Math 42-Number Theory
Problem Set #3
Due Thursday, February 24, 2011

1. List the squares in $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$. How many squares are there in each case? Make a general statement about the number of squares in $\mathbb{Z}_p$ when p is prime.

2. Prove that if $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.

3. Compute $\varphi(1400)$.

4. Give and justify a formula for $\varphi(p^k)$ where p is a prime and k is an natural number.

5. Compute $3^{483} \mod 1400$.

6. Prove that for any a in U_m, $a^{\varphi(m)} \equiv 1 \mod m$.

7. Compute 4! in U_5, 6! in U_7 and 10! in U_{11}. (A suggestion: mod out as you go. That is, if I were trying to compute $12! \mod 13$, instead of saying $12! = 479001600$ and then reducing mod 13, I would say $2 \cdot 3 = 6$, then $6 \cdot 4 = 24 \equiv 11 \mod 13$, then $11 \cdot 5 = 55 \equiv 3 \mod 13$ and so on.) Make a general statement about $(p-1)! \mod p$.

8. In U_p, which elements are their own inverses? Explain why.

9. Prove your statement from problem 7 about $(p-1)! \mod p$. Use problem 8.

10. Using induction, show that for any natural number n, $(1+2+3+\ldots+n)^2 = 1^3+2^3+3^3+\ldots+n^3$.

11. *Extra Credit*: Explain the flaw in the following proof that every bear is the same color.

We'll show that every bear is the same color by showing that when you take any set of bears, every bear in that set is the same color. We proceed by induction on the number of bears in a set. If we only consider sets containing one bear, clearly every bear is the same color as itself, so in a set of one bear, every bear in the set is the same color. That is our base case. For the inductive step, suppose that any set containing up to $n-1$ bears has all bears of the same color. We want to show that any set with n bears in it has all bears of the same color. So take a set of n bears. Removing one bear (call him Yogi), we have a set of $n-1$ bears, and by assumption, all those bears are the same color. But we can remove a different bear (say, Bruno) from the set and put Yogi back in to get a different set of $n-1$ bears, and we see that these bears are all the same color. But since Yogi and Bruno were both the same color as all the other bears in the set, Yogi and Bruno are also the same color as each other, and in fact all n bears are the same color. This proves that in any set of bears, all bears are the same color.