Modular Arithmetic

Definition. *Modular arithmetic is an arithmetic system using only the integers $0, 1, 2, ..., n-1$. When working in this system, we say that we are working with the integers **modulo** n. The number n is called the **modulus** of the system.*

Definition. *We say that two integers a and b are congruent modulo n is any of the following equivalent conditions hold:*

(i) $a - b$ *is divisible by* n
(ii) $a = b + nk$ *for some* $k \in \mathbb{Z}$
(iii) a *and* b *have the same remainder when divided by* n.

Definition. *Suppose we are working with modulus n. For each integer m there exists a unique integer r such that $0 \leq r < n$ and $m \equiv r \mod n$. We refer to r as modulo-n **residue** of m.*

Definition. *Suppose we are working with modulus n. For each integer r such that $0 \leq r < n$ we refer to the set of all integers which are congruent to $r \mod n$ as a **congruence class**. The set of all integers can be partitioned into n disjoint congruence classes modulo n.*

Theorem. *Let n be an integer greater than 1, and $a, b, c, d \in \mathbb{Z}$.*

(i) If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

(ii) If

$$a \equiv b \mod n,$$
$$c \equiv d \mod n,$$

then

$$a + c \equiv b + d \mod n.$$

(iii) If

$$a \equiv b \mod n,$$
$$c \equiv d \mod n,$$

then

$$ac \equiv bd \mod n.$$

(iv) If $a \equiv b \mod n$ and $m \in \mathbb{N}$, then

$$a^m \equiv b^m \mod n.$$

Remark. *The above properties effectively tell us that when performing modular arithmetic and we are adding, subtracting, or multiplying integers, then we can always reduce numbers down to their residues to make the calculations easier. However, we cannot simply reduce exponents down to their residues. For example, $5 \equiv 0 \mod 5$, but $2^5 \not\equiv 2^0 \mod 5$.*

Theorem (Fermat's Little Theorem). *Suppose $a \in \mathbb{Z}$ and p is prime. Then,*

$$(*) \qquad a^p \equiv a \mod p.$$

Proof. We will prove this by induction on $a \in \mathbb{N}$. From this, the result when a is negative follows immediately. First, it is clear that the result is true when $a = 0$ or $a = 1$. Let us consider the inductive case: Assume that $(*)$ holds for $a = k$. We will show that $(*)$ holds for $a = k + 1$.

$$\begin{aligned}(k+1)^p &= \sum_{i=0}^{p} \binom{p}{i} k^i 1^{p-i} \\ &= \binom{p}{p} k^p + (\text{some numbers that are divisible by } p) + \binom{p}{0} 1^p \\ &\equiv k^p + 1 \mod p \\ &\equiv k + 1 \mod p\end{aligned}$$

The second equality above relies on the fact that

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \mod p$$

when p is a prime and $1 \leq i \leq p - 1$. □

REMARK. *If* $\gcd(a,p)=1$*, then an alternative form of Fermat's Little Theorem is*

$$a^{p-1} \equiv 1 \mod p.$$

Clearly this identity implies $(*)$*. Conversely, if we assume* $(*)$*, then* $a(a^{p-1}-1) = a^p - a = np$ *for some* $n \in \mathbb{Z}$*. Then, since* $\gcd(a,p)=1$*, we have that* $p|(a^{p-1}-1)$*.*