The authors present statistics and heuristics to justify the assertion that, asymptotically, the group $(\mathbb{Z}/n\mathbb{Z})^*$ can be generated modulo $n$ by primes up to say $G(n)$ which is $< \frac{\log n \log \log n}{\log 2}$. Thus the primality of $n$ may be determined in $O(\log n)^2$ multiplications by pseudoprime testing without appealing to the ERH. As a rigorous result the authors show the average of $G(n)$ up to $N$ is $> (1 + o(1)) \log n \log \log \log n$.

Reviewer: H. Cohn (New York)

MSC:

11Y11 Primality
11-04 Software, source code, etc. for problems pertaining to number theory
11N25 Distribution of integers with specified multiplicative constraints
11Y70 Values of arithmetic functions; tables

Keywords:

primality; pseudoprime testing

Full Text: DOI

References:


[33] G. Tonelli, Bemerkung über die Auflösung quadratischer Congruenzen, Gött. Nachr. (1891), 344-346. · Zbl 23.0194.02

[34] D. Suryanarayana, On \( \Delta (\ell,\ell) = (\ell,\ell) - (\ell,\ell)/\ell \), Proc. Amer. Math. Soc. 44 (1974), 17 – 21. · Zbl 0284.10001


[36] Samuel S. Wagstaff Jr., Greatest of the least primes in arithmetic progressions having a given modulus, Math. Comp. 33 (1979), no. 147, 1073 – 1080. · Zbl 0407.10034


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.