TheNumbersBook.com 2010

Dummit & Foote (3.2) 16, 18, 19, 22

3.2.16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

Let $G = \mathbb{Z}/p\mathbb{Z}^\times$. For any $a \in \mathbb{Z}$, we have $a = np + g$ for some $g \in G$ (where we view elements of G as elements of $\mathbb{Z}$). Now note that:

$$\begin{aligned} a^p &= (np+g)^p \\ &= (np)^p + \binom{p}{1}(np)^{p-1}g + \cdots + \binom{p}{p-1}npg^{p-1} + g^p \\ &\equiv g^p \end{aligned}$$

so it's sufficient to focus on $g \in G$.

First note that if $a \in G$, then $\gcd(a,p) = 1$ for otherwise $a^k \mod p \equiv 0$ (for some $k \in \mathbb{Z}^+$), contradicting the fact that G is a group. Thus, every element is relatively prime to p. Furthermore, $|(\mathbb{Z}/p\mathbb{Z})^\times| = \phi(p) = p - 1$. It is well-known that $g^{|G|} = 1$. Thus, for any $g \in G$

$$g^{p-1} = 1 \Rightarrow g^p = g$$

which equivalently says that $g^p \equiv g \mod p$, as desired. ∎

3.2.18 Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

Let $h \in H$ and $|h| = p$. Now consider the coset of h, that is $hN \in G/N$, and suppose that it has order k. Since the order of any element divides the order of the group, $k||G : N|$. Now note that $(hN)^p = h^pN = 1N = N$ so $k|p$ and so $k||H|$. Since $|H|$ and $|G : N|$ are relatively prime, it must be that $k = 1$. Thus, $(hN)^1 = N$ and so $h \in N$. Thus, $H \leq N$. ∎

3.2.19 Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

Suppose that there is some other normal subgroup H that has order $|N|$ and $(|H|, |G : H|) = 1$. Since $|H| = |N|$, $(|H|, |G : N|) = 1$ and by Exercise 3.2.18, $H \leq N$. Alternatively, since $|N| = |H|$, $(|N|, |G : H|) = 1$ and by Exercise 3.2.18, $N \leq H$. Thus, $H = N$ and so N is the unique subgroup of G of order $|N|$. ∎

3.2.22 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem*: $a^{\varphi(n)} \equiv 1 \mod n$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

Let $G = (\mathbb{Z}/n\mathbb{Z})^\times$. First note that if $a \in G$, then $\gcd(a, n) = 1$ for otherwise $a^k \mod n \equiv 0$ (for some $k \in \mathbb{Z}^+$), contradicting the fact that G is a group. Thus, every element is relatively prime to n. Furthermore, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$. As discussed in 3.2.16, it is sufficient to focus on $g \in G$. Thus, we have $g^{\phi(n)} = 1$ so $g^{\phi(n)} \equiv 1 \mod n$, as desired. $\blacksquare$