Lehman’s Primality Test

Lehman’s primality test

- Lehmann test is a primality test; it determines probalistically whether a given integer is composite or a prime.
- The algorithm:

  Let n be an odd number. For any random number a in Z_n^*define:

$$e(a,n) = a^{\frac{n-1}{2}}\, mod\, n$$

$$G = \{e(a,n)\}: G, \boldsymbol{a} \in \boldsymbol{Z_n^*}$$

  Where $Z_n^* = \{1, 2, \dots, n-1\}$.

Lehman's test

- Example: n=7, a = {2, 3, 4, 5, 6}

$$2^{\frac{7-1}{2}} = 1\,mod\,7 = 1,$$
$$3^3 = 6\,mod\,7 = 6,$$
$$4^3 = 1\,mod\,7 = 1,$$
$$5^3 = 6\,mod\,7 = 6,$$
$$6^3 = 6\,mod\,7 = 6.$$

- Example: n=15, a = {2, 3, 4, 5, 6}

$$2^{\frac{15-1}{2}} = 8\,mod\,15 = 8$$ Composite
$$3^7 = 12\,mod\,15,$$
$$4^7 = 4\,mod\,15,$$
$$5^7 = 5\,mod\,15,$$
$$6^7 = 6\,mod\,15.$$

Once a composite result is obtained, the test can stop because the number has failed the test.

- Thus, we have the following test:

```
if (gcd(a,n) >1) return('composite')
else
   if ($a^{(n-1)/2}=1$) or ($a^{(n-1)/2}=-1$)
         return('prime witness')
   else
         return('composite')
```

If for a given $\boldsymbol{n}$ the test returns prime witness for 100 randomly chosen $\boldsymbol{a}$, then the probability of $\boldsymbol{n}$ not being not prime (i.e. being a composite disguised as a prime) is less than 2^{-100}.