Lecture Notes: Abstract Algebra (Course By: Alvaro Lozano-Robledo)

Thobias K. Høivik

March 3, 2025

1 Fermat's Little Theorem

Let $P \leq 2$ be a prime number and let a be an integer relatively prime to p $gcd(a, p) = 1$. Then $p \mid a^{p-1} - 1 \Leftrightarrow (a^{p-1} \equiv 1 \bmod p)$. More generally, if b is any integer, then $p \mid b^p - b \Leftrightarrow b^p \equiv b \bmod p$.

Example

p = 5, $2^4 - 1 = 16 - 1 = 15 = 3 \times 5$. $3^4 - 1 = 80 = 16 \times 5$.
p = 7, $3^6 - 1 = 729 - 1 = 728 = 104 \times 7$.
p = 5, $2^5 - 2 = 2(2^4 - 1) = 2 \times (3 \times 5)$.

Proof without A.A

Let a be an integer, relatively prime to p. Consider the map $\{1, 2, 3, \ldots, p-1\} \rightarrow \{a \times 1, a \times 2, \ldots, a \times (p-1)\}$. If $a \times i \equiv a \times j \bmod p \Rightarrow i \equiv j \bmod p$, $\because$ a is relatively prime to p $\Rightarrow$ a has an inverse modulo p. $1 \leq i \leq j \leq p-1$, but no pair of distinct elements in that set can be congruent to each other since p is prime, hence $i = j$. Then $\{1, 2, 3, \ldots, p-1\}$ and $\{a \times 1, a \times 2, \ldots, a \times (p-1)\}$ are the same modulo p. $1 \times 2 \times 3 \times \cdots \times (p-1) \equiv a(a \times 2) \ldots (a \times (p-1)) \bmod p$. $a(a \times 2) \ldots (a \times (p-1)) \equiv a^{p-1} \times (1 \times 2 \cdots \times (p-1) \bmod p$. $1 \times 2 \times \cdots \times (p-1) = N \Rightarrow N = a^{p-1} \times N \bmod p$. Divide by N on both sides and obtain $1 \equiv a^{p-1} \bmod p$. $\square$

Proof with A.A

Consider $(Z/pZ)^x = U(p)$ those elements in Z/pZ that have multiplicative inverses. Because p is prime $U(p) = \{1, 2, 3, \ldots, p-1 \bmod p\}$ and so $|U(p)| = p-1$. Let $a \in \mathbb{Z}$ relatively prime to p, and suppose $a \equiv i \bmod p$ with $1 \leq i \leq p-1$. Consider $H =< a >= \{1, a, a^2, \ldots, a^{n-1}\}$ where ord(a)=n. By Lagrange's theorem $| < a > | = n = | < i > |$ divides $|U(p)| = p-1$, so $n \mid p-1$ where n is the order of a. If we write $p-1 = nk, k \in \mathbb{Z}$, then $a^{p-1} \equiv i^{p-1} \equiv (i^n)^k \equiv 1^k \equiv 1 \bmod p, a \equiv i \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$. $\square$

2 Euler's Theorem

Let $n \geq 1$, and let a be a number that is relatively prime to n. Then $a^{\phi(n)} \equiv 1 \bmod n$ where $\phi(n) = \#\{1 \leq a \leq n : gcd(a, n) = 1\}$ the number of numbers up to n relatively prime to n.

Proof

Consider $(Z/nZ)^x = U(n) = \{1 \leq a \leq n$: have multiplicative inverses mod n$\}$ $\phi(n) = \#U(n)$. Hence if a is relatively prime to n $\Rightarrow a^{\phi(n)} \equiv 1 \bmod n$ by Lagrange's theorem. $\square$