Frobenius Pseudoprimes

Let $f(x) \in \mathbf{Z}[x]$ be a monic polynomial of degree d with discriminant Δ. An odd integer $n > 1$ is said to pass the **Frobenius probable prime test** with respect to $f(x)$ if we have $\gcd(n, f(0)\Delta) = 1$, and n is declared to be a probable prime by the following algorithm. (Such an integer will be called a **Frobenius probable prime** with respect to $f(x)$.) All computations are done in $(\mathbf{Z}/n\mathbf{Z})[x]$.

Factorization Step Let $f_0(x) = f(x) \bmod n$. For $1 \leq i \leq d$, let $F_i(x) = \gcd(x^{n^i} - x, f_{i-1}(x))$, and let $f_i(x) = f_{i-1}(x)/F_i(x)$. If any of the gcds fail to exist, declare n to be composite and stop. If $f_d(x) \neq 1$, declare n to be composite and stop.

Frobenius Step For $2 \leq i \leq d$, compute $F_i(x^n) \bmod F_i(x)$. If it is nonzero for some i, declare n to be composite and stop.

Jacobi Step Let $S = \sum_{2|i} \deg(F_i(x))/i$.

If $(-1)^S \neq \left(\frac{\Delta}{n}\right)$, declare n to be composite and stop.

A Theorem in Analytic Number Theory

Let $f(t) \in \mathbf{Z}[t]$ be a monic polynomial with splitting field K, $[K : \mathbf{Q}] = n$. Then we have real numbers $x_{1/3}, \eta_{1/3} > 0$ and an integer $q_{1/3}(x) > \log x$, depending on K, such that the following statement holds. If $q \leq x^{\eta_{1/3}}$, $\gcd(a, q) = 1$, $q_{1/3}(x) \not| q$, $x \geq x_{1/3}$ and $x^{1/2} < y < x$, then the number of primes $p < y$ that are $a \bmod q$ and such that $f(t)$ splits into linear factors mod p (equivalently, p splits completely in K) is at least $\frac{1}{2\phi(q) n \pi(x)}$.