

homomorphisms and modular arithmetic

1

arithmetic in \mathbb{Z} and \mathbb{Z}_n

- congruence “modulo n ” in \mathbb{Z}
let $n \in \mathbb{N}, n \geq 1$, for $u, v \in \mathbb{Z}$ define

$$u \equiv v \pmod{n} \stackrel{\text{def}}{\iff} u - v \pmod{n} = 0 \\ \iff n \mid u - v$$

- properties of congruence
 - $\equiv \pmod{n}$ is an equivalence relation on \mathbb{Z}
 - $\equiv \pmod{n}$ is compatible with addition and multiplication

$$\left. \begin{array}{l} u \equiv v \pmod{n} \\ u' \equiv v' \pmod{n} \end{array} \right\} \implies \left\{ \begin{array}{l} u + u' \equiv v + v' \pmod{n} \\ u \cdot u' \equiv v \cdot v' \pmod{n} \end{array} \right.$$

2

- definition of \mathbb{Z}_n

notation

$$[u]_n = \{v \in \mathbb{Z}; u \equiv v \pmod{n}\}$$

(residue classes mod n)

$$\mathbb{Z}_n := \{[u]_n; n \in \mathbb{Z}\} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

becomes a ring by defining

$$[u]_n \oplus [v]_n := [u + v]_n$$

$$[u]_n \odot [v]_n := [u \cdot v]_n$$

3

- canonical homomorphism

$$\mathbb{Z} \rightarrow \mathbb{Z}_n : u \mapsto [u]_n$$

system of representatives $\{0, 1, \dots, n-1\}$

$$\text{addition} : (u, v) \mapsto u + v \pmod{n}$$

$$\text{multiplication} : (u, v) \mapsto u \cdot v \pmod{n}$$

- the rings \mathbb{Z}_n are the only homomorphic images of \mathbb{Z} !

4

– existence of inverses and computing inverses

$$\begin{aligned}u \in \mathbb{Z}_n \text{ invertible} &\iff \exists v \in \mathbb{Z}_n : u \cdot v = 1 \pmod n \\ &\iff \exists v \in \mathbb{Z}_n \exists k \in \mathbb{Z} : u \cdot v = 1 + k \cdot n \\ &\iff \exists v \in \mathbb{Z}_n \exists k \in \mathbb{Z} : u \cdot v - k \cdot n = 1 \\ &\iff \gcd(u, n) = 1\end{aligned}$$

– computation uses extended Euclidean algorithm!

$$u \cdot v - k \cdot n = 1 \text{ means: } v = u^{-1} \pmod n$$

5

group of units modulo n

notation:

the set of invertible elements of a ring R is a group, called the *group of units* of R , denoted by $U(R)$ write U_n instead of $U(\mathbb{Z}_n)$

$$U_n = \{u \in \mathbb{Z}_n ; \gcd(u, n) = 1\}$$

so that $\#U_n = \phi(n)$, where

$$\phi(n) = \prod_{\substack{i \\ \alpha_i > 0}} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \prod_{p|n, p \text{ prime}} \left(1 - \frac{1}{p}\right)$$

(EULER's ϕ -function)

6

$$\begin{aligned}\mathbb{Z}_n \text{ is a field} &\iff \text{all } 0 \neq u \in \mathbb{Z}_n \text{ are invertible} \\ &\iff U_n = \mathbb{Z}_n \setminus \{0\} \\ &\iff n \text{ is a prime number} \\ &\iff \phi(n) = n - 1\end{aligned}$$

7

LAGRANGE's theorem:

for any finite group G and any subgroup H of G one has $\#H \mid \#G$

for any finite group G and any element $x \in G$ there is a minimal positive number k such that x^k is the neutral element of G ; this is the cardinality of the cyclic subgroup generated by x — called the *order of x in G* . By LAGRANGE's theorem, this number must divide $\#G$.

take in particular $G = U_n$ and $x \in U_n$, then this number is called *the order of x modulo n* , written as $\text{ord}_n(x)$. This is the least natural number k such that $x^k \equiv 1 \pmod n$

