Homework 6, Math 4150

1. Exercise Set 5.1, #9. Let p be an odd prime number and let r be an integer with $p \nmid r$. Prove that r is a primitive root modulo p if and only if $r^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

   Solution.

   ($\Rightarrow$) Given that r is a primitive root modulo p we know the order of r is $\phi(p) = p-1$ as p is prime. Now we know that for any k for which we have $r^k \equiv 1 \pmod{p}$ we have $ord_p r \mid k$. Now assume that we have for some prime divisor of $p-1$, q (so note that $q \neq 1$) for which we get,

   $$r^{(p-1)/q} \equiv 1 \pmod{p}$$

   Now this means that we have $p-1 \mid (p-1)/q$. But as $q \neq 1$ meaning $q \geq 2$ we have $\frac{p-1}{q} < p-1$ and this means that $p-1 \mid (p-1)/q$ is not possible as a larger number cannot divide a smaller number. Hence, we cannot find any q for which we have $r^{(p-1)/q} \equiv 1 \pmod{p}$ which means that for all prime divisors q of $p-1$ we have $r^{(p-1)/q} \not\equiv 1 \pmod{p}$

   ($\Leftarrow$) Now assume for all prime divisors q of $p-1$ we have $r^{(p-1)/q} \not\equiv 1 \pmod{p}$. Now using eulers theorem we know $r^{(p-1)} \equiv 1 \pmod{p}$. Now we need to show that $p-1$ is the smallest positive integer for which we have equivalency with 1. Assume there exists a smaller number say k so we have $ord_p r = k$ and $k \mid p-1$ or $km = p-1$. Now choose q for which it's a prime divisor of m then we have,

   $$r^{(p-1)/q} \equiv r^{km/q} \equiv (r^k)^{m/q} \equiv 1 \not\equiv 1 \pmod{p}$$

   A contradiction. Hence, there cannot be any $k < p-1$ for which we have $r^k \equiv 1 \pmod{p}$ and we have that the order is $p-1$ which means that r is a primitive root.

2. Exercise Set 5.2, #11(d). Find all incongruent integers having order 10 modulo 61 [HINT: First find a primitive root modulo 61].

Solution.

First we need a primitive root modulo 61. We have $\phi(61) = 60$ so possible orders are $1, 2, 3, 5, 6, 10, 12, 15, 20, 30, 60$

Try 2: We have $2, 4, 8, 32, 3, 48, 9, 11, 47, 60 = -1, 1$.

Hence we have 2 is a primitive root. Now we know the following is true,

$$\begin{aligned} ord_{61}(2^i) &= \frac{ord_{61}(2)}{(ord_{61}(2), i)} \\ &= \frac{60}{(60, i)} \end{aligned}$$

We need all the numbers with order 10 so we need numbers with $ord_{61}(2^i) = 10$ note that all possible numbers will be of form 2^i as 2 being a primitive root means that the powers of it will form a reduced residue class. So we have,

$$\begin{aligned} \frac{60}{(60, i)} &= 10 \\ (60, i) &= 6 \\ (10, \frac{i}{6}) &= 1 \end{aligned}$$

Now the numbers smaller than 10 coprime to it are $1, 3, 7, 9$ hence we have $i = 6, 18, 42, 54$

So all incongruent integers having order 10 modulo 61 are $2^6, 2^{18}, 2^{42}, 2^{54}$ which are $3, 27, 41, 52$ modulo 61 respectively.

3. Exercise Set 5.2, #12. Let p be an odd prime number.

   (a) Prove that any primitive root r modulo p is a quadratic non-residue modulo p. Deduce that $r^{(p-1)/2} \equiv -1 \pmod{p}$.

   Solution.

   We have $r^{(p-1)/2} \equiv k \pmod{p}$. Now squaring both sides we get $r^{p-1} \equiv k^2 \equiv 1 \pmod{p}$. Now we have two solutions for k either $k = 1, -1$. If $k = 1$ then we have $r^{(p-1)/2} \equiv 1 \pmod{p}$ but this means that r is not a primtive root as the order is smaller than $p - 1$, hence this means we have $k = -1$ or that we have,

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

   which means that r is a quadratic non-residue modulo p.

   (b) Prove that there are exactly $\frac{p-1}{2} - \phi(p-1)$ incongruent quadratic non-residues modulo p that are not primitive roots modulo p.

   Solution.

