Number Theory Notes
November 13, 2021

1 Primitive Roots in terms of group theory

We have already discussed these results in the last week's notes in an elementary manner. In this section, these results are described in the modern group theoretic language. These proofs have been put here for the sake of completion, and may be skipped on the first reading.
Notation. We write $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n$ or $\mathbb{Z}_n$ for the additive group of integers mod n under the operation of addition mod n. Similarly, we also write $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/n)^*$ for $\mathbb{Z}_n^*$, the group of integers coprime to n under the operation of multiplication mod n.

• **Proposition.** $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if, and only if, $n = 2, 4, p^r$ or $2p^r$ for some odd prime p. In these cases, a generator is called a primitive root modulo n.
Proof.
If $n = p_1^{a_1} \cdots p_r^{a_r}$, then consider the homomorphism

$$\mathbb{Z}/n \to \mathbb{Z}/p_1^{a_1} \times \cdots \mathbb{Z}/p_r^{a_r}$$

given by $\bar{1} \mapsto (\bar{1}, \cdots, \bar{1})$.
Here, of course, we have used $\bar{1}$ to denote elements in different groups. Clearly, θ is 1-1 and, therefore, onto as well as the sets are finite. This is nothing but the usual Chinese remainder theorem.
Now, let us consider the restriction of θ above to the subset $(\mathbb{Z}/n)^*$ consisting of all $\bar{r}$ with $r \leq n$ and $(r, n) = 1$. This subset is a subgroup under multiplication modulo n. Its image under the above θ maps into the subset $(\mathbb{Z}/p_1^{a_1})^* \times \cdots (\mathbb{Z}/p_r^{a_r})^*$ of $\mathbb{Z}/p_1^{a_1} \times \cdots \mathbb{Z}/p_r^{a_r}$.
Note that θ restricted to this subset is actually, a group homomorphism under multiplication modulo n.
Once again, this is 1-1 as it has trivial kernel because $a \equiv 1$ mod n if $a \equiv 1$ mod $p_i^{a_i}$ for all $i \leq r$. Hence, being finite a map of finite sets, it is onto as well and thus

$$(\mathbb{Z}/n)^* \cong (\mathbb{Z}/p_1^{a_1})^* \times \cdots (\mathbb{Z}/p_r^{a_r})^*.$$

Let us note that a direct product of $r > 1$ cyclic groups is cyclic if, and only if, their orders are pairwise co-prime.

Therefore, it suffices to check that $(\mathbb{Z}/p^a)^*$ for a prime p is cyclic if, and only if, p is odd or $p = 2$ and $a = 1, 2$.
Of course, $(\mathbb{Z}/p^a)^*$ has order $p^{a-1}(p-1)$. Let p be odd first. It suffices to produce elements g and h of the coprime orders p^{a-1} and $p-1$ respectively since gh would then have order $p^{a-1}(p-1)$.
By the binomial theorem, if $a \geq 2$ and $p > 2$,

$$(1+p)^{p^{a-2}} \equiv 1 + p^{a-1} \ \ modulo \ \ p^a,$$

$$(1+p)^{p^{a-1}} \equiv 1 \ \ modulo \ \ p^a.$$

In other words, the element $\overline{1+p} \in (\mathbb{Z}/p^a)^*$ has order p^{a-1} if p is odd and $a > 1$.
We shall now show the existence of an element of order $p-1$ in $(\mathbb{Z}/p^a)^*$ for p odd and $a \geq 1$.
First, in the field $\mathbb{Z}/p$ of p elements, every non-zero polynomial has at the most its degree number of roots by the remainder theorem. Thus, for each d, there are at most d elements x of $(\mathbb{Z}/p)^*$ satisfying $x^d = 1$. By what we have proved earlier, the group $(\mathbb{Z}/p)^*$ must be cyclic. If $\bar{r}$ is a generator, then the corresponding element r^{p-1} in $(\mathbb{Z}/p^a)^*$ has order some power p^k of p. Therefore, in $(\mathbb{Z}/p^a)^*$, the element r^{p^k} has order $p-1$. Thus, the problem is solved when p is odd.
For $p = 2$, $a > 2$, we see by the binomial theorem that

