MATH 3070
Assignment # 5 Solutions
Due Thursday, October 30, 2008

1. (a) We first try if 2 is a primitive root mod 23. We calculate

k	1	2	3	4	5	6	7	8	9	10	11
$2^k \pmod{23}$	2	4	8	-7	9	-5	-10	3	6	-11	1

so 2 is not a primitive root, nor is any number in the above table. So we skip ahead to try 5 and find that $5^2 \equiv 2 \pmod{23}$ so 5 must be a primitive root (as the order of 2 is 11 which is $\varphi(23)/2$, so its square root must have order 22). Indeed, we find that

k	1	2	3	4	5	6	7	8	9	10	11
$5^k \pmod{23}$	5	2	10	4	-3	8	-6	-7	11	9	-1
k	12	13	14	15	16	17	18	19	20	21	22
$5^k \pmod{23}$	-5	-2	-10	-4	3	-8	6	7	-11	-9	1

The indices that are coprime to $\varphi(23) = 22$ are the ones that generate the primitive roots. So the set of primitive roots mod 23 is $\{5, 10, -3, -6, 11, -2, -4, -8, 7, -9\}$, or equivalently $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$.

(b) Since 5 does not divide $\varphi(23) = 22$ there are no elements of order 5. To obtain the elements of order 11 we square the primitive roots and find that the list becomes $\{2, 4, 8, -7, 9, -10, 3, 6\}$. (A shortcut, of course, is to look at the table for powers of $2 \equiv 5^2$ with the powers coprime to 22. Noting that 11 is odd, we find that the numbers we skipped over in the first half of the list gets counted in the second half of the list, so the set is the entire list from $k = 1$ to 10 in the first table.) The only elements not counted are 1 and -1, and only -1 has order 2.

2. (a) Let $d = \gcd(k, \ell)$, and set $x = \mathrm{ord}_{mn}(a)$. Since $a^x \equiv 1 \pmod{mn}$, we must have $a^x \equiv 1 \pmod{m}$ and $a^x \equiv 1 \pmod{n}$. Therefore $k \mid x$ and $\ell \mid x$. Thus x is a common multiple of k and ℓ and so $\mathrm{lcm}(k, \ell) \mid x$.

Conversely, $a^{\mathrm{lcm}(k,\ell)} = (a^k)^{\ell/d} = (a^\ell)^{k/d}$. The first is clearly $1 \pmod{m}$ and the second is clearly $1 \pmod{n}$. So if $(m, n) = 1$ then by the Chinese Remainder Theorem we have $a^{\mathrm{lcm}(k,\ell)} \equiv 1 \pmod{mn}$. Therefore $x \mid \mathrm{lcm}(k, \ell)$. Since both of these numbers are positive, we may conclude they are equal.

(b) We know that $k \leq \varphi(m)$ and $\ell \leq \varphi(n)$. If we want a to be a primitive root, we must have $\mathrm{ord}_{mn}(a) = \varphi(mn) = \varphi(m)\varphi(n) = k\ell/d$. Thus we must have $k = \varphi(m)$ and $\ell = \varphi(n)$ and $d = 1$. But we know for any $x > 2$, $\varphi(x)$ is even. So the only way $d = 1$ is if one of m or n is 2.

(c) Let $x = \mathrm{ord}_{p^{k+1}}(a)$. Then $a^x \equiv 1 \pmod{p^{k+1}}$. Therefore $a^x \equiv 1 \pmod{p^k}$.
So $\varphi(p^k) = \mathrm{ord}_{p^k}(a) \mid x$.

(d) By part (c), we know that $\operatorname{ord}_{p^2}(a)$ is a multiple of $\varphi(p) = p-1$. Thus $(p-1)\operatorname{ord}_{p^2}(a^{p-1}) = \operatorname{ord}_{p^2}(a)$. Now, we know $\operatorname{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1)$. Cancelling the $p-1$ on both sides yields $\operatorname{ord}_{p^2}(a^{p-1}) \mid p$. So either $\operatorname{ord}_{p^2}(a^{p-1}) = 1$ or it is p, in which case $\operatorname{ord}_{p^2}(a) = p(p-1)$ and a is a primitive root mod p^2.

(e) If $a^{p-1} \equiv 1 \pmod{p^2}$,
then $(a+p)^{p-1} = a^{p-1} + a^{p-2}p(p-1) + \text{higher powers of } p \equiv a^{p-1} - a^{p-2}p \pmod{p^2}$.
Now, since $(a,p) = 1$, $a^{p-2} \not\equiv 0 \pmod{p}$ and so $a^{p-2}p \not\equiv 0 \pmod{p^2}$.
Therefore, $(a+p)^{p-1} \equiv 1 - a^{p-2}p \not\equiv 1 \pmod{p^2}$. But $a+p$ is a primitive root mod p since a is. So by part (d), $a+p$ must be a primitive root $\pmod{p^2}$.

(f) We induct on k, the base case being $k = 2$, which is trivial. Now suppose for fixed $k > 2$, if a is a primitive root mod p^2 then a is a primitive root mod p^ℓ for all $2 \leq \ell < k$. We want to show that a is a primitive root mod p^k.

