# Math 173B: Midterm 1 Solutions

**Problem 2.**

(a) Describe each step in the ElGamal cipher.

*Solution.* Say Bob wants to send a message to Alice.

1. Alice and Bob publicly agree on a prime $p$ and element $g$ modulo $p$ (it could be a primitive root, but it's usually chosen to have large prime order).
2. Alice chooses a random $a$ with $1 \leq a \leq p-1$ and publishes $A = g^a \pmod{p}$.
3. Bob chooses his message $m \in \mathbb{Z}/p\mathbb{Z}$. He chooses a random $k$ and computes

$$c_1 = g^k \pmod{p}, \quad c_2 = mA^k \pmod{p}.$$

He sends the pair $(c_1, c_2)$ to Alice.

4. Alice decrypts by computing

$$(c_1^a)^{-1} \cdot c_2 \equiv m \pmod{p}. \tag{1}$$

□

(b) If eve has an oracle for the discrete log problem, how can she decrypt the message? Give a step-by-step explanation.

*Solution.* Eve knows $p, g, A = g^a \pmod{p}, c_1 = g^k \pmod{p}$, and $c_2 = mg^k \pmod{p}$. She has an oracle, that, given $g, p, h$ returns $x$ such that $g^x \equiv h \pmod{p}$ if it exists. She can then give her oracle $g, p$, and $A$ and it will give her $a \pmod{p-1}$. She can then perform the same decryption calculation (1) as Alice. □

**Problem 3.** Let $p$ be a prime number and let $g$ be a primitive root in $\mathbb{F}_p^\times$.

(a) Let $r$ be an integer such that $\gcd(r, p-1) = 1$. Prove that $g^r$ is a primitive root in $\mathbb{F}_p^\times$.

*Proof.* Here's one way to do it. Let $k$ be the order of $g^r$. $g^r$ is a primitive root if and only if its order is $p-1$. Since $(g^r)^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem, we know that $k | p-1$. Now we also have

$$(g^r)^k = g^{rk} \equiv 1 \pmod{p},$$

so the order of $g$ must divide $rk$. But the order of $g$ is $p-1$ since $g$ is a primitive root, so $p-1 | rk$. Since $p-1$ and $r$ are coprime, we must then have that $p-1 | k$. We have then shown that $k | p-1$ and $p-1 | k$, so $k = p-1$ and $g^r$ is a primitive root.

Here's a more algebraic way. Consider the map $f : \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{F}_p^\times$ given by $f(x) = g^{rx} \pmod{p}$. $g^r$ is a primitive root if and only if $f$ is surjective. We know that $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so $f$ is surjective if and only if it is injective (a map from a finite set to itself is surjective if and only if it is injective). Suppose that $f(x) = f(y)$, that is

$$g^{rx} \equiv g^{ry} \pmod{p}.$$

Since $g$ is a primitive root, this happens if and only if $r(x - y) \equiv 0 \pmod{p-1}$. Since $r$ is coprime to $p-1$, it is invertible mod $p-1$ and we obtain $x \equiv y \pmod{p-1}$, so $f$ is injective, and therefore surjective, which makes $g^r$ a primitive root. $\square$

(b) Prove that there are $\phi(p-1)$ primitive roots in $\mathbb{F}_p^\times$.

*Proof.* By part (a) we have that $g^r$ is a primitive root when $r$ is coprime to $p-1$. There are then *at least* $\phi(p-1)$ primitive roots in $\mathbb{F}_p^\times$. Suppose that $r$ is *not* coprime to $p-1$. There is then some $d > 1$ that divides both $p-1$ and $r$. We'd then have

$$(g^r)^{\frac{p-1}{d}} \equiv (g^{r/d})^{p-1} \equiv 1 \pmod{p-1}.$$

Note that $\frac{p-1}{d}$ and $\frac{r}{d}$ are indeed integers. The order of $g^r$ is then at most $\frac{p-1}{d}$, which is strictly less than $p-1$, so $g^r$ can't be a primitive root when $r$ isn't coprime to $p-1$. We conclude that there are *at most* $\phi(p-1)$ primitive roots. Combining this with part (a), we arrive at *exactly* $\phi(p-1)$ primitive roots. $\square$

(c) Find all primitive roots of $\mathbb{F}_{11}^\times$. (HINIT: 2 is a primitive root of $\mathbb{F}_{11}^\times$.)

*Solution.* By parts (a) and (b) and the hint, $2^r \pmod{11}$ is a primitive root if and only if $r$ is coprime to $11 - 1 = 10$. Our primitive roots are then

$$2^1 \equiv 2,\ 2^3 \equiv 8,\ 2^7 \equiv 7,\ 2^9 \equiv 9 \pmod{11}.$$

$\square$