4 CHAPTER Number Theory and Cryptography

4.1.2 Division

- When one integer is divided by a second nonzero integer, the quotient mayor may not be an integer.
- For example, 12∕3 = 4 is an integer, whereas 11∕4 = 2.75 is not.

Definition:

If a and b are integers with a ≠ 0, we say that a divides b if there is an integer c such that b = ac (or equivalently, if $\frac{b}{a}$ is an integer). When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a. The notation a | b denotes that a divides b. We write a ∤ b when a does not divide b.

- Remark: We can express a | b using quantifiers as ∃c(ac = b), where the universe of discourse is the set of integers.

Example: Determine whether 3 | 7 and whether 3 | 12.

Solution:
- 3 ∤ 7, because 7∕3 is not an integer.
- On the other hand, 3 | 12 because 12∕3 = 4

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where a ≠ 0. Then

(i) if a | b and a | c, then a | (b + c);

(ii) if a | b, then a | bc for all integers c;

(iii) if a | b and b | c, then a | c

Proof

i. **:** if a | b and a | c then a | (b +c)

- from the definition of divisibility we get:
- b=au and c=av where u,v are two integers. Then(b+c) = au +av = a(u+v)

- **Thus a divides b+c.**

ii. **:** if a | b then a | bc for all integers c

- If a | b, then there is some integer u such that b = au.
- Multiplying both sides by c gives us bc = auc, so by definition, a | bc.

- **Thus a divides bc.**

Corollary 1: If a, b, and c are integers, where a ≠ 0, such that a | b and a | c, then

a| mb + nc whenever m and n are integers.

Proof:

We will give a direct proof. By part (ii) of Theorem 1 we see that a | mb and a | nc whenever m and n are integers. By part (i) of Theorem 1 it follows that a | mb + nc

Primes

Definition:

A positive integer p that is greater than 1 and that is divisible only by 1 and byitself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2, 1 |3 and 3 | 3, etc

Definition:

A positive integer that is greater than 1 and is not a prime is called **a composite**

Examples : 4, 6, 8, 9, …Why?

2 | 4

3 | 6 or 2 | 6

2 | 8 or 4 | 8

3 | 9

Fundamental theorem of Arithmetic:

Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- 12 = 2*2*3
- 21 = 3*7

- Process of finding out factors of the product:

factorization.Factorization of composites to primes:

- 100 = 2*2*5*5 = 2^2*5^2
- 99 = 3*3*11 = 3^2 *11

- **How to determine whether the number is a prime or a composite?**

- **Simple approach (1):**

- Let n be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.

Example 1:

- Assume we want to check if 17 is a prime?
- The approach would require us to check:
- 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

- **Is this the best we can do?**
- **No.** The problem here is that we try to test all the numbers. But this is not necessary.
- **Idea:** Every composite factorizes to a product of primes. So it is sufficient to test only the primes $x < n$ to determine the primality of n.

Approach 2:

- Let n be a number. To determine whether it is a prime we can test if

any prime number x < n divides it. If yes it is a composite.
If we test all primes $x < n$ and do not find a proper divisor then n is a prime.

Example 2: Is 31 a prime?

- Check if 2,3,5,7,11,13,17,23,29 divide it
- It is a prime !!

Example 3: Check if Is 91 a prime number?

- Easy primes 2,3,5,7,11,13,17,19 …
- But how many primes are there that are smaller than 91?

Caveat:

- If n is relatively small the test is good because we can enumerate(memorize) all small primes
  But if n is large there can be larger not obvious primes

Theorem 2: If n is a composite then n has a prime divisor less than or equal to $\sqrt{n}$

Approach 3:

- Let n be a number. To determine whether it is a prime we can test if any prime number $x \leq \sqrt{n}$ divides it.

Example 4: Is 101 a prime?

Primes smaller than or equal to $\sqrt{101} \approx 10.04987$ are: 2,3,5,7

- 101 is not divisible by any of them
- **Thus 101 is a prime**

- **Question:** How many primes are there?

Theorem 3: There are infinitely many primes.

The Division Algorithm

Theorem 4: **[The Division Algorithm]** Let a be an integer and d a positive integer. Then there are unique integers, q and r, with $0 \leq r < d$, such that

$$\mathbf{a = dq + r}.$$

Definition:

In the equality given in the division algorithm, **d** is called the **divisor**, **a** is called the **dividend**, **q** is called the **quotient**, and r is called the remainder. This notation is used to express the quotient and remainder: **q = a div d**, **r = a mod d.**

Example 5:

a= 14, d = 3

14 = 3*4 + 2

14/3=3.666

14 div 3 = 4

14 mod 3 = 2

Greatest common divisor

Definition:

Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?
- Check 2,3,4,6,12 gcd(24,36) = 12
- gcd(11,23) = ?