Using part (c), we know that $\operatorname{ord}_{p^k}(a)$ is a multiple of $\varphi(p^{k-1}) = p^{k-2}(p-1)$. Following the same argument as part (d), we find that either $a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$ or a is a primitive root mod p^k. We show that the first case is impossible.

Suppose not. Then $a^{p^{k-2}(p-1)} - 1 \equiv 0 \pmod{p^k}$. Factor the left side to find that

$$(a^{p^{k-3}(p-1)} - 1)(a^{p^{k-3}(p-1)(p-1)} + a^{p^{k-3}(p-1)(p-2)} + \cdots + a^{p^{k-3}(p-1)} + 1) \equiv 0 \pmod{p^k}.$$

But a is a primitive root mod p^{k-1}, so $a^{p^{k-3}(p-1)} \not\equiv 1 \pmod{p^{k-1}}$, so there can be at most $k-2$ factors of p in the first factor, and thus there must be at least 2 factors of p in the second. That is,

$$a^{p^{k-3}(p-1)(p-1)} + \cdots + a^{p^{k-3}(p-1)} + 1 \equiv 0 \pmod{p^2}.$$

Now, each of the $a^{p^{k-3}(p-1)i} \equiv 1 \pmod{p^{k-2}}$. Denote the above sum by S. We need to break this up into two cases. If $k \geq 4$, then we may replace each of the $a^{p^{k-3}(p-1)i}$ by $1 + c_i p^2$, since it is congruent to 1 mod p^{k-2}, with $k-2 \geq 2$. Therefore, $S = (1 + c_{p-1}p^2) + \cdots + (1 + c_1 p^2) + 1 \equiv p \pmod{p^2} \not\equiv 0 \pmod{p^2}$, a contradiction.

If $k = 3$, then $S = 1 + a^{p-1} + \cdots + (a^{p-1})^{p-1}$. But a is a primitive root $\pmod{p^2}$ so $a^{(p-1)i} \not\equiv 1 \pmod{p^2}$ for any $1 \leq i < p$. But by Fermat's little Theorem it is congruent to 1 mod p. So we may write $a^{(p-1)i} = 1 + c_i p$ where $(c_i, p) = 1$. But as a is a primitive root $\pmod{p^2}$, we know the $a^{(p-1)i}$ are pairwise incongruent mod p^2, and thus the c_i are incongruent mod p. Since we have $p-1$ of them, they are all the non-zero residue classes mod p and so $c_1 + \cdots + c_{p-1} \equiv 1 + 2 + \cdots + (p-1) \pmod{p} \equiv 0 \pmod{p}$ if p is odd. Therefore, $S = p + p(c_1 + c_2 + \cdots + c_{p-1}) \equiv p \pmod{p^2}$, again a contradiction.

(Note that this fails in the case where $p = 2$ and $k = 3$, as the sum of the c_i is odd, which avoids the contradiction.)

(g) By parts (c)–(f), for every odd prime p and every positive integer k we can find a primitive root a mod p^k. Now, 1 is a primitive root mod 2. So if a is odd, then by part (a) we have $\operatorname{ord}_{2p^k}(a) = \operatorname{ord}_2(a)\operatorname{ord}_{p^k}(a) = 1 \cdot \varphi(p^k) = \varphi(2p^k)$. If a is even, then $a + p^k$ is odd and is also a primitive root mod p^k. So by the same argument $a + p^k$ is a primitive root mod $2p^k$.

3. (a) Using indices base 5 and the table we calculated above, we find that

$$I(4x^4) = I(4) + 4I(x) \equiv 4 + 4I(x) \equiv I(9) \equiv 10 \pmod{22}.$$

We easily find that $4I(x) \equiv 6 \pmod{22}$ so $2I(x) \equiv 3 \pmod{11}$, and $I(x) \equiv 7 \pmod{11}$. Thus $x \equiv 5^7, 5^{18} \pmod{23}$, so $x \equiv -6, -10 \pmod{23}$.

(b) Since $76 = 4 \cdot 19$, we apply the Chinese Remainder Theorem and solve the system

$$\begin{aligned} x^{10} &\equiv 1 \pmod{4} \\ x^{10} &\equiv 7 \pmod{19} \end{aligned}$$

We can solve the first by inspection, $x \equiv \pm 1 \pmod{4}$ (or equivalently x is odd, so $x \equiv 1 \pmod{2}$).

To solve the second, We use indices base 2 (so we can be lazy and use the table constructed in class) to find that

$$10I(x) \equiv I(7) \equiv 6 \pmod{18}.$$

Thus $5I(x) \equiv 3 \pmod{9}$, so that $I(x) \equiv 6 \pmod{9}$. This yields $x \equiv 2^6, 2^{15} \pmod{19} \equiv 7, 12 \pmod{19}$. Combining these solutions with the mod 4 solution, we find that the solutions are $x \equiv 7, 31 \pmod{38}$, or equivalently $x \equiv 7, 31, 45, 69 \pmod{76}$.