# Rabin-Miller-Test

(explanation)

## Usage in SICP

1. Pick random integer $a < n$ .
2. Calculate $a^{n-1} \, mod \, n$ using fast exponentiation method, which uses the congruence regarding modulo $n$ to keep them low.
    1. When calculating the square in fast exponentiation, check for non-trivial square roots of 1 regarding modulo a number.

## Definitions

### Fermat’s Little Theorem

If $n$ is prime and $a \in \mathbb{N} \wedge a < n$ then $a^{n-1} \equiv 1 (mod \, n)$ .

## Proof 1 (Homomorphic Rule for Multiplication)

For: $(ab) \operatorname{mod} p = ((a \operatorname{mod} p) \cdot (b \operatorname{mod} p)) \operatorname{mod} p$

If (a mod p) is the remainder of a division a / p then there is an a_i for which:

$$a_i \, p + (a \operatorname{mod} p) = a$$

(the a_i, which is the integer quotient, needed to add up to the dividend again!)

For b the same:

$$b_i \, p + (b \operatorname{mod} p) = b$$

Now we multiply a and b by using the binomial formula.

$$\begin{array}{rcll} ab & = & [a_i p + (a \operatorname{mod} p)] \cdot [b_i p + (b \operatorname{mod} p)] & | \text{ binom. formula} \\ & = & [a_i p \, b_i \, p] + [a_i p \, (b \operatorname{mod} p)] + [b_i \, p (a \operatorname{mod} \ p)] + [(a \operatorname{mod} p) \cdot (b \operatorname{mod} p)] & | \text{ simplify: } pp = p^2 \\ & = & [a_i b_i p^2] + [a_i \, p (b \operatorname{mod} p)] + [b_i \, p (a \operatorname{mod} \ p)] + [(a \operatorname{mod} p) \cdot (b \operatorname{mod} p)] & | \end{array}$$

In this term we can see that the first three summands each contain a factor $p$ , which means, that they are divided by $p$ :

$$p | a_i b_i p^2$$
$$p | a_i \, p \, (b \operatorname{mod} p)$$
$$p | b_i \, p \, (a \operatorname{mod} \ p)$$

This means only the last summand matters for determining whether the sum is divided by $p$ .

This means if we already know, that $p|ab$ , then $p \mid (a \bmod p)(b \bmod p)$ .

We can weaken the equivalence to a congruence writing it with modulo:

$$ab \equiv \left[a_i b_i p^2 + a_i p(b \bmod p) + b_i p(a \bmod p) + (a \bmod p) \cdot (b \bmod p)\right] \pmod p$$

Now the first three parts we can leave away, because they contain $p$ anyway:

$$ab \equiv \left[(a \bmod p) \cdot (b \bmod p)\right] \pmod p$$

Rewrite this interpreting mod as an infix operator:

$$ab \bmod p = ((a \bmod p) \cdot (b \bmod p)) \bmod p$$

Which is exactly what we wanted to prove.

Furthermore we can add summands on both sides:

$$ab + 1 \bmod p = ((a \bmod p) \cdot (b \bmod p) + 1) \bmod p$$

# Proof 2 (can take out the square in exponentiation)

We want to reduce computation costs in case of even exponent.

Instead of $n^{2a} \bmod p$ we want to calculate $(n^a \bmod p)^2 \bmod p$ . Since the exponent is only half as big, the computation will not take as long. Only after we calculated the remainder in the mod step, we square the term. To be sure, that we are still in the range of possible remainders, we do mod $p$ again.

But are the two terms equivalent?

The question is: $n^{2a} \equiv (n^a \bmod p)^2 \pmod p$ ?

We can write $n^{2a}$ as $n^a \cdot n^a$ and then substitute with $a$ and $b$ :

$n^a \cdot n^a \equiv a \cdot b \equiv (a\ mod\ p) \cdot (b\ mod\ p) \pmod p$ . This is exactly what we already proved in proof 1:

$$ab \equiv \left[(a \bmod p) \cdot (b \bmod p)\right] \pmod p \quad .$$

And so: $n^{2a} \equiv (n^a\ mod\ p)^2 \pmod p$ . QED