SOLUTIONS TO MATH 38B GRADED HOMEWORK 4

Exercise 1
Let $m \geq 2$ be an integer. We dene a primitive root modulo m as an element a relatively prime to m such that the smallest natural number e such that $a^e \equiv 1 \bmod m$ is $\varphi(m)$. We have proved in class that when m is a prime p, there is always a primitive root modulo p.

(a) Show that when a is a primitive root mod m, the integers $a, a^2, a^3, ..., a^{\varphi(m)}$ are all uncongruent modulo m.
(b) Find a primitive root modulo 4. Find a primitive root modulo 9. Find a primitive root modulo 25. Find a primitive root modulo 27.
(c) Using an exercise in preceding homework, show that there is no primitive root modulo 63.
(d) Using an exercise in the first midterm, show that there exist no primitive root modulo 2^n if $n \geq 3$.
(e) Let p and q be two odd distinct prime numbers. Show that there exist no primitive root modulo pq.
(f) Can you make a conjectural answer to the question: for which integers n there exist a primitive root modulo n.

Solution.

(a) Let $1 \leq \ell \leq k \leq \varphi(m)$. If $a^k \equiv a^\ell \bmod m$ then $a^{k-\ell} \equiv 1 \bmod m$ and since $k - \ell < \varphi(m)$ we conclude by definition of primitive root that $k = \ell$.
(b) I'm not going to write down any specific examples. You could do this by hand, possibly quickly or slowly and then find the answers. Instead let me point you to the exercise solution (f) below. There it says that if a is a primitive root modulo p then either a is a primitive root modulo p^2 or $a + p$ is a primitive root modulo p^2 and this only depends on $a^{p-1} \bmod p^2$. Further, if a is a primitive root modulo p^2 then it is a primitive root modulo p^k for all $k \geq 2$.

For example, to find a primitive root modulo 27, start with the primitive root 2 mod 3. Then, either 2 or 5 is a primitive root modulo 9. Since $2^2 = 4 \not\equiv 1 \bmod 9$ we conclude that 2 is still a primitive root modulo 9. Thus 2 is a primitive root modulo 27 as well.
(c) In exercise 2(c) of HW 3 we showed that if $\gcd(a, 63) = 1$ then $a^6 \equiv 1 \bmod 63$. On the other hand, $\varphi(63) = 6 \cdot 3(2) = 36$.
(d) By problem 4(e) on the first midterm, we showed that if a was odd then $a^{2^{n-2}} \equiv 1 \bmod 2^n$ for all $n \geq 3$. On the other hand, $\varphi(2^n) = 2^{n-1}$ and so there can be no primitive root.
(e) Let a be relatively prime to pq, i.e. both p and q. We have $a^{p-1} \equiv 1 \bmod p$ and $a^{q-1} \equiv 1 \bmod q$ so by exercise 2(a) of homework 3, $a^{\operatorname{lcm}(p-1,q-1)} \equiv 1 \bmod pq$. We claim, and this is all we need since $\varphi(pq) = (p-1)(q-1)$, that $\operatorname{lcm}(p-1, q-1) < (p-1)(q-1)$. There are many ways to see this but perhaps the easiest is using the formula that $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$. Since $p - 1$ and $q - 1$ are both *even* numbers we have $\gcd(p-1, q-1) > 1$ and hence $\operatorname{lcm}(p-1, q-1) < (p-1)(q-1)$.
(f) If n and m are relatively prime integers ≥ 3 then there is no primitive root modulo nm. That is because $\varphi(n) > 1$ and also $\varphi(n)$ is even (the same for m). Thus suppose $\gcd(a, nm) = 1$. By Euler, $a^{\varphi(n)} \equiv 1 \bmod n$ and $a^{\varphi(m)} \equiv 1 \bmod m$. By exericse 2(a) of homework 3 we have $a^{\operatorname{lcm}(\varphi(n),\varphi(m))} \equiv 1 \bmod nm$. Since $\varphi(n)$ and $\varphi(m)$ are both even, we get as above that $\operatorname{lcm}(\varphi(n), \varphi(m)) < \varphi(nm)$, hence a is not a primitive root modulo nm.

This observation rules all numbers except those of the form 2, 4, p^r and $2p^r$ with $r \geq 1$. One could use the Chinese remainder theorem to see that knowing there are primitive roots modulo p^r for each $r \geq 1$ implies the same for $2p^r$. We see it easily for 2 and 4 so we only need to check that odd prime powers have primitive roots. For the rest of this problem, let p be an odd prime.

