How to choose group elements uniformly at random.

Finite group = $\mathbb{G}$:

for $i = 1$ to t

$x \leftarrow\$ \{0,1\}^n$

if $x \in \mathbb{G}$, return x.

$x \in \mathbb{G}$ → Membership test. Can be done efficiently.

Failure prob.

$$\left(1 - \frac{|\mathbb{G}|}{2^n}\right)^t$$

if $x < N$

Special case:-

$\mathbb{G} = \mathbb{Z}_N$.

Let us assume $n = \|N\|$

Failure prob:

$$\left(1 - \frac{|\mathbb{Z}_N|}{2^n}\right)^t$$

Special case:

$N = 35$.

$N \geq 2^{n-1}$

$G = \mathbb{Z}_N^*$.

110110

for $i = 1$ to t

$x \leftarrow \$ \{0,1\}^n$, where $n = \|N\|$.

if $x < N$ and $\gcd(x, N) = 1$, return x

end for.

return "fail".

Failure prob.

Succes prob $:= \frac{|\mathbb{Z}_N^*|}{2^n} = \frac{\phi(N)}{2^n}$.

$$k = \frac{2^n}{|\mathbb{Z}_N^*|} = \frac{2^n}{\phi(N)} = \frac{2^n}{N} \cdot \frac{N}{\phi(N)}$$

$$\leq \frac{2^n}{2^{n-1}} \cdot \frac{N}{\phi(N)} = 2 \cdot \frac{N}{\phi(N)} < 4$$

Lemma: $\frac{N}{\phi(N)} < 2$, where $n = \|N\|$.

Let N be a odd prime.

$$\phi(N) = N - 1.$$

$$N \leq 2^n$$

$$N \geq 2^{n-1}$$

$$N - 1 \geq 2^{n-1}$$

$$\frac{N}{N-1} \leq \frac{2^n}{N-1} < \frac{2^n}{2^{n-1}} = 2$$

Let $N = p \cdot q$.

$$\frac{p}{p-1} < \frac{3}{2}$$

$$\frac{N}{\phi(N)} = \frac{pq}{(p-1)(q-1)} = \frac{p}{p-1} \cdot \frac{q}{q-1} < \frac{3}{2} \cdot \frac{5}{4} < 2.$$

$$2p < 3p - 3$$

$$\Rightarrow p > 3.$$

$$\left(1-\frac{|G_2|}{2^n}\right)^t = \left(1-\frac{1}{k}\right)^t = \left(\left(1-\frac{1}{k}\right)^k\right)^n \leq e^{-n} \leq 2^{-n} \quad (\because 2 < e < 3)$$

$$k = \frac{2^n}{|G_2|} \qquad \text{Set } t = k \cdot n$$

$$t = 4n \cdot$$

How to choose a generator of a finite cyclic group uniformly at random.

Lemma:-

Let g be a generator of the finite cyclic group of G of order q.
Let $h = g^x \in G$. h is a generator of G iff $\gcd(x, q) = 1$.

Generators of a finite cyclic group of order q is the following set

$$\{h = g^x : x \in \mathbb{Z}_q^*\}.$$

The number of generators of G is $\phi(q)$.

Lemma: Let G be a group of order q. Let $q = \prod_{i=1}^{k} p_i^{e_i}$, $e_i \geq 1$.

Set $q_i = q/p_i$. Then h is a generator of G iff

$$h^{q_i} \neq 1 \quad \text{for } i = 1, \ldots k.$$

order of h is $q' < q$. $q' \mid q$. $q' = \prod_{i=1}^{k} p_i^{e_i'}$ - $e_i' \geq 0$

$q_j = p_j^{e_j - 1} \prod_{i \neq j} p_i^{e_i}$ $q' \mid q_j$

Input: Group order q, prime factors $\{p_i\}_{i=1}^{k}$ of q, and $h \in G_q$.

output: decision whether h is a generator or not.

for $i = 1$ to k:

if $h^{q/p_i} = 1$, then return "h is not a generator".

end for.

return "h is a generator!"

$$\frac{\phi(q)}{q} \geq \Omega\left(\frac{1}{\|q\|}\right)$$

$$q = \prod_{i=1}^{k} p_i^{e_i} \geq \prod_{i=1}^{k} p_i \geq 2^k$$

$$k \leq \log_2 q = \|q\|$$

Remark: There is no known poly time algorithm for choosing a generator of a cyclic group G of finite order q when the factorization of q is "unknown".

