JUNE 8TH MODULAR ARITHMETIC PROBLEM SET

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.– Leonhard Euler

1. Consider the following equations. Solve each of them for x (x must be a whole number) or decide there is no solution.

(a) $3x \equiv_5 2$.

(b) $3x \equiv_9 2$.

(c) $2x \equiv_{26} 7$.

(d) $8x \equiv_{12} 4$.

2. Some of the equations above have more than one solution. What are all the possible x that work?

We now recall the idea of the greatest common denominator or GCD. $\gcd(a, b)$ is the largest number ≥ 1 that divides both a and b evenly (without remainder). For instance $\gcd(6, 9) = 3$ and $\gcd(5, 7) = 1$. We say that a and b are *relatively prime* if $\gcd(a, b) = 1$. This just means that a and b have no common factors (besides 1).

3. Suppose that a and n are relatively prime. Consider the sequence of numbers

$$\{a \pmod n, a^2 \pmod n, a^3 \pmod n, a^4 \pmod n, \ldots\}.$$

Show that there must be distinct exponents $i < j$ with $a^i \pmod n = a^j \pmod n$ (in other words, $a^i \equiv_n a^j$).

4. In the context of **3.**, show that $a^{j-i} \equiv_n 1$.

Hint: We know that $a^j \equiv_n a^i$. Thus n divides $(a^{j-i} - 1)a^i$. Use the fact that a and n have no common factors.

5. Explain to your group why this shows that the multiplicative inverse of a mod n can be taken to be a^{j-i-1}.

Hint: Remember, b is called the multiplicative inverse of a if $ab \equiv_n 1$. Also remember the formula that $a^x a^y = a^{x+y}$.