# Randomized Algorithms, Lecture No. 2

Sara Miner, scribe

Tuesday, January 13, 1998

**Theorem** The size of a subgroup $H$ divides the size of a group $G$. Define $g_1 \sim_H g_2$ if $g_2 = g_1 h$ for some $h \in H$.

**Lemma 1** $\forall g \, |[g]_{\sim_H}| = |H|$.
*Proof* Recall that $[g]_{\sim_H} = g' | g' \sim_H g$. Define $M_g : H \to [g]$. $M_g(h) = gh$. $M_g$ is onto from the definition of $\sim_H$. $M_g$ is one-to-one, since if $gh_1 = gh_2$, then $h_1 = 1h_1 = g^{-1}gh_1 = g^{-1}gh_2 = 1h_2 = h_2$. Therefore, $|[g]_{\sim_H}| = |H|$.

**Lemma 2** $\sim_H$ is an equivalence relation.
*Proof* An equivalence relation must be reflexive, symmetric, and transitive.
Reflexive: Since $1 \in H$ and $g = 1g$, then $g \sim_H g$.

Symmetric:
$$\begin{aligned} g_1 \sim_H g_2 &\Rightarrow g_2 = g_1 h \\ &\Rightarrow g_1 = g_2 h^{-1} \\ &\Rightarrow g_2 \sim_H g_1. \end{aligned}$$

Transitive: Assume $g_1 \sim_H g_2$, $g_2 \sim_H g_3$. This implies that $g_2 = g_1 h_1$ and $g_3 = g_2 h_2$. So $g_3 = g_1 h_1 h_2$. Since $H$ is closed under multiplication, $h_1 h_2 \in H$. So $g_1 \sim_H g_3$.

Proof of Theorem from Lemmas: Since $\sim_H$ is an equivalence, it partitions $G$ into equivalence classes. By Lemma 2, each equivalence class is of size $|H|$. Therefore, $|G| = |H| *$ the number of classes.
**Lemma 3** If $H$ is a nonempty finite subset of a group and is closed under multiplication, then $H$ is a subgroup.
*Proof* Choose any $h \in H$. Since the subset is closed under multiplication, then all powers of $h$ are in $H$. Namely, $h, h^2, h^3, ..., h^t \in H$. But since the subset is finite, then, $h^i = h^j$ for some $i < j$. So, $h^{j-i} = 1$, and therefore, $hh^{j-i-1} = 1$, so $h^{j-i-1} = h^{-1}$. This implies that $1, h^{-1} \in H$. Therefore, $H$ satisfies the properties of a subgroup.

Let $h \in Z_p^*$. Define $H_h = \{h^t | t = 0, 1, ...\}$. $H_h$ is a subgroup of $Z_p^*$ (where $p$ is prime). Therefore $|H_h|$ divides $|Z_p^*| = p - 1$. And we have that $h^{|H_h|} = 1$.

Let $k = (p-1)/|H_h|$.

So, $h^{p-1} = (h^{|H_h|})^k = 1^k = 1$.

**Fermat's Little Theorem** If $p$ is prime, then for every $g \in Z_p^*$, $g^{p-1} \equiv 1 \bmod p$.

This fact is used in a heuristic to check primality. But we are not guaranteed that our $p$ is prime just because this equivalence is true for some $g$. There are also infinitely many composites, called Carmichael numbers, where this equation holds.

*Computing $g^{p-1}$ efficiently* $g^{b_1 \dots b_k} \bmod N$

If $b_{i+1} = 0$, $g^{b_1 \dots b_i b_{i+1}} = g^{2(b_1 \dots b_i)} = (g^{(b_1 \dots b_i)})^2 \bmod N$.

If $b_{i+1} = 1$, $g^{b_1 \dots b_i b_{i+1}} = g(g^{b_1 \dots b_i})^2 \bmod N$.

Worst case: 2 multiplications per bit, then take remainder $\bmod N$.

When $p$ is an odd prime, then $p-1$ is even. So $g^{(p-1)/2}$ will be either 1 or -1 when $g^{p-1} = 1$. These should each occur about half of the time. This is what allows us to distinguish between primes and Carmichael numbers.

**Probabalistic Algorithm**

If $p$ has a square root or cube root, etc., output "not prime".

Pick many random $g_1, ..., g_t \in Z_p^*$.

For each, compute $g_i^{(p-1)/2}$.