A systematic way to find the gcd using factorization:

- Let **a**=$p_1^{a_1}$ $p2^{a_2}$ $p_3^{a_3}$ $\dots_k^{a_k}$ and **b**= $p_1^{b_1}$ $p_2^{b_2}$ $p_2^{b_3}$ $\dots$ $p_k^{b_k}$
- gcd(a,b)= $p_1^{\min(a1,b1)}$ $p_2^{\min(a2,b2)}$ $p_3^{\min(a3,b3)}$ $\dots$ $p_k^{\min(ak,bk)}$

Example 6 :

- gcd(24,36) = ?
- 24 = 2*2*2*3=2^3*3

- $36 = 2*2*3*3 = 2^2 * 3^2$
- gcd(24,36) $= 2^2 * 3 =$ **12**

Least common multiple

Definition:

Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer thatis divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example 7:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**
- **Yes.** Try 36. Both 12 and 9 cleanly divide 36

A systematic way to find the lcm using factorization:

- Let **a**$= p_1^{a_1}\ p2^{a_2}\ p_3^{a_3} \ldots_k^{a_k}$ and **b**$= p_1^{b_1}\ p_2^{b_2}\ p_2^{b_3} \ldots p_k^{b_k}$
- lcm(a,b)$= p_1^{\max(a1,b1)}\ p_2^{\max(a2,b2)}\ p_3^{\max(a3,b3)} \ldots p_k^{\max(ak,bk)}$

Example 8:

- **What is lcm(12,9) =?**
- $12 = 2*2*3 = 2^2*3$
- $9 = 3*3 = 3^2$
- **lcm(12,9)** $= 2^2 * 3^2 = 4 * 9 =$ **36**

Euclid algorithm

Finding the greatest common divisor requires factorization

Factorization can be cumbersome and time consuming since we need to find all factors the two integers that can be very large.

- Luckily a more efficient method for computing the gcd is the **Euclid's algorithm.**

Example 9:

- Find the greatest common divisor of 666 and 558

Solution

gcd(666,558) = gcd(558,108) = gcd(108,18) = **18**	666=1*558 + 108 558=5*108 + 18 108=6*18 + 0

Example 10:

- Find the greatest common divisor of 286 and 503:

Solution

• gcd(503,286) =gcd(286, 217) =gcd(217, 69) = gcd(69,10) =gcd(10,9) = gcd(9,1) =**1**	503=1*286 + 217 286=1*217 + 69 217 = 3*69 + 10 69 = 6*10 + 9 10=1*9 + 1

Modular arithmetic

In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24hour clock after 50 hours?

Answer: the result is 2 am

How did we arrive to the result:

- Divide 50 with 24. The reminder is the time on the 24 hour clock.50= 2*24 + 2

  so the result is 2 am.

Congruency

Definition:

If a and b are integers and m is a positive integer, then **a is congruent to b modulo n** if m divides a-b. We use the notation **a = b (mod m)** to denote the congruency. If a and b are not congruent we write a ≠ b (mod m).

Theorem 5. If a and b are integers and m a positive integer. Then a=b (**mod** m) if and only if **a** mod **m** = **b** mod **m**.

Example 11: Determine if 17 is congruent to 5 modulo 6?

Solution:

17 mod 6 = **5**
5 mod 6 = **5**
Thus 17 is congruent to 5 modulo 6.

Theorem 6. Let **m** be a positive integer. The integers **a** and **b** are congruent modulo m if and only if there exists an integer k such that **a**=**b**+**mk**.

Theorem 7. Let **m** be a positive integer. If **a**=b (mod **m**) and **c**=**d**(mod **m**) then:

a+c = **b+d** (mod **m**) and **ac**=**bd** (mod **m**).

Modular arithmetic in Computer Science

Modular arithmetic and congruencies are used in Science:

- **Pseudorandom number generators**
- **Hash functions**
- **Cryptology**

Pseudorandom number generators

- **Some problems we want to program need to simulate a random choice.**
- **Examples: flip of a coin, roll of a dice**
- **We need a way to generate random Outcomes**
- **Basic problem:**
  - assume outcomes: 0, 1, .. N
  - generate the random sequences of outcomes
  - Pseudorandom number generators let us generate sequences that look random
  - **Next:** linear congruential method

Linear congruential method

- We choose 4 numbers:
- the modulus m,
- multiplier a,
- increment c, and
- seed x_0,

such that $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.

- We generate a sequence of numbers $x_1, x_2\ x_3 \ldots x_n \ldots$ such that $0 \leq x_n < m$ for all *n* by successively using the congruence:
  - $x_{n+1} = (a.x_n + c) \bmod m$

Example 12:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- x_1= 7*3+4 mod 9= 25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....