

104B Problem Set 1

Rino Sanchez

January 23, 2003

7.1, # 3, 5a, 11, 12

3. For which of the following integers m is there a primitive root modulo m ?

- (a) $m = 54$: The main tool to answer this question (at least for this section) is Proposition 7.1.4, which tells us that for most m there are no primitive roots modulo m , depending on the prime factorization of m . In section 7.2 we find out that for the remaining m (i.e. those m not considered in 7.1.4) we know there exist primitive roots modulo m , but it doesn't help for the problems from section 7.1.

Since $54 = 2 \cdot 3^3$, 7.1.4. doesn't really help us, but we know from reading ahead that there is a primitive root modulo 54. Section 7.3 will give us excellent ways of finding one, but we should be able to figure out using only results from 7.1. Only real way left available to us then is to actually find a primitive root.

We know from Corollary 4.2.4 that $\phi(54) = 3^2(3-1) = 18$. Let's pick a number relatively prime to 54, like 5, which is the smallest one bigger than 1. We know from Corollary 7.1.5 that $\text{ord}_{54}(5)$ divides $18 = \phi(54)$, so we just need to eliminate all the other divisors of 18. Now we compute $5^1, 5^2, 5^3, 5^6, 5^9$ modulo 54:

$$\begin{aligned}5^2 &\equiv 25 \pmod{54} \\5^3 &\equiv 125 \equiv 17 \pmod{54} \\5^6 &\equiv (17)^2 \equiv 289 \equiv 19 \pmod{54} \\5^9 &\equiv 5^3 \cdot 5^6 \equiv 17 \cdot (17+2) \equiv 17^2 + 2 \cdot 17 \equiv 19 + 34 \equiv 53 \pmod{54}\end{aligned}$$

Since none of these are congruent to 1 modulo 54, we know that 5 must be a primitive root. In fact, we only had to check 5^6 and 5^9 (why is that?).

- (b) $m = 686$: Since $686 = 2 \cdot 7^3$, we know there exists a primitive root modulo 686. Let us check to see if 3 is a primitive root. Since $\phi(686) = 294$, we need only check the following powers of 3: $294/7=42$, $294/3=98$,

$294/2=147$ (for the same reasons I alluded to in part a. This is Proposition 7.2.14 in disguise since the case we're using is modulo a nonprime, but the proof still holds if slightly modified).

The easiest way is using the binary expansion of these powers and repeated squaring. Let's calculate 3^{42} modulo 686 this way. We first write 42 as a sum of powers of 2, as in $42 = 32 + 8 + 2$. Then we successively square $3 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 9^2 \equiv 81$, $3^8 \equiv (81)^2 \equiv 299$, $3^{16} \equiv (299)^2 \equiv 221$, and finally $3^{32} \equiv (221)^2 \equiv 135$, so $3^{42} \equiv 3^{32} \cdot 3^8 \cdot 3^2 \equiv 135 \cdot 299 \cdot 9 \equiv 391 \not\equiv 1 \pmod{686}$. Similarly, $3^{98} \equiv 19 \pmod{686}$ and $3^{147} \equiv -1 \pmod{686}$. Hence 3 is a primitive root modulo 686.

- (c) $m = 100$: Since $100 = 2^2 \cdot 5^2$, we know by 7.1.4 that there is no primitive root modulo 100.
- (d) $m = 752$: Since $752 = 2^4 \cdot 47$, we again know by 7.1.4 that there is no primitive root modulo 752.

