MAT 311: Number Theory
Spring 2006

Solutions to HW8

1. (Davenport, pp.219, ex. 3.04) To find primitive roots modulo a (big) prime p we use the fact that the order of any x coprime to p has to be a divisor of $(p-1)$ (since $x^{p-1} \equiv 1 \mod p$). In other words, if x is NOT a primitive root, then there exists a strict positive divisor m of $p-1$ such that $x^m \equiv 1 \mod p$. So, to check whether or not a number x is a primitive root mod p, it suffices to check wether $x^m \equiv 1 \mod p$, when m divides $p-1$. This will dramatically reduce the needed work.
   As an example, take $p = 19$. Then $p-1 = 18 = 2 \cdot 3^2$. Its divisors are 1, 2, 3, 6, 9, 18. For example, let us check whether 10 is a primitive root mod 19. An easy calculation shows $10^2 \equiv 5$, $10^3 \equiv 10 \cdot 5 \equiv 50 \equiv 12$, $10^6 \equiv (10^2)^3 \equiv 5^3 \equiv 11$, $10^9 \equiv 18$. And of course $10^{18} \equiv 1 \mod 19$. So, this shows that the smallest power of x such that 10^m is 1 (mod 19) is 18. Hence $\operatorname{ord}_{19} 10 = 18$, that is, 10 is a primitive root mod 19.
   Let's see what would happen if we took $x = 5$. Then, by the above computation, $5^3 \equiv 11$, and $5^9 \equiv 1 \mod 19$. So 5 cannot be a primitive root mod 19.
   Similarly, you can do the rest of the homework by yourselves. The complete list of primitive roots is:

mod 3 :	2
mod 5 :	$2, 3$
mod 7 :	$3, 5$
mod 11 :	$2, 6, 7, 8$
mod 13 :	$2, 6, 7, 11$
mod 17 :	$3, 5, 6, 7, 10, 11, 12$
mod 19 :	$2, 3, 10, 13, 14, 15$

   Once you have found $\varphi(p-1)$ many primitive roots mod p, you are done, because mod p there are exactly $\varphi(p-1)$ distinct primitive roots.

2. (Davenport, pp.219, ex. 3.05) It is easy to check that $10^8 \equiv 1 \mod 73$ and $2^9 \equiv 1 \mod 73$. We would like to show that $\operatorname{ord}_{73} 20 = 72$. Proceed as in the previous problem. $73 - 1 = 72 = 2^3 \cdot 3^2$. The proper divisors are 1,2,3,4,6,8,9,12,24,36. But for none of them we have $20^m \equiv 1 \mod 73$. To see this, use the above two congruences. For instance, $20^{24} = (2^6)^4 (10^8)^3 \equiv (9)^4 \equiv 37 \mod 73$ etc. The rest is similar.

3. (Davenport, p.219, ex. 3.11) We will show that the product of the primitive roots modulo a prime $p > 3$ is congruent to 1 mod p. Fix a primitive root α mod p. Then the set $\{\alpha, \alpha^2, \dots, \alpha^{p-1}\}$ coincides with the set $\{1, 2, \dots, p-1\}$. In particular, any primitive root is of the form α^m for some m (necessarily coprime to $p-1$, by Lagrange's theorem). On the other hand, observe that if x is a primitive root mod p, so is x^{-1}. So, if α^m is a primitive root, so is $\alpha^{-m} = \alpha^{p-1-m}$. We know that the number of primitive roots mod p is $\varphi(p-1)$. If $p > 3$ then $\varphi(p-1)$ is even (recall prob. 2 in 5th hw). So, if we multiply all primitive roots mod p, then a root of the form α^m will cancel with its inverse α^{-m}; thus, we get 1.

4. (Davenport, p.219, ex. 3.12) Let p be a prime of the form $p = 4k + 1$. Assume that g is a primitive root mod p. We claim that $-g$ (which is congruent to $p - g$) is a primitive root mod p, too. Since g is a primitive root, the set $\{g, g^2, \dots, g^{p-1}\}$ coincides with $\{1, 2, \dots, p-1\}$ mod p. To show $-g$ is a primitive root is equivalent to showing that $\{-g, (-g)^2, \dots, (-g)^{p-1}\}$ coincides with the same set, too. It is clear that $(-g)^{2m} = g^{2m}$. So it suffices to consider odd powers. To show this, first note that (-1) must be *quadratic residue* mod p, that is, (-1) is a square (or in terms of Legendre symbol: $(\frac{-1}{p}) = 1$). Indeed, $g^{p-1} \equiv g^{4k} \equiv 1 \mod p$ by FlT; and so, g^{2k} is congruent to either $+1$ or -1. But it cannot be congruent to $+1$, because that would contradict to g being a primitive root (since $\operatorname{ord}_p g = p - 1 = 4k$).

So $-1 \equiv (g^k)^2 \mod p$, as desired (one could also use Euler's theorem: $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$). So $-g \equiv g^{2k} \cdot g \equiv g^{2k+1} \mod p$. Consequently, odd powers in $\{-g, (-g)^2, \dots, (-g)^{p-1}\}$ coincides with odd powers in $\{g, g^2, \dots, g^{p-1}\}$, as required (the order shifted by $2k$).