$$(1+4)^{2^{a-3}} \equiv 1 + 2^{a-2} \ \ modulo \ \ 2^a,$$

$$(1+4)^{2^{a-2}} \equiv 1 \ \ modulo \ \ 2^a.$$

Hence, if $a \geq 2$, the group $(\mathbb{Z}/2^a)^*$ of order 2^{a-1} is generated by the element -1 of order 2 and the element 5 of order 2^{a-2}. Now, if -1 were to be a power of 5, the orders would force $-1 = 5^{2^{a-2}}$ in $(\mathbb{Z}/2^a)^*$.
Then, we would get

$$-1 \equiv 1 + 2^{a-1} \ \ modulo \ \ 2^a$$

which is impossible when $a > 2$.
Therefore, if $a > 2$, then $(\mathbb{Z}/2^a)^*$ is isomorphic to the direct product of the group of order 2 and the cyclic group of order 2^{a-2}; so it is not cyclic.
Of course, $(\mathbb{Z}/2)^*$ is trivial and $(\mathbb{Z}/4)^*$ is the cyclic group of order 2.

Let us note from the above proof that, for $n \geq 3$,

$$(\mathbb{Z}/2^n)^* \{\pm 5^k : 1 \leq k \leq 2^{n-2}\} \cong \mathbb{Z}/2^{n-2} \times \mathbb{Z}/2.$$

Recall that we already proved the following proposition in an elementary manner. We give a proof using group theory now.

Proposition. *Let m be a positive integer such that a primitive root mod m exists (that is, $\mathbb{Z}_m^*$ is a cyclic group). Then, for a positive integer n and an integer a co-prime to m, the congruence $x^n \equiv a$ mod m has a solution if, and only if, $a^{\phi(m)/(n,\phi(m))} \equiv 1$ mod m. In this case, the number of solutions is $(n, \phi(m))$.*

Proof using group theory.

The proof is clear because an element of the cyclic group $\mathbb{Z}_m^*$ is an n-th power if, and only if, it is an $(n, \phi(m))$-th power. An element of a cyclic group of order N is a d-th power for a divisor of N if, and only if, its (N/d)-th power is 1. Further, the kernel of the (N/d)-th power map is precisely the unique subgroup of order N/d. Hence, for our case $N = \phi(m)$, $d = n/(n, \phi(m))$; so $x^n \equiv a$ mod m has exactly $(n, \phi(m))$ solutions.

2 Power residues mod prime powers

Let us look at the question of solvability of congruences of the form

$$x^n \equiv a \ \ mod \ \ p^r$$

for odd as well as even primes p.
Recall that the proposition below was proved by us in class using elementary arguments and the last section gave a group theoretic proof.

Proposition. *Let m be a positive integer such that a primitive root mod m exists. Then, for a positive integer n and an integer a co-prime to m, the congruence $x^n \equiv a$ mod m has a solution if, and only if, $a^{\phi(m)/(n,\phi(m))} \equiv 1$ mod m. In this case, the number of solutions is $(n, \phi(m))$.*

We also have:

Proposition. *Let p be an odd prime, and let $n > 0, a$ be integers coprime to p. If $x^n \equiv a$ mod p has a solution, then the congruences $x^n \equiv a$ mod p^r have solutions for all $r \geq 1$. The number of solutions of each of them is the same.*
The proof is simple. If $x_k^n \equiv a$ mod p^k (for some $k \geq 1$), consider $x_{k+1} = x_k + up^k$ for any u (to be determined suitably). Write $x_k^n = a + bp^k$.

$$x_{k+1}^n \equiv x_k^n + nup^k \equiv a + (b + nu)p^k \ \ mod \ \ p^{k+1}.$$

We may choose u so that $b + nu \equiv 0$ mod p since $(p, n) = 1$. Hence,

$$x_{k+1}^n \equiv a \ \ mod \ \ p^{k+1}.$$

Moreover, the number of solutions is the same because $(n, \phi(p^k)) = (n, p-1)$ for all $k \geq 1$.

