CS181A Notes #4 Basic Details of ElGamal

Here we describe the ElGamal *probabilistic* public-key cryptosystem. Suppose the input is a positive integer k (also called the security parameter).

Setup phase Bob prepares his cryptographic keys as follows:

1. Choose a random k-bit prime numbers p.
2. Choose a *generator* g for the group $\mathcal{G} = \mathbb{Z}_p^\star$.
   Note: g is a generator iff $\{g^i : i = 1, \dots, p-1\} = \mathcal{G}$.
3. Choose a random exponent $b \in \mathbb{Z}_{p-1}$.
4. Compute $a \equiv g^b \pmod{p}$.

The *public* keys are (p, g, a) and the *secret* key is b.

Encryption For Alice to encrypt a message $x \in \mathcal{G}$, she performs these steps:

1. Choose a random exponent $\beta \in \mathbb{Z}_{p-1}$.
2. Compute $\alpha \equiv g^\beta \pmod{p}$. We call this the *half-mask*.
3. Compute $\omega \equiv a^\beta \pmod{p}$. We call this the *full-mask*.
4. Compute $y \equiv x\omega \pmod{p}$.
5. Send the ciphertext pair (y, α).

So, $\mathrm{Enc}(x) = (x\omega, \alpha)$ (where the entities are computed modulo p). Note that the encryption is probabilistic since β is chosen randomly for each message (which will mask a repeated message). Also, $\omega = \alpha^b$ and therefore Bob can recover the full-mask using his secret key b.

Decryption For Bob to decrypt the ciphertext pair (y, α), he simply computes $\mathrm{Dec}(y, \alpha) = y(\alpha^b)^{-1} \pmod{p}$.

Existence of generators Here, we show that for any prime p, the group $\mathbb{Z}_p^\star$ always has a generator. In what follows, we fix a prime p.

Claim 1. *Any polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree $d \geq 1$ has at most d roots.*

Claim 2. $x^{p-1} - 1 \equiv \prod_{i=1}^{p-1}(x-i) \pmod{p}$.

Claim 3. *Let $d \mid p-1$. Then, $x^d \equiv 1 \pmod{p}$ has exactly d solutions.*

For an element a modulo p, let $\mathrm{ord}_p(a)$ be the **order** of a modulo p, which is the smallest $t > 0$ so that $a^t \equiv 1 \pmod{p}$. We will need the following function ψ defined as:

$$\psi(d) = |\{x \in \mathbb{Z}_p^\star : \mathrm{ord}_p(x) = d\}|,$$

where d divides $p-1$. So, $\psi(d)$ counts the number of elements modulo p with order d.

Möbius Inversion We make a detour to describe the beautiful theory of Möbius inversion. Let $\mu(m)$ be the following function:

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } m \text{ is not square-free} \\ (-1)^k & \text{if } m = p_1 \ldots p_k \text{, for distinct primes } p_j\text{'s} \end{cases}$$

Fact 1. *For $m > 1$, we have $\sum_{d|m} \mu(d) = 0$.*

Proof. Suppose $m = \prod_i p_i^{e_i}$. Then,

$$\sum_{d|m} \mu(d) = \sum_{\varepsilon_i \in \{0,1\}} \mu(p_1^{\varepsilon_1}, \ldots, p_k^{\varepsilon_k}) = 1 - k + \binom{k}{2} - \ldots \pm (-1)^k.$$

The claim follows since the last expression equals $(1-1)^k$. ☐

Definition 1. *For $f, g : \mathbb{Z}^+ \to \mathbb{C}$, we define the convolution of f and g as*

$$(f \star g)(m) = \sum_{d_1 d_2 = m} f(d_1) g(d_2).$$

Let $\mathbb{I}$ be a function defined as $\mathbb{I}(m) = [\![m = 1]\!]$ and let I be the always-one function, that is $I(m) = 1$, for all m. The following properties can be verified easily:

1. $f \star (g \star h) = (f \star g) \star h$.
2. $\mathbb{I} \star f = f \star \mathbb{I} = f$.
3. $I \star f = f \star I$ and $(I \star f)(n) = \sum_{d|n} f(d)$.
4. $I \star \mu = \mu \star I = \mathbb{I}$.

The next theorem states the the Möbius inversion theorem.

