MA2202 (Algebra I)

Jia Cheng

September 2021

1 Definitions

Sets

$$\mathbb{N} = \mathbb{Z}^+$$

Functions

Functional equality: 2 functions $f_1 : A \to B, f_2 : C \to D$ are equal iff $A = B \wedge C = D$ and their elementwise images are equal.

Equivalence Class Given a set S, an equivalence relation $\equiv$ on S. Then the equivalence class of an element $a \in S$ is denoted

$$Cl(a) = \{x \in S : a \equiv x\}$$

2 Elementary Number Theory

Coprime cancellation Suppose a, b, c are non-zero integers and $gcd(a, c) = 1$ and $a|bc$.

There are 2 ways to prove $a|b$.

First way, use Bezout's Lemma and multiple b on both sides.
Second way actually also uses Bezout's Lemma underlyingly, but we can view it atomically as follows.

Lemma $gcd(a, c) = 1$, then there exists an "inverse" c' of c such that $cc' \equiv 1(\mod a)$.

Since $bc \equiv 0(\mod a)$, we multiply c' on both sides to get $b \equiv bcc' \equiv 0(\mod a)$. Hence $a|b$.

Fermat's Little Theorem Given prime p, $a \in \mathbb{Z}$, we have

$$a^p \equiv a(\mod p)$$

If p does not divide a, then we use cancellation to get $a^{p-1} \equiv 1(\mod p)$

Chinese Remainder Theorem Taken from Brilliant

THEOREM

Chinese Remainder Theorem

Given pairwise coprime positive integers $n_1, n_2, \ldots, n_k$ and arbitrary integers $a_1, a_2, \ldots, a_k$, the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution, and the solution is unique modulo $N = n_1 n_2 \cdots n_k$.

The following is a general construction to find a solution to a system of congruences using the Chinese remainder theorem:

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute
$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$
3. For each $i = 1, 2, \ldots, k$, compute $z_i \equiv y_i^{-1} \bmod n_i$ using Euclid's extended algorithm (z_i exists since $n_1, n_2, \ldots, n_k$ are pairwise coprime).
4. The integer $x = \sum_{i=1}^{k} a_i y_i z_i$ is a solution to the system of congruences, and $x \bmod N$ is the unique solution modulo N.

3 Groups

Group axioms

- When proving axiom G4, closure under inverses, to show that y is an inverse of $x \in G$, **we need to show that** $y \in G$ in addition to showing that $xy = yx = e$. Too frequently the detail that $y \in G$ is not explicitly proven.
- This also applies if we want to prove a certain element is the identity. We may need to prove that the element lies in G first.

4 Counterexamples

Operations Commutative but not associative

- Taking arithmetic mean/geometric mean of 2 numbers
- Taking the difference of 2 numbers $|a - b|$

Associative but not commutative

- Function composition
- Matrix multiplication
- $(x, y) \mapsto y$

5 Symmetric groups

Isomorphism between 2 permutation groups Let S_n be the symmetric group of order n, and S_Y be the permutation group on Y, where $|Y| = n$. We write $Y = \{x_1, \ldots, x_n\}$
Then there are 2 ways in which we can define an isomorphism $\phi : S_n \to S_Y$.

First, a more indirect definition. Let $f : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Then $f \in S_n$. Define $\phi(f)$ as the mapping

$$\phi(f) : x_i \mapsto x_{f(i)}$$

It is then easy to prove the homomorphic properties of ϕ. $\phi(f \circ g)(x_i) = x_{(f\circ g)(i)} = x_{f(g(i))} = (\phi(f) \circ \phi(g))(x_i)$.

Second, we define the mapping $T : i \to x_i$ and consequently, $\phi = T \circ f \circ T^{-1}$.
Then $\phi(f \circ g) = T \circ f \circ g \circ T^{-1} = T \circ f \circ T^{-1} \circ T \circ g \circ T^{-1}$.

Cyclic notations Given 2 products A, B of disjoint permutation cycles, themselves also being pairwise disjoint. There are permutations f, g such that A represents f and B represents g. Now we want to prove the following properties.

