Useful Number Theory Facts

- **Modular arithmetic:** Suppose that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then,

$$a + c \equiv b + d \bmod m$$

$$a - c \equiv b - d \bmod m$$

$$ac \equiv bd \bmod m$$

$$a^n \equiv b^n \bmod m \quad \forall n \in \mathbb{N}$$

- **Unique factorization:** (a.k.a. the Fundamental Theorem of Arithmetic) Every integer can be written uniquely as a product of prime numbers, up to changing the order of the prime factors.

- **Chinese remainder theorem:** If m and n are coprime, then the system

$$x \equiv a \bmod m$$

$$x \equiv b \bmod n$$

  has a unique solution mod mn. The same is true for any number of simultaneous congruences, as long as the moduli are pairwise coprime.

- **Bezout's identity:** If m and n are two integers with greatest common divisor (gcd) d there exist integers a and b such that $am + bn = d$. In other words, m has a multiplicative inverse mod n if m and n are coprime and vice versa.

- **Fermat's little theorem:** If p is a prime number and a is not divisible by p then

$$a^{p-1} \equiv 1 \bmod p$$

Warm up

(a) What kinds of remainders do squares have mod 3?
(b) What kinds of remainders do squares have mod 5?
(c) What kinds of remainders do cubes have mod 9?
(d) What is the largest power of 3 that divides $27! = 27 \cdot 26 \cdot 25 \cdots 2 \cdot 1$?
(e) Simplify $2^{100}3^{20}$ mod 10.
(f) Simplify 67^{24} mod 7. (Hint: Use Fermat's Little Theorem to make this go faster)
(g) Simplify 65^{4321} mod 77. (Hint: Use the Chinese Remainder theorem)