PROVING AN INTEGER IS COMPOSITE

Given $n$, choose $a$, $1 < a < n$. If

$$a^{n-1} \not\equiv 1 \ (\text{mod} \ n)$$

then FLT fails for this value of $a$. Hence $n$ is composite and $a$ is called a Fermat witness for $n$.

If $a^{n-1} \equiv 1 \ (\text{mod} \ n)$ we can continue with the Miller-Rabin Test. Since $n - 1$ is even we can write it as

$$n - 1 = 2^k \cdot q \quad \text{with} \ q \text{ odd}$$

Then, if none of the congruences

$$a^q \equiv 1 \ (\text{mod} \ n)$$
$$a^{2^i q} \equiv -1 \ (\text{mod} \ n) \quad 0 \leq i < k$$

are satisfied then $n$ is composite.

Reason: If $d$ is even we have the factorization $x^d - 1 = (x^{d/2} + 1)(x^{d/2} - 1)$. Applying this repeatedly to $x^{n-1} - 1$ we get the factorization

$$x^{n-1} - 1 = (x^{2^{k-1}q} + 1)(x^{2^{k-2}q} + 1) \cdots (x^q + 1)(x^q - 1)$$

If $n$ were prime, then $a$ is a root of the polynomial $x^{n-1} - 1$ in $\mathbb{Z}_p$ by FLT. Hence it must be a root of one of the polynomials on the right. This implies one of the congruences is satisfied. Hence if none of the congruences is satisfied, $n$ must be composite.

Another way of seeing this shows that $n$ is composite is by showing it produces a square root of 1 other than $\pm 1$. The reason for this is that if for some $1 \leq i \leq k$

$$a^{2^i q} \equiv 1 \ (\text{mod} \ n)$$
$$a^{2^{i-1}q} \not\equiv \pm 1 \ (\text{mod} \ n)$$

then letting $b \equiv a^{2^{i-1}q} \ (\text{mod} \ n)$ we would get $b^2 \equiv 1 \ (\text{mod} \ n)$ since

$$b^2 \equiv (a^{2^{i-1}q})^2 \equiv a^{2^i q} \equiv 1 \ (\text{mod} \ n)$$

Hence the polynomial $x^2 \equiv 1 \ (\text{mod} \ n)$ would have a solution other than $\pm 1 \ (\text{mod} \ n)$, which cannot occur if $n$ is prime.

If the value $a$ shows $n$ is composite, then $a$ is called a Miller-Rabin witness for $n$. If the value $a$ satisfies one of the congruences, i.e. does not show $a$ is composite, then $a$ is called a misleder. The probability that a randomly chosen $a$ will be a misleder is $< 1/4$, so i.e. if we choose 100 different values of $a$, and none of these values show $n$ is composite, then the chances of $n$ being composite is $< 1/4^{100}$ which is extremely low. Although we can’t prove a number is prime using Miller-Rabin, such a number would be classified as probably prime. We could then try to show it is prime using the procedure on the reverse.
PROVING AN INTEGER IS PRIME

TEST TO SHOW A NUMBER IS PRIME: If $1 < a < n$

$$a^{(n-1)} \equiv 1 \ (mod \ n)$$

and

$$a^{(n-1)/q} \not\equiv 1 \ (mod \ n)$$

for all primes $q$ dividing $n - 1$ then $n$ is a prime number and $a$ is a primitive root for $n$.

REASON:

If the above is satisfied then the smallest exponent $e$ that satisfies $a^e \equiv 1 \ (mod \ n)$, called $ord_n(e)$, must divide $n - 1$. If it is not $n - 1$ it must divide $(n - 1)/q$ for some prime $q$ dividing $n - 1$. But then $a^{(n-1)/q} \equiv 1 \ (mod \ n)$. Thus if $a^{(n-1)/q} \not\equiv 1 \ (mod \ n)$ for all primes $q$ dividing $n$ we must have $e = n - 1$. But we also know that $e = ord_n(a)$ has the property that $e \leq \phi(n)$. However $\phi(n) \leq n - 1$ and $\phi(n) = n - 1$ only if $n$ is prime. Hence we conclude that $n$ must be prime and $a$ is a primitive root for $n$.

NOTE: Recall that if $n$ is prime, a primitive root is a value $a$ with $ord_n(a) = n - 1$. What we are really doing is showing $n$ is prime by finding a primitive root.

One can give a simple proof that an integer $n$ is prime by giving the value of $a$ and the factorization of $n - 1$, then anyone with a computer can easily verify the above congruences.

The main problem with applying the above test is that one has to factor $n - 1$. One is helped by the fact that $n - 1$ is even, however it might have large factors that one can’t be sure are prime or composite. Thus a proof that the integer $n$ is prime might include proofs that the factors of $n - 1$ are prime, and one might need to keep repeating the above test until one is finally reduced to factors one can be sure are prime. Such a proof is called a Pratt certificate.

EXAMPLE: Fermat numbers are of the form:

$$n = 2^{2^k} + 1 \text{ for some } k \geq 0$$

Fermat conjectured these numbers are all prime. Note that the only prime dividing $n - 1$ is 2, so the above test can be easily applied. As an example, let

$$n = 2^{2^4} + 1 = 65,537$$

$$n - 1 = 2^{2^4} = 2^{16} \text{ so } (n - 1)/2 = 2^{15}.$$  We have

$$5^{2^{16}} \equiv 1 \ (mod \ n) \text{ but } 5^{2^{15}} \not\equiv 1 \ (mod \ n)$$

Thus $n = 2^{2^4} + 1$ is prime and 5 is a primitive root. In this case the proof that $n$ is prime can simply be given by:

$$a = 5, \ n - 1 = 2^{16}$$