Deterministic polynomial-time primality tests

D. J. Bernstein
University of Illinois at Chicago
NSF DMS–0140542

`http://cr.yp.to`
`/papers.html#aks`

Thm (Agrawal, Kayal, Saxena 2002):
Assume that q and r are prime,
q divides $r-1$,
$n^{(r-1)/q} \bmod r \notin \{0,1\}$,
and $\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}$.
If n has no prime divisors $< s$,
and $(x+b)^n = x^n + b$
in the ring $(\mathbf{Z}/n)[x]/(x^r-1)$
for all $b \in \{0,1,\ldots,s-1\}$,
then n is a power of a prime.

Polynomial-time primality test:
Find q, r, s with $rs \in (\lg n)^{10+o(1)}$.
Check remaining conditions.

Bottleneck in computation:
$s \lg n$ multiplications of
huge integers, each $\approx 2r \lg n$ bits.
Time $r^{1+o(1)} s(\lg n)^{2+o(1)}$.

Conjecturally: Can find q, r, s with $rs \in (1024 + o(1))(\lg n)^4$. (AKS)

$(2.25\ldots + o(1))(\lg n)^4$. (me)

$(0.017\ldots + o(1))(\lg n)^4$:
change $2\lfloor\sqrt{r}\rfloor$ to $\lfloor\sqrt{r}\rfloor$;
change $q + s - 1$ to $\varphi(r) + s - 1$
if n is a primitive root mod r.
(H. W. Lenstra, Jr.)