3.4 The Extended Riemann Hypothesis (ERH)

A **(complex) character** mod n is a function

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

with the properties:

1. χ has period n.
2. $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{Z}$.
3. $\chi(x) = 0$ if and only if $\mathrm{ggT}(x, n) > 1$.

The characters mod n bijectively correspond to the group homomorphisms

$$\bar{\chi} : \mathbb{M}_n \longrightarrow \mathbb{C}^\times$$

in a canonical way.

Examples are the **trivial character** $\chi(a) = 1$ for all a that are coprime with n, and the Jacobi **character** $\chi(a) = (\frac{a}{n})$ known from the theory of quadratic reciprocity, see Appendix A.5.

A character defines an **L-function** by the Dirichlet series

$$L_\chi(z) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^z}.$$

This series converges absolutely and locally uniformly in the half-plane $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 1\}$ because $a^{i \cdot \mathrm{Im}(z)} = e^{i \cdot \ln(a) \cdot \mathrm{Im}(z)}$ has absolute value 1, hence

$$\left| \frac{\chi(a)}{a^z} \right| = \left| \frac{\chi(a)}{a^{\mathrm{Re}(z)} \cdot a^{i \cdot \mathrm{Im}(z)}} \right| = \frac{1}{a^{\mathrm{Re}(z)}} \qquad \text{or} \qquad = 0.$$

It admits an analytic continuation to the right half-plane $\mathrm{Re}(z) > 0$ as a holomorphic function, except for the trivial character where 1 is a simple pole.

The function L_χ has the Riemann **property** if all its zeroes in the strip $0 < \mathrm{Re}(z) \le 1$ are on the line $\mathrm{Re}(z) = \frac{1}{2}$. The Riemann hypothesis states just this property for the Riemann zeta function, the **extended** Riemann **hypothesis (ERH)**, for all L-functions for characters mod n.

The zeta function is defined for $\mathrm{Re}(z) > 1$ by

$$\zeta(z) := \sum_{a=1}^{\infty} \frac{1}{a^z} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^z}}$$

where the last equation is Euler's product formula. Hence for the trivial character χ_1 mod n we have:

$$L_{\chi_1}(z) = \sum_{\gcd(a,n)=1} \frac{1}{a^z} \quad = \quad \zeta(z) \cdot \prod_{p|n \text{ prime}} \left(1 - \frac{1}{p^z}\right);$$

and this L-function has the same zeroes as ζ in $\mathrm{Re}(z) > 0$.

Proposition 11 (Ankeney/Montgomery/Bach) *Let* $c = 2/\ln(3)^2 = 1.65707\ldots$. *Let* χ *be a nontrivial character* $\bmod n$ *whose L-function* L_χ *has the* Riemann *property. Then there is a prime* $p < c \cdot \ln(n)^2$ *with* $\chi(p) \neq 1$.

We omit the proof.

Corollary 1 *Suppose ERH is true. Let* $G < \mathbb{M}_n$ *be a proper subgroup. Then there is a prime* p *with* $p < c \cdot \ln(n)^2$ *whose residue class* $\bmod n$ *is in the complement* $\mathbb{M}_n - G$.

Proof. There exists a nontrivial homomorphism $\mathbb{M}_n/G \longrightarrow \mathbb{C}^\times$, thus a character $\bmod n$ with $G \subseteq \ker \chi \subseteq \mathbb{M}_n$. $\diamond$

Proposition 12 (Miller) *Let the integer* $n \geq 3$ *be odd and a strong pseudoprime to all prime bases* $a < c \cdot \ln(n)^2$ *with* c *as in Proposition 11. Assume that the L-function of each character for each divisor of* n *has the* Riemann *property. Then* n *is prime.*

Proof. We first show that n is squarefree.

Assume $p^2 \mid n$ for some prime p. The multiplicative group $\mathbb{M}_{p^2}$ is cyclic of order $p(p-1)$. In particular the homomorphism

$$\mathbb{M}_{p^2} \longrightarrow \mathbb{M}_{p^2}, \quad a \mapsto a^{p-1} \bmod p^2,$$

is nontrivial. Its image is a subgroup $G < \mathbb{M}_{p^2}$ of order p, and is cyclic, hence isomorphic with the group of p-th roots of unity in $\mathbb{C}$. The composition of these two homomorphisms yields a character $\bmod p^2$. Thus Proposition 11 gives a prime $a < c \cdot \ln(p^2)^2$ with $a^{p-1} \not\equiv 1 \bmod p^2$. The order of a in $\mathbb{M}_{p^2}$ divides $p(p-1)$. Suppose $a^{n-1} \equiv 1 \bmod n$. Then the order also divides $n-1$. Since p is coprime with $n-1$ the order divides $p-1$, contradicting the definition of a. Hence $a^{n-1} \not\equiv 1 \bmod n$, and this in turn contradicts the strong pseudoprimality of n. Therefore n is squarefree.

Next we show that n doesn't have two different prime factors.

Assume p and q are two different prime divisors of n. Denote the 2-order of an integer x by $\nu_2(x)$. We may assume that $\nu_2(p-1) \geq \nu_2(q-1)$. Let

$$r = \begin{cases} p, & \text{if } \nu_2(p-1) > \nu_2(q-1), \\ pq, & \text{if } \nu_2(p-1) = \nu_2(q-1). \end{cases}$$

Again by Proposition 11 there is an $a < c \cdot \ln(r)^2$ with $(\frac{a}{r}) = -1$. If u is the odd part of $n-1$, and $b = a^u$, then also $(\frac{b}{r}) = -1$, in particular $b \neq 1$. By strong pseudoprimality there is a k with $b^{2^k} \equiv -1 \bmod n$. Thus b has order 2^{k+1} in $\mathbb{M}_p$ and in $\mathbb{M}_q$. In particular $2^{k+1} \mid q-1$.

In the case $\nu_2(p-1) > \nu_2(q-1)$ even $2^{k+1} \mid \frac{p-1}{2}$. We conclude $b^{(p-1)/2} \equiv 1 \pmod{p}$, but this contradicts $(\frac{b}{p}) = (\frac{b}{r}) = -1$ by EULER's criterion for quadratic residues.

In the case $\nu_2(p-1) = \nu_2(q-1)$ we have $(\frac{b}{p})(\frac{b}{q}) = (\frac{b}{r}) = -1$. Thus (without restriction) $(\frac{b}{p}) = -1$, $(\frac{b}{q}) = 1$. By EULER's criterion $b^{(q-1)/2} \equiv 1 \pmod{q}$, hence $2^{k+1} \mid \frac{q-1}{2}$, $k+2 \leq \nu_2(q-1) = \nu_2(p-1)$, hence also $b^{(p-1)/2} \equiv 1 \pmod{p}$, contradicting $(\frac{b}{p}) = -1$. $\diamond$

Therefore for MILLER's primality test it suffices to perform the strong pseudoprime test for all prime bases $a < c \cdot \ln(n)^2$. This makes total costs of $\mathrm{O}(\log(n)^5)$.

As an example, for a 512-bit integer, that is $n < 2^{512}$, testing the 18698 primes < 208704 is sufficient. Despite its efficiency this procedure takes some time. Therefore in practice this test is modified in way that is (in a sense yet to specify) not completely exact, but much faster. This is the subject of the next section.