Project

Edwin Park

July 2022

Contents

1 Integers

1.1 Divisors

1.2 Primes

1.3 Congruences

Theorem. (Chinese Remainder Theorem)

Given:

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \\ \gcd(m,n) &= 1, \end{aligned}$$

a solution is given by

$$x = arm + bsn,$$

where $rm + sn = 1$.

1.4 Integers Modulo N

Definition. Euler's totient functions is defined as:

$$\varphi(n) = \#k \,|\, (k < n \wedge (n,k) = 1).$$

For any $n \in \mathbb{N}$:

$$\varphi(n) = \prod_i \left(1 - \frac{1}{p_i}\right)$$

Theorem. (Euler)

$$(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

2 Functions

2.1 Functions

2.2 Equivalence Relations

Notation. The collection of equivalence classes of S under relation $\sim$ is denoted by $S/\sim$.

2.3 Permutations

Definition. A permutation of a set S is a bijection $\sigma : S \to S$. A cycle of length k is a permutation satisfying:

$$\sigma(a_i) = a_{(i+1)\%k}$$
$$\sigma(x) = x, \text{ otherwise}$$

where $a_1, \ldots, a_k \in S$. Two cycles are disjoint if their respective $\{a_i\}$ have no overlaps.

Theorem. Every cycle in S_n may be written as a unique product of disjoint cycles.

Theorem. Transposition-decompositions of permutations always have the same parity.

3 Groups

3.1 Definition of a Group

Definition. A set G is a group under an operation $*$ if $*$ is an associative binary operation on G, G contains an identity element, and G is closed under inversion.

3.2 Subgroups

Theorem. (Lagrange)

$$H \leq G \Rightarrow |H| \mid |G|$$

3.3 Constructing Examples

Property.

$$H, K \leq G \wedge h^{-1}kh \in K \Rightarrow HK \leq G$$

3.4 Isomorphisms

3.5 Cyclic Groups

Theorem. Every subgroup of a cyclic group is cyclic.

3.6 Permutation Groups

Theorem. (Cayley) Every group is isomorphic to a permutation group (subgroup of S_n).

3.7 Homomorphisms

Definition. A subgroup H of G is normal iff $ghg^{-1} \in H$.

3.8 Cosets, Normal Subgroups, and Factor Groups

Definition. A coset takes the form aH where $H \leq G$. The index is the number of cosets;

$$[G : H] := \frac{|G|}{|H|}.$$

Theorem. The set of cosets of a normal subgroup form a group under multiplication. The group of cosets of a normal subgroup is called the factor group of G determined by N, denoted by G/N. Note that left and right cosets of a normal subgroup are always equivalent.

Theorem. Where N is a normal subgroup of G, there is a bijection between subgroups of G/N and subgroups of G containting N.

Proof. First we note that homomorphisms preserve subgroups, and normality if surjective. Furthermore, the pseudo-inverse operation of the homomorphism $\phi : G_1 \to G_2$,

$$\phi^{-1}(H_2 \leq G_2) = \{x \in G_1 \mid \phi(x) \in H_2\},$$

preserves subgroups and normality.
The bijection is given by the natural projection $\pi : G \to G/N, \quad \pi(x) = xN$. Note that the actual bijection, using a slight abuse of notation, is:

$$\pi(H \leq G) = \bigcup_{x \in H} \{xN\}.$$

Note that in the pseudo-inverse function, $\pi^{-1}(K \leq G/N) = \{x \in G \mid xN \in K\}$, the output always contains N as it is the identity in G/N (and in turn K contains it). To show bijectivity, ... cbf

Theorem. (Fundamental Homomorphism Theorem)

$$G/\ker(\phi) \cong \phi(G),$$

where $\phi : G \to H$ is a homomorphism, G and H are groups.

4 Polynomials

4.1 Fields; Roots of Polynomials

Definition. A field is a set F which is a group under two binary operations + and $*$, which also satisfy distributivity.

Multiplication of polynomial coefficients:

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$$

4.2 Factors

4.3 Existence of Roots

$\langle p(x)\rangle$ denotes the set of all polynomials divisible by $p(x)$.

Theorem. Given that $p(x)$ is non-constant, $F[x]/\langle p(x)\rangle$ is a field iff. $p(x)$ is irreducible over F.

The congruence class $[x]$ in $F[x]/\langle p(x)\rangle$ satisfies $p([x]) = [0]$.

4.4 Polynomials over Z, Q, R and C

5 Commutative Rings

5.1 Commutative Rings; Integral Domains

Definition. A commutative ring is a field without the requirement that inversion is closed with respect to $*$.

A subring must share identities with its parent.

Definition. An integral domain is a commutative ring where $1 \neq 0$ and the product of non-zero elements is always non-zero.

Theorem. Any subring of a field is an integral domain.

Theorem. Any finite integral domain is a field.

5.2 Ring Homomorphisms

Definition. The characteristic of a commutative ring is the minimal natural number satisfying $n * 1 = 0$; if no such number exists, then the characteristic is zero.

Definition. A ring homomorphism preserves sums, products and the identity.

5.3 Ideals and Factor Rings

Definition. An ideal I is a non-empty subset of a commutative ring R closed under addition, subtraction and multiplication by any element in R.

Theorem. R/I is a commutative ring, called the factor ring of R modulo I.

Theorem. Given that I is a proper ideal of the commutative ring R,

$$R/I \text{ is a field} \iff I \text{ is maximal}$$
$$R/I \text{ is an integral domain} \iff I \text{ is prime.}$$

5.4 Quotient Fields