Number Theory II

Discrete Algebraic Structures

Thomas J. Friese

December 19, 2024

Congruent numbers

For any numbers a, b and m, the following two are equivalent:

- a and b have the same remainder in division by m
- $a - b$ is divisible by m

We say a and b are congurent modulo m.

- $a \equiv_m b$
- $a \equiv b$
- $a \bmod m \equiv b \bmod m$
- $[a] = [b] \rightarrow a$ and b share the same equivalence class in $\mathbb{Z}/\equiv_m$

Modular arithmetic and inverses

Can calculate with equivalence classes:

- $[a] + [b] = [a + b]$
- $[a] \cdot [b] = [a \cdot b]$

b is modular inverse of a modulo m if $ab \equiv 1 \bmod m$

- exists if and only if a and m are coprime
- if b is inverse of a, then so is every $c \in [b]_m$

Euler's totient function and Fermat's little theorem

$\varphi(n) = |\{a \in \{0, \ldots n-1\} | \gcd(n, a) = 1\}|$, so the number of smaller non-negative integers coprime to n.

For prime factor decomposition $n = p_1^{e_1} \cdots p_k^{e_k}$ we have

$$\varphi(n) = p_1^{e_1 - 1} \cdots p_k^{e_k - 1}(p_1 - 1) \cdots (p_k - 1)$$

If a and m are coprime,

$$a^{\varphi(m)} \equiv 1 \bmod m$$

i.e. $a^{\varphi(m)-1}$ is the modular inverse of a.

Chinese remainder theorem

Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists exactly one $c \in \{0, \ldots, mn-1\}$ such that $c = a \bmod m$ and $c = b \bmod n$.
How do we find c?

- $\diamond$ find Bézout coefficients u, v, such that $u \cdot m + v \cdot n = 1$
- $\diamond$ then c is remainder in division of $vna + umb$ by mn

$\rightarrow$ $vna + umb = q \cdot (mn) + c$