Exercise 4: Exercise 1.33 from the Course Text

Proposition 0.1 (Proposition 1.29)**.** *Let p be a prime and let a be an integer not divisible by p. Suppose that $a^n \equiv 1(\mod p)$. Then the order of $a \mod p$ divides n. In particular, the order of a divides $p-1$*

Theorem 0.2. *(Primitive Root Theorem) Let p a prime number. Then there exists an element $g \in F_p^*$ whose powers give every element of F_p^*. i.e.,*

$$F_p^* = \{1, g, g^2, g^3, \cdots, g^{p-2}\}.$$

Elements with this property are called primitive roots *of F_p or* generators *of F_p^*. They are the elements F_p^* having order $p-1$.*

Task

Let p be a prime and let q be a prime that divides $p-1$.

1. Let $a \in F_p^*$ and let $b = a^{(p-1)/q}$. Prove that either $b = 1$ or else b has order q. (Recall that the order of b is the smallest $k \geq 1$ such that $b^k = 1$ in F_p^*. *Hint:* Use Proposition 1.29.)

2. Suppose that we want to find an element of F_p^* of order q. Using (1), we can randomly choose a value of $a \in F_p^*$ and check whether $b = a^{(p-1)/q}$ satisfies $b \neq 1$. How likely are we to succeed? in order words, compute the value of the ratio

$$\#\{a \in F_p^* : a^{(p-1)/q} \neq 1\}/\#F_p^*.$$

(*Hint:* Use the Primitive Root Theorem)

Proof. 1. Let $a \in F_p^*$ and let $b = a^{(p-1)/q}$. Since q is a prime that divides $p-1$, then $p-1 = kq$ for some integer k. This means the order of every element a in F_p^* divides $p-1$.

Since $b = a^{(p-1)/q}$, we have $b^q = (a^{(p-1)/q})^q = a^{p-1}$. By Fermat's Little Theorem, we have $a^{p-1} = 1 \mod p$. Thus $b^q = 1$.

Now the order of b must be a divisor of q by Proposition 1.29, since $b^q = 1$. The divisors of q are 1 and q. If the order is 1, then b must be 1 otherwise q is the order of b.

2. The number of elements in F_p^* with order q is $\phi(q)$, where ϕ is the Euler totient function. But $\phi(q) = q-1$. Also, the number of of elements in F_p^* is $p-1$. Therefore the likelihood of finding such an element is $\frac{q-1}{p-1}$.

□

Exercise 5: Exercise 1.35 from the Course Text

Proposition 0.3. *Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying*

- $g \not\equiv 0(\mod p)$
- $g \not\equiv \pm(\mod p)$
- $g^q \not\equiv 1(\mod p)$

Prove that g is a pimitive root modulo p.

Proof. By the Primitive Root Theorem, there exists an element in F_p^* whose powers give every element of $\mathbb{Z}_p^*$. By Proposition 0.1, the order of any $g \in \mathbb{Z}_p^*$ must divide $p-1 = 2q$, which is the order of $\mathbb{Z}_p^*$. The possible factors of $2q$ are $1, 2, q$ and $2q$.

Since $g \not\equiv 0(\mod p)$, then there is no zero elements in the multiplicative group. In addition, since $g \not\equiv \pm(\mod p)$, then g cannot have order 1 or 2. Finally, since $g^q \not\equiv 1(\mod p)$, g cannot have order q.

So, the only possible oder is $p-1 = 2q$. Thus, g is of order $2q$, and hence a primitive root modulo p.

□