To have a remedy of this, one often chooses a group of order $q = 2p+1$, where p is prime

Factorization.

0 0 = 0
0 1 = 1
1 0 = 2
1 1 = 3

$x_1 \cdot x_2$

(1, 1)
(1, 3)
(3, 1)
(3, 3).

Odd : $\frac{4}{16} = \frac{1}{4}$

Even = $\frac{3}{4}$.

Generating a prime uniformly at random:-

Input: n, bit length of the prime.

output:- A prime.

for $i = 1$ to t.

{

$p' \leftarrow \$ \{0,1\}^{n-1}$

$p \leftarrow 1 \| p'$.

if p is prime, then return p.

}

return "fail"

$\sqrt{p} = p^{1/2}$ $= p^{\frac{\|p\|}{2}}$ $\sqrt{2^T} = ?$

Primality testing.

Miller-Rabin primality testing: 1st attempt.

Suppose N is a odd prime.

for any $a \in \{1, .. N-1\}$, $a^{N-1} \equiv 1 \bmod N$

N is an odd prime $\Rightarrow \forall a \in \{1, .. N-1\}$ $a^{N-1} \equiv 1 \bmod N$

$\exists a \in \{1, .. N-1\}$ $a^{N-1} \not\equiv 1 \bmod N \Rightarrow N$ is not an odd prime.

If $a \notin \mathbb{Z}_N^*$, then $a^{N-1} \not\equiv 1 \bmod N$.

$\gcd(a, N) = d > 1$

$d \mid a, \; d \mid N$

$d \mid a^{N-1}, \; d \mid N$

Suppose $a^{N-1} \equiv 1 \bmod N$

$\Rightarrow N \mid (a^{N-1} - 1)$

$\Rightarrow d \mid a^{N-1} - 1$

$d \mid 1 \Rightarrow\Leftarrow$

Defn: An element $a \in \{1, \ldots N-1\}$ is called a witness if $a \in \mathbb{Z}_N^*$ and $a^{N-1} \not\equiv 1 \bmod N$

MR-primality Test:

Input:- an integer N, and a parameter t.

Output: Decision whether N is prime or not.

for $i = 1$ to t.

$a \xleftarrow{\$} \{1, \ldots N-1\}$.

if $a^{N-1} \not\equiv 1 \bmod N$, return "Composite".

end for

return "prime".

Total failure prob.

$\left(1 - \frac{1}{3n}\right)^t$, set $t = 3n^2$.

Success probability in a trial.

Prime number theorem:

For any $n > 1$, the fraction of n bit integers that are prime is at least $1/3n$.

Let S be the set of n bit integers that are prime.

$|S| \geq 2^n/3n$

Lemma: Let H be a strict subgroup of a finite group G. Then $|H| \leq |G|/2$.

Pf: $\bar{h} \in G \setminus H$.

$$\bar{H} = \{h\bar{h} : h \in H\}.$$

$|\bar{H}| = |H|$, $\bar{H} \cap H = \emptyset$

$$|G| \geq |H| + |\bar{H}|$$

Lemma: Fix N, Say there exists a witness that N is composite. Then at least half of the elements of $\mathbb{Z}_N^*$ are also witnesses.

Pf: Let **Bad** be the set of elements of $\mathbb{Z}_N^*$ that are not witnesses.

$1 \in$ Bad. Let $a, b \in$ Bad.

$ab \in$ Bad.

$a^{N-1} \equiv 1 \bmod N$
$b^{N-1} \equiv 1 \bmod N$
$\Rightarrow (ab)^{N-1} \equiv 1 \bmod N$

Bad is a subgroup of $\mathbb{Z}_N^*$.

Is Bad a strict subgroup of $\mathbb{Z}_N^*$?

$|\text{Bad}| \leq \frac{|\mathbb{Z}_N^*|}{2}$.

There are composite numbers n for which there does not exist any witness.

Such composite numbers are called "Carmichael numbers".