15-251: Great Theoretical Ideas In Computer Science

Recitation 8

Mathematicians in Paris

It turns out there's a pretty strong relationship between the Chinese Remainder Theorem and Lagrange Interpolation. The following restatements will hopefully make it clear the two are, in fact, essentially the same.

The Chinese Remainder Theorem Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers greater than 1, and let $r_1, r_2, \ldots, r_k$ be integers. The system of congruences

$$\begin{aligned} x &\equiv r_1 \bmod m_1 \\ x &\equiv r_2 \bmod m_2 \\ &\vdots \\ x &\equiv r_k \bmod m_k \end{aligned}$$

has a unique solution $\bmod m_1 m_2 \cdots m_k$. In particular, it has a unique solution $0 \leq x < m_1 m_2 \cdots m_k$.

The Lagrange Interpolation Theorem Let $x_1, x_2, \ldots, x_k$ be distinct elements of a field F and let $y_1, y_2, \ldots, y_k \in F$. The system of polynomial congruences

$$\begin{aligned} P(X) &\equiv y_1 \bmod (X - x_1) \\ P(X) &\equiv y_2 \bmod (X - x_2) \\ &\vdots \\ P(X) &\equiv y_k \bmod (X - x_k) \end{aligned}$$

has a unique solution $\bmod (X - x_1)(X - x_2) \cdots (X - x_k)$. In particular, it has a unique solution of degree at most $k - 1$.

(**The Remainder Theorem**, which we proved in lecture, states that the remainder of the division of a polynomial $Q(X)$ by $X - a$ is equal to $Q(a)$. Note that by this theorem, $P(X) \equiv y_i \bmod (X - x_i)$ is exactly equivalent to $P(x_i) = y_i$.)

The Lagrange Interpolation Theorem is usually stated very differently from the above; in lecture, we gave it as

The Lagrange Interpolation Theorem (from Lecture) Let pairs $(a_1, b_1), (a_2, b_2), \ldots, (a_{d+1}, b_{d+1})$ from a field F be given (with all a_is distinct). Then there is exactly one polynomial $P(X)$ of degree at most d with $P(a_i) = b_i$ for all i.

Can you see how the Lagrange Interpolation Theorem as covered in lecture follows from the Chinese Remainder Theorem-esque interpretation introduced above?

Forgot About Groups

$(A, \circ)$ is defined as a **group** when the following four conditions are met:

Closure For all $x, y \in A$, $x \circ y \in A$.

Associativity For all $x, y, z \in A$, $(x \circ y) \circ z = x \circ (y \circ z)$.

Identity There is an $e \in A$ such that for all $x \in A$, $x \circ e = e \circ x = x$.

Inverses For every $x \in A$, there is a $y \in A$ such that $x \circ y = y \circ x = e$.

We define $(A, \circ)$ as **abelian** (commutative) if for every $x, y \in A$, $x \circ y = y \circ x$. **Danger!** Commutativity is not a group axiom. There are plenty of groups that are not commutative.

(a) Is $\mathbb{Z}^+$ equipped with the following function a group? If $a \neq b$ then $f(a, b) = \max(a, b)$. Otherwise, $f(a, b) = 1$.

(b) Given a group G under a binary operation $\circ$, a subset H of G is called a **subgroup** of G if H also forms a group under the operation $\circ$.

Prove that if G is a group and the following hold:

(1) $H \subseteq G$.

(2) H is nonempty.

(3) For all $x, y \in H$, $x \circ y^{-1} \in H$.

then $H \leq G$ (H is a subgroup of G).

(c) Let G be a group with a nontrivial abelian subgroup H (i.e. $H \neq \{1\}$). Is G necessarily abelian?

Morph Money Morph Problems

We define a **homomorphism** from a group $(A, \circ)$ to a group $(B, *)$ as a function $f : A \to B$ such that for every $x, y \in A$, $f(x \circ y) = f(x) * f(y)$. $(A, \circ)$ is homomorphic to $(B, *)$ if and only if there is a homomorphism from $(A, \circ)$ to $(B, *)$.

We define an **isomorphism** as a bijective homomorphism. Two groups are isomorphic if there is an isomorphism between them. Since under isomorphism we can map each element from one group to the other and back while preserving the group operation, the two groups are essentially "the same," just with a different label for each element.

We define an **automorphism** as an isomorphism between a group and itself. Informally, it is a permutation of the group elements such that the group's structure (its multiplication table) remains unchanged.

(a) If f is a homomorphism from a group A to a group B, and e_A is the identity of A, is $f(e_A)$ the identity of B?

(b) If f is a homomorphism from a group A to a group B, and $x \in A$, if $f(x^{-1}) = f(x)^{-1}$?

(c) Is $(\mathbb{Z}, +)$ homomorphic to $(\mathbb{Q}, +)$?

(d) Is $(\mathbb{Z}, +)$ isomorphic to $(\mathbb{Q}, +)$?

(e) Is $(\mathbb{R}, +)$ isomorphic to $(\mathbb{Q}, +)$?

(f) Let A be a group. Let B be the set of automorphisms on A. Does B under functional composition form a group?