5. Determine a primitive root modulo 19, and use it to find all the primitive roots.

Let's check to see if 2 is a primitive root. Since $\phi(19) = 18$, we can check that 2 is a primitive root by computing the following powers of 2 modulo 19: $18/2 = 9$ and $18/3 = 6$.

$$\begin{aligned} 2^6 &\equiv 2^4 \cdot 2^2 \equiv 16 \cdot 4 \equiv -3 \cdot 4 \equiv -12 \equiv 7 \pmod{19} \\ 2^9 &\equiv 2^6 \cdot 2^3 \equiv 7 \cdot 8 \equiv 56 \equiv -1 \pmod{19} \end{aligned}$$

To find the other primitive roots, we make use of Lemma 7.1.8 which says that if $(a, n) = 1$ then $\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{(k, \text{ord}_n(a))}$. In this case we have $a = 2$. Since a is a primitive root, the powers of a (along with 0) form a complete residue system modulo 19, so all the other primitive roots modulo 19 are of the form a^k . By Lemma 7.1.8, a^k is a primitive root modulo 19 if and only if $(k, \text{ord}_{19}(a)) = 1$. Since $\phi(19) = 18$, we have exactly $\phi(18) = 6$ values of k where $(k, \text{ord}_{19}(a)) = 1$, namely 1, 5, 7, 11, 13, and 17. Taking these powers of 2 modulo 19, we find that 2, -6, -5, -4, 3, and -9 are all the primitive roots modulo 19.

11. Suppose $\text{ord}_m(a) = k$ and $\text{ord}_n(a) = l$. If $(m, n) = 1$, show that the order of a modulo mn is $[k, l]$, the least common multiple of k and l .

By definition $a^k \equiv 1 \pmod{m}$ and $a^l \equiv 1 \pmod{n}$, and also by definition, k and l divide $[k, l]$. Therefore, we have $a^{[k, l]} \equiv 1 \pmod{m}$ and $a^{[k, l]} \equiv 1 \pmod{n}$. Because $(m, n) = 1$ we know that $a^{[k, l]} \equiv 1 \pmod{mn}$, and by Corollary 7.1.5 it follows that $\text{ord}_{mn}(a)$ divides $[k, l]$.

Suppose $a^j \equiv 1 \pmod{mn}$. Then clearly $a^j \equiv 1 \pmod{m}$ and $a^j \equiv 1 \pmod{n}$, so by Proposition 7.1.3, we know that $k = \text{ord}_m(a)$ and $l = \text{ord}_n(a)$ both divide j . Hence by definition, $[k, l]$ divides j . This completes the proof that $\text{ord}_{mn}(a) = [k, l]$.

12. (a) Suppose a has order k and b order l modulo n with $(k, l) = 1$. Show that $\text{ord}_n(ab) = kl$.

(b) Investigate what happens if $(k, l) \neq 1$. What can you say about $\text{ord}_n(ab)$?

(a) It is clear that $(ab)^{kl} = (a^k)^l (b^l)^k \equiv 1 \cdot 1 \equiv 1 \pmod{n}$, so $\text{ord}_n(ab)$ divides kl . Now suppose that $(ab)^j \equiv a^j b^j \equiv 1 \pmod{n}$. Then b^j is the inverse of a^j modulo n . It is also clear that $xy \equiv 1 \pmod{n}$ implies that $\text{ord}_n(x) = \text{ord}_n(y)$ ($x^n \equiv 1 \pmod{n}$ if and only if $y^n \equiv 1 \pmod{n}$). Therefore, $\text{ord}_n(b^j) = \text{ord}_n(a^j)$. Using Lemma 7.1.8 we attain the following formula: $\frac{k}{(j, k)} = \text{ord}_n(a) = \text{ord}_n(b) = \frac{l}{(j, l)}$, which is equivalent to

$$k \cdot (j, l) = l \cdot (j, k)$$

Now, l divides the left hand side, but $(k, l) = 1$, so l must divide (j, l) , which means that l must divide j . If we play this game with the right hand side, we get that k must also divide j . Again, since $(k, l) = 1$, kl must divide j , completing the proof.

(b) The first half of our proof of (a) did not assume $(k, l) = 1$, so it is always true that $\text{ord}_n(ab)$ divides kl . Basically, for any divisor d of (k, l) , we can find examples of a and b where $\text{ord}_n(ab) = kl/d$.

