8 - Algorytm AKS

Tuesday, 18 June 2024 19:23

Primes $\in P$

Lemat 1:

$n, a \in \mathbb{Z}$ oraz $gcd(n,a) = 1$:

$(X+a)^n = X^n + a^n \pmod n$ iff n jest pierwsze.

AKS

1. Jeśli $n = m^k$ dla $k \geq 2$:
   return złożona
2. Znajdź min. r takie, że rząd n modulo r jest $\geq \log^2 n$. $O(\log^5 n)$
3. Jeśli $1 < gcd(n,a) < n$ dla $a \leq r$:
   return złożona
4. Jeśli $n \leq r$
   return pierwsza
5. Niech $l = r^{\frac{1}{2}} \cdot \log n$
   Jeśli $(X+a)^n \neq X^n + a \pmod{p, X^r - 1}$
   dla pewnego $a \leq l$:
   return złożona
6. return pierwsza