8

an immediate consequence is EULER's theorem

for $b \in \mathbb{Z}, n \in \mathbb{N}, n > 1$ with $\gcd(b, n) = 1$ one has

$$b^{\phi(n)} \equiv 1 \pmod{n}$$

and in particular also FERMAT's theorem

for any prime number p and $b \not\equiv 0 \pmod{p}$ one has

$$b^{p-1} \equiv 1 \pmod{p}$$

9

the Chinese remainder theorem (simplest version)

- p, q positive integers with $\gcd(p, q) = 1$
- u, v Bézout coefficients for $p, q : u \cdot p + v \cdot q = 1$
- for integers b, c the number $x = c \cdot u \cdot p + b \cdot v \cdot q$ satisfies

$$x \equiv b \pmod{p} \text{ and } x \equiv c \pmod{q}$$

- uniqueness: any other integer y with $y \equiv b \pmod{p}$ and $y \equiv c \pmod{q}$ satisfies $y \equiv x \pmod{n}$

10

Chinese remainder theorem for multiple moduli

- m_1, m_2, \dots, m_r pairwise relatively prime positive integers,
 $M = m_1 \cdot \dots \cdot m_r$

- u_i, v_i Bézout coefficients for m_i and M/m_i :

$$u_i \cdot m_i + v_i \cdot (M/m_i) = 1$$

- for integers c_1, c_2, \dots, c_r the number

$$x = \sum_{1 \leq i \leq r} c_i \cdot v_i \cdot (M/m_i)$$

satisfies

$$x \equiv c_i \pmod{m_i} \quad (1 \leq i \leq r)$$

- uniqueness: any other integer y with $x \equiv c_i \pmod{m_i} \quad (1 \leq i \leq r)$ satisfies $y \equiv x \pmod{M}$

11

the main point in the construction is the fact that the

$$e_i := v_i \cdot (M/m_i) \quad (1 \leq i \leq r)$$

have the property

$$e_i \equiv \begin{cases} 1 & \pmod{m_i} \\ 0 & \pmod{m_j} \text{ for } i \neq j \end{cases}$$

this resembles closely the familiar idea of LAGRANGE interpolation

— this is not an accident!!

12

the algebraic version of the Chinese remainder theorem

Theorem: let m_1, \dots, m_r be numbers that are mutually relatively prime, i.e., $\gcd(m_i, m_j) = 1$ ($i \neq j$),

let $M = m_1 \cdot \dots \cdot m_r$,

then the following mapping is a bijection

$$\varphi : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r} : x \mapsto \langle x \bmod m_1, \dots, x \bmod m_r \rangle$$

and is indeed an *isomorphism of rings*

13

consequence: φ is an isomorphism of groups:

$$\varphi : U_M \xrightarrow{\sim} U_{m_1} \times \dots \times U_{m_r} : x \mapsto \langle x \bmod m_1, \dots, x \bmod m_r \rangle$$

consequence: let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \dots$ denote the prime factorization of n , then

$$\mathbb{Z}_n \cong \prod_{i \geq 1} \mathbb{Z}_{p_i^{\alpha_i}} \quad (\text{isomorphism of rings})$$

$$U_n \cong \prod_{i \geq 1} U_{p_i^{\alpha_i}} \quad (\text{isomorphism of groups})$$

14

the Chinese remainder theorem for arbitrary moduli

– for positive integers p, q there is an isomorphism of rings

$$\mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{\gcd(p,q)} \times \mathbb{Z}_{\text{lcm}(p,q)}$$

– corollary:

each finite abelian group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r}$ is isomorphic to precisely one group of type

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_k}$$

where $2 \leq d_1 | d_2 \dots | d_k$ (the *elementary divisors*)

15

the scheme of modular arithmetic

$$\begin{array}{ccc} \mathbb{Z}_M & \xrightarrow{\varphi} & \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r} \\ \downarrow_{+,*,\wedge^{(-1)}} & & \downarrow_{+,*,\wedge^{(-1)}} \dots \downarrow_{+,*,\wedge^{(-1)}} \\ \mathbb{Z}_M & \xleftarrow{\varphi^{-1}} & \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r} \end{array}$$

note: φ is an “evaluation map” and φ^{-1} is an “interpolation map”.

16