3.1 The Pseudoprime Test

How can we identify an integer as prime? The "naive" approach is trial divisions by all integers $\leq \sqrt{n}$, made perfect in the form of ERATOSTHENES sieve. An assessment of the cost shows that this approach is not efficient since $\sqrt{n} = \exp(\frac{1}{2}\log n)$ grows exponentially with the length $\log n$ of n.

An approach to identify primes without trial divisions is suggested by FERMAT's theorem: If n is prime, then $a^{n-1} \equiv 1 \pmod{n}$ for all $a = 1, \ldots, n-1$. Note that this is a necessary condition only, not a sufficient one. Thus we say that n is a (FERMAT) **pseudoprime to base** a if $a^{n-1} \equiv 1 \pmod{n}$. Hence a prime number is a pseudoprime to each base $a = 1, \ldots, n-1$.

Examples

1. The congruence $2^{14} \equiv 4 \pmod{15}$ shows that 15 is not prime.

2. We have $2^{340} \equiv 1 \pmod{341}$ although $341 = 11 \cdot 31$ is not prime. Anyway $3^{340} \equiv 56 \pmod{341}$, hence 341 fails the pseudoprime test to base 3.

The pseudoprime property is not sufficient for primality. Therefore we call n a CARMICHAEL **number** if n is a pseudoprime to each base a that is coprime with n, but n is not a prime.

Another way to express pseudoprimality is that the order of a in $\mathbb{M}_n$ divides $n-1$. Thus n is a CARMICHAEL number or prime if and only if $\lambda(n) \mid n-1$ with the CARMICHAEL function λ.

Unfortunately there are many CARMICHAEL numbers, so pseudoprimality cannot even considered as "almost sufficient" for primality. In 1992 ALFORD, GRANVILLE, and POMERANCE proved that there are infinitely many CARMICHAEL numbers.

The smallest CARMICHAEL number is $561 = 3 \cdot 11 \cdot 17$. This is a direct consequence of the next proposition.

Proposition 9 *A natural number n is a* CARMICHAEL *number if and only if it is not prime, squarefree, and $p-1 \mid n-1$ for each prime divisor p of n. An odd* CARMICHAEL *number has at least 3 prime factors.*

Proof. "$\Longrightarrow$": Let p be a prime divisor of n.

Assume $p^2|n$. Then $\mathbb{M}_n$ contains a subgroup isomorphic with $\mathbb{M}_{p^e}$ for some $e \geq 2$, hence by Proposition 18 in Appendix A.3 also a cyclic subgroup of order p. This leads to the contradiction $p \mid n-1$.

Since $\mathbb{M}_n$ contains a cyclic group of order $p-1$ it has an element a of order $p-1$, and $a^{n-1} \equiv 1 \pmod{n}$, hence $p-1 \mid n-1$.

"$\Longleftarrow$": Since n is squarefree by the chinese remainder theorem the multiplicative group $\mathbb{M}_n$ is the direct product of the cyclic groups $\mathbb{F}_p^\times$ where p runs through the prime divisors of n. Since all $p-1 \mid n-1$ the order of each element of $\mathbb{M}_n$ divides $n-1$.

Proof of the addendum: Let n be an odd CARMICHAEL number. Suppose $n = pq$ with two primes p and q, say $p < q$. Then $q-1 \mid n-1 = pq-1$, hence $p-1 \equiv pq-1 \equiv 0 \pmod{q-1}$. This contradicts $p < q$. $\diamond$