Mathematics 3159A **Bradley Assaly-Nesrallah**
Introduction to Cryptography
Assignment 4, Problem 1 Due Date: November 17, 2020

Solution

We fix a prime p > 3. Let a be an integer such that $p \nmid a$. We say that a is a cubic residue mod p if there exists b such that $a \equiv b^3 \mod p$.

1. We first show that the product of two cubic residues mod p is again a cubic residue.

Proof. Let c and d be cubic residues mod p, then there exists e,f such that $c \equiv e^3 \mod p$ and $d \equiv f^3 \mod p$,
Thus $cd = (ef)^3 \mod p$ so cd is also a cubic residue mod p as required so we are done. □

2. Suppose that a and b are not divisible by p, we claim that it is not necessarily the case that at least one of a, b and ab is a cubic residue mod p.

Proof. We want to show that it is not necessarily the case that one of a,b and ab is a cubic residue mod p, so it is sufficient if we give a counterexample.
Consider p=7, a = 2, b =5, where clearly $p \nmid a$ and $p \nmid b$ with ab=10≡ 3 mod 7 in this case we check all possible cubes of the range 1,...,p-1 as follows $1^3 \equiv 1 \mod 7$, $2^3 \equiv 1 \mod 7$, $3^3 \equiv 6 \mod 7$, $4^3 \equiv 1 \mod 7$, $5^3 \equiv 6 \mod 7$, $6^3 \equiv 6 \mod 7$.
Thus none of a, b or ab are cubic residues mod p, thus it is not necessarily the case that at least one of a, b and ab is a cubic residue mod p, so we are done. □

3. Fix a primitive root $g \in \mathbb{F}_g^*$. We determine the values of k such that g^k is a cubic residue mod p.

Proof. We will determine the values of k, for which the element g^k is a cubic residue mod p as follows, we first consider what p is mod 3.
There are 3 options, that p is 0,1 or 2 mod 3 however we know that p>3 but p is prime thus not divisible by 3, thus p cannot be 0 mod 3. So we consider the cases the p is 1 or 2 mod 3. We will consider only non-zero cubic residues.
First consider when $p \equiv 2 \mod 3$, by Bezout's lemma we have $x, y \in \mathbb{Z}$, such that 1=3x + (p-1)y,
So for any m mod p, $\equiv m^{3x+(p-1)b} \equiv m^{3a} \cdot m^{(p-1)y} \equiv m^{3x} \equiv (m^x)^3 \mod p$.
Thus for all $0 < k \leq p$ g^k is a cubic residue mod p.
If $p \equiv 1 \mod 3$ we have three cases if k=3n, k=3n+1 or k=3n+2 $n \in \mathbb{N}$
If k=3n then $g^k = g^{3n} = (g^n)^3$ is a cubic residue so we are done, thus g^k is a cubic residue for k when k is a multiple of 3.
Now we consider k=3n+1,
Suppose g^k is a cubic residue, say $g^k \equiv c^3 \mod p$.
By fermats little theorem $c^{p-1} \equiv 1 \mod p$,

thus $c^{p-1} \equiv (c^3)^{\frac{p-1}{3}} \equiv (g^k)^{\frac{p-1}{3}} \equiv (g^{3n+1})^{\frac{p-1}{3}} \equiv g^{n(p-1)} \cdot g^{\frac{p-1}{3}} \mod p$.
By Fermat's little theorem $g^{n(p-1)} \equiv (g^{p-1})^n \equiv 1^n \equiv 1 \mod p$,
Thus $g^{\frac{p-1}{3}} \equiv 1 \mod p$ contradicting that g is a primitve root, thus when k is of the form k=3n+1 g^k is a cubic nonresidue.
Likewise we consider k=3n+2,
Suppose g^k is a cubic residue, say $g^k \equiv c^3 \mod p$.
By fermats little theorem we $c^{p-1} \equiv 1 \mod p$,
Thus $c^{p-1} \equiv (c^3)^{\frac{p-1}{3}} \equiv (g^k)^{\frac{p-1}{3}} \equiv (g^{n+2})^{\frac{p-1}{3}} \equiv g^{n(p-1)} \cdot g^{2\frac{p-1}{3}} \mod p$.
By Fermat's little theorem $g^{n(p-1)} \equiv (g^{p-1})^n \equiv 1^n \equiv 1 \mod p$,
Thus $g^{2\frac{p-1}{3}} \equiv 1 \mod p$ contradicting that g is a primitve root, thus when k is of the form k=3n+2 g^k is a cubic nonresidue.
Thus we conclude if $p \equiv 1 \mod 3$ then g^k is a cubic residue exactly when k is a multiple of 3, meanwhile when $p \equiv 2 \mod 3$ then g^k is a cubic residue for all $1 \leq k \leq p$, so we are done. $\square$