The analogues of the above two results for powers of 2 are more difficult. We have:

Proposition. *Let $e \geq 3$. Consider $x^n \equiv a$ mod 2^e with a odd.*
(a) If n is odd, there is a unique solution for x mod 2^e.
(b) If n is even, then the congruence has a solution if, and only if, $a \equiv 1$ mod 4, $a^{2^{e-2}/(n,2^{e-2})} \equiv 1$ mod 2^e. In this case, the number of solutions is $2(n, 2^{e-2})$.
Proof.
Note that $\mathbb{Z}_{2^e}^*$ has order 2^{e-1}. Hence the power map by any odd number is an automorphism. Hence (a) follows immediately. For (b), once again, it suffices to consider only those $n > 1$'s which are powers of 2. We put $n = 2^N$ with $N \geq 1$. Now, first assume that $x^n = a$ has a solution $\mathbb{Z}_{2^e}^*$. Then, since the order of the group is 2^{e-1}, we have

$$x^n = y^{(n,2^{e-1})} = a.$$

So, firstly $a \equiv 1$ mod 4 since $N > 0$. Also, recalling that the group $\mathbb{Z}_{2^e}^* = \pm 5^k$ where 5 has order 2^{e-2}, we have $y = \pm 5^k$ for some k. Now,

$$a^{2^{e-2}/(n,2^{e-2})} == 1$$

writing a as a power of y and y as $\pm 5^k$ because we will then have a power of 5 which has 2^{e-2} times an integer in the exponent.
Let us now show the converse that if $a \equiv 1$ mod 4 satisfies $a^{2^{e-2}/(n,2^{e-2})} = 1$ in our group, then there exists x with $x^n = a$. Now, writing $a = 5^k$ (minus sign is not there as a is assumed to be 1 mod 4) and $n = 2^N$, we get in terms of powers of 5 that $a^{2^{e-2}/(n,2^{e-2})} = 5^t = 1$ where

$$t = 2^{e-2}k/2^{min(N,e-2)}.$$

As the order of 5 is 2^{e-2}, we have k to be a multiple of $2^{min(N,e-2)}$. Write $k = 2^{min(N,e-2)}v$ for some v. This is given to us. To solve for x or y such that $x^n = y^{(n,2^{e-1})} = y^{2^{min(N,e-1)}} = a$, put $y = \pm 5^u$.
Then, $a = 5^k = 5^v$ with $v = 2^{min(N,e-1)}u$. Thus, the order 2^{e-2} of 5 divides $2^{min(N,e-1)}u - k$.
That is, given N and k (which is a multiple of $2^{min(N,e-2)}$), we want to choose u so that 2^{e-2} divides $2^{min(N,e-1)}u - 2^{min(N,e-2)}v$.
Dividing by $2^{min(N,e-2)}$, this divisibility is equivalent to $2^{e-2-min(N,e-2)}$ dividing $2^{min(N,e-1)-min(N,e-2)}u - v$.
If $N \geq e - 2$, this is no condition.

Assume $N < e-2$. The condition 2^{e-2-N} divides $u-v$.
Therefore, we can clearly choose $u = v+$ multiple of 2^{e-2-N}.
Finally, let us count the number of solutions given that there is a solution. We have already shown that if $N \geq e-2$, every x is a solution.
If $N < e-2$, as we saw $u = v+$multiple of 2^{e-2-N}. As u can go up to 2^{e-2} (as $y = \pm 5^u$). Thus, there are 2^N choices for u and hence 2^{N+1} choices for y.
Note that $2(n, 2^{e-2}) = 2^{N+1}$ if $N < e-2$ and 2^{e-1} (order of the whole group) when $N \geq e-2$. This completes the proof.

Example. Here is a nice fact on primitive roots. Let $p = 2^n + 1 > 3$ be a prime. We will show that 3 is a primitive root mod p.
As $p-1$ is a power of 2, the order of 3 will be a power of 2 which means that 3 is a primitive root if, and only if, it is not a square. We will show that -3 is not a square which suffices since -1 is a square (as $p \equiv 1$ mod 4).
Suppose, if possible, $-3 \equiv b^2$ mod p. We may assume that b is odd as we may add multiples of p. Write $b = 2a+1$ to get

$$-3 \equiv (2a+1)^2.$$

So, $4a^2 + 4a + 4 \equiv 0$ mod p. As p is odd, we get $a^2 + a + 1 \equiv 0$ mod p. This implies,

$$0 = a^3 - 1 = (a-1)(a^2 + a + 1) \equiv 0$$

but $a \not\equiv 1$ mod p (else $3 \equiv 9$). Therefore, a has order 3 mod p which gives $p \equiv 1$ mod 3. This is a contradiction as a Fermat prime $2^n + 1 > 3$ is 2 mod 3.