

## 1 Lecture Plan

- Prime numbers and divisibility
- Greatest common divisor
- Modular Arithmetic

## 2 Prime Numbers and Divisibility

Public-key cryptography is based on the hardness of certain number-theoretic problems. For the next few lectures, we will cover some topics in number theory and algebra. We will then see constructions of public-key encryption and signature schemes.

- For  $a, b \in \mathbb{Z}$ , we say that  $a$  divides  $b$  (written as  $a \mid b$ ) if there exists an integer  $c$  such that  $b = ac$ . If  $a$  does not divide  $b$ , we write  $a \nmid b$ .
- **Observation:** If  $a \mid b$  and  $a \mid c$ , then  $a \mid (Xb + Yc)$  for any  $X, Y \in \mathbb{Z}$ .
- If  $a \mid b$  and  $a$  is positive, we call  $a$  a *divisor* of  $b$ .
- A positive integer  $p > 1$  is *prime* if it has only two divisors: 1 and itself.
- A positive integer greater than 1 that is not prime is called *composite*. By convention, the number 1 is neither prime nor composite.
- Every integer greater than 1 can be expressed *uniquely* (up to ordering) as a product of primes. That is, any positive integer  $N > 1$  can be written as  $N = \prod_i p_i^{e_i}$  where  $p_i$ 's are distinct primes and the  $e_i$ 's are integers such that  $e_i \geq 1$  for all  $i$ .
- **Proposition 8.1:** Let  $a$  be an integer and let  $b$  be a positive integer. Then there exist unique integers  $q, r$  for which  $a = qb + r$  and  $0 \leq r < b$ .
- Computing the integers  $q$  and  $r$  in the above proposition can be done in time which is polynomial in  $\|a\|$  and  $\|b\|$ . Here  $\|a\|$  denotes the length of the binary representation of  $a$ . For example,  $\|3\| = 2$  and  $\|17\| = 5$ .
- The *greatest common divisor* of two integers  $a, b$  not both zero, written  $\gcd(a, b)$ , is the largest integer  $c$  such that  $c \mid a$  and  $c \mid b$ .
  - The value  $\gcd(0, 0)$  is undefined.

- For  $b \geq 1$ ,  $\gcd(b, 0) = \gcd(0, b) = b$ .
- If  $p$  is a prime, then  $\gcd(a, p)$  is either 1 or  $p$ .
- If  $\gcd(a, b) = 1$ , we say that  $a$  and  $b$  are *relatively prime*.
- Given  $a$  and  $b$ , the *Euclidean algorithm* can be used to calculate their gcd in time polynomial in  $\|a\|$  and  $\|b\|$ .

**Algorithm 1** Euclidean Algorithm

**Input:** Integers  $a, b$  with  $a \geq b > 0$

**Output:**  $d = \gcd(a, b)$

**procedure** GCD( $a, b$ )

**if**  $b$  divides  $a$  **then return**  $b$

**else return** GCD( $b, a \bmod b$ )

- **Lemma:** For integers  $a, b, q, r$ , if  $a = qb + r$ , then  $\gcd(a, b) = \gcd(b, r)$ .
- **Proposition 8.2:** Let  $a, b$  be positive integers. Then there exist integers  $X, Y$  such that  $Xa + Yb = \gcd(a, b)$ . Furthermore,  $\gcd(a, b)$  is the smallest positive integer that can be expressed this way.
- Given  $a$  and  $b$ , the *extended Euclidean algorithm* can be used to calculate their gcd in time polynomial in  $\|a\|$  and  $\|b\|$ . See Algorithm B.10 on page 552 of KL.
- **Proposition 8.3:** Let  $c \mid ab$  and  $\gcd(a, c) = 1$ , then  $c \mid b$ . Thus, if  $p$  is prime and  $p \mid ab$  then either  $p \mid a$  or  $p \mid b$ .
- **Proposition 8.4:** Let  $a \mid N, b \mid N$  and  $\gcd(a, b) = 1$ , then  $ab \mid N$ .

### 3 Modular Arithmetic

- Let  $a, b, N \in \mathbb{Z}$  with  $N > 1$ . We use the notation  $[a \bmod N]$  to denote the remainder of  $a$  upon division by  $N$ .
- We say that  $a$  and  $b$  are *congruent modulo  $N$* , written  $a = b \bmod N$ , if  $[a \bmod N] = [b \bmod N]$ . Note that  $a = b \bmod N$  if and only if  $N \mid (a - b)$ .
- Congruence modulo  $N$  obeys the standard rules of arithmetic with respect to addition, subtraction, and multiplication. But not division in general.
- In general,  $a = a' \bmod N$  and  $b = b' \bmod N$  does not necessarily mean  $a/b = a'/b' \bmod N$ . For example,  $6 = 30 \bmod 24$ . But  $3 \neq 15 \bmod 24$ .
- We can define division if some conditions hold. If for a given integer  $b$  there exists an integer  $c$  such that  $bc = 1 \bmod N$ , we say  $b$  is *invertible modulo  $N$*  and call  $c$  a *multiplicative inverse* of  $b$  modulo  $N$ . It is convenient to denote the multiplicative inverse of  $b$  by  $b^{-1}$ .
- Multiplicative inverses modulo  $N$  are unique when they exist.

- Division by  $b$  modulo  $N$  is *only defined* when  $b$  is invertible modulo  $N$ .
- **Proposition:** Let  $b, N$  be integers with  $b \geq 1$  and  $N > 1$ . Then  $b$  is invertible modulo  $N$  if and only if  $\gcd(b, N) = 1$ .

## 4 References and Additional Reading

- Section 8.1 from Katz/Lindell