

Equivalence Classes and CRT

1. Prove that $\forall k \geq 1, \exists N \in \mathbf{Z}$ s.t $N \pmod{M = \prod_{i=1}^k p_i}$ satisfies the following by constructing a N such that:
 - (a) $N \equiv -1 \pmod{p_i} \forall i \in [k]$
 - (b) $N \equiv 2^i \pmod{p_i} \forall i \in [k]$

Induction

1. Prove that every integer $n > 1$ can be written uniquely as the product of primes. Prove existence and uniqueness.
2. Let $S = \{6a + 9b + 20c \text{ s.t } a, b, c \in \mathbb{Z}_{\geq 0}\}$. Prove that any integer $n \geq 44$ is in S .

Wilson's Theorem

1. For what n does $(n-1)! \equiv -1 \pmod{n}$ hold? Prove this as an iff relationship.

Fermat's Little Theorem

1. Compute $7^{529} \pmod{23}$
2. Find $37^{-1} \pmod{101}$