5. Consider the polynomial $f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1$. This is a polynomial with integer coefficients, and it is of degree $\leq p-1$. However, modulo p it has p roots which are $0, 1, 2, \dots p-1$ (note that we use Fermat's little theorem). Lagrange's theorem tells us basically in that kind of situation (where the number of roots exceeds the degree) the polynomial must be identically zero mod p. That is, each coefficient of $f(x)$ is 0 mod p, i.e. divisible by p. Observe that the constant term of $f(x)$ is $f(0) = (p-1)! + 1$, which must be $\equiv 0 \mod p$. But this is precisely what Wilson's theorem says.

6. Let q be an odd prime such that $p = 2q+1$ is also a prime. Let a be an integer such that $1 < a < p-1$. We will show that $(-a^2)$ (which is congruent to $p-a^2$) is primitive root mod p. Indeed, this is equivalent to showing that $\text{ord}_p(-a^2) = p-1 = 2q$. If not, then the order is smaller; more precisely, by Lagrange's theorem it is a proper divisor of $p-1 = 2q$. Thus $\text{ord}_p(-a^2)$ is either 1, 2 or q. $\text{ord}_p(-a^2)$ cannot be 1, because otherwise $(-a^2) \equiv -1 \mod p$ implies that $a^2 \equiv 1 \mod p$, and thus $a \equiv \pm 1 \mod p$, which is a contradiction (a was assumed to be $1 < a < p-1$). Second, $\text{ord}_p(-a^2)$ cannot be 2, because otherwise $(-a^2)^2 = a^4 \equiv 1 \mod p$, that is, $p \,|\, a^4 - 1 = (a-1)(a+1)(a^2+1)$. So p divides (at least) one of the factors. But since $a \not\equiv \pm 1 \mod p$, this forces us to conclude that $p \,|\, a^2 + 1$, i.e. $a^2 \equiv -1 \mod p$. But this congruence has no solution since p is of the form $4k+3$ (by Euler's theorem $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^q = -1$). Similarly, $\text{ord}_p(-a^2)$ cannot be q (same idea). So we conclude that $\text{ord}_p(-a^2) = p-1$, as required.

7. We will solve the following congruences using index arithmetic. First note that 5 is a primitive root mod 23 (do a similar calculation as in the first problem)

   (a) $3x^5 \equiv 1 \mod 23$. Take index to the base 5. Then $\text{ind}_5 3 + 5 \,\text{ind}_5 x \equiv \text{ind}_5 1 \equiv 0 \mod 22$. It is a matter of computation to see that $5^{16} \equiv 3 \mod 23$, so $\text{ind}_5 3 = 16$. Also observe that the inverse of 5 mod 22 is 9, since $5 \cdot 9 = 45 \equiv 1 \mod 22$. So $\text{ind}_5 x \equiv (-16) \cdot 9 \equiv 6 \cdot 9 = 54 \equiv 10 \mod 22$. Hence, $x \equiv 5^{10} \equiv 9 \mod 23$. Note that this congruence has a unique solution despite the fact that it is of degree 5.

   (b) $3x^{14} \equiv 2 \mod 23$. Similarly, this implies $\text{ind}_5 3 + 14 \,\text{ind}_5 x \equiv \text{ind}_5 2 \mod 22$. Again, $\text{ind}_5 3 = 16$ and $\text{ind}_5 2 = 2$. So, we have $14 \,\text{ind}_5 x \equiv 2 - 16 \equiv 8 \mod 22$. This implies Since $14 = 2 \cdot 7$, and 7 has an inverse mod 22 (since $(7, 22) = 1$) which is 19, we have $2 \,\text{ind}_5 x \equiv 19 \cdot 8 \equiv 20 \mod 22$. This says that 22 divides $2 \,\text{ind}_5 x - 20$, or equivalently 11 divides $\text{ind}_5 x - 10$. So $\text{ind}_5 x$ is equal to either 10 or 21. Thus x is either $5^{10} \equiv 9$ or $5^{21} \equiv 14$ mod 23. So there are two solutions: 9 and 14.

   (c) $3^x \equiv 2 \mod 23$. This time take index to the base 5. Then, $x \,\text{ind}_5 3 = x \cdot 16$ and $\text{ind}_5 2 = 2$, so $16x \equiv 2 \mod 22$. So 22 divides $16x - 2$, or equivalently, 11 divides $8x - 1$. So $8x \equiv 1 \mod 11$, which implies $x \equiv 8^{-1} \equiv 7 \mod 11$. So $x = 7 + 11k$ for some k. Thus we conclude that $x = 7$ and 18 are the only solutions.

8. Consider the congruence $ax^4 \equiv 2 \mod 13$. We are looking for positive integers a such that his congruence has (at least) a solution x. By the first problem, 2 is a primitive root mod 13. So if we take index to the base 2, we get $\text{ind}_2 a + 4 \,\text{ind}_2 x \equiv \text{ind}_2 2 \equiv 1 \mod 12$. So if we call $\text{ind}_2 a = A$, and $\text{ind}_2 x = X$, we obtain $A + 4X \equiv 1 \mod 12$. So 12 must divide $A - 1 + 4X$. In particular, $A - 1$ must be divisible by 4, that is, A is allowed to be equal to either one of 1, 5, or 9 (it cannot be larger than 12). Thus, $a = 2^A$ is either 2, 6 or 5. Now, let us see in which cases we have solutions. If $a = 2$, then $2x^4 \equiv 2 \mod 13$ has an obvious solution, which is $x = 1$. If $a = 6$, then it is easy to see that $x = 4$ is a solution, and if $a = 5$ then $x = 2$ is a solution. So, the congruence is solvable precisely for $a = 1, 5, 6$.