Finding a generator in a cyclic group

We will be concerned about finding a generator over arbitrary cyclic group of order q, where q not necessarily a prime number.

- Our approach: We will randomly sample an element, say x, and check whether $x \in \mathbb{G}$ and x is a generator of $\mathbb{G}$ or not.

① How to efficiently test that whether a given element is a generator of the given cyclic group G.

② Fraction of elements which are generators of G.

Thm: Let G be a cyclic group of order $q \geq 1$. with a generator g. Then there are $\phi(q)$ generators in G, namely all the elements of the set $\{g^x : \gcd(x,q)=1\}$.

Pf: Suppose $h \in G$ $\quad x = d\alpha$

Therefore $h = g^x$. $\quad q = d\beta$.

Suppose $\gcd(x,q) = d > 1$

Compute $h^\beta = g^{x\beta} = g^{d\alpha\beta} = (g^{d\beta})^\alpha = (g^q)^\alpha = 1$

order of $h \leq \beta < q$

Therefore h is not a generator.

- If $\gcd(x, q) = 1$

Let i be the order of h, where $i \leq q$.

$h^i = 1$

Then $g^0 = 1 = h^i = g^{xi}$

We know that order of g is q.

$\Rightarrow q \mid xi \Rightarrow q \mid i \Leftrightarrow i = q$.

Therefore h is a generator of G.

Conclusion:

$h, h^2, h^3 \ldots\ldots h^q$

If $\gcd(x, q) = 1$, then $h = g^x$ is a generator of G

Since # of elements which are co prime to q in $\phi(q)$, the no. of generators of G is $\phi(q)$.

Given an element $h \in G$, how do you check whether h is a generator or not ?

The obvious choice does not work !

– Suppose you know one of the generators of G. let 'g' be a generator of G.
Then given $h \in G$, how do you determine whether h is a generator or not.'

Since $h \in G \Rightarrow h = g^x$
Check whether $\gcd(x, qv) = 1$ }

$x = \log_g h$ (Hard to compute)

- If we know the factorization of q, then the problem is easy.

Thm: Let G be a cyclic group of order q and $q = \prod_{i=1}^{k} p_i^{e_i}$, where $\{p_i\}_{i=1}^{k}$ are the distinct primes and $e_i \geq 1$. Let $q_i = q/p_i$ for all $i = 1, \ldots, k$. Then $h \in G$ is a generator iff

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

h is a generator of $G \Rightarrow \forall i = 1, \ldots k \quad h^{\frac{q}{p_i}} \neq 1 \bmod q$.

Suppose $\exists i$ such that

$h^{\frac{q}{p_i}} = 1 \bmod q$ (Trivial).

$\forall i = 1 \ldots k \quad h^{\frac{q}{p_i}} \neq 1 \bmod q \Rightarrow h$ is a generator.

Suppose h is not a generator of G.

$\text{ord}(h) = q' < q$.

$\Rightarrow q' \mid$ order of $G = q' \mid q \Rightarrow q' = \prod_{i=1}^{k} p_i^{e_i'}$ where $e_i \geq 0$ and there exists at least one index j such that $e_j' < e_j$

Then, q' divide $q_j = p_j^{e_j - 1} \prod_{i \neq j}^{k} p_i^{e_i}$

Now you compute

$$h^{q_j} = h^{q_j \bmod q'} = h^0 = \underline{1}$$

So, we find a q_j such that $h^{q_j} = \underline{1} \bmod q'$.

Algorithm:

Input: Cyclic group G and it's order q and also the prime factors $p_1 \dots p_k$, and $h \in G$.

output: A decision as to whether h is a generator.

for all $i = 1, \ldots K$

set $q_i = q / p_i$

if $h^{q_i} \equiv 1 \bmod q$, return "not a generator"

return h is a generator.

$O(\|q_i\|)$.

Time complexity $\|q\| \cdot O(\|q\|) = O(\|q\|^2)$.

