1 Euclid's algorithm

We say that a *divides* b, denoted by $a \mid b$, if an element $k \in \mathbb{Z}$ exists such that $ak = b$.

Recall the Euclid's algorithm for finding the greatest common divisor of natural numbers a_0 and a_1: We set $(u_0, v_0) = (1, 0)$, $(u_1, v_1) = (0, 1)$ and $i = 1$ and then until $a_i > 0$ we compute $a_{i+1} = (a_{i-1}) \bmod a_i$, $q_i := (a_{i-1}) \operatorname{div} a_i$ and then values $(u_{i+1}, v_{i+1}) = (u_{i-1}, v_{i-1}) - q_i(u_i, v_i)$ and $i = i+1$. The output is $a_{i-1} = \gcd(a_0, a_1)$ and the Bézout coefficients u_{i-1}, v_{i-1} satisfying $\gcd(a_0, a_1) = u_{i-1}a_0 + v_{i-1}a_1$.

1.1. Using the Euclid's algorithm

(a) find $\gcd(37, 10)$ and the corresponding Bézout coefficients,

(b) calculate 10^{-1} in the field $\mathbb{Z}_{37}$.

1.2. Using the Euclid's algorithm

(a) compute $\gcd(1023, 96)$ and the corresponding Bézout coefficients,

(b) find $\operatorname{lcm}(1023, 96)$ and its prime decomposition,

(c) find some integer solution to the equation $1023x + 96y = 18$.

1.3. Find $\gcd(89, 55)$ and the corresponding Bezout coefficients. Explain how the fact that these are two consecutive terms in the Fibonacci sequence affect the

1.4. Find invers elements 27^{-1}, 2^{-1}, 8^{-1} in the field $\mathbb{Z}_{41}$.

1.5. Calculate the greatest common divisor and the corresponding Bézout coefficients

(a) $\gcd(2^{92} - 1, 2^{31} - 1)$,

(b) $\gcd(2k + 1, 3k + 1)$ for arbitrary $k \in \mathbb{N}$.

1.6. Find all the integer solutions or prove that there aren't any of the equations

(a) $3x + 4y = 1$,

(b) $3x + 4y = 5$,

(c) $18x + 24y = 6$,

(d) $18x + 24y = 5$,

(e) $18x + 24y = 12$.

We say that *a is congruent to b modulo m*, denoted by $a \equiv b (mod\ m)$ if $m \mid (a - b)$.

We will prove soon that for any $a, b \in \mathbb{Z}$, $b \neq 0$ there exist unique $k, r \in \mathbb{Z}$, such that

$$a = bk + r \qquad \wedge \qquad 0 \leq r <\mid b \mid$$

1.7. Let m be a natural number

(a) Prove that the congruence modulo m is an equivalence relation.

(b) Prove that $a \equiv b$ if and only if a and b have the same remainder after dividing by m.

(c) Count the number of equivalence classes with respect to m.