7.2, # 1bd, 6, 10, 11a

1. Determine the primitive roots modulo the following integers.

(b) 27: The best way to construct primitive roots is to use Theorem 7.2.10. Since $27 = 3^3$, we first find a primitive root modulo 3, namely $g = 2$. Part (a) of the theorem says either 2 or 5 is a primitive root modulo 9. Since $\phi(9) = 6$, we only check that 2^2 and 2^3 are not congruent to 1 (mod 9) (5 is also a primitive, but we only need one). Part (b) of the theorem says that 2 is also a primitive root modulo 27. For the rest of the primitive roots, we find integers relatively prime to $\phi(27) = 18$, namely 1, 5, 7, 11, 13, and 17. Taking these powers of 2, we find that 2, 5, -7, -4, 11, and 14 are primitive roots modulo 27.

- (d) 98: Since $98 = 2 \cdot 7^2$, we first find a primitive root modulo 7, like 3. Then either 3 or 10 is a primitive root modulo 49. Since $\phi(49) = 42$, to see that 3 is a primitive root modulo 49, we need only compute the following powers of 3: $42/7 = 6$, $42/3 = 14$, and $42/2 = 21$. One can readily check that $3^6 \equiv -6 \pmod{49}$, $3^{14} \equiv -19 \pmod{49}$, and $3^{21} \equiv -1 \pmod{49}$. Now by part (b) of the theorem, we know that 3 is a primitive root modulo 7^k for any $k \geq 1$. Then part (c) tells us that 3 is a primitive root modulo $2p^k$ for $k \geq 1$, so in particular, 3 is a primitive root modulo 98. To find the other primitive roots, we take 3^k where k is relatively prime to $\phi(\phi(49)) = \phi(42) = 12$ (like 1, 5, 7, and 11), and this gives us 3, 47, 31, and 37 as primitive roots modulo 98.

6. Suppose that $p \nmid a$. Show that the equation $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Suppose that z is a solution to $x^2 \equiv a \pmod{p}$. Then

$$a^{(p-1)/2} \equiv (z^2)^{(p-1)/2} \equiv z^{p-1} \equiv 1 \pmod{p}$$

The last step follows because of Fermat's Little Theorem (here we use $p \nmid a$).

Now suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. It is clear that p is meant to be an odd prime (otherwise $(p-1)/2$ is not an integer - besides, p stands for odd prime), so there exists a primitive root modulo p , so let's call it ξ . We know $\xi^j \equiv a \pmod{p}$ for some integer $1 \leq j \leq p-1$, so by our assumption, $\xi^{j(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$. As $\text{ord}_p(\xi) = p-1$, we know $p-1$ divides $j(p-1)/2$, and this means that j must be even, so say $j = 2k$. We take $z = \xi^k$ and we have $z^2 \equiv \xi^{2k} \equiv \xi^j \equiv a \pmod{p}$, so we have our solution.

10. Prove the following statements:

- (a) Show that for g odd, $g^{2^{k-2}} \equiv 1 \pmod{2^k}$ for $k \geq 3$.
 (b) Show by induction that $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ for $k \geq 3$.

(a) Let us try proof by induction. The case $k = 3$ gives us the equation $g^2 \equiv 1 \pmod{8}$ for every g odd, which can easily be checked. Now let g be any odd integer, and let us assume that $g^{2^{k-2}} \equiv 1 \pmod{2^k}$ for some $k \geq 3$, so that $g^{2^{k-2}} = 1 + 2^k n$ for some integer n . Then,

$$g^{2^{k-1}} = (g^{2^{k-2}})^2 = 1 + 2^{k+1}n + 2^{2k}n^2 \equiv 1 \pmod{2^{k+1}}$$

In the last part we used the fact that $2k \geq k+1$ (which is definitely true because we have $k \geq 3$).

(b) Let's try proof by induction again. The base case where $k = 3$ is the equation $3^1 \not\equiv 1 \pmod{8}$, which is clearly true. Now assume that $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ for some $k > 3$. Then we have $3^{2^{k-2}} - 1 = (3^{2^{k-3}} - 1)(3^{2^{k-3}} + 1)$, and we know that $3^{2^{k-3}} - 1$ has at most $k-1$ factors of 2 because of our inductive hypothesis. If we can show that $3^{2^{k-3}} + 1$ is not divisible by 4, then we're done because then we would know that $3^{2^{k-2}} - 1 \not\equiv 0 \pmod{2^{k+1}}$. Because $k > 3$, we know 2^{k-3} is even, and $3^2 \equiv 1 \pmod{4}$, so $3^{2^{k-3}} \equiv -1 \pmod{4}$. This completes the proof.

