1 Pseudoprimes

1.1 Fermat Pseudoprimes

Pierre de Fermat (1607-1665) proved a the following theorem:

Theorem 1 (Fermat's Little Theorem)**.** *Let n be prime. Then for any integer a,*

$$a^n \equiv a \pmod{n}. \tag{1}$$

Introducing the concept of a probable prime:

Definition 1 (Probable Prime)**.** *An integer n is called a **probable prime** base a for an integer a, if 1 holds.*

A **(Fermat-) Pseudoprime** is a composite number that is a probable prime.
Fermat Pseudoprimes are sparsely distributed compared to actual primes:

Theorem 2. *For a fixed integer $a \geq 2$, the number of Fermat pseudoprimes base a not exceeding x is*

$$o(\pi(x)) \quad \text{as} \quad x \to \infty,$$

where $\pi(x)$ is the number of primes not exceeding x.

There are also infinitely many Fermat Pseudoprimes for a given basis:

Theorem 3 (Infinitude of Fermat Pseudoprimes)**.** *For each integer $a \geq 2$, there are infinitely many pseudoprimes base a.*

1.2 Carmichael Numbers

There are composite integers that are pseudoprimes to any basis a:

Definition 2 (Carmichael Numbers)**.** *A composite integer n for which*

$$a^n \equiv a \pmod{n}$$

holds for all integers a is called a Carmichael number.

Unfortunately for primality testing, there are infinitely many Carmichael numbers:

Theorem 4 (Infinitude of Carmichael Numbers)**.** *There are infinitely many Carmichael numbers. In particular for x sufficiently large, the number $C(x)$ of Carmichael number exceeding x satisfies*

$$C(x) > x^{2/7}.$$

2 Strong Probable Primes and Witnesses

There is another group of pseudoprimes, which is a subset of the Fermat-pseudoprimes. We again need the following statement, which serves a very similar purpose as Fermat's Little Theorem:

Theorem 5. *Let n be an odd prime represented as $n = t \cdot 2^s + 1$ with t odd. If n does not divide a, then*

$$\begin{cases} \text{either } a^t \equiv 1 \pmod{n} \\ \text{or} \quad a^{2^i t} \equiv -1 \pmod{n} \quad \text{for some } 0 \leq i \leq s-1. \end{cases} \tag{2}$$

We will now make the following definition:

Definition 3 (Strong Probable Prime)**.** *An odd integer $n > 3$ for which (2) holds for some basis $1 < a < n-1$ is called a **strong probable prime** base a.*

Analogously to Definition 1, we define a **strong pseudoprime** as a strong probable prime which is composite.
A key to identifying a strong probable prime is finding a witness:

Definition 4. *A **witness** for an odd composite integer n is a base a, $1 \leq a \leq n-1$ for which n is **not** a strong pseudoprime.*

Using Theorem 5, one can design the **Miller-Rabin-Test**, which takes an integer n and then checks for a random basis a, if n is composite or a strong probable prime base a.
The Miller-Rabin-Test runs in polynomial time and it can be shown, that the probability of this test failing to produce a witness when presented an odd composite integer $n > 9$ is smaller than $\frac{1}{4}$.
By repeating this algorithm k times independently, this probability is lowered to 4^{-k}. This is also true if the input is a Carmichael Number!

2.1 "Industrial-grade prime" generation

One can also use the Miller-Rabin-Test for **"Industrial-grade prime" generation**, i.e. for generating numbers that are likely to be prime.
The idea is to repeatedly generate an integer at random and check if it is composite using the Miller-Rabin-Test, until an integer passes the test.
The probability $P(k,T)$ of this algorithm generating a composite integer n is bounded: $P(k,T) \leq (\frac{1}{4})^T$.
In the case $T = 1$ it can be shown that if we choose k large enough, $P(k,1) \leq k^2 4^{2-\sqrt{k}}$. For specific k-values even better results are possible. Choosing $k = 500$ for example gives $P(500,1) \leq 4^{-28}$.