Novice Number Theory - Solutions

Andre Kessler

September 29, 2010

1. (1 point) Note that $3^{111890} = 3^{111888+2} = 3^{111 \cdot 1008+2} = 9\left(3^{1008}\right)^{111}$. Since 1009 is prime, by Fermat's Little Theorem we have that $3^{1008} \equiv 1 \pmod{1009}$. Hence $9\left(3^{1008}\right)^{111} \equiv 9 \cdot 1 \equiv \boxed{9} \pmod{1009}$.

2. (1 point) Since 2011 is prime, by Wilson's theorem $2010! \equiv -1 \equiv 2011 - 1 \equiv 2010 \pmod{2011}$. Thus dividing out 2010 from each side we see that $2009! \equiv \boxed{1} \pmod{2011}$.

3. (2 point) Suppose $n+1$ is prime. Then Wilson's theorem says that $n! \equiv -1 \pmod{n+1}$, so $n!+1 \equiv 0 \pmod{n+1}$. Clearly in this case our answer would be $n+1$. Now suppose $n+1$ is composite. If we think for a bit, we realize that $n! \equiv 0 \pmod{n+1}$ for composite n, as the product $n!$ contains two factors of $n+1$. In this case, $n!+1$ is relatively prime to $1, 2, \ldots, n, n+1$, so the gcd with $(n+1)!$ is 1. Thus our answer is: *If $n+1$ is composite, 1; if $n+1$ is prime, $n+1$.*

4. (2 points) From problem 2, we know that $2009! \equiv 1 \pmod{2011}$, so this problem is the same as computing $\dfrac{1}{2009} \pmod{2011}$. To do this, note that $2009 \equiv -2 \pmod{2011}$, so $\boxed{1005} \cdot -2 \equiv -2010 \equiv 1 \pmod{2011}$.

5. (2 points) Because 101 is prime, we know that $9^{100} \equiv 1 \pmod{101}$ by Fermat's Little Theorem. Since $9^{10^{11}} = 9^{100 \cdot 10^9} = \left(9^{100}\right)^{10^9}$, we get our answer to be $\boxed{1} \pmod{101}$.

6. (2 points) What this problem is really asking for is $13^{1022} \pmod{31}$. Because 31 is prime, we know that $13^{30} \equiv 1 \pmod{31}$, and hence $13^{1022} = 13^{30 \cdot 34+2} \equiv 13^2 \equiv \boxed{14} \pmod{31}$.

7. (3 points) Last three digits means we want to look at the number mod 1000. First, we show that $7^{10000} \equiv 1 \pmod{1000}$, as our desired three digits can then be found simply by inverting 7. To simplify the exponent, let's try to find an analog of Fermat's Little Theorem for $\pmod{n}$, where we let n be any integer instead of only primes. Notice we will only be able to cancel numbers from both sides the way we did when n was prime if the number being canceled is relatively prime to n. In addition, a will have to be relatively prime to n (do you see why?). Let $S = \{1, k_0, k_2, \ldots, n-1\}$ be the set of all integers less than and relatively prime to n. We can do something similar to what we did before, namely

$$a \cdot k_0 a \cdot k_1 a \cdots (m-1)a \equiv 1 \cdot k_0 \cdot k_1 \cdots (n-1) \pmod{n}$$

We need a way to count the numbers less than and relatively prime to n. Therefore, we define a function $\varphi(n)$ that returns the desired number. This is known as **Euler's totient function**. Now we can do what we did before and cancel $1 \cdot k_0 \cdot k_1 \cdots (n-1)$ from both sides, yielding

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

This is known as **Euler's generalization** of Fermat's Little Theorem. We find $\varphi(1000) = 1000 - 500 - 200 + 100 = 400$, so $7^{10000} = 7^{400 \cdot 25} = \left(7^{400}\right)^{25} \equiv 1$ as desired. Now we can quickly compute 7^{-1} by noting $7 \cdot \boxed{143} = 1001 \equiv 1 \pmod{1000}$.

8. (3 points) We cleverly rewrite $n^4 - n^2 + 57 \equiv n^4 - 74n^2 + 1225 \equiv (n-5)(n-7)(n+5)(n+7) \pmod{73}$. Thus our solutions are $\boxed{5, 7, 66, 68}$.