- AB represents $f \circ g$. Proving this would allow us to make use of the properties of functional composition to claim that $A(BC) = (AB)C$, where A, B, C are products of disjoint permutation cycles. (and A, B, C are themselves pariwise disjoint).
  To prove this we consider cases: whether x lies in the cycles of A, whether x lies in the cycles of B, or neither. Note that if x does not lie in the cycles of A for e.g., then $f(x) = x$.
- $AB = BA$. To show this we only need to consider 3 cases. Whether x lies in the cycles of A, whether x lies in the cycles of B, or neither.

Showing equivalence of 2 cycles Suppose c, d are 2 cycles such that $\exists i, \forall n \in \mathbb{N}, c^n(i) = d^n(i)$, where for a function f, f^n denotes composition n times.

We first write out $c = (i, c(i), \dots, c^{|c|-1}(i))$

Then in particular $\forall n \in \{0, 1 \dots, |c| - 1\}, c^n(i) = d^n(i)$, $d^n(i) = c^n(i)$ and $d^{|c|}(i) = c^{|c|}(i) = i$, which says that $d = (i, c(i), \dots, c^{|c|-1}(i))$. Hence $d = c$.

Notice that the key part of this argument is to show that d loops around, i.e. $d(c^{|c|-1}(i)) = i$.

Decompositions

- $(1, 2, \dots, n) = (1, n)(1, n-1) \dots (1, 3)(1, 2)$
- $(1, 2, \dots, n) = (1, 2)(2, 3) \dots (n-2, n-1)(n-1, n)$

Making transpositions Suppose we have the transpositions $(i, i + 1)$, for each $1 \le i \le n - 1$.
Aim: Make $(1, i), 1 \le i \le n$.
Observe that $(1, 2, \dots, i) = (1, i)(1, i-1) \dots (1, 2) = (1, i) \dots (1, 2, \dots, i-1)$ and that $(1, 2, \dots, i-1)$ has the decomposition $(1, 2)(2, 3) \dots (i-2, i-1)$. Hence we have $(1, i) = (1, 2) \dots (i-1, i)((1, 2)(2, 3) \dots (i-2, i-1))^{-1} = (1, 2) \dots (i-1, i)(i-2, i-1) \dots (1, 2)$.

Suppose we have the transpositions $(1, i), 1 \le i \le n$.
Aim: Make $(i, j), 1 \le i, j \le n, i \ne j$.
Observe that $(1, i, j)$ has 2 decompositions, $(1, j)(1, i)$ and $(1, i)(i, j)$. Hence, $(i, j) = (1, i)^{-1}(1, j)(1, i) = (1, i)(1, j)(1, i)$.

Note that having all transpositions trivially means being able to generate all n-permutations, since every permutation can be decomposed into a product of transpositions.

Conjugating permutations with cycle If $c = (i_1, i_2, \dots, i_k)$ is a cycle in S_n and $f \in S_n$,

$$f \circ c \circ f^{-1} = (f(i_1), f(i_2), \dots, f(i_k))$$

A direct corollary of this is that

$$f^n \circ c \circ f^{-n} = (f^n(i_1), f^n(i_2), \dots, f^n(i_k))$$

where f^n denotes composing f n times.

Two applications, both seen in a previous section.

1. Let $\sigma = (1, 2, 3, \dots, n)$. Then $\sigma^n \circ (1, 2)\sigma^{-n} = (\sigma^n(1), \sigma^n(2)) = (n + 1, n + 2)$. We can view σ^n as a successor function.
2. $(i, n-1)(n-1, n)(i, n-1) = (c(n-1), c(n)) = (i, n)$ where $c = (i, n-1)$. This application of the lemma is not as useful because it is easier to see the transitive equality $(i, n-1)(n-1, n) = (i, n-1, n) = (i, n)(i, n-1)$.

Product groups Given groups G_1, G_2 of finite order, the product group $G_1 \times G_2$ has order $|G_1| \cdot |G_2|$.

Application: Suppose we have natural numbers p, q and we want to quickly find a group of order pq. One example we can consider is then the product group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.