UW Math Circle

April 21, 2016

Homework

1. We saw in class that $3^4 \equiv 1 \pmod 5$, so $3^5 \equiv 3 \pmod 5$. Check yourself that $2^7 \equiv 2 \pmod 7$ and that $3^{11} \equiv 3 \pmod{11}$. (That last one might take a calculator– go check!) At the same time, 3^6 is not equivalent to 3 modulo 6.

   Your task is to show that if p is a prime number, then $a^p \equiv a \pmod p$. Here is an outline:

   (a) First, prove that $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots \binom{p}{p-1}a + 1$. Remember that $\binom{a}{b}$ is the number of ways to choose b things from a things, and that we have a nice formula for it: $\binom{a}{b} = \frac{a!}{b!(a-b)!}$.

   (b) Now use induction to show that $a^p \equiv a \pmod p$. The base case is $a = 1$– and indeed $1^p \equiv 1 \pmod p$. Now, suppose that $a^p \equiv a \pmod p$, and consider $(a+1)^p$, and use the previous problem to write $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots \binom{p}{p-1}a + 1$. Use the fact that p is prime to say that $a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots \binom{p}{p-1}a + 1 \equiv a^p + 1 \pmod p$, and then use your inductive hypothesis.

2. Use the previous problem to show that if p doesn't evenly divide a, then $a^{p-1} \equiv 1 \pmod p$. **Hint**: Remember our criteria from class for when $ax \equiv 1 \pmod n$ has a solution.

3. Use the previous problem to solve the following problems:

   (a) What is $3^{31} \equiv ? \pmod 7$?

   (b) If $N = 2008^2 + 2^{2008}$, what is the units digit of $N^2 + 2^N$? (ie what is $N^2 + 2^N$ modulo 10?)

   (c) What is $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ modulo 7?