   First we know that there are $\frac{p-1}{2}$ quadratic residues and non-residues. Now we know that every primitive root is a quadratic non-residue and hence is in the list of $(p-1)/2$. Moreover the count of the number of primitive roots are $\phi(p-1)$ which are also non-residues. So the total non-residues that are not primitive roots are $\frac{p-1}{2} - \phi(p-1)$

4. Exercise Set 5.3, #24(c).

   (a) Find a primitive root that works modulo 13^m for every positive integer m. Justify your choice.

   Solution.

   First we know that 2 is a primitive root modulo 13. And we claim that 2 is also a primitive root for any 13^m where m is a positive integer. We do this by induction. The base case is that it is a root for $m = 1$, i.e. $ord_{13}2 = 12$. Now assume true for some case $m = k$. So we have $ord_{13^k}2 = \phi(13^k) = 12 \cdot 13^{k-1}$. We need to show that for case $k + 1$ it also holds true.

   Note that for 13^{k+1} the orders must divide $12 \cdot 13^k$ and further note if order modulo 13^k is $12 \cdot 13^{k-1}$ then modulo 13^{k+1} cannot be smaller than that. Assume for contradiction that for some $n < 12 \cdot 13^{k-1}$ is the order for 13^{k+1} then we have as $13^{k+1} \mid 2^n - 1$ we also have $13^k \mid 2^n - 1$ or that $2^n \equiv 1 \pmod{13^k}$ which means that the order modulo 13^k is smaller the $12 \cdot 13^{k-1}$, a contradiction. So the only possible orders of 2 modulo 13^{k+1} are $12 \cdot 13^k, 12 \cdot 13^{k-1}$.

   Now it is enough to show that $12 \cdot 13^{k-1}$ does not work for 13^{k+1} which would mean that 2 is a primitive root modulo 13^{k+1} as well. Now note for 13 we have $2^{12} \equiv 1 \pmod{1}3$. And note that modulo 13^2 we have $2^{12} \equiv 40 \not\equiv 1 \pmod{1}3^2$. So for $k = 1$ it fails. Now chaining this we can say for any arbitrary k going up a level to $k + 1$ the order of the previous doesn't work. Hence $12 \cdot 13^{k-1}$ doesn't work and the order must be $12 \cdot 13^k$ which makes 2 a primitive root.

   Hence 2 is a primitive for any 13^m where m is a positive integer.

5. Exercise Set 5.4, #30(a),(e). Use indices to find all incongruent solutions of each congruence below.

(a) $8x^7 \equiv 5 \pmod{13}$

Solution.

Let r be a primitive root. Then $ind_r 8x^7 \equiv ind_r 5 \pmod{12}$ we can expand it as follows,

$$\begin{aligned} ind_r 8 + ind_r x^7 &\equiv ind_r 5 \pmod{12} \\ ind_r 8 + 7ind_r x &\equiv ind_r 5 \pmod{12} \\ 7ind_r x &\equiv ind_r 5 - ind_r 8 \pmod{12} \end{aligned}$$

Now a primitive root modulo 13 is 2. So we have x such that

$$7ind_2 x \equiv ind_2 5 - ind_2 8 \pmod{12}$$

And we have $ind_2 5 = 9$ and $in_2 8 = 3$. So,

$$7ind_2 x \equiv 6 \pmod{12}$$

Note 7 has an inverse as we have $12 \cdot 3 - 7 \cdot 5 = 1$ so inverse of 7 modulo 12 is -5. Hence we have,

$$ind_2 x \equiv -30 \equiv 6 \pmod{12}$$

Now this means that we have $x \equiv 2^6 \equiv 12 \pmod{13}$

(b) $7x^5 \equiv 2 \pmod{17}$

Solution.

We have $\phi(17) = 16$. We can easily check the 3 is a primitive root modulo 17. Now note that,

$$\begin{aligned} ind_3 7x^5 &\equiv ind_3 2 \pmod{16} \\ ind_3 7 + 5ind_3 x &\equiv ind_3 2 \pmod{16} \end{aligned}$$

Now we have $ind_3 7 = 11$ and $ind_3 2 = 14$ so,

$$5ind_3 x \equiv 3 \pmod{16}$$

Now $(16, 5) = 1$ and $16 + 5 \cdot -3 = 1$ so inverse of 5 modulo 16 is -3 which gives us,

$$ind_3 x \equiv 7 \pmod{16}$$

So we have $x \equiv 3^7 \equiv 11 \pmod{17}$

6. Exercise Set 5.4, #35. Let p be a prime number and let r and s be primitive roots modulo p. Let $a \in \mathbb{Z}$ with $p \nmid a$.

