MAT 311: Number Theory
Spring 2006

Solutions to HW9

1. (Davenport, pp.219, ex. 3.14) Let p be a prime, and assume that g is a primitive root mod p^2. In this case, g is a primitive root mod p: Suppose not, i.e. g is not a primitive root mod p. Then there is some n with $1 \leq n < p-1$ such that $g^n \equiv 1 \mod p$. By Lagrange's theorem n must be a (proper) divisor of $p-1$, i.e. $n \,|\, p-1$. But then, $g^{np} \equiv 1 \mod p^2$ (write $g^n = 1 + kp$, and take the p'th power, then all terms except the constant term 1 have at least a p^2 factor). But this is a contradiction to the assumption that $\operatorname{ord}_{p^2} g = \varphi(p^2) = p(p-1)$, since a smaller power (namely np) makes g congruent mod p^2.
   The converse is not true: 7 is a primitive root mod 5, but it is NOT a primitive root mod $5^2 = 25$ as $\operatorname{ord}_{25} 7 = 4$.
2. (Davenport, p.219, ex. 3.15) Assume that p and $4p+1$ are both primes. Observe that p cannot be equal to 2. We will show that 2 must be a primitive root mod $4p+1$. By Fermat, $2^{4p} \equiv 1 \mod 4p+1$ and $2^p \equiv 2 \mod p$. By Lagrange's theorem, it suffices to check that $2^m \not\equiv 1 \mod 4p+1$ for $m = 2, 4, p, 2p$ (proper divisors of $4p$). The cases for $m = 2$ and $m = 4$ are trivial to check. Now, since $\left(\frac{2}{4p+1}\right) = (-1)^{\frac{(4p+1)^2-1}{8}} = -1$, 2 is a quadratic nonresidue mod p. Thus we cannot have the congruence $2^p \equiv 1 \mod 4p+1$, because multiplying both sides by 2 yields $2^{p+1} \equiv 2 \mod 4p+1$ which would imply that 2 is a quadratic residue since $p+1$ is even. A contradiction. Similarly, $2^{2p} \not\equiv 1 \mod 4p+1$.
3. (Davenport, p.219, ex. 3.18) Constructing the table of indices for 41 is straightforward. Observe that the difference of indices for a and $-a$ is always 20. To see this: let $A := \operatorname{ind}_6 a$ and $B := \operatorname{ind}_6(-a)$. Then $a \equiv 6^A$ and $-a \equiv 6^B \mod 41$. Thus, $6^{A-B} \equiv -1 \mod 41$. Taking ind_6 and noting that $6^{20} \equiv -1 \mod 41$ (since 6 is a primitive root) we obtain the result.
4. (Davenport, p.219, ex. 3.19) Note that quadratic residues mod 8 are 0,1 and 4; and the 4th-power (quartic) residues are 0 and 1.
5. Recall the following useful fact: if a is a primitive root modulo a prime p, then either a or $a+p$ is a primitive root mod p^2. So, to find a root mod 17^2, first one needs to find a primitive root mod 17. It is easy to show that 3 works. Since $\operatorname{ord}_{p^2} x$ is either $p-1$ or $p(p-1)$ for any primitive root x (recall the proof of the above mentioned fact), this implies that $\operatorname{ord}_{17^2} 3$ is either 16 or 272. Using a pocket calculator it is easy to see that $3^{16} \neq 17 \mod 17^2$, thus, 3 is a primitive root mod 17^2.
6. As an application of Lucas' converse of Fermat's little theorem, let us show that 101 is a prime. So our n is going to be 101, and hence $n - 1 = 100 = 2^2 \cdot 5^2$. To show that 101 is a prime, we need to find an x such that $x^100 \equiv 1 \mod 101$ but $x^d \not\equiv 1 \mod 101$ for any prime divisor d of 100. Indeed, $x = 2$ works, i.e. none of 2^d where $d = 2, 5$, is congruent to 1, however $2^100 \equiv 1 \mod 101$ (this is a tedious but straightforward calculation). This shows that 101 is a prime number.
7. Assume that there exists an integer x such that $x^{2^{2^n}} \equiv 1 \mod F_n$ and $x^{2^{2^n-1}} \not\equiv 1 \mod F_n$ where $F_n = 2^{2^n} + 1$ is the n-th Fermat number. We claim that in this case F_n is actually prime. Indeed, the first condition tells us that $x^{F_n - 1} \equiv 1 \mod F_n$. But the only prime number dividing $F_n - 1 = 2^{2^n}$ is 2, and $(F_n - 1)/2 = 2^{2^n - 1}$, so the second condition tells us that $x^{(F_n-1)/2} \not\equiv 1 \mod F_n$. Then by Lucas' converse of Fermat's little theorem, we deduce that F_n must be prime.
8. Let n be a positive integer possessing a primitive root, say a. Observe that $\{a, a^2, \ldots, a^{\varphi(n)-1}, a^{\varphi(n)} \equiv 1\}$ coincides with the subset of numbers from 1 to $n-1$ which have an inverse $\mod n$. We know that these are all such integers relatively prime to n. Their product is $\prod_{j=1}^{\varphi(n)} a^j = a^{\sum_{j=1}^{\varphi(n)} j} =$

$a^{\varphi(n)(\varphi(n)+1)/2} = (a^{\varphi(n)/2})^{\varphi(n)+1} \equiv (-1)^{\varphi(n)+1} \equiv -1 \mod n$, as required. Notice that $\varphi(n)/2$ makes sense because $\varphi(n)$ is even (see HW5, Prob. 2) which also implies that the exponent $\varphi(n)+1$ is odd; and also we have $a^{\varphi(n)} \equiv 1$ and $a^{\varphi(n)/2} \equiv -1$ since a is a primitive root mod n.

9. We will compute the minimal universal exponent of 884, i.e. $\lambda(884)$. In general, if $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_m^{\alpha_m}$, then $\lambda(n) = [\lambda(2^{\alpha_0}), \varphi(p_1^{\alpha_1}), \dots, \varphi(p_m^{\alpha_m})]$ where $\lambda(2^{\alpha_0}) = 2^{\alpha_0 - 2}$ if $\alpha_0 \geq 2$ and 1 otherwise. Observe that $884 = 2^2 \cdot 13 \cdot 17$. So $\lambda(2^2) = 1$, $\varphi(13) = 12$, $\varphi(17) = 16$. Their LCM is 48.

10. We will find all positive integers n with $\lambda(n) = 2$. Notation as above: if LCM is 2, then each of $\lambda(2^{\alpha_0}), \varphi(p_1^{\alpha_1}), \dots, \varphi(p_m^{\alpha_m})$ is either 1 or 2, and there is at least one equal to 2. First observe that $\varphi(p^\alpha) \geq 2$ for any odd prime p and $\alpha \geq 1$ (because 1 and 2 are coprime to p^α), and $\varphi(p^\alpha) = 2$ only if $p = 3$ and $\alpha = 1$. Now assume that $\lambda(n) = 2$. Then α_0 is either 0,1,2 or 3. If n is divisible by an odd prime, then the only prime that divides n must be 3 (otherwise the LCM is going to be ≥ 2). So the possibilities are $2^0 \cdot 3 = 3$, $2^1 \cdot 3 = 6$, $2^2 \cdot 3 = 12$ and $2^3 \cdot 3 = 24$. If not, i.e if n is not divisible by an odd prime, then n is a power of 2, and consequently $2^3 = 8$.