Lecture 7.

Factoring into Primes

Prime numbers are used in many cryptographic algorithms.

Def An integer $p > 1$ is called a prime number if it has exactly two positive divisors, namely 1 and p.

We denote the set of all primes by $\mathbb{P}$:

$$\mathbb{P} = \{2, 3, 5, 7, \ldots\}$$

An integer $a > 1$ that is not a prime is called composite: e.g. $6 = 2 \cdot 3$

If the prime p divides the integer a, then p is called prime divisor of a.

We are interested in factorization of integers (decomposition) as a product of primes.

- question 1: Is every integer can be written as a product of primes
- question 2: Is such a decomposition (if it exist) is unique
- question 3: define effivient factorization algorithms, find a complexity of factorization algorithms.

May be You know the very popular factorization algorithm RSA?

Th 1. Every integer $a > 1$ has a prime divisor.

Proof. The integer (a) has a divisor that is greater than 1, namely (a). But (a) can be not a prime number. Among all divisors of (a) that are greater than 1, let p be the smallest. Then p must be prime. Otherwise, p would have a divisor b with

$$1 < b < p \leq a$$

This contradicts the assumption that p is the smallest divisor of (a) that is greater than 1. ▷

Th 2. If a prime number divides the product of two integers $a \cdot b$, then it divides at least one factor

(this statement seems to be trivial, but we must give a strict proof!

Proof. (Explain a example

$24 = 3 \cdot 8 \;/\; 6 = 4$

but 6 is not a divisor of 3 or 8.)

Suppose that p (a prime number) divides ab but not (a).

Since p is a prime number we must have

$$\gcd(a, p) = 1$$

We remember that for any a and b there are integers x and y with

$$ax + by = \gcd(a, b).$$

In our case

$$\gcd(a, p) = 1, \quad \text{thus}$$

there are integers x, y with

$$ax + py = 1.$$

This implies

$$b = abx + pby$$

Since p divides ab and pb, then p is a divisor of b.

Th 3. If a prime number p divides a product $\prod_{i=1}^{k} q_i$ of prime numbers, then p is equal to one of the factors $q_1, q_2, \dots, q_k$.

Proof. The proof is based on induction on k. If $k=1$ then p is a divisor of q_1, which is greater than 1, hence $p = q_1$.

If $k > 1$, then p divides

$$q_1 (q_2 \cdots q_k).$$

By Th. 2 the prime p divides q_1 or $q_2 \cdots q_k$.

Because both products have fewer than k factors, the assertion follows from the induction hypothesis (that assert is valid for $\prod_{i=1}^{m} q_i$, $m < k$.), ▷

The main theorem of elementary number theory

Th. 4 Every integer $a > 1$ can be written as the product of prime numbers. Up to permutation the factors in this product are uniquely determined.

Proof The theorem is proved by induction on a.

- For $a = 2$ the theorem is true.
- Let $a > 2$. It follows from Th. 1 there is a prime divisor p of a.
  If $a/p = 1$ then $a = p$ and the assertion of theorem holds.
  Let $a/p > 1$. By the induction hypothesis
  a/p is a product of primes.
  Therefore a is also a product of primes

- This ~~proofes~~ proves the existence of the prime factor decomposition of ~~primes~~ a.
- Next we must show the uniqueness of decomposition.

So let

$a = p_1 p_2 \cdots p_k$ and $a = q_1 q_2 \cdots q_\ell$

be factorizations of a into prime numbers. By Th. 3. the prime p_1 is equal to one of the primes $q_1, q_2, \ldots, q_\ell$. By permuting the q_j, we can make ~~sho~~ sure that

$$p_1 = q_1.$$

By the induction hypothesis the factorization of $a/p_1 = a/q_1$ into prime numbers is unique, hence $k = \ell$ and $q_i = p_i$ after permutation of q_ℓ. ▷