zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin

PRIMES is in P. (English) Zbl 1071.11070

Ann. Math. (2) 160, No. 2, 781-793 (2004).

This is a historical breakthrough which solved the complexity theoretical question PRIMES (distinguishing prime numbers from composites) in deterministic polynomial time. The results excels not only by its importance but also by the elegance and simplicity of the arguments. Thus, the reader of this note is well advised to consult the original paper.

If n is an integer to be tested for primality, all previous algorithms to this respect did use some version of the Pocklington Lemma, thus essentially seeking elements $\alpha \in A(n)$ of high order in some group $A(n)$ related to n – for instance $A(n) = \mathbb{Z}/n\mathbb{Z}$.

Compared to this, the idea of AKS consists in considering a certain subgroup

$$G \subset A(n) = \left(\mathbb{Z}[\zeta]/\left(n \cdot \mathbb{Z}[\zeta]\right)\right)^{\times}$$

as an abelian group with generators; here $\zeta \in \mathbb{C}$ is a primitive rth root of unity and r is an integer satisfying the crucial size restriction $\mathrm{ord}_r(n) = (\#\langle n \bmod r\rangle) > (2\log(n))^2$.

The test of AKS essentially consists in verifying that

$$(\zeta + a)^n \equiv \zeta^n + a \bmod n\mathbb{Z}[\zeta] \quad \text{for } 1 \leq a \leq \ell \quad \text{and } \ell = \lfloor \varphi(r)\log(n) \rfloor. \tag{t}$$

If these and some simple additional conditions on r, n are verified, then n is prime.

The proof is based on the concept of introspection: let $p \mid n$ be a possible prime divisor. A pair (α, m), $\alpha \in \mathbb{Z}[\zeta], m \in \mathbb{Z}$ with $(m, r) = 1$ is introspective (with respect to p) if $\alpha^m \equiv \sigma_m(\alpha) \bmod p\mathbb{Z}[\zeta]$, with σ_m the Galois map given by $\zeta \to \zeta^m$; introspection is multiplicative with respect to both components. Let A be the multiplicative group generated by $\{a + \zeta : 1 \leq a \leq \ell\} \subset \mathbb{Z}[\zeta]$ and $I = \{p^i \cdot n^j : i, j \geq 0\} \subset \mathbb{N}$. Then the product $A \times I$ is introspective for given p; if $\wp \subset \mathbb{Z}[\zeta]$ is some maximal ideal over p, then $G = A \bmod \wp$ is a subgroup of the multiplicative group of a field o characteristic p. If n is not a power of p then Agrawal, Kayal and Saxena use the above introspection relations in order to derive contradictory upper and lower bounds on the size of G, which is the group with fgenerator mentioned above. This proves the consistency of the algorithm.

Reviewer: Preda Mihailescu (Göttingen)

MSC:

11Y11	Primality
11Y16	Number-theoretic algorithms; complexity
68Q25	Analysis of algorithms and problem complexity
68Q15	Complexity classes (hierarchies, relations among complexity classes, etc.)
11A51	Factorization; primality

Cited in **29** Reviews
Cited in **139** Documents

Keywords:

historical breakthrough; solution of the complexity theoretical question PRIMES; distinguishing prime numbers from composites; deterministic polynomial time

Full Text: DOI