§2.2 Fundamental Theorem of Arithmetics.

Theorem (FTA). Every positive integer can be written as a product of primes in the unique way (up to order).

Proof. Existence: by induction.

1 is an empty product ($2^0 = 1$
$0! = 1$)

2 is prime (product of one prime number)

Assume every number between 1 and n is a product of primes. Consider $n+1$.

(a) $n+1$ is prime ✓

(b) $n+1 = d_1 d_2$, $1 < d_1, d_2 \leq n$

Then by assumption, d_1, d_2 are products of primes

$\Rightarrow$ so is $d_1 d_2$ ✓

Uniqueness: Assume $p_1 p_2 \dots p_d = q_1 q_2 \dots q_s$ where $p_1, \dots, p_d, q_1, \dots, q_s$ are prime and $d \leq s$

$p_1 \mid p_1 p_2 \cdots p_d = q_1 q_2 \cdots q_s \Rightarrow p_1$ divides one of q_i's (by Lemma).

After reordering $p_1 \mid q_1 \Rightarrow p_1 = q_1$.

$\Rightarrow p_2 \cdots p_d = q_2 \cdots q_s$

$\Rightarrow p_3 \cdots p_d = q_3 \cdots q_s$

$\Rightarrow \ldots \Rightarrow 1 = q_{d+1} \cdots q_s$

This is only possible if $d = s$ (empty product on the right hand side)

$\boxtimes$

Remark: In some other number systems FTA may be false.

($\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$).

§2.3 Factorisation.

Q1: Given positive integer n how to check that it is prime?

Q2: How to factorize it?

For large n they non-trivial.

One can check primality for up to 50000 - 70000 digit numbers and factorize up to 220-230 digit numbers.

Naive factorization method (trial division): try small divisors d of n.

- We can consider prime d.
- Check values d up to $\sqrt{n}$ (If $n = d_1 d_2$ then one of d_1, d_2 is $\leq \sqrt{n}$).

Example: $n = 2191$

Try $d = $ 2 3 5 7
✗ ✗ ✗ ✓

$2191 = 7 \cdot 313$

For 313 try $d = $ 7 11 13 17 19
✗ ✗ ✗ ✗

stop here.

$19^2 = 361 > 313$

Final factorization: $2191 = 7 \cdot 313$.

Fermat factoring method.

Assume n is odd.

Idea: write n as a difference of two squares

$n = m^2 - k^2 = (m-k)(m+k)$

- We start with smallest $m \geq \sqrt{n}$.

- We go up until $m^2 - n$ becomes a square.

Example: $n = 2183$

$\sqrt{n} = 46. \ldots$

We start with $m = 47$.

$47^2 - 2183 = 26$ X

$48^2 - 2183 = 121 = 11^2$ ✓

Then $2183 = 48^2 - 11^2 = 37 \cdot 59$.

Remark: Fermat method is efficient in finding $n = d_1 d_2$ where d_1 and d_2 are close to each other.

§2.4. Distribution of primes.

First primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Q: Are there infinitely many primes?

A: Yes!

Theorem (Euclid): There are inf. many primes.

Proof. Assume there are finitely many

$$p_1, p_2, \dots, p_d$$

Consider $N = p_1 p_2 \cdots p_d + 1$

By FTA. we have prime $q \mid N$.

$$\underbrace{\gcd(\cancel{q}\, N, p_i)}_{=1} \quad \text{for } 1 \le i \le d$$

$\Rightarrow \gcd(q, p_i) = 1 \Rightarrow q$ is not on the list — contradiction. $\boxtimes$

By analogy one can prove that there are inf. many primes of the form $3n+2$ or $4n+3$.

(Ex*)