AN EXPOSITION OF THE AGRAWAL-KAYAL-SAXENA PRIMALITY-PROVING THEOREM

DANIEL J. BERNSTEIN

Theorem 1 (Manindra Agrawal, Neeraj Kayal, Nitin Saxena)**.** *Let n be a positive integer. Let q and r be prime numbers. Let S be a finite set of integers. Assume that q divides $r-1$; that $n^{(r-1)/q} \bmod r \notin \{0,1\}$; that $\gcd\{n, b-b'\} = 1$ for all distinct $b, b' \in S$; that $\binom{q+\#S-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$; and that $(x+b)^n = x^n + b$ in the ring $(\mathbf{Z}/n)[x]/(x^r-1)$ for all $b \in S$. Then n is a power of a prime.*

Proof. Find a prime divisor p of n such that $p^{(r-1)/q} \bmod r \notin \{0,1\}$. (If every prime divisor p of n has $p^{(r-1)/q} \bmod r \in \{0,1\}$ then $n^{(r-1)/q} \bmod r \in \{0,1\}$.)

By hypothesis, $(x+b)^n = x^n + b$ in $\mathbf{F}_p[x]/(x^r-1)$ for all $b \in S$. Substitute x^{n^i} for x: $(x^{n^i}+b)^n = x^{n^{i+1}} + b$ in $\mathbf{F}_p[x]/(x^{n^i r}-1)$, hence in $\mathbf{F}_p[x]/(x^r-1)$. By induction, $(x+b)^{n^i} = x^{n^i} + b$ for all $i \geq 0$. By Fermat's little theorem, $(x+b)^{n^i p^j} = (x^{n^i}+b)^{p^j} = x^{n^i p^j} + b$ for all $j \geq 0$.

Consider the products $n^i p^j$ with $0 \leq i \leq \lfloor\sqrt{r}\rfloor$ and $0 \leq j \leq \lfloor\sqrt{r}\rfloor$. There are $(\lfloor\sqrt{r}\rfloor+1)^2 > r$ such pairs (i,j), so there are distinct pairs $(i,j),(k,\ell)$ such that $n^i p^j \equiv n^k p^\ell \pmod{r}$. Write $t = n^i p^j$ and $u = n^k p^\ell$. Then $(x+b)^t = x^t + b = x^u + b = (x+b)^u$ in $\mathbf{F}_p[x]/(x^r-1)$ for all $b \in S$.

Find an irreducible polynomial h in $\mathbf{F}_p[x]$ dividing $(x^r-1)/(x-1)$. A standard fact about cyclotomic polynomials is that $\deg h$ is the order of p modulo r; so $\deg h$ is a multiple of q; so $\deg h \geq q$.

Now $(x+b)^t = (x+b)^u$ in the finite field $\mathbf{F}_p[x]/h$ for all $b \in S$. Note that $x+b \in (\mathbf{F}_p[x]/h)^*$, since $\deg h \geq q \geq 2$. Define G as the subgroup of $(\mathbf{F}_p[x]/h)^*$ generated by $\{x+b : b \in S\}$; then $g^t = g^u$ for all $g \in G$.

G has at least $\binom{q+\#S-1}{\#S}$ elements: specifically, all products $\prod_{b\in S}(x+b)^{e_b}$ with $\sum_b e_b \leq q-1$. (The irreducibles $x+b$ are distinct in $\mathbf{F}_p[x]$, because each difference $(x+b)-(x+b') = b-b'$ is coprime to n by hypothesis; so these products $\prod_{b\in S}(x+b)^{e_b}$ are distinct in $\mathbf{F}_p[x]$. These products have degree smaller than q, hence smaller than $\deg h$, so they remain distinct modulo h.)

G is a finite multiplicative subgroup of a field, so it has an element g of order $\#G$. But $g^t = g^u$, and $|t-u| < n^{2\lfloor\sqrt{r}\rfloor} \leq \binom{q+\#S-1}{\#S} \leq \#G$, so $t = u$. In other words, $n^i p^j = n^k p^\ell$. If $i = k$ then $p^j = p^\ell$ so $(i,j) = (k,\ell)$, contradiction. Consequently n is a power of p. □

Appendix: how the AKS algorithm works. Agrawal, Kayal, and Saxena use Theorem 1 to determine in polynomial time whether a given integer $n > 1$ is prime.

The idea is to find a small odd prime r such that $n^{(r-1)/q} \bmod r \notin \{0,1\}$ and $\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}$; here q is the largest prime divisor of $r-1$, and s is any integer

---

Date: 20020810.
1991 *Mathematics Subject Classification.* Primary 11Y16.

on the same scale as q. A theorem of Fouvry implies that a suitable r exists on the scale of $(\log n)^6$. (A standard conjecture implies that a suitable r exists on the scale of $(\log n)^2$.)

Given such a (q, r, s), one can easily test that n has no prime divisors smaller than s, and test that $(x + b)^n = x^n + b$ in the ring $(\mathbf{Z}/n)[x]/(x^r - 1)$ for all $b \in S$ where $S = \{0, 1, \ldots, s - 1\}$. Any failure of the first test reveals a prime divisor of n. Any failure of the second test proves that n is composite. If both tests succeed, then n is a prime power by Theorem 1. One can easily check whether n is a square, cube, etc. to see whether n is prime.

Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607–7045

Email address: `djb@cr.yp.to`