TESTING FOR PRIMALITY

Definition : ——————————————————————————————————————
Property :
any positive odd integer $n \geqslant 3$ *can be expressed as* $n - 1 = 2^k q$ *with* $k > 0,\ q$ *odd.*

Proof :
if $n \geqslant 3$ *and* n *is odd, obviously* $n - 1$ *is even we will start deviding by* 2 *untill we have it odd again some* k *time wich gives* $n - 1 = 2^k q$ *with* $k > 0,\ q$ *odd.*

Property :
if p *is prime and* a *is a positive integer less then* $p,\ a^2 \bmod p = 1$ *if and only if* $a \bmod p = 1$ *or* $a \bmod p = -1 = p - 1.$

Proof :
for p *is prime and* a *is a positive integer less then* p, *if* $a^2 \bmod p = 1$ *then* $a^2 \equiv 1 \bmod p$ *which implies* $\left(a^2 - 1\right) \equiv 0 \bmod p$ *that means* $p|(a+1) \times (a-1)$ *because* $1 \leqslant a \leqslant p - 1$ *and* p *is prime, the only two value we can achiver with* $a + 1$ *and* $a - 1$ *that can be devid* p *and doesn't contradict the condition above, its* 0 *or* p *so if* $p|(a+1)$ *then* $p = (a+1)$, *hence* $a = p - 1$ *or* $p|(a-1)$ *then* $0 = (a-1)$, *hence* $a = 1$, *which gives* $a \bmod p = 1$ *or* $a \bmod p = -1 = p - 1$, *now if* $a \bmod p = 1$ *or* $a \bmod p = -1 = p - 1$, *then* $(a \bmod p)^2 = 1$ *by the modulo arithmetic's* $(a \bmod p)^2 \equiv 1 \bmod p$ *implyes* $a^2 \bmod p = 1 \bmod p = 1.$

Property :
let p *be a prime number with* $p > 2$. *Miller–Rabin Algorithm* $p - 1 = 2^k q$ *with* $k > 0$ *and* q *odd, and let* a *be in the range* $1 < a < p - 1$ *one of the following statement is true*
1. $a^q \equiv 1 (\bmod p)$
2. *There is some number* j *in the range* $1 \leqslant j \leqslant k$ *such that* $a^{2^{j-1} q} \bmod p = -1 (\bmod p) = p - 1$

Proof :
let p *be a prime number with* $p > 2$. *Miller–Rabin Algorithm* $p - 1 = 2^k q$ *with* $k > 0$ *and* q *odd, and let* a *be in the range* $1 < a < p - 1$, *by Fermat' theorem* $a^{p-1} \equiv 1 (\bmod p)$, *that means* $a^{2^k q} \equiv 1 \bmod p$, *we take* $x_k = a^{2^k q}$, *we notice* $x_0 = a^q$ *and* $x_{k+1} = (x_k)^2$, *if* $x_0 \equiv 1 \bmod p$, *then all the others will verify it, if* $x_0 \not\equiv 1 \bmod p$ *let* $1 \leqslant j \leqslant k$ *be the minimal index that verify* $x_j \bmod p = 1$, *that means* $x_{j-1} \bmod p \neq 1$ *but we have* $x_j = (x_{j-1})^2$ *so by the first property* $x_{j-1} \bmod p = 1$ *or* $x_{j-1} \bmod p = -1$ *the first is imposible because* $x_{j-1} \bmod p \neq 1$, *hence* $x_{j-1} \bmod p = -1 \bmod p = p - 1.$
——