If any are not 1 or -1, output "not prime".

If <u>all</u> are = 1, output "not prime".

Else, output "prime".

**Claim**[1] If $p$ prime, Prob[output "not prime"] $= 2^{-t}$.

If $p$ composite, Prob[output "prime"] $\leq 2^{-t}$.

We want to show: 1) there are only two possible square roots of 1.

2) 1 and -1 are equally distributed when $p$ is prime.

[1] Since we have error on both sides, this algorithm is <u>not</u> in RP. Instead, this is in BPP, where we have a Bounded Probability of error. But there are other algorithms for primality testing in RP. In fact, PRIMALITY $\in$ RP, and PRIMALITY $\in$ co-RP.

**Theorem 2** Let $p$ be a prime and $f(x)$ be a degree $d$ polynomial. Then there are at most $d$ values of $x \in Z_p^*$ so that $f(x) = 0 \bmod p$.

**Lemma** (stated without proof) Let $f(x), g(x)$ be polynomials with degree $deg(g(x)) \leq deg(f(x))$. Then $\exists q(x), r(x)$ with $deg(r(x)) < deg(g(x))$ such that $f(x) \equiv q(x)g(x) + r(x) \bmod p$.

**Proof of Thm 2** Let $f(x_1) \equiv 0 \bmod p$.

$f(x) = (x - x_1)q(x) + r(x)$. But $r(x)$ has degree 0, so its a constant. Call it $\hat{r}$.

Now $f(x_1) = 0 = 0q(x_1) + \hat{r}$. Therefore, $\hat{r} = 0$.

Then, $f(x) = (x - x_1)q(x)$. But $q(x)$ has degree $d - 1$. By induction, then $q(x) = 0$ is true for values of $x \leq d - 1$.

But $f(x) = 0$ only if one of the terms equals 0. So the roots of $f$ are either $x_1$ or the roots of $q$. Therefore, there are at most $d$ roots total.

Next, we want to show that we expect an equal distribution of 1 and -1. From Theorem 2, $x^2 = 1$ has at most 2 roots. Since 1 and -1 are roots, these must be the only roots. (Assuming $p \neq 2$!)

Now, $(g^{(p-1)/2})^2 = g^{p-1} = 1 \bmod p$. So $g^{(p-1/2)} = 1$ or $g^{(p-1)/2} = -1$. At most $(r - 1)/2$ g's can satisfy the first option, and similarly, at most $(r - 1)/2$ g's can satisfy the second. Therefore, all $p - 1$ can satisfy one or the other, and exactly half can satisfy each option.

So clearly, when $p$ is prime, Prob[ouptut "not prime"] $= 2^{-t}$. This is the same as the probability of a coin flip coming up heads $t$ times in a row.

Say $p$ is not prime and has at least two prime factors $q_1$ and $q_2$. (The case of only one prime factor is handled by the algorithm's first step.)

Let $H = g \in Z_p^* | g^{(p-1)/2} \in 1, -1$.

$H$ is closed under multiplication, and $1 \in H$. So $H$ is a subgroup of $Z_p^*$.

In particular, if $H \neq Z_p^*$ then $|H| \leq (|Z_p^*|/2)$. And the probability that a random $g \in H$ is at most $1/2$.

So, as claimed earlier, the probability of not finding a counterexample when $p$ is not prime is $\leq 2^{-t}$.

**Claim** If $H = Z_p^*$, then $\forall g \in Z_p^*, g^{(p-1)/2} = 1$.

*Proof by contradiction*

Assume $g^{(p-1)/2} = -1/bmodp$.

Then $g^{(p-1)/2} = -1$ must hold both $\bmod q_1$ and $\bmod q_2$.

Let $g' = (g \bmod q_2)(q_1)(q_1^{-1} \bmod q_2) + (q_2)(q_2^{-1} \bmod q_1)$.

So, $g' \bmod q_1 = 1$,

and $g' \bmod q_2 = g \bmod q_2$

Therefore we have that $(g')^{(p-1)/2} \equiv 1 \bmod q_1 = 1$

and $(g')^{(p-1)/2} \equiv g^{(p-1)/2} \bmod q_2 = -1$

So, $(g')^{(p-1)/2} \neq 1, -1 \bmod p$ (since $q_1$, $q_2$ are both factors of $p$.)

This implies that $g' \notin H$. And this is a contradiction, since $H = Z_p^*$.