4 Number Theory and Cryptography

4.3 Primes and greatest common divisors

1. A prime p is an integer greater than 1 whose only positive factors are 1 and p (note that 2 is the smallest prime number, and the only even prime number). If an integer greater than 1 is not prime, then it is a composite number. Note that only integers that are greater than or equal to 2 are either primes or composite.

2. Fundamental Theorem of Arithmetic: every positive integer greater than 1 can be uniquely written as product of primes (where the factors are arranged in an increasing order)
   i.e.: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_\alpha$, where $p_i \leq p_{i+1}$ for $1 \leq i \leq \alpha - 1$

3. If n is a composite integer, then n has prime divisors less than or equal to $\sqrt{n}$ (so in searching for divisors in a factorization of n, one should only look up to $\sqrt{n}$)

4. There are infinitely many primes (Use contradiction assuming it is finite, and construct a new prime $p = p_1 \cdot p_2 \cdot \ldots p_n + 1$)

5. The prime number theorem: The ratio of the number of primes not exceeding x and $\frac{x}{\ln x}$ approaches 1 as $x \to \infty$. Its usefulness comes in estimating the odds of choosing a random number that is prime (the distribution of primes).

6. gcd of two numbers = greatest common divisor: $\gcd(12, 30) = 6$

7. lcm of two numbers = least common multiple: $\text{lcm}(12, 30) = 60$

8. Integers a and b are relatively prime (or also called coprimes) if $\gcd(a, b) = 1$: The numbers 7 and 9 are relatively prime

9. The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if all of them are relatively prime pairwise (i.e. $\gcd(a_i, a_j) = 1, \forall i, j$ with $1 \leq i \neq j \leq n$).

10. Note: $ab = \gcd\ (a, b) \cdot \text{lcm}(a, b)$

11. Euclidean Algorithm: gives an alternative way to find the gcd of two numbers a, and b, without using the prime factorization of the two numbers but rather the fact that $gcd(a, b) = gcd(b, r)$, where r is the remainder (i.e. $a \,\mathbf{mod}\, b = r$).

12. From above, we can write the $\gcd(a, b) = d$ as a linear combination $d = \alpha a + \beta b$, for some $\alpha, \beta \in \mathbb{Z}$

13. Particularly, if a and b are relatively prime, then $1 = \alpha a + \beta b$, for some $\alpha, \beta \in \mathbb{Z}$

14. If p is a prime such that $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$, then $p|a_i$ for some i $(1 \leq i \leq n)$

15. Simplifications in modular arithmetic:

$$\textbf{if } a, b, c, m \in \mathbb{Z} \ (m > 0) \text{ and } \gcd(c, m) = 1,$$

$$\textbf{then } ac \equiv bc (\operatorname{mod} m) \Rightarrow a \equiv b (\operatorname{mod} m)$$

16. However, if $\gcd(c, m) \neq 1$, the above result doesn't hold