Worksheet 10: February 26 (Solutions)

1 A Few More Words on Fermat

1. State and prove Fermat's Little Theorem (I really want you to be able to do this!)
   Note: The print version of this worksheet accidentally asked for a proof of Fermat's *Last* Theorem, which I decidedly do *not* expect you to be able to prove – Fermat himself couldn't, and neither could anyone else for 358 years!
   Theorem: If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$.
   Proof: a has a multiplicative inverse modulo p; call it b. Let $S = \{1, 2, 3, \ldots, p-1\}$. Then the function $f : S \to S$ defined by $f(x) = ax \mod p$ is invertible, because its inverse is $f^{-1}(y) = by \mod p$. Thus:

   $$\{1 \bmod p, 2 \bmod p, \ldots, (p-1) \bmod p\} = \{1a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$$

   $$1 \times 2 \times \cdots \times (p-1) \equiv 1a \times 2a \times \cdots \times (p-1)a \mod p$$
   $$1 \times 2 \times \cdots \times (p-1) \equiv a^{p-1}(1 \times 2 \times \cdots \times (p-1)) \mod p$$

   The number on the left is not divisible by p (because p is prime), so it has a modular inverse. Multiply both sides by this inverse to get $1 \equiv a^{p-1} \mod p$.

2. Evaluate the following congruences:

   (a) $7^{1462} \mod 11$
   Solution: $7^{1462} \equiv 7^2 \equiv 49 \equiv 5 \mod 11$

   (b) $19^{603} \mod 7$
   Solution: $19^{603} \equiv 19^3 \equiv 2^3 \equiv 8 \equiv 1 \mod 7$

   (c) $34^{567} \mod 17$
   Solution: 0

2 Induction

3. Prove that for any $n \in \mathbb{Z}^+$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ (the n-th *triangular number*).
   Solution: The base case is $1 = \frac{1(1+1)}{2}$, which holds. If we assume $1 + 2 + \cdots + (n-1) = \frac{(n-1)n}{2}$, then $1 + 2 + \cdots + n = \frac{(n-1)n}{2} + n = \frac{n^2 - n}{2} + \frac{2n}{2} = \frac{n^2 + n}{2} = \frac{n(n+1)}{2}$.

4. Prove that for any $n \in \mathbb{Z}^+$, $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ (the n-th *square pyramidal number*).

   Solution: The base case is $1^2 = \frac{1(1+1)(2+1)}{6}$, which holds. If we assume $1^2 + 2^2 + \cdots + (n-1)^2 = \frac{(n-1)n(2n-1)}{6}$, then $1^2 + 2^2 + \cdots + n^2 = \frac{(n-1)n(2n-1)}{6} + n^2 = \frac{2n^3 - 3n^2 + n}{6} + \frac{6n^2}{6} = \frac{2n^3 + 3n^2 + n}{6} = \frac{n(n+1)(2n+1)}{6}$.

5. Prove that for any $n \in \mathbb{Z}^+$, $\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$

   Solution: The base case is $\frac{1}{2} = 1 - \frac{1}{2^1}$, which holds. If we assume that $\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} = 1 - \frac{1}{2^{n-1}}$, then $\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = \left(1 - \frac{1}{2^{n-1}}\right) + \frac{1}{2^n} = 1 - \frac{2}{2^n} + \frac{1}{2^n} = 1 - \frac{1}{2^n}$.

6. Consider the following inductive "proof" that all horses are the same color.

   > Let $P(n)$ be the statement that all groups of n horses are the same color. Clearly $P(1)$ is true, because if you only have one horse then all the horses you have are the same color. In the inductive step, suppose that $P(n)$ is true. Then if you have $n+1$ horses, the first n are all the same color, and the last n are the same color. The $n-1$ horses shared between these two groups must all be the same color, so the first and last horse must also be the same color, and therefore all $n+1$ horses are the same color. Therefore $P(n) \to P(n+1)$ is true for all n, and since we have the base case $P(1)$, we have that $P(n)$ is true for all n.

   Why is this wrong?

   Solution: The inductive step $P(n) \to P(n+1)$ doesn't work for $n = 1$, because when you only have two horses, there aren't any horses shared between the first one and the last one ($n - 1 = 0$).