Math 302 Theorem Set 8: Powers Modulo n

Math 302: Introduction to Proofs via Number Theory

Instructor: Professor Stephanie Treneer, Stephanie.Treneer@wwu.edu

Theorem 8.1. Let p be prime and let a be an integer with $\gcd(a, p) = 1$. Then the numbers a, $2a$, $3a$, ..., $(p-1)a$ are pairwise incongruent modulo p.

Theorem 8.2. Let p be prime and let a be an integer with $\gcd(a, p) = 1$. Then

$$a(2a)(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Theorem 8.3 (Fermat's Little Theorem)**.** Let p be prime and let a be an integer with $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 8.4. Let p be prime and let a be any integer. Then $a^p \equiv a \pmod{p}$.

Definition. If n is a natural number, we define $\phi(n)$ to be the number of integers in the set

$$\{a : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

Theorem 8.5 (Euler's Theorem)**.** ($\star$) Let n be a natural number, and let a be an integer with $\gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Note. Fermat's Little Theorem is actually a special case of Euler's Theorem, since every number $1, 2, 3, \ldots, p-1$ is coprime to p, and hence $\phi(p) = p - 1$ for every prime p. To prove Euler's Theorem, try to mimic the proof of Fermat's Little Theorem. Write down and prove analogues of Theorems 8.1 and 8.2 for a general modulus n, then use them to prove Euler's Theorem.