Lehmann primality test

Lehmann test is a primality test – it determines whether the given integer is composite or a prime.

Description

Little Fermat's theorem states that for every prime p it holds that

$$a^{p-1} \equiv 1 \mod p$$

Hence it also holds

$$a^{p-1} - 1 \equiv 0 \mod p$$

If we use the formula $A^2 - B^2 = (A - B) \cdot (A + B)$ to expand the expression, we get

$$a^{p-1} - 1 = (a^{(p-1)/2} - 1) \cdot (a^{(p-1)/2} + 1)$$

From divisibility of numbers, we know

$$p \mid (x \cdot y) \Rightarrow (p \mid x) \vee (p \mid y)$$

So, if the equation $a^{p-1} - 1 \equiv 0 \mod p$ holds, than one of the following conditions must also hold

$$\begin{aligned} a^{(p-1)/2} - 1 \equiv 0 \mod p \quad &\Rightarrow \quad a^{(p-1)/2} \equiv 1 \mod p \quad \Rightarrow \quad a^{(p-1)/2} = 1 \;\; in \;\; Z_p \\ a^{(p-1)/2} + 1 \equiv 0 \mod p \quad &\Rightarrow \quad a^{(p-1)/2} \equiv -1 \mod p \quad \Rightarrow \quad a^{(p-1)/2} = -1 = p - 1 \;\; in \end{aligned}$$

Finally, provided that

$$a^{(p-1)/2} = 1 \;\; in \;\; Z_p \quad \vee \quad a^{(p-1)/2} = -1 = p - 1 \;\; in \;\; Z_p$$

than p may be a prime. In any other case p is a composite number, because it contradicts the Little Fermat's theorem. It can be shown that every iteration of Lehmann test eliminates at least fifty percent of composite numbers.

Probability that the number is a prime after k iterations of Lehmann test can be expressed as

$$p = 1 - \frac{1}{2^k}$$

– Pavel Mička

Founder and administrator of web encyclopedia Algoritmy.net