TESTS FOR PRIMALITY UNDER THE RIEMANN HYPOTHESIS

Jacques Vélu (CNRS)

Ecole Polytechnique
Centre de Mathématiques
91128 - Palaiseau FRANCE

Abstract :

Assuming the extended Riemann hypothesis (ERH), G. Miller produced in a very interesting paper [1], an algorithm which tests primality and runs in $O((\log n)^{4+\varepsilon})$ *steps. We provide a short proof of this result.*

Let n be an odd integer and let $(Z/nZ)^x$ denote the multiplicative group of prime residue classes modulo n. The function $X_n : x \mapsto x^{\frac{n-1}{2}} (\frac{x}{n})$ mod n where $(\frac{x}{n})$ denotes the Jacobi symbol is an endomorphism of $(Z/nZ)^x$. R. Solovay and V. Strassen have shown in [3] the following

Theorem 1 : X_n trivial $\Leftrightarrow$ n prime.

On the other hand, the strengthening of Ankeny's theorem due to H. Montgomery [2] states :

Theorem 2 : If ERH is true, there exists a constant $c > 0$ such that for any integer $n \geq 1$, any abelian group G and any non-trivial homomorphism $X : (Z/nZ)^x \to G$, the least integer $x \geq 1$ such that $X(x)$ is non-trivial is $\leq C (\log n)^2$.

Our algorithm is as follows.

For each $x \leq C (\log n)^2$ compute the value $X_n(x)$. 1) If at any stage $X_n(x) \not\equiv 1 \pmod n$, we conclude that n is composite and we are done.

2) Otherwise n is prime.

Theorems 1 and 2 guarantee that this algorithm will work. Since $X_n(x)$ can be computed in $O(\log n)^{2+\varepsilon}$ steps, the test can be completed in time $O((\log n)^{4+\varepsilon})$.

References

[1] G. Miller :"Riemann's hypothesis and tests for primality." Proceedings of 17th Annual ACM Symposium on Theory of Computing (1975).

[2] H. Montgomery : "Topics in multiplicative Number Theory." Lecture Note 227. Springer Verlag.

[3] R. Solovay and V. Strassen : "A fast Monte-Carlo test for primality". SIAM J. Comput. Vol. 6, N° 1, March 1977.