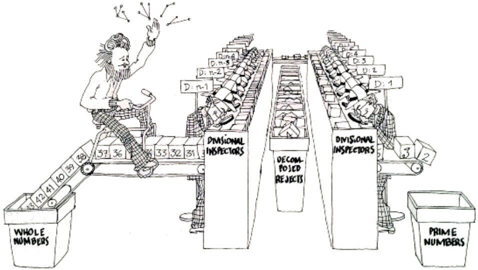
Primality Test - RECAP



Curiosities about known prime numbers

As of January 2014, the largest known prime number is the *Mersenne* prime $2^{57885161} - 1$. This number has 17 425 170 decimal digits.

Fact

Even though we have proven that there are infinitely many primes, there is no known useful formula (algorithm) to define (find) all of the prime numbers.

Question: How to find *new* prime numbers?

Answer: Pick a random integer $N \in \mathbb{Z}$ and *test* whether it is prime.

Probabilistic tests

FACTs

The problem to decide whether a given integer N is a prime or not was recently shown to be in **P** (Manindra Agrawal et al. 2002)

However, this has not yet resulted in efficient tests.

In practice, one uses probabilistic tests. These may erroneously claim that a composite number is prime, but the probability for this can be made arbitrarily small.

Fermat's primality test

The idea behind the algorithm

Fermat's Little Theorem states that:

$$p \text{ prime} \implies a^{p-1} \bmod p = 1, \ \forall a \in \mathbb{Z}_p^* \ .$$

Thus, Fermat's test for primeness of an integer $n \in \mathbb{Z}$ runs as follows:

1. Pick random $a \in \mathbb{Z}$ and compute $a^{n-1} \bmod n$.
2. If result is $\neq 1$, declare n composite.
3. Repeat the above steps t times; if all results are 1, declare n prime.

Running time

Using fast algorithms for modular exponentiation, the running time of this algorithm is $O\big(t \log^2(n) \log(\log n) \log(\log(\log n))\big)$, where t is the number of times we test a random element a, and n is the number we want to test for primality.

Fermat's primality test

By choosing t suitably big, one hopes to bound probability that the test returns n prime even if n is composite.

However:

Carmichael numbers

There are (rare) composite numbers n, called **Carmichael numbers**, for which $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ for all $a \in \mathbb{Z}_n^*$.

The three smallest Carmichael numbers are $561, 1105, 1729$.
It is proven that there are infinitely many Carmichael numbers!