Problem set.

(1) Suppose $n$ is a natural number. Prove that every (positive) factor of $n$ is a product of primes from the factorization of $n$. Then, for each value of $n$ below, list the (positive) factors of $n$.
   (a) $n = 10 = 2 \cdot 5$
   (b) $n = 201 = 13 \cdot 17$
   (c) $n = 96 = 2^5 \cdot 3$
   (d) $n = 3969 = 3^4 \cdot 7^2$

Is there a general formula for the number of factors of $n = p_1^{e_1} \cdots p_k^{e_k}$?

(2) Let $a, b,$ and $c$ be integers. Their greatest common divisor $\gcd(a, b, c)$ is the greatest positive integer which is a common factor of all three.
   (a) Prove that the set of integer combinations $\{ma + nb + oc : m, n, o \in \mathbb{Z}\}$ is equal to the set of multiples of $\gcd(a, b, c)$. Hint: Use our theorem about $\gcd(a, b)$ to reduce to the case of two integers, $\gcd(a, b)$ and $c$.
   (b) Prove by counterexample that we could have $\gcd(a, b, c) = 1$ without $a$, $b$, and $c$ being pairwise relatively prime.

(3) Let $a, n$ be positive integers and $d = \gcd(a, n)$. Consider the function

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

$$f(\overline{x}) = \overline{a} \cdot \overline{x}$$

We have already seen that $f$ is a bijection if $d = 1$. In the more general case, describe the image of $f$, and describe the “kernel” of $f$:

$$\ker(f) := \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : f(\overline{x}) = \overline{0}\}$$

(4) Calculate the following without a calculator.
   (a) $46^{100,000} \mod 47$ (Hint: Use FLT.)
   (b) $2^{100,000} \mod 35$ (Hint: Use CRT.)
   (c) $12^{100,000} \mod 689$ (Hint: 689 = 13 · 53. This one is a tour de force.)

(5) Warmup for the RSA algorithm.
   (a) Let $p$ be a prime and let $a$ be any integer. Prove that

   If $k \equiv 1 \mod (p - 1)$ then $a^k \equiv a \mod p$.

   (b) Let $p$ and $q$ be distinct primes and let $a$ be any integer. Prove that

   If $k \equiv 1 \mod (p - 1)(q - 1)$ then $a^k \equiv a \mod pq.$
**Revision.** The revision to the writing assignment from HW10 will be due on Friday, Dec 5th.