Math 126, Number Theory

Quiz Answers

20 Mar 2006

Scale: 8–10 A. 6–7 B. 3–5 C.

Problem 1. [3 points] How many totatives are there modulo 72?

The number of totatives (integers relatively prime to n modulo n) is given by Euler's phi function. So, we need to compute $\phi(72)$. The prime factorization of 72 is $72 = 2^3 3^2$. Since ϕ is a multiplicative function,

$$\phi(72) = \phi(2^3)\,\phi(3^2).$$

These last two values, $\phi(2^3)$ and $\phi(3^2)$, can be computed by formula, since $\phi(p^n) = p^{n-1}(p-1)$, or simply counted since 8 and 9 are small numbers. Then $\phi(72) = 4 \cdot 6 = 24$.

Problem 2. [3 points] According to table 2 in our text, the smallest positive primitive root for the prime 101 is 2. Given that, determine 2^{50} modulo 101. (Do not raise 2 to high powers to answer this question.)

Since 101 is prime, $\phi(101) = 100$, and since 2 is a primitive root modulo 101, the order of 2 is 100. That means that $2^{100} \equiv 1 \pmod{101}$, but no smaller power of 2 is congruent to 1 modulo 101. Hence, the square of 2^{50} is congruent to 1 modulo 101, but 2^{50} itself is not. Note that $(2^50)^2 \equiv 1 \pmod{101}$. Modulo 101, there are exactly 2 values for x such that $x^2 \equiv 1$, namely $x \equiv \pm 1$. Since 2^{50} is not congruent to 1, it must be congruent to -1.

Problem 3. [4; 2 points each part] On orders.

a. Why can't $\mathrm{ord}_{11}(x)$ ever equal 7?

The order of an element in $\mathbf{Z}_n$ must divide $\phi(n)$, and $\phi(11) = 10$, so the only values that $\mathrm{ord}_{11}(x)$ can have are 1, 2, 5, and 10.

b. Compute $\mathrm{ord}_{11}(3)$.

The possible values of $\mathrm{ord}_{11}(3)$ are 1, 2, 5, and 10. It's not 1, since $3 \not\equiv 1 \pmod{11}$. Also, $3^2 = 9 \not\equiv 1 \pmod{11}$, so it's not 2.

Let's find $3^5 \pmod{11}$. Since $3^3 = 27 \equiv 5 \pmod{11}$, therefore

$$3^5 = 3^2 3^3 \equiv 9 \cdot 5 \equiv 45 \equiv 1 \pmod{11}.$$

Therefore, $\mathrm{ord}_{11}(3) = 11$.