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

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

Solution: If $a \equiv b \mod m$ and $c \equiv d \mod m$, then by definition, $m \mid (b-a)$ and $m \mid (d-c)$. In other words, there are integers k and ℓ such that $b - a = mk$ and $d - c = m\ell$. Then notice that

$$bd - ac = bd - ad + ad - ac = d(b-a) + a(d-c) = mkd + m\ell a.$$

Thus, $m \mid (bd - ac)$, and $ac \equiv bc \mod m$.

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

Solution: Claim: $\varphi(p^k) = p^k - p^{k-1}$.

To prove this claim, consider the numbers 1, 2, 3, $\ldots, p^k$. To compute $\varphi(p^k)$, we need to count the numbers in this set that are relatively prime to p^k. Now, since p is prime, for a number a to be relatively prime to p^k just means that $p \nmid a$. So we need to count the numbers a such that $1 \leq a \leq p^k$ and $p \nmid a$. There are $p^k/p = p^{k-1}$ multiples of p between 1 and p^k (inclusive). Thus, there are $p^k - p^{k-1}$ natural numbers between 1 and p^k (inclusive) that are relatively prime to p^k, and indeed $\varphi(p^k) = p^k - p^{k-1}$.

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

Solution: We follow the proof of Fermat's little theorem from class. Let $u_1, u_2, \ldots u_{\varphi(m)}$ be the elements of U_m, and consider all the multiples of a in U_m: $a \cdot u_1, a \cdot u_2, \ldots a \cdot u_{\varphi(m)}$. Clearly $a \cdot u_i$ is still in U_m since it's a product of elements of U_m, but we will also show that all the multiples of a are different. This will imply that the multiples of a run through all the elements of U_m.

If $a \cdot u_i \equiv a \cdot u_j \mod m$, then $m \mid (a \cdot u_i - a \cdot u_j)$. But since a is in U_m, $(a, m) = 1$ and by the fundamental theorem of arithmetic, we must have $m \mid (u_i - u_j)$. Thus, u_i and u_j must be equivalent mod m, and we see that the multiples of a are all different mod m. Therefore, the multiples of a run through all the elements of U_m.

Therefore, we have $u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)} \equiv a \cdot u_1 \cdot a \cdot u_2 \cdot \ldots \cdot a \cdot u_{\varphi(m)} \mod m$. Rearranging terms, we get

$$u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)} \equiv a^{\varphi(m)} \cdot u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)} \mod m.$$

Because $u_1 \cdot u_2 \cdot \ldots \cdot u_{\varphi(m)}$ is a product of elements of U_m, it must have an inverse mod m. Multiplying both sides of the above equation by this inverse, we get

$$a^{\varphi(m)} \equiv 1 \mod m.$$

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

Solution: In U_p, the only elements that are their own inverses are 1 and -1. This is because for an element to be its own inverse, it must satisfy $x^2 \equiv 1 \mod p$, or in other words, $p \mid (x^2 - 1)$. But if $p \mid (x^2 - 1)$, then $p \mid (x-1)(x+1)$ and because p is prime, $p \mid (x-1)$ or $p \mid (x+1)$. Thus, $x \equiv \pm 1 \mod p$.

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

Solution: We will prove that $(p-1)! \equiv -1 \mod p$. We can think of $(p-1)! \mod p$ as the product of all the elements of U_p. Now, every element a of U_p has an inverse, and either a has an inverse that is different from a or a is its own inverse. We showed in problem 8 that only

1 and -1 are their own inverses, so all other elements of U_p pair up with their inverses. Then, multiplying all the elements of U_p we get a factor of 1 for every pair a, a^{-1} where a and a^{-1} are different, and we have 1 and -1 left unpaired. Thus, $(p-1)! \equiv -1 \mod p$.

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

Solution: Base case: $n = 1$. It is true that $1^2 = 1^3$, so the base case is done.

Inductive step: Suppose the statement is true for $1 \leq k < n$. We'll now show it's true for n. If the statement is true for $1 \leq k < n$, in particular it's true for $n-1$, and we know that

$$(1+2+3+\ldots+(n-1))^2 = 1^3+2^3+3^3+\ldots+(n-1)^3.$$

Now consider $(1+2+3+\ldots+n)^2$. We can think of this as

$$((1+2+3+\ldots+(n-1))+n)^2 = (1+2+3+\ldots+(n-1))^2 + 2n(1+2+3+\ldots+(n-1)) + n^2.$$

Using the inductive hypothesis, we get

$$(1+2+3+\ldots+n)^2 = 1^3+2^3+3^3+\ldots+(n-1)^3 + 2n(1+2+3+\ldots+(n-1)) + n^2.$$

But now $1+2+3+\ldots+(n-1) = \frac{n(n-1)}{2}$, so substituting, we get

$$(1+2+3+\ldots+n)^2 = 1^3+2^3+3^3+\ldots+(n-1)^3 + n^2(n-1) + n^2 = 1^3+2^3+3^3+\ldots+n^3.$$

Therefore, for all $n \in \mathbb{N}$, we have$(1+2+3+\ldots+n)^2 = 1^3+2^3+3^3+\ldots+(n-1)^3+n^2(n-1)+n^2 = 1^3+2^3+3^3+\ldots+n^3$.

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.

Solution: The flaw in this proof is that the inductive step doesn't work when going from 1 to 2. If we are trying to prove that in every set of two bears, both bears are the same color, our proof would have us take one bear (Yogi) out of the set temporarily, leaving a lone bear (Bruno). Then Bruno is the same color as himself. The proof then has us temporarily remove Bruno, leaving just Yogi, who is the same color as himself also. The problem is that there was no bear that both Yogi and Bruno were compared. The proof relies on the fact that there was overlap between the set without Yogi and the set without Bruno, which isn't true when the set has just two bears.