Generating Big Random Primes

To generate a random 500 bits prime:
1. Pick a random odd number $2^{499} < n < 2^{500}$.
2. Check whether $n$ is prime
3. If $n$ is not prime, go to step 1.

The number of repetitions depends on how many prime numbers are there between $2^{499}$ and $2^{500}$.
There are about $n = \ln n$ primes between 2 and $n$.
There are about $n/2 \ln n$ primes between $n/2$ and $n$.
By picking a random odd number, there is a chance in $\ln n$ of picking a prime.
There are efficient $O((\log n)^3)$ time algorithms to check whether $n$ is prime. The algorithms use randomness.

General Idea for Randomized Primality Testing

On input a big integer $n$, want to decide whether it’s prime or composite.
Use randomness.
Look for "evidence" that $n$ is composite.
If can find evidence, say that $n$ is composite. Otherwise say that $n$ is prime.

Fermat’s Little Theorem

If $n$ is prime, then for every $a \in \mathbb{Z}_n^*$,

$$a^{n-1} \equiv 1 \pmod{n}$$

If, on input $n$, we find an $a$ such that $a^{n-1} \neq 1 \pmod{n}$, then this proves that $n$ is not prime.

Not a Necessary Condition

There are integers $n$ (e.g. 561) that are not prime, yet for every $a \in \mathbb{Z}_n$, $a \neq 0$, we have $a^{n-1} \equiv 1 \pmod{n}$.
They are called Carmichael Numbers, and there are infinitely many (but they are rare).

**Theorem:** If $n$ is a Carmichael number, it cannot be a power of a prime.
Modular Square Roots

If $n$ is prime, then the equation

$$x^2 = 1 \pmod{n}$$

has only two solutions in $\mathbb{Z}_n$: $x = 1$ and $x = (-1 \pmod{n})$.

If, on input $n$, we find an $a$ such that $a \neq 1 \pmod{n}$, $a \neq -1 \pmod{n}$, but $a^2 = 1 \pmod{n}$, then this proves that $n$ is not prime.

Rabin-Miller Test

On input integer $n$:

Pick a random $a$ in $\{1, \ldots, n-1\}$.

Compute $a^{n-1} \pmod{n}$ using the modular exponentiation algorithm (with repeated squaring).

If find nontrivial root of 1 at some stage of modular exponentiation, output composite. If $a^{n-1} \neq 1 \pmod{n}$, output prime.

Correctness

If $n$ is prime, then no matter how we choose $a$, the algorithm output the right answer, because it can never find a $a$ such that $a^{n-1} \neq 1 \pmod{n}$ and it can never find a non-trivial root of 1.

If $n$ is composite, we want to prove that are choices of $a$ for which the algorithm gives the right answer, and in fact the right answer is given with probability $> 1/2$.

Analysis of Error Probability in Miller-Rabin

Fix a composite $n$.

Consider the set $B$ of bad choices of $a$ such that MillerRabin says that $n$ is prime when the random choice $a$ is made.

We want to prove $B < (n-1)/2$. We do so by proving that $B$ is always contained in a proper subgroup of $\mathbb{Z}_n^*$.
**Group**

A group is a set $G$ with an operation $\otimes$, that given two elements of $G$ returns an element of $G$ such that

1. For every $a, b \in G$, $a \otimes b = b \otimes a$;
2. For every $a, b, c \in G$, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$;
3. There exists an element $u \in G$ such that for every $a \in G$, $a \otimes u = u \otimes a = a$;
4. For every element $a \in G$ there exists an element $a^0 \in G$ such that $a \otimes a^0 = u$.

**Examples**

- $\mathbb{Z}_n$ with the operation $\cdot + \mod n$ is a group, $u = 0$.
- $\mathbb{Z}_n^*$ with the operation $\cdot \mod n$ is a group, $u = 1$.

**Subgroup**

Let $G$ be a group with operation $\otimes$.

A subset $S \subset G$ is a subgroup if $u \in S$, and for every $a, b \in S$ we have $a \otimes b \in S$ and also $a^0, b^0 \in S$.

If $G$ is a group and $S$ is a subgroup of $G$, then $S$ is also a group.

**Theorem:** If $S$ is a subgroup of $G$ then $|S|$ divides $|G|$.

**Proof of Fermat’s Little Theorem**

Let $n$ be prime.

Fix an element $a \in \mathbb{Z}_n^*$.

Consider the set $\{1, a, a^2 \mod n, a^3 \mod n, \ldots\}$ of all possible powers of $a$. It is a subset of $\mathbb{Z}_n^*$, and so it is finite.

Then, at some point, we get a power that we have already seen: there are $s, r$, $0 \leq r < s \leq n - 1$ such that $a^s = a^r \mod n$.

**Size of $B$, first case**

Suppose $n$ is composite and is not a Carmichael number. Then there is some $a \in \mathbb{Z}_n^*$ such that $a^{n-1} \not\equiv 1 \mod n$.

Define the set $G := \{a : a^{n-1} = 1 \mod n\}$. This is a subgroup of $\mathbb{Z}_n^*$ (verify) and it is a proper subgroup. Then $|G| \leq |\mathbb{Z}_n^*|/2 < (n-1)/2$.

And also $B \subseteq G$, so $|B| < (n-1)/2$. 

**Size of B, second case**

Suppose $n$ is a Carmichael number.

Then $n$ has at least two different prime factors. We can write $n = n_1n_2$ where $\gcd(n_1, n_2) = 1$.

Let $t$ be the number of consecutive zeroes in the least significant digits of $n - 1$, i.e. write $n - 1 = 2^t u$ where $u$ is odd.

For each $a$ that could be picked at random in RabinMiller, consider the sequence

$$(a^u \mod n, a^{2u} \mod n, a^{4u} \mod n, \ldots, a^{2^t u} \mod n)$$

These are intermediate values computed during the computation of $a^{n-1} \mod n$.

Consider the largest $j$ such that there is a $v$ such that $v^{2^j u} = -1 \pmod{n}$. Fix the corresponding $v$.

Define $G = \{ a : a^{2^j u} = \pm 1 \pmod{n} \}$.

Then:
- $B \subseteq G$,
- $G$ is a subgroup of $\mathbb{Z}_n^*$,
- there is an element $w \in \mathbb{Z}_n^*$ such that $w \notin G$.

**Proving that $G \neq \mathbb{Z}_n^*$**

Consider the system

$$\begin{align*}
x &= v \pmod{n_1} \\
x &= 1 \pmod{n_2}
\end{align*}$$

There is a $w \in \mathbb{Z}_n^*$ that satisfies the system.

When we raise $w$ to $2^j u$ we have

$$\begin{align*}
w^{2^j u} &= -1 \pmod{n_1} \\
w^{2^j u} &= 1 \pmod{n_2}
\end{align*}$$

So it is impossible that $w^{2^j u} = 1 \pmod{n}$ or that $w^{2^j u} = -1 \pmod{n}$.

Then $w \notin G$.

**Error Probability**

Then for every composite $n$, the probability that Miller-Rabin makes a mistake (i.e. says that $n$ is prime) is $< 1/2$.

If we take $k$ Miller-Rabin tests, and say that $n$ is prime iff all $k$ tests indicate that is prime, then the probability of making a mistake becomes $1/2^k$.

Using $k = 50$ gives very high confidence.