
- **The value of any given positive integer can be specified by simply listing all the nonzero exponents in the foregoing formulation.**

Example

The integer 12 is represented by $\{k_2 = 2, k_3 = 1\}$.

The integer 18 is represented by $\{k_2 = 1, k_3 = 2\}$.

Multiplication

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

Given $a = \prod_{p \in P} p^{a_p}, b = \prod_{p \in P} p^{b_p}$ **define** $k = ab$.

K can be represented as $k = \prod_{p \in P} p^{k_p}$

It follows that $k_p = a_p + b_p$ **for all** $p \in P$.

Example a=12, b=18. **Check for** k=ab.

$k = 12 \text{ x } 18 = (2^2 \text{ x } 3) \text{ x } (2 \text{ x } 3^2) = 216$

$k_2 = 2 + 1 = 3$; $k_3 = 1 + 2 = 3$

$216 = 2^3 \text{ x } 3^3 = 8 \text{ x } 27$

Division

- **Any integer of the form can be divided only by an integer that is of a lesser or equal power of the same prime number, p_j with $j \le n$.**

- **If** $a = \prod_{p \in P} p^{a_p}, b = \prod_{p \in P} p^{b_p}$**, and $a \mid b$, then $a_p \le b_p$ for all p.**

Example

Given a = 12, b = 36, and 12|36.

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

$a_2 = 2 = b_2$, $a_3 = 1$, $b_3 = 2$

$\Rightarrow a_p \le b_p$ for all p.

9.1.1 Continued

Greatest Common Divisor

- It is easy to determine the **greatest common divisor** of two positive integers if we express each integer as the product of primes.
- The following relationship always holds:
  If k = **GCD**(a,b) then k_p = **min**(a_p, b_p) for all p.

Example Find GCD(300,18).

$300 = 2^2 \times 3^1 \times 5^2$

$18 = 2^1 \times 3^2$

$GCD(300,18) = 2^1 \times 3^1 \times 5^0 = 6$

Infinite Number of Primes

Note

There is an infinite number of primes.

Number of Primes

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

Example

As a trivial example, assume that the only primes are in the set {2, 3, 5, 7, 11, 13, 17}. Here P = 510510 and P + 1 = 510511. However, 510511 = 19 × 97 × 277; none of these primes were in the original list. Therefore, there are three primes greater than 17.

Example

Find the number of primes less than 1,000,000.

Solution

The approximation gives the range 72,383 to 78,543. The actual number of primes is 78,498.

9.1.3 Checking for Primeness

- ***Given a number n, how can we determine if n is a prime?***

- ***We need to see if the number is divisible by all primes less than $\sqrt{n}$***

- ***We know that this method is inefficient, but it is a good start.***

Example

Is 97 a prime?

Solution

The floor of $\sqrt{97}$ = 9. The primes less than 9 are 2, 3, 5, and 7. We need to see if 97 is divisible by any of these numbers. It is not, so 97 is a prime.

Example

Is 301 a prime?

Solution

The floor of $\sqrt{301}$ = 17. We need to check 2, 3, 5, 7, 11, 13, and 17. The numbers 2, 3, and 5 do not divide 301, but 7 does. Therefore 301 is not a prime.

9.1.3 Continued

Sieve of Eratosthenes

Sieve of Eratosthenes is an algorithm for finding all the prime numbers in a segment [1,n].

Example **Find the primes in [1,16].**

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	**3**	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	**11**	~~12~~	13	~~14~~	~~15~~	~~16~~
2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~	**11**	~~12~~	**13**	~~14~~	~~15~~	~~16~~

9.1.3 Continued

Sieve of Eratosthenes

Example **Find the primes in [1,100].**

	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~~

References

- **Chapter 9 -** Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 3rd Edition, 2015.

- **Chapter 8 -** William Stallings, Cryptography and Network Security Principles and Practices, 7th Edition, Pearson Education, 2017.