Number Theory

Emil Straschil

ETH Zurich

2026

Basics

Remainders

For all a and $b \neq 0$ there are q and $0 \leq r < |b|$ with

$$a = bq + r$$

- Such r is the **remainder** $R_b(a)$
- We write $x|y$ iff x divides y
- $x|y \iff \exists c xc = y$

Ideals

Ideal

$(a, b) = \{a\alpha + b\beta | \alpha, \beta \in \mathbb{Z}\}$

- For example, in $(2, 3) = \mathbb{Z}$, since $-1 * 2 + 1 * 3 = 1$ and we can generate any number from there

Prime Factors

Every integer has a unique prime factorization. We write

$$x = \prod_i p_i^{e_i}$$

where p_i are the prime factors

- For example, $30 = 2 * 3 * 5$

Remember that 1 is **not** a prime and that $\prod_{\emptyset} = 1$

GCD

Greatest Common Divisor

The greatest common divisor of x and y is a number g such that

$$g|x \wedge g|y$$

and g is divided by all other common divisors of x and y.

$\gcd(x, y)$ denotes the positive gcd. A gcd can in general also be negative and there can be more than one.

- If $\gcd(x, y) = 1$ then they are **coprime**
- There are α, β such that $\gcd(a, b) = \alpha a + \beta b$
- Section 4.3.3.: Representation with prime factors

Euclid Algorithm

$gcd(m, n) = gcd(m, R_m(n))$

Euclid Algorithm

1. Start with m and n.
2. Take the larger number and calculate its remainder modulo the smaller number. Replace the larger number with that
3. Repeat (2) until the remainder is 0. The other number left is the gcd.

Example:

- (75, 10)
- (5, 10) because 75 - 7*10 = 5
- (5, 0) because 10 - 2*5 = 0
- gcd is 5

Modular Arithmetic

$$
\begin{aligned}
& a \equiv_m b \\
\iff & m \mid (a-b) \\
\iff & a = b + km \quad \text{for some } k \\
\iff & b = a + km \quad \text{for some } k \\
\iff & R_m(a) = R_m(b)
\end{aligned}
$$

- When calculating under $\equiv_m$, we can always add any multiple of m to any number. So $5 \equiv_6 11 \equiv_6 -1$

Remainders

Pulling R inside

$R(x^n) = R(R(x)^n)$ for any remainder.

This does **not** hold for the power! It does **not** hold that $R(x^n) = R(x^{R(n)})$

- $R_5(6^{123123}) = R_5(R_5(6)^{123123}) = R_5(1) = 1$

Not exam relevant tricks:

- If the sum of digits is divisible by 3 / 9, then the number is too
- If the last 2 / 3 digits are divisible by 4 / 8, then the number is too
- and more ...

Multiplicative Inverse

Multiplicative Inverse

If $gcd(x, m) = 1$ then there is a c such that $xc \equiv_m 1$. This c is the multiplicative inverse of x modulo m.

How do we find it?

- We need c with $xc \equiv_m 1$
- Which means there is k with $xc + km = 1$
- Extended Euclid Algorithm finds such c and k
- In the exam: Extended Euclid or trial and error or have a table with them on cheatsheet for small x and m