11. Compute $\lambda(800)$.

This is a straightforward use of Proposition 7.2.12. First we factor $800 = 2^5 \cdot 5^2$, and then we compute $\lambda(2^5) = \phi(2^5) = 2^4$ and $\lambda(5^2) = \phi(5^2) = 4 \cdot 5$. Then we know that $\lambda(800) = [16, 20] = 80$.

7.3, # 1,2,3

1. Suppose p is prime and g is a primitive root modulo p . Determine the index of -1.

Remember that whenever we were checking that some integer g was a primitive root, we would always get $g^{\phi(p)/2} = g^{(p-1)/2} \equiv -1 \pmod{p}$. Why is that? Well, if g is a primitive root, then $\text{ord}_p(g) = p-1$, so $g^{(p-1)/2}$ is a square root of 1 modulo p . In the integers, the only square roots of 1 are ± 1 , so is this also true modulo p ? Yes, because $x^2 - 1 = (x-1)(x+1)$, so if p divides $x^2 - 1$, either p divides $x+1$ or $x-1$, which means $x \equiv \pm 1 \pmod{p}$. Therefore the index of -1 modulo p is always $(p-1)/2$.

2. Solve the following equations:

- (a) $2^x \equiv 35 \pmod{37}$
- (b) $59^x \equiv 63 \pmod{71}$

(a) First we find a primitive root. It so happens that 2 is a primitive root modulo 37, and we can check this by verifying that $2^{12} \equiv -11 \pmod{37}$ and $2^{18} \equiv -1 \pmod{37}$ using Proposition 7.2.14. Now we can take ind_2 of both sides, and this gives us an equivalence modulo $\phi(37) = 36$. Since ind_2 works like a logarithm (look at Proposition 7.3.3), we get $x \equiv x \cdot \text{ind}_2(2) \equiv \text{ind}_2(35) \pmod{36}$, so we need to find $\text{ind}_2(35)$. Luckily, $35 \equiv -2 \pmod{37}$ and $2^{18} \equiv -1$

(mod 37), so we can see that $2^{19} \equiv -2 \pmod{37}$ and $\text{ind}_2(35) = 19$. Hence, the solution is $x \equiv 19 \pmod{36}$.

(b) It's easiest if one realizes that 59 is a primitive root modulo 71 (I used Mathematica). We need to find $\text{ind}_{59}(63)$ to finish. Actually, 63 is also a primitive root modulo 71 (again Mathematica), so we know $\text{ind}_{59}(63)$ is relatively prime to 70 which helps a little. In fact, after using this (and Mathematica), I found that $59^{41} \equiv 63 \pmod{71}$ so $\text{ind}_{59}(63) = 41$. Hence the solution is $x \equiv 41 \pmod{71}$.

3. Suppose g and h are primitive roots modulo n . Show that

$$\text{ind}_h(y) \equiv \text{ind}_h(g)\text{ind}_g(y) \pmod{\phi(n)}$$

By definition we know that $h^{\text{ind}_h(y)} \equiv y \pmod{n}$, $h^{\text{ind}_h(g)} \equiv g \pmod{n}$, and $g^{\text{ind}_g(y)} \equiv y \pmod{n}$. Now raise the middle equation to the $\text{ind}_g(y)$ -th power, and we get

$$h^{\text{ind}_h(y)\text{ind}_g(y)} \equiv (h^{\text{ind}_h(g)})^{\text{ind}_g(y)} \equiv g^{\text{ind}_g(y)} \equiv y \pmod{n}$$

Then we can use Proposition 7.3.3 (d) to conclude that $\text{ind}_h(y) \equiv \text{ind}_h(g)\text{ind}_g(y) \pmod{\phi(n)}$.