MAT 311 Introduction to Number Theory

Problem Set 7

Solutions

Problems 8 and 10 sec 2.8 are easy, just use Thm 2.37 from the book (look at its proof for question 10).

Problem 18 sec 2.8. If p is an odd prime, g and g' primitive roots mod p, show that gg' can't be a primitive root.

Solution. If g and g' are primitive roots, then $g^{p-1} = (g')^{p-1} = 1$ but $g^{(p-1)/2} = (g')^{(p-1)/2} = -1$. It follows that $(gg')^{(p-1)/2} = g^{(p-1)/2}(g')^{(p-1)/2} = 1$, so gg' is not a primitive root.

Problem 20 sec 2.8. Of 101 integers in a complete residue system mod 101^2 that are $\equiv 2 \mod 101$, which one is not a primitive root mod 101^2?

Solution. The problem seems to suggest that 2 is a primitive root mod 101. Let's check this: we need to make sure that 2^d is not congruent to 1 for any $d < 100 = \phi(101)$. But such a d would necessarily be a divisor of 20 or of 50, so we need to check that 2^{20} and 2^{50} are not 1 mod 101. Compute $2^{10} = 1024 \equiv 14 \mod 101$, $2^{20} \equiv 14^2 = 196 \equiv -6 \mod 101$, $2^{50} \equiv (2^{20})^2 2^{10} \equiv 36 \cdot 14 = 504 \equiv -1 \mod 101$.

Now follow the strategy from the proof of Thm 2.39. If $x \equiv 2 \mod 101$, then $x^{100} \equiv 2^{100} \equiv 1 \mod 101$; moreover, for any smaller $d|100$ $x^d \equiv 2^d$ will not be congruent to 1 since 2 is a primitive root. Since 101 is prime, $\phi(101^2) = 100 \cdot 101$, the order of such an x mod 101^2 can only equal to $100 \cdot 101$ (in which case we get a primitive root) or to 100 (in which case we don't). So we are looking for $x \equiv 2 \mod 101$ such that $x^{100} \equiv 1 \mod 101^2$. This means that x lifts the solution $a = 2$ of $x^{100} \equiv 1 \mod 101$ to a solution of $x^{100} \equiv 1 \mod 101^2$. But we know how to lift roots from sec 2.6: write $x = 2 + 101t$, look for t that solves the congruence

$$tf'(a) \equiv -\frac{f(a)}{101} \mod 101,$$

where $f(x) = x^{100} - 1$. So $f'(a) = 100 \cdot 2^{99} \equiv -2^{99} \mod 101$, $f(a) = 2^{100} - 1$, the congruence to solve becomes

$$-2^{99}t \equiv -\frac{2^{100} - 1}{101} \mod 101.$$

Multiplying by -2 and using Fermat's, we get that

$$t \equiv \frac{2^{101} - 2}{101} \mod 101.$$

Then $101t \equiv 2^{101} - 2 \mod 101^2$, and $x = 2 + 101t \equiv 2^{101} \mod 101^2$. Let's stop here: evaluating $2^{101} \mod 101^2$ seems (to me) a formidable task, even with all the numerical techniques. (But if you use a calculator, you get $t = 83$, same as the answer in the book!)

Problem 22 sec 2.8. Let g be a primitive root mod p. Prove that

$$(p-1)! \equiv g \cdot g^2 \dots g^{p-1} \equiv g^{p(p-1)/2} \mod p$$

and get a proof of Wilson's thm from this.

Solution. Both $g, g^2, \ldots g^{p-1}$ and $1, 2, \ldots p-1$ form a reduced system mod p, so the products of all elements in each system must be congruent to each other. This gives the first congruence above; the second is just the summing up the exponents, $1+2+\ldots(p-1) = p(p-1)/2$. For Wilson's thm, note that $g^{(p-1)/2} \equiv -1$ since g is a primitive root; then $(p-1)! \equiv g^{p(p-1)/2} \equiv (-1)^p \equiv -1 \mod p$ if p is an odd prime. (For $p = 2$, check Wilson's directly.)

Problem 37 sec 2.8. Show that n does not divide $2^n - 1$ for $n > 1$.

Solution. Since $2^n - 1$ is odd, the statement is clearly true for n even. Suppose that some n odd divides $2^n - 1$, and let p be the least prime divisor of n. Then we have $(p-1, n) = 1$: if not, we can pick a prime divisor of $(p-1, n)$, and it would be a prime divisor of n that is smaller than p. Now, let d denote the order of 2 modulo p. Then d divides $\phi(p) = p-1$. On the other hand, since n divides $2^n - 1$, and $p|n$, we have that $2^n \equiv 1 \mod p$. This implies that d divides n. But then d divides $(p-1, n) = 1$, so $d = 1$, but $2 \equiv 1 \mod p$ is a contradiction.