Last name ______________________

First name ______________________

LARSON—MATH 350—CLASSROOM WORKSHEET 22
Fermat's Theorem

Review

- What does it mean for integer a to *divide* integer b (that is, $a|b$)?
- What is a *prime* number?
- If a, b are integers and $b = aq + r$ (for integers q, r with $0 \leq r < a$), what are q and r called?
- (**Claim:**) Every positive integer can be written as the product of primes.
- (**Claim:**) Every positive integer can be written *uniquely* as the product of primes.
- (**Claim:**) $\sqrt{2}$ is irrational.
- (**Claim:**) There are infinitely many primes.
- (**Claim:**) For every positive integer k, there exist k consecutive composite integers.

New

We will show that, for any prime p, and any positive integer a, that:

$$p|(a^p - a)$$

1. Check that $p|(a^p - a)$ is true for $a = 0$ and any prime p.

2. Check that $p|(a^p - a)$ is true for $a = 1$ and any prime p.

3. Let $a = 2$ and check that $p|(a^p - a)$ is true for $p = 2$.

4. Let $a = 2$ and check that $p|(a^p - a)$ is true for $p = 3$.

5. Let $a = 2$ and check that $p|(a^p - a)$ is true for $p = 5$.

6. Can you explain why $p|(2^p - 2)$ for *any* prime p?

7. (**Claim:**) $p|\binom{p}{k}$ for prime p and any k where $0 < k < p$.

8. Now can you explain why $p|(2^p - 2)$ for *any* prime p?

9. Let's assume that $p|(a^p - a)$ for any prime p and an integer a for $a = 0, \dots, k$. That's our inductive hypothesis. So, what are we assuming exactly?

10. How can we use this to prove $p|(a^p - a)$ for $a = k + 1$?