Number Theory Notes
First Week of November, 2021

1 Primitive roots

Definition. Given a positive integer m, an integer $a \leq m$ and coprime to m, is said to be "*a primitive root mod m*" if its order mod m is $\phi(m)$ (the maximum possible).
Later, we will see that this is the same as saying that "the group $\mathbb{Z}_m^*$ is cyclic."

The first theorem is due to Gauss and it should be remarked that the proof is group-theoretic although the notions of modern group theory were developed only later!
Beforr stating the theorem, we make a useful observation concerning the totient function.
For any positive integer n, $\sum_{d|n} \phi(d) = n$.
This can be seen to be true as follows. Consider the n fractions $\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}$. When we reduce each fraction to its lowest terms, the fractions $\frac{a}{d}$ that have a particular denominator d (which evidently divides n) are precisely those for which $(a, d) = 1$. Being bounded by 1, this gives $\phi(d)$ such fractions. This proves the identity stated above.

Theorem (Gauss). *For any odd prime p, there exist $\phi(p-1)$ primitive roots mod p.*
Proof. Recall the set $\mathbb{Z}_p^*$ of positive integers $a < p$. Each a in it has some order d mod p and d divides $p-1$ by Fermat's little theorem. Let us decompose $\mathbb{Z}_p^*$ as a union of disjoint subsets $G(d)$ for divisors d of $p-1$ where $G(d)$ contains all those elements which have order equal to d. Then, the cardinality count gives

$$p - 1 = \sum_{d|(p-1)} |G(d)|.$$

Of course, $G(d)$ may, a priori, be empty for some d. The theorem asserts that $G(p-1)$ has cardinality $\phi(p-1)$. Now, consider any possible non-empty $G(d)$ and an element $a \in G(d)$. As a has order d mod p, the powers $a, a^2, \cdots, a^{d-1}, a^d = 1$ mod p are distinct. But, these elements are d distinct solutions of the congruence $x^d - 1 \equiv 0$ mod p in $\mathbb{Z}_p$. We know that a polynomial congruence mod p of degree d can have at the most d solutions. So, these powers of a are all the solutions. In other words, any element b of $\mathbb{Z}_p$ satisfying $b^d = 1$ in $\mathbb{Z}_p$ must be one of the powers of a mod p. Among these powers, the elements of $G(d)$ are those powers a^i for which $(i, d) = 1$ (because we have seen that order of a is d implies order of a^i is $d/(i, d)$). Thus, $|G(d)| = \phi(d)$. Therefore, we have shown that either $|G(d)| = 0$ or $|G(d)| = \phi(d)$. In particular, $|G(d)| \leq \phi(d)$ for all d. But $p - 1 = \sum_{d|(p-1)} \phi(d)$ as observed earlier. Thus,

$$p - 1 = \sum_{d|(p-1)} |G(d)| \leq \sum_{d|(p-1)} \phi(d) = p - 1.$$

Therefore, $|G(d)| = \phi(d)$ for every $d|(p-1)$. In particular, the case $d = p-1$ proves the theorem.

Lemma 1. *Let p be an odd prime and $n \geq 2$. Then, there exists a primitive root a mod p such that $a^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n. In fact, ANY primitive root a mod p which has the property above for $n = 2$ has the property for each $n \geq 2$.*

Proof. From Gauss's theorem, we know there exists a primitive root a mod p. We prove the lemma by induction on n. First, let $n = 2$. If $a^{p-1} \not\equiv 1$ mod p^2, we have nothing more to prove. If $a^{p-1} \equiv 1$ mod p^2, look at $a + p$ which is also a primitive root mod p. Now

$$(a+p)^{p-1} - 1 = a^{p-1} - 1 + (p-1)a^{p-2}p + p^2u$$

for some integer u. Therefore,

$$(a+p)^{p-1} \equiv a^{p-1} - 1 - pa^{p-2} \quad mod \ p^2.$$

As $a^{p-1} - 1 \equiv 0$, we must have $a^{p-2} \equiv 0$ mod p which is impossible as $(a, p) = 1$. Therefore, the case $n = 2$ is proved ($a + p$ works if a does not).

Assume the result holds for some $n \geq 2$. Thus, we have a primitive root a mod p for which

$$a^{p^{n-2}(p-1)} \not\equiv 1 \quad mod \quad p^n.$$

Of course, since $\phi(p^{n-1}) = p^{n-2}(p-1)$, by Euler's congruence, we do have

$$a^{p^{n-2}(p-1)} \equiv 1 \quad mod \quad p^{n-1}.$$

Writing $a^{p^{n-2}(p-1)} = 1 + up^{n-1}$ we have $(p, u) = 1$. Raising to the p-th power, we have $a^{p^{n-1}(p-1)} = 1 + up^n$ mod p^{n+1}. Clearly, $1 + up^n \not\equiv 1$ mod p^{n+1} as $(p, u) = 1$. The lemma follows by induction now.

Note that we have shown above that any primitive root a mod p which satisfies $a^{p-1} \not\equiv 1$ mod p^2 also satisfies $a^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n for every $n \geq 2$.