Suppose $(a, p) = 1$. Then $a^{p-1} \equiv 1 \bmod p$. We want to know whether a is primitive root modulo p^2. Let k be the least integer such that $a^k \equiv 1 \bmod p^2$. We know that $a^{p(p-1)} \equiv 1 \bmod p^2$ and hence $k \mid p(p-1)$. Since $a^k \equiv 1 \bmod p$ we also know that $p - 1 \mid k$. Thus $k = p - 1$ or

$k = p(p-1)$. If $k \neq p-1$ then we have a is a primitive root modulo p^2. Otherwise consider $a+p$. It is a primitive root if we can see that $(a+p)^{p-1} \not\equiv 1 \bmod p^2$. We can check something slightly stronger however. We can see that a^{p-1} and $(a+p)^{p-1}$ are not congruent modulo p^2. That is not hard to see though because using the binomial theorem,

$$\begin{aligned}(a+p)^{p-1} - a^{p-1} &= (p-2)a^{p-2}p + \text{terms involving } p^2 \\ &\equiv -2a^{p-2}p \bmod p^2.\end{aligned}$$

Since p being odd and a is coprime to p we have that $p \nmid -2a^{p-2}$ so we are good.

Now suppose that a is a primitive root modulo p^2. We claim by induction that a is a primitive root modulo p^r for all $r \geq 2$. The case $r = 2$ is assumed. By Euler we know that $a^{p^r(p-1)} \equiv 1 \bmod p^{r+1}$. Let k be the least integer such that $a^k \equiv 1 \bmod p^{r+1}$. We know since a is a primitive root modulo p^r (by induction) that $p^{r-1}(p-1) \leq k \leq p^r(p-1)$. Since $p-1 \mid k$ as well we have that $k = p^{r-1}(p-1)$ or $k = p^r(p-1)$. We now eliminate the first possibility. Since a is a primitive root moudulo p^2 we have $a^{p-1} \not\equiv 1 \bmod p^2$. Put $a^{p-1} = 1 + cp$ with $\gcd(c,p) = 1$. Then,

$$a^{p^{r-1}(p-1)} = (1+cp)^{p^{r-1}} = 1 + p^{r-1}cp + \text{terms involving } p^{r+1} \text{ and higher.}$$

Since $\gcd(c,p) \neq 1$ we have $a^{p^{r-1}(p-1)} \not\equiv 1 \bmod p^{r+1}$.

■

Exercise 2

For which prime p does the congruence $x^2 + 4x + 5 \equiv 0 \bmod p$ have a solution? Same question for the congruence $x^2 + 6x + 7 \equiv 0 \bmod p$?

Solution. We have $x^2 + 4x + 5 = (x+2)^2 + 1$ so we are asking for those p which have a solution to $(x+2)^2 \equiv -1 \bmod p$. Thus the answers are all p for which -1 is a quadratic residue, equivalently, all $p \equiv 1 \bmod 4$.

We have $x^2 + 6x + 7 = (x+3)^2 - 2$ so we are asking for those p such that that there is a solution to the equation $a^2 \equiv 2 \bmod p$, i.e. when is 2 a quadratic residue. The answer is when $p \equiv \pm 1 \bmod 8$. ■

Exercise 3

Let $p > 3$ be a prime such that $p \equiv 3 \bmod 4$. Assume that $2p+1$ is also prime. Show that $2p+1 \mid M_p$ (where M_p is the Mersenne number $2^p - 1$) and that M_p is not prime.

Give an example of p satisfying the hypotheses of the exercise and give the factorization into a product of primes of the corresponding Mersenne number M_p.

Solution. Let $q = 2p+1$. We want to show that $2^p - 1 \equiv 0 \bmod q$. Since $p \equiv 3 \bmod 4$ we $p = 3+4k$ have $p \equiv -1 \bmod 8$ and hence there is an a such that $a^2 \equiv 2 \bmod q$ by quadratic reciprocity. Then,

$$\begin{aligned}2^p - 1 &\equiv a^{2p} - 1 \bmod q \\ &\equiv a^{q-1} - 1 \bmod q \\ &\equiv 0 \bmod q,\end{aligned}$$

using Fermat's little theorem. Thus $2p+1 \mid M_p$. If M_p is prime then $2p+1 = M_p$. This reduces to the equality $2^{p-1} = p+1$ which is clearly false for $p > 3$, by calculus if you like.

Lets take the simplest example $p = 11$. Then, $q = 23$ is indeed prime and $2^{11} - 1 = 23 \cdot 89$ is the factorization of M_p into primes. ■