Modular Arithmetic Problems, 2

The following problems concern division $\mod m$. Before giving them a try, it might be useful to remind yourselves about the *greatest common divisor* of two integers.

Given two integers, p and q, we write $\gcd(p, q)$ for the greatest common divisor of p and q. In other words, if $\gcd(p, q) = d$, for any integer, r, that divides both p and q, we must have $r \mid d$. Moreover, if $\gcd(p, q) = d$ we can write

$$p = p'd, \;\; q = q'd,$$

where $\gcd(p', q') = 1$, i.e. are *co-prime*.

Problem 6) If p is a prime number, and q is another integer, show that

$$\gcd(p, q) \begin{cases} p & \text{if } p \mid q \\ 1 & \text{otherwise} \end{cases}$$

Problem 7) If a, b, c, m are integers with m positive, $\gcd(c, m) = d$, and $ac \equiv bc \mod m$, prove

$$a \equiv b \mod \frac{m}{d}.$$

Here's a *really* useful consequence of the previous problem:

If a, b, c, m are integers with m positive, $\gcd(c, m) = 1$, and $ac \equiv bc \mod m$, then

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

Problem 8) Assuming the results of **Problems 6, 7**, what can we say about division $\mod p$, when p is a prime? Concretely: if c is an integer not divisible by p, and a and b are integers such that

$$ac \equiv bc \mod p,$$

what can we say about the relationship between a and $b \mod p$?

Problem 9) If $a \not\equiv 0 \mod p$ how many different residue classes $\mod p$ are represented in the following list:

$$a, 2a, 3a, 4a, \ldots (p-1)a?$$

More generally, working mod m, consider the case where $\gcd(a, m) = 1$.

$$a, 2a, 3a, 4a, \ldots (m-1)a?$$

Problem 10) Remember that if n is a positive integer, we define

$$n! = n \times (n-1) \times \cdots \times 2 \times 1$$

(for what it's worth, we define $0! = 1$). When might $(n-1)! \equiv 0 \mod n$?

Problem 11) Working mod p, what can you say about the relationship, between

$$a \times (2a) \times \cdots \times (p-1)a \text{ and } (p-1)! \text{ ?}$$

(You might find the above "consequence" helpful here).

Problem 12) If you've managed to make it through these exercises, the following result (below) due to Fermat, is (essentially) yours. See if you can fill in the details.

Theorem 0.1 (Fermat's Little Theorem) *Given a prime, p, for any integer, a,*

$$a^p \equiv a \mod p.$$