Theorem 1. *If* $g(m) = \sum_{d|m} f(d)$*, then* $f(m) = \sum_{d|m} \mu(d) g(m/d)$*.*

Proof. Note that $g = f \star I$. Thus, $g \star \mu = f \star I \star \mu = f \star \mathbb{I} = f$. □

Fact 2. $\sum_{d|m} \phi(d) = m$*.*

Proof. Look at the fractions $1/m, 2/m, \ldots$, and m/m reduced to the lowest terms a/b where $\gcd(a, b) = 1$. Then, each divisor d of m appears as a denominator $\phi(m)$ times. □

Theorem 2. *For a prime* p*, the group* $\mathbb{Z}_p^\star$ *has a generator.*

Proof. Let $d \mid p - 1$. The size of the subgroup $B = \{x \in \mathbb{Z}_p^\star : x^d \equiv 1 \pmod{p}\}$ is d by Claim 3. Thus, $\sum_{a|d} \psi(a) = d$. By Möbius inversion, we get

$$\psi(d) = \sum_{a|d} a\mu(d/a) = \phi(d).$$

Thus, $\psi(p - 1) = \phi(p - 1)$. For $p > 2$, we have $\phi(p - 1) \geq 1$. □

Generating random generators To generate random generators for $\mathbb{Z}_p^\star$, we choose a random element of $\mathbb{Z}_p^\star$ and test that it is a generator. To simplify testing, we assume that p is of the form $p = 2q + 1$ for some other prime q. Primes of this form are called *safe* primes (or Sophie Germain primes). It remains open if there are infinitely many such primes.

Theorem 3. *Let* p *be a prime and suppose* g *is a generator for* $\mathbb{Z}_p^\star$*. Then,* g^t *is a generator iff* $\gcd(t, p - 1) = 1$*.*

Proof. Suppose $\gcd(t, p-1) = 1$ and let r be the order of g^p. Then, $p-1|tr$ since g is a generator. Because t and $p-1$ are relatively prime, we must have $p-1|r$. We also have $r|p-1$ since the order of any element divides $p-1$. Therefore, $r = p-1$.

Now, suppose g^t is a generator. Assume that $d = \gcd(t, p-1)$ where $d > 1$. Then, $(g^t)^{(p-1)/d = (g^{p-1})^{t/d}} \equiv 1 \pmod{p}$, which implies that g^t is not a generator since it has order at most $(p-1)/d < p-1$. □

Combined, Theorems 2 and 3 imply that there are $\phi(p-1)$ many elements in $\mathbb{Z}_p^\star$ which are generators. If $p = 2q+1$ is a safe prime, then $\phi(p-1) = \phi(q) = q-1$ (since ϕ is multiplicative). So, there is a fraction of $(q-1)/(p-1) \sim 1/2$ of elements which are generators.

A Missing proofs

Claim 4. *Any polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree d has at most d roots, where $d \geq 1$.*

Proof. By induction on d. If $d = 1$, then $f(x) = ax + b$ and $ax + b \equiv 0 \pmod{p}$ has exactly one root, namely, $x \equiv a^{-1}b \pmod{p}$. Assume that the claim holds for any polynomial of degree at most d. Say, f has degree $d+1$. If f has no roots, then we are done. Otherwise, let a be so that $f(a) = 0$. By the Division Algorithm for polynomials, we have $f(x) = q(x)(x-a) + r(x)$, where the degree of r is smaller than 1. Since $f(a) = 0$, we see that $r = 0$. Thus, $f(x) = q(x)(x-a)$ where q is a polynomial of degree d. By inductive assumption, g has at most d roots. Thus, f has at most $d+1$ roots. □

Claim 5. $x^{p-1} - 1 \equiv \prod_{i=1}^{p-1}(x-i) \pmod{p}$.

Proof. Let $f(x) = x^{p-1} - 1$ and $g(x) = \prod_{i=1}^{p-1}(x-i)$ modulo p. Now, define $h(x) = f(x) - g(x)$. Note that $h(x)$ is of degree at most $p-2$ but it satisfies $h(1) = \ldots = h(p-1) = 0 \pmod{p}$. This implies that h is the zero polynomial since h can have at most $p-2$ zeros. Thus, $f(x) = g(x)$ for all x. □

Remark: The above claim also follows from Fermat's Little Theorem.

Claim 6. *Let $d \mid p-1$. Then, $x^d \equiv 1 \pmod{p}$ has exactly d solutions.*

Proof. Suppose $p-1 = ad$. Then, $x^{p-1} - 1 = (x^d - 1)g(x)$, where $g(x) = \sum_{j=0}^{a-1}(x^d)^j$. Since $x^{p-1} - 1$ has $p-1$ roots, $x^d - 1$ must have d roots. □

Fact 3. *If* $m = p_1^{a_1} \dots p_k^{a_k}$ *then* $\phi(m) = m \prod_{i=1}^{k}(1 - 1/p_i)$.

Proof. Since $m = \sum_{d|m} \phi(d)$, by Möbius inversion, we have

$$\phi(m) = \sum_{d|m} \mu(d)(m/d) = m \left(1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \dots \right) = m \prod_i \left(1 - \frac{1}{p_i}\right).$$

$\square$

Fact 4. *For any integers* $m, n \geq 1$, $\phi(mn) = \phi(m)\phi(n)$ *whenever* $\gcd(m, n) = 1$.

Proof. Consider the bijection between $\mathbb{Z}_{mn}^\star$ and $\mathbb{Z}_m^\star \times \mathbb{Z}_n^\star$ provided by the Chinese Remainder Theorem. Since $|\mathbb{Z}_N^\star| = \phi(N)$, this proves the claim. $\square$