   (a) Prove that $\text{ind}_s a \equiv (\text{ind}_r a)(\text{ind}_s r) \pmod{p-1}$.
   (This corresponds to the change-of-base formula for logarithms).

   Solution.

   Let $ind_s a = x, ind_r a = y, ind_s r = z$. Now by definition we have,

   $$s^x \equiv a, r^y \equiv a, s^z \equiv r \pmod{p}$$

   So we get putting the second into the third we have,

   $$\begin{aligned}(s^z)^y &\equiv r^y \pmod{p} \\ s^{yz} \equiv r^y &\equiv a \pmod{p}\end{aligned}$$

   But we also know that $s^x \equiv a \pmod{p}$. This gives us,

   $$s^x \equiv s^{yz} \pmod{p}$$

   which means we have,

   $$\begin{aligned}x &\equiv yz \pmod{p-1} \\ ind_s a &\equiv (ind_r a)(ind_s r) \pmod{p-1}\end{aligned}$$

   (b) Prove that $\text{ind}_r(p-a) \equiv \text{ind}_r a + \frac{p-1}{2} \pmod{p-1}$. (This congruence yields all indices relative to r after half of these indices are computed).

   Solution.

   Let $ind_r(p-a) = x$ so $r^x \equiv p - a \pmod{p}$ and $r^x \equiv -a \equiv ar^{(p-1)/2} \pmod{p}$. Note that we have $r^{(p-1)/2} \equiv -1 \pmod{p}$ as r is a primitive root implying that it's not a quadratic residue. So we have $ind_r(p-1) \equiv x \equiv ind_r(ar^{(p-1)/2}) \pmod{p-1}$. Now note that expanding the last we get $ind_r(ar^{(p-1)/2}) \equiv ind_r a + ind_r r^{(p-1)/2} \equiv ind_r a + (p-1)/2 \pmod{p-1}$. So we get,

   $$ind_r(p-a) \equiv ind_r a + (p-1)/2 \pmod{p-1}$$

7. Exercise Set 5.4, #36.

(a) Let p be an odd prime number. Prove that the congruence $x^4 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{8}$.

Solution.

($\Rightarrow$) We have $x^4 \equiv -1 \pmod{p}$ so $x^8 \equiv 1 \pmod{p}$, but note that the squareroot of x^8, i.e. x^4 is not equivalent to 1 hence the order of x is 8. But we know the order must divide $p-1$ so we have $8 \mid p-1$ or that $p \equiv 1 \pmod{8}$

($\Leftarrow$) We have $p \equiv 1 \pmod{8}$ or $8 \mid p-1$. So 8 is a possible order for p and we can further say that we can find an element smaller than p for which we have $x^8 \equiv 1 \pmod{p}$ i.e. with order 8 as we have $\phi(8)$ elements with order 8. But if we have $x^8 \equiv 1 \pmod{p}$ and 8 is the order then we have $x^4 \equiv \pm \pmod{p}$ but it cannot be equivalent to 1 as it would mean the order is 4 hence we have $x^4 \equiv -1 \pmod{p}$.

(b) Prove that there are infinitely many primes expressible of the form $8n+1$ where n is a positive integer.
[Hint: Parallel the proof from Question 6 on Homework 5.]

Solution.

Assume we have finitely many primes say $p_1, \ldots, p_r$ now consider $N = 16p_1^4 \ldots p_r^4 + 1$. Now take $k = 4p_1 \ldots p_r$ so we have $N = k^4 + 1$ or that $k^4 \equiv -1 \pmod{N}$. Now let p be a prime factor of N so we also have $k^4 \equiv -1 \pmod{p}$. From (a) we know this means that $p \equiv 1 \pmod{8}$ so p is expressible in the form $8n+1$ for some $n \in Z$. But this means that p is in our list $\{p_1, \ldots, p_r\}$ say p_i. So p_i is a factor of N which means $p_i \mid k^4 + 1$ expanding this we get $p_i \mid 16p_1^4 \ldots p_r^4 + 1$. However, note that $p_i \mid 16p_1^4 \ldots p_r^4$ as p_i is in the list of primes. Which means we need $p_i \mid 1$. But p_i is an odd prime greater than 1 and hence this is not possible. A contradiction. Hence it cannot be true that there are finitely many primes of the form $8n+1$.

Blank page: