Prime Numbers and Complexity Analysis

1 Introduction to Primes

A positive integer $p \in \mathbb{Z}_{>0}$ is called a **prime** if p has exactly two divisors, namely 1 and p.

$$a|p \implies a = 1 \vee a = p \tag{1}$$

In fact, there is a much broader perspective on prime numbers including the theory of rings and divisibility. Since we analyze the application of primes to cryptography we restrict our discussion to $R = \mathbb{Z}$. In the following we want to discuss some basics about prime numbers and their structure in $\mathbb{Z}$. This also contains the complexity analysis of two basic but very powerful algorithms. To do so we wil introduce the notation of asymptotic behaviour.

First we want to introduce a basic relation between the set of primes $\mathbb{P}$ and an arbitrary natural number $n \in \mathbb{N}$:

Theorem (Fundamental Theorem of Arithmetic). *For each $n \in \mathbb{N}$ there is a unique factorization*

$$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$$

where exponents $a_i \in \mathbb{Z}_{>0}$ and $p_1 < p_2 < \ldots < p_k$ are primes.

2 Asymptotics

For the analysis of algorithms as well as for comparison of different functions it turned out that the asymptotic notation is quite useful. Assume $f, g; \mathbb{R}_{>0} \to \mathbb{R}$. Then, we distinguish three different classifications:

1. **f is asymptotic to g as x goes to infinity:**

$$f(x) \sim g(x) \Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

2. **f is big-$\mathcal{O}$ of g:** $f(x) = \mathcal{O}(g(x))$

$$\Leftrightarrow \exists C \in \mathbb{R}_{>0} \quad \exists x_0 \in \mathbb{R}_{>0} : |f(x)| \leq C|g(x)| \quad \forall x \geq x_0$$

3. **f is little-o of g:**

$$f(x) = o(g(x)) \Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$$

Of course both limits require the existence of the limits itself.

3 Extended Euclidean Algorithm

Definition (Greatest Common Divisor). $d \in \mathbb{Z}_{>0}$ is called the **greatest common divisor** of elements $a_1, ..., a_n \in \mathbb{Z}$ if

1. $d|a_1, ..., d|a_n$
2. $c|a_1, ..., c|a_n \implies c|d$ with $c \in \mathbb{Z}$

For $x, y \in \mathbb{Z}$ and not both 0, the extended euclidean Algorithm computes $a, b \in \mathbb{Z}$ and the greatest common divisor such that

$$a \cdot x + b \cdot y = \gcd(x, y) \tag{2}$$

Complexity analysis shows an unexpected connection to the Fibonacci numbers. Thus, the complexity of the extended Euclidean algorithm for $x, y \in [1, N], N \in \mathbb{N}$ is $T(N) = \mathcal{O}(\ln^2(N))$.

4 Quadratic Residues

Quadratic Residues are defined:

Definition (Quadratic Residues). For $a \in \mathbb{Z}, m \in \mathbb{Z}_{>0}$ with $\gcd(a, m) = 1$ we say that a is a **quadratic residue modulo** m if and only if

$$x^2 \equiv a \mod m \tag{3}$$

is solvable for $x \in \mathbb{Z}$. If not, a is called **quadratic non-residue modulo** m.

The Legendre and the Jacobi Symbol are cloesely related to the theory of quadratic residues:

Definition (Legendre Symbol). For $p \neq 2 \in \mathbb{Z}$ prime, we define the **Legendre Symbol**:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \mod p \\ 1, & \text{if } \exists x \in \mathbb{Z} : x^2 \equiv a \mod p \\ -1, & \text{if } \nexists x \in \mathbb{Z} : x^2 \equiv a \mod p \end{cases} \tag{4}$$

Definition (Jacobi Symbol). According to the fundamental theorem of arithmetic, there is for $m \in 2\mathbb{N}_0 + 1$ a unique prime factorization. For such m and $a \in \mathbb{Z}$, we define the **Jacobi Symbol**:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{t_i} \tag{5}$$

where p_i and t_i denote the factors of the unique prime factorization of m.

Relations of both symbols enable us to compute the Jacobi and Legendre Symbol with the same complexity as the Euclidean algorithm.

5 Infinitude of Primes

The following statement about the infinitude of primes was proven by Euclid 300 BC.

Theorem (Euclid). *There are infinitely many prime numbers.*

The Prime-counting Function counts the number of primes not exceeding a given threshold $x \in \mathbb{Z}$:

$$\pi(x) = \#\{p \leq x : p \in \mathbb{P}\} \tag{6}$$

Combinatorical arguments about the prime counting function using the fundamental theorem of arithmetic can be used to prove Euclids theorem as well as the classic argument made by Euclid. For another connection we need to consider the Riemann zeta function:

Definition. The Riemann zeta function is defined for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ as follows:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{7}$$

The infinitude statement can be proved also by using the properties of the Riemann zeta function:

Theorem (Euler Product)**.** *For* $\mathrm{Re}(s) > 1$ *and* $\mathbb{P}$ *the set of primes, it holds*

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \tag{8}$$

As we know the Riemann function diverges as $s \to 1^+$ and therefore the number of factors cannot be finite.

6 Distribution of Primes

Not only the infinitude of primes is an interesting part of research. The distribution of primes also is of great importance. The most fundamental theorem was conjectured by Gauss and is called the Prime Number Theorem:

Theorem (Prime Number Theorem)**.**

$$\pi(x) \sim \frac{x}{\ln(x)} \tag{9}$$

It is a quite good estimation of the number of primes not exceeding a specific threshold and therefore provides information about the distribution of primes in genereal.