Proposition 1. *For any odd prime and any n, there exists a primitive root a mod p^n. Moreover, either a or $a + p^n$ is also primitive roots mod $2p^n$.*

Proof. Consider a primitive root a mod p as in the lemma above; so, $a^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n. By Euler's congruence, $a^{p^{n-1}(p-1)} \equiv 1 \quad mod \quad p^n$. Thus, the order d of a mod p^n divides $p^{n-1}(p-1)$ and, since a has order $p-1$ mod p, we have $(p-1)|d$. So, $d = p^r(p-1)$ with $r \leq n-1$. If $r \leq n-2$, we have $a^{p^r(p-1)} \not\equiv 1$ mod p^n as we know $a^{p^{n-2}(p-1)} \not\equiv 1$ mod p^n. Therefore, $d = p^{n-1}(p-1)$; that is, a is a primitive root mod p^n.

Finally, such an a can be taken to be odd (else, we may replace a by $a + p^n$); then, $a^{p^{n-1}(p-1)} \equiv 1$ mod 2. As $\phi(p^n) = \phi(2p^n)$, the last assertion also follows.

Lemma 2. *There exists a primitive root mod 2^n if, and only if, $n \leq 2$.*
Proof. The cases $n = 1, 2$ are easy to see as 1 and 3 are primitive roots mod 2^n for $n = 1, 2$ respectively.
Let $n \geq 3$. We show by induction that for each odd a,

$$a^{2^{n-2}} \equiv 1 \mod 2^n.$$

This will show primitive roots mod 2^n cannot exist for $n \geq 3$. Indeed, we prove the above congruences by induction on $n \geq 3$. The case $n = 3$ is clear as $a^2 \equiv 1$ mod 8 for every odd a.
Assuming for some $n \geq 3$ that $a^{2^{n-2}} \equiv 1$ mod 2^n, we may write $a^{2^{n-2}} = 1 + 2^n u$. Squaring both sides, it is clear that $a^{2^{n-1}} = 1 + 2^{n+1}u + 2^{2n}u^2 \equiv 1$ mod 2^{n+1}. The lemma is proved.

Theorem. *Primitive roots mod n exist if, and only if, $n = 2, 4, p^r$ or $2p^r$ with p an odd prime.*
Proof. In view of Proposition 1 and Lemma 2, the following assertion would prove the theorem:
For $(m, n) = 1$ and $m, n > 2$, there is no primitive root mod mn.
To prove this, observe that $\phi(m), \phi(n)$ are both even. So, their LCM L is $< \phi(m)\phi(n)/2$. Also, from the expressions for the totient function, $\phi(u)\phi(v) \leq \phi(uv)$ for all u, v. In particular,

$$L := LCM(\phi(m), \phi(n)) \leq \frac{\phi(m)\phi(n)}{2} = \frac{\phi(mn)}{2}.$$

For any a coprime to mn, we have $a^L \equiv 1$ mod m and $a^L \equiv 1$ mod n; this implies $a^L \equiv 1$ mod mn as $(m, n) = 1$. Therefore, the order of a mod mn is less than $\phi(mn)$. This completes the proof of the theorem.

If m admits a primitive root, then determining which integers mod m are powers is comparatively easier as follows:

Lemma. *Let m be a positive integer such that primitive roots mod m exist (therefore, m is one of the integers mentioned in the above theorem, but we do not use it below). Let $(b, m) = 1$. Let k be a y positive integer. Then, there exists c such that $b \equiv c^k$ mod m if, and only if, $b^{\phi(m)/(\phi(m),k)} \equiv 1$ mod m.*
Proof. The "only if" part (which does not use the assumption that m admits a primitive root) is clear because $b \equiv c^k$ implies

$$b^{\phi(m)/(\phi(m),k)} \equiv (c^{\phi(m)})^{k/(\phi(m),k)} \equiv 1 \mod m.$$

For the "if" part, assume $b^{\phi(m)/(\phi(m),k)} \equiv 1 \bmod m$. Let a be a primitive root mod m. Then, the set of powers $a^r(1 \leq r \leq \phi(m))$ mod m is the full set $\mathbb{Z}_{>}{}^*$ as the powers are distinct and are $\phi(m)$ in number. Thus, we may write $b \equiv a^r$ for some r. The assumption $b^{\phi(m)/(\phi(m),k)} \equiv 1 \bmod m$ implies that $a^{r\phi(m)/(\phi(m),k)} \equiv 1 \bmod m$, which means $(\phi(m), k)$ divides r; say $(\phi(m), k)s = r$. Hence, $b = a^r = a^{(\phi(m),k)s} = d^{(\phi(m),k)}$ where $d = a^s$. Writing $(\phi(m), k) = kv - \phi(m)u$ for some POSITIVE integers u, v we get

$$d^{kv} = d^{u\phi(m)} d^{(\phi(m),k)} \equiv d^{(\phi(m),k)} \equiv b \ \ mod \ \ m.$$

Therefore $b \equiv c^k \bmod m$ where $c = d^v$. The proof is complete.