Number Of Cubes in Finite Field

User 2237 • 3 Jan 2025

https://functor.network/user/2237/entry/787

In this post, I will state the following proposition about finite field and give its proof:

Proposition The number of cubes in the finite field with p elements is $p-1$ if $3 \nmid p-1$, and $\frac{p-1}{2}$ if $3 \mid p-1$.

Proof Let G be the group $\mathbb{F} \setminus \{0\}$. So, $|G| = p-1$. If $3 \nmid |G|$, then there is no subgroup of order 3 by the Lagrange's theorem. So there is no element $a \in G$ such that $a^3 = 1$ other than 1, because otherwise, the powers of a, of which there are 3 distict elements

$$a, a^2, 1$$

in total, forms a cyclic group. This means that for $f\colon G \to G\colon x \mapsto x^3$, the kernel $\ker f$ is $\{1\}$. Since the kernel of f is trivial, f is surjective. Now we have shown that if 3 does not divide $p-1$, then the number of cubes in the group G is $p-1$.

For the case p is divisible by 3, we will use the fact

> $\mathbb{F}_p \setminus \{0\}$ is a cyclic group.

Since 3 divides $p-1$, we can write $p-1 = 3m$ where m is a positive integer. So $G \cong C_{3m}$, to which we have the following claim.

> **Claim.** In a cyclic group of order m, any subgroup H, formed by all elements $x \in G$ such that $x^p = 1$, where $p \mid m$, is of order p. In addition, the set H is exactly
>
> $$\{a^{\frac{km}{p}} \mid k = 0, 1, 2, \ldots, p-1\}.$$

Proof Of Claim We consider the isomoprhism $g\colon a^n \mapsto [n]$ between C_m and $\mathbb{Z}/m\mathbb{Z}$. It suffices to show that $g(H)$, the set of $x \in \mathbb{Z}/m\mathbb{Z}$ such that $[px] = [0]$, is equal to $\{[\frac{km}{p}] \mid k = 0, 1, 2, \ldots, p-1\}$. If $x \equiv \frac{km}{p}$, then

$px \equiv 0 \pmod{m}$. So it is established that
$\left\{ \left[\frac{km}{p}\right] \mid k = 0, 1, 2, \ldots, p-1 \right\} \subset g(H)$. Conversely,
$b \in g(H) \implies pb \equiv 0 \pmod{m} \implies b \equiv 0 \pmod{\frac{m}{p}}$ since $p \mid m$, from which it follows that $[x] = [k\frac{m}{p}]$ for some $k \in \mathbb{Z}$ hence

$$g(H) \subset \left\{ \left[\frac{km}{p}\right] \mid k = 0, 1, 2, \ldots, p-1 \right\}.$$

So $|f(G)| = |\mathbb{F}_p^\times|/|\ker f| = \frac{p-1}{3}$ by the 1st isomorphism theorem and Lagrange's theorem.

Perceivably, this fact generalises to the nth power.