Claim: $K \le \log_2 q$

Pf: $q = \prod_{i=1}^{K} p_i^{e_i} \ge \prod_{i=1}^{K} p_i \ge \prod_{i=1}^{K} 2 = 2^K$

The no. of generators of a cyclic group is $\phi(q)$.

Therefore, the prob. that a randomly sampled group element will be a generator is $\frac{\phi(q)}{q} \geq \frac{1}{2\|q\|}$

PRIMALITY TESTING ALGORITHM:

Suppose N is prime and $a \in \mathbb{Z}_N^* = \{1, \ldots N-1\}$

then $a^{N-1} \equiv 1 \bmod N$.

N is a prime $\Rightarrow \forall a \in \mathbb{Z}_N^* \quad a^{N-1} \equiv 1 \bmod N$

$\exists a \in \mathbb{Z}_N^* : a^{N-1} \not\equiv 1 \bmod N \Rightarrow N$ is not a prime.

Algorithm

Input: N

output: A decision whether N is prime or not

for $i = 1$ to t

$a \leftarrow \$ \{1, \ldots, N-1\}$

if $\gcd(a, N) \neq 1$, return "composite"

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

Return "prime".

Such a for which
$a^{N-1} \not\equiv 1 \bmod N$ is called a witness that
N is a composite number.

- Suppose, N is a prime number.

Co-RP Primality test $\in$ Co-RP.

$P \in$ Co-RP then $A(P) = 1$ always.

$P \notin$ Co-RP then $A(P) = 1$ with some prob.

Such a for which
$a^{N-1} \not\equiv 1 \bmod N$ is called a witness that
N is a composite number.

- Suppose, N is a prime number.
Then the alg. always outputs prime.
- Suppose N is a composite number.

Such a for which
$a^{N-1} \not\equiv 1 \bmod N$ is called a witness that
N is a composite number.

- Suppose, N is a prime number.
Then the alg. always outputs prime.
- Suppose N is a composite number.

We hope that when N is composite, then there are many witnesses, so that at every iteration the alg finds such a witness with high prob

Prop: Let G be a group and $H \subseteq G$. If H contains e and for all $a, b \in H$, $ab \in H$, $\Rightarrow H$ is a subgroup of G.

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

Thm: Let N be a positive integer. Assume that there exists a witness that N is composite. Then at least half of the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

Pf: $Bad = \{a \in \mathbb{Z}_N^* : a^{N-1} \equiv 1 \bmod N\}$.

Prove that Bad is a strict subgroup of $\mathbb{Z}_N^*$

$\Rightarrow |Bad| \leq |\mathbb{Z}_N^*|/2$

Therefore, the number of witnes that N is composite is at least $|\mathbb{Z}_N^*|/2$.

Conclusion: If $\exists$ a witnes that N is composite, then there are at least $|\mathbb{Z}_N^*|/2$ witneses that N is composite.

what is the prob. that the alg. either finds a witness. or find an a not in $\mathbb{Z}_N^*$

$$\#\text{ of witnesses} \geq |\mathbb{Z}_N^*|/2$$

# of elements in $\{1, \ldots, N-1\}$ that is not coprime to N is $(N-1) - |\mathbb{Z}_N^*|$

$$\text{Therefore the prob} \geq \frac{|\mathbb{Z}_N^*|/2 + (N-1) - |\mathbb{Z}_N^*|}{N-1}$$

$$= 1 - \frac{|\mathbb{Z}_N^*|}{2(N-1)} \geq 1 - \frac{|\mathbb{Z}_N^*|}{2|\mathbb{Z}_N^*|} \quad \left(\because (N-1) \geq |\mathbb{Z}_N^*| \right)$$

$$= 1/2$$

Therefore the alg. does not find a witness. and any a such that $\gcd(a, N) \neq 1$ in any of the t-iterations is at most $1/2$.

Therefore, the failure prob is at most $\frac{1}{2^t}$

The solution is not complete.

'561' → Such composite numbers are Carmichael numbers.

$N-1 = 2^r u$

$a^{2^r u} \equiv 1 \bmod N$

$a^u, a^{2u}, a^{4u} \ldots$