Pragmatic Programming

Session 13 - A Strange Thing

Max Nilsson

February 23rd

A Strange Thing

- Let p be a prime and q its *conjugate exponent* in the sense that $p^{-1} + q^{-1} = 1$ (coming from the fact that the dual of L^p is L^q).
- Consider the expression

$$\frac{1}{p}k^p + \frac{1}{q}k$$

  for some integer $k \geq 1$.
- Extensive testing has shown that this expression is always a whole number. Strange!
- The special case $p = 2$ gives the statement

$$\frac{k^2 + k}{2} \in \mathbb{Z},$$

  i.e., the parity of a number k is preserved after squaring it.
- One can simplify and get that

$$\frac{1}{p}k^p + \frac{1}{q}k = \frac{k^p + (p-1)k}{p} \in \mathbb{Z}$$

  is true if and only if $p \mid k^p - k$ which is Fermat's little theorem.

Counting Necklaces

- Let $n, k \geq 1$ be integers. A (n, k)-necklace is intuitively a chain of n beads, with each bead having one of k colors. Rotating a (n, k)-necklace still gives the same necklace.
- Consider **The Necklace Enumeration Problem**: Given n and k, how many (n, k)-necklaces are there?
- Let's consider the special case $(n, k) = (6, 2)$. Then we can list the necklaces

$$000000, 111111$$
$$100000, 011111$$
$$110000, 101000, 100100, 001111, 010111, 011011$$
$$111000, 110100, 110010, 101010$$

  and so in total we have 14 different necklaces.
- But the answer for $(n, k) = (6, 5)$ is 2635.

Group Actions

- Let X be the set of words of length n over an alphabet of size k with size $|X| = k^n$.
- Consider the cyclic group of order n, $G := C_n \cong \mathbb{Z}/n\mathbb{Z}$.
- Since G is abelian we can let G act on X by rotations

  $$G \times X \ni (g, x) \mapsto gx$$

  such that

  $$1x = x, \quad (gh)x = g(hx)$$

  holds for all $g, h \in G$ and $x \in X$.
- Recall the concept of an **orbit** of x

  $$Gx := \{gx \mid g \in G\}.$$

  Note that $x \in Gx$ and if $z \in Gx \cap Gy$ then

  $$z = gx = g'y \implies x = g^{-1}g'y$$

  and $Gx = Gy$. Therefore, the orbits partition X.
- If we divide away G from X, $X/G := \{Gx \mid x \in X\}$, we can formulate the necklace enumeration problem as determining $|X/G|$.

The Orbit-Stabilizer Theorem

- The Orbits $Gx \subset X$ are closely related to the **stabilizer** subgroups of $G_x \subset G$ defined by

$$G_x := \{g \in G \mid gx = x\}.$$

- G_x is trivially closed under inverses ($g^{-1}x = x \iff x = gx$) and multiplication ($g(hx) = gx = x$) and so it is indeed a subgroup of G.
- Now for some fixed $x \in X$ define $f : G \to X$ by $f(g) = gx$. Then by definition $f(G) = G_x$ and $f(g) = f(h)$ if and only if $g^{-1}hx = x \iff gG_x = hG_x$.
- One can easily see that the left cosets of G_x, $G/G_x := \{gG_x \mid g \in G\}$ partition G into equivalence classes of equal amounts of elements. The function f above shows a bijective relationship between the orbit Gx and the left cosets of the stabilizer subgroup G/G_x, which implies that

$$|Gx| = |G/G_x| = |G|/|G_x|.$$

Burnside's Lemma

- We can see that

$$|X/G| = \sum_{Gx \in X/G} 1 = \sum_{Gx \in X/G} \sum_{y \in Gx} \frac{1}{|Gx|}$$
$$= \sum_{x \in X} \frac{1}{|Gx|}$$

- By the Orbit-Stabilizer Theorem we have that

$$|G||X/G| = \sum_{x \in X} |G_x|$$
$$= |\{(g, x) \in G \times X \mid gx = x\}|$$
$$= \sum_{g \in G} |\{x \in X \mid gx = x\}.|$$

- The last expression is defined as **fixed point set** $X^g \subset X$ of some $g \in G$. This is Burnside's Lemma

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

The Answer to Counting Necklaces

- Burnside's Lemma holds in general for any set X, group G with a group action $G \times X \to X$. Let us now instead focus when X is the set of words of length n with alphabet size k and $G = C_n$.
- Since $|G| = n$, all that remains is computing the sizes of the fixed point sets X^g.
- Let $g_m \in C_n$ be associated with $m \in \mathbb{Z}/n\mathbb{Z}$. Since C_n is generated by $g_1 = (1\ 2 \ldots n)$, we have that X^{g_m} must consist of elements which have equal colors on each of its c_m cycles, i.e.,

$$|X^g| = k^{c(g)}.$$

- It follows $c_m = n/k_m$ where k_m is the cycle lengths associated with g_m, that is the smallest positive integer such that

$$c_m m \equiv 0 \bmod n.$$

- In other words, k_m is the smallest positive integer that contains all the prime factors of n except those already appearing in m:

$$k_m = \frac{n}{\gcd(n,m)} \implies c_m = \gcd(n,m) \implies |X/G| = \frac{1}{n}\sum_{k=1}^{n} k^{\gcd(n,k)}$$

Some Special Cases

- When $n = 6$ we get the expression

$$|X/G| = \frac{k + k^2 + k^3 + k^2 + k + k^6}{6}$$

  we get that $k = 2$ gives 14 and $k = 5$ gives 2635.
- In general, suppose we want to answer the necklace problem modulo some large prime P when $n, k \leq \texttt{1e5}$. Then we need to compute the multiplicative inverse n^{-1} in $\mathbb{Z}/P\mathbb{Z}$ in $\mathcal{O}(\log P)$, pre-compute all values k^e modulo P in $\mathcal{O}(n)$ and compute all greatest common divisors in naively $\mathcal{O}(n \log n)$, but can be optimized to $\mathcal{O}(n)$. In total, we can answer the modulo necklace problem in $\mathcal{O}(n)$.
- Note that when $n = p$ is prime, then

$$\frac{1}{p}\sum_{k=1}^{p} k^{\gcd(p,k)} = \frac{1}{p}\left(k^p + \sum_{k=1}^{p-1} k\right) = \frac{k^p + (p-1)k}{p} = \frac{1}{p}k^p + \frac{1}{q}k$$

  which trivially lies in $\mathbb{Z}$. Therefore, we have proved Fermat's little theorem by counting necklaces.

The Last Slide