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 s be a positive integer. Let r be an odd prime number. Let q be the largest prime divisor of $r-1$. Assume that n has no prime divisor smaller than s; that $n^{(r-1)/q} \bmod r \notin \{0,1\}$; 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 positive integers $b \leq s$. Then n is a power of a prime.*

Proof. There is a prime divisor p of n such that $p^{(r-1)/q} \bmod r \notin \{0,1\}$. (Otherwise $p^{(r-1)/q} \bmod r \in \{0,1\}$ for every prime divisor p of n, so $n^{(r-1)/q} \bmod r \in \{0,1\}$; contradiction.)

The order of p in $(\mathbf{Z}/r)^*$ is at least q. (Otherwise it is coprime to q; but it divides $r-1$, because $p^{r-1} \bmod r = 1$; so it divides $(r-1)/q$; so $p^{(r-1)/q} \bmod r = 1$, contradiction.)

Select an irreducible polynomial h in $(\mathbf{Z}/p)[x]$ dividing $x^{r-1} + x^{r-2} + \cdots + 1$. The degree of h is at least q. (For readers not familiar with cyclotomic polynomials: Start from the fact that h divides $x^{p^d} - x$, where d is the degree of h. By construction h also divides $x^r - 1$, so it divides $x^{\gcd\{p^d-1,r\}} - 1$. If $d < q$ then $p^d - 1$ is coprime to r, so h divides $x-1$, so $h = x-1$; but $x-1$ does not divide $x^{r-1} + \cdots + 1$, because $r \neq 0$ in $\mathbf{Z}/p$.)

Define F as the finite field $(\mathbf{Z}/p)[x]/h$. Define G as the subgroup of F^* generated by $\{x-1, x-2, \ldots, x-s\}$: i.e., the set of products $(x-1)^{e_1} \cdots (x-s)^{e_s} \bmod h$.

G has at least $\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}$ elements: namely, all $(x-1)^{e_1} \cdots (x-s)^{e_s} \bmod h$ with $e_1 + \cdots + e_s \leq q-1$. (If $e_1 + \cdots + e_s \leq q-1$ and $f_1 + \cdots + f_s \leq q-1$ and $(x-1)^{e_1} \cdots (x-s)^{e_s} \equiv (x-1)^{f_1} \cdots (x-s)^{f_s} \pmod{h}$, then $(x-1)^{e_1} \cdots (x-s)^{e_s} = (x-1)^{f_1} \cdots (x-s)^{f_s}$; but $p \geq s$, so $x-1, \ldots, x-s$ are distinct irreducible polynomials in $(\mathbf{Z}/p)[x]$, so $(e_1, \ldots, e_s) = (f_1, \ldots, f_s)$.)

Find a generator $(x-1)^{e_1} \cdots (x-s)^{e_s} \bmod h$ of G. Lift this generator to the polynomial $g = (x-1)^{e_1} \cdots (x-s)^{e_s}$ in $(\mathbf{Z}/p)[x]$. The order of $g \bmod h$ is the size of G, so it is at least $n^{2\lfloor\sqrt{r}\rfloor}$.

By hypothesis $(x-b)^n \equiv x^n - b \pmod{x^r - 1}$ for $1 \leq b \leq s$. Thus $g^n = ((x-1)^n)^{e_1} \cdots ((x-s)^n)^{e_s} \equiv (x^n-1)^{e_1} \cdots (x^n-s)^{e_s} = g(x^n) \pmod{x^r-1}$.

Define T as the set of positive integers e such that $g^e \equiv g(x^e) \pmod{x^r-1}$. Then $n \in T$. Furthermore, $g^p = g(x^p)$, so $p \in T$; and $g^1 = g(x^1)$, so $1 \in T$.

T is closed under multiplication. (If $g^f \equiv g(x^f) \pmod{x^r-1}$ then $g(x^e)^f \equiv g(x^{ef}) \pmod{x^{er}-1}$ so $g(x^e)^f \equiv g(x^{ef}) \pmod{x^r-1}$; if also $g^e \equiv g(x^e) \pmod{x^r-1}$ then $g^{ef} = (g^e)^f \equiv g(x^e)^f \equiv g(x^{ef})$.) Thus every product $n^i p^j$ is in T.

Date: 20020808.
1991 *Mathematics Subject Classification.* Primary 11Y16.

Consider the products $n^i p^j$ with $0 \le i \le \lfloor\sqrt{r}\rfloor$ and $0 \le j \le \lfloor\sqrt{r}\rfloor$. 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 $t \equiv u \pmod r$, so $g(x^t) \equiv g(x^u) \pmod{x^r - 1}$; but $t \in T$ and $u \in T$, so $g(x^t) \equiv g^t$ and $g(x^u) \equiv g^u$. Thus $g^t \equiv g^u \pmod{x^r - 1}$. Consequently $g^t \equiv g^u \pmod h$; in other words, $t - u$ is divisible by the order of $g \bmod h$. But t and u are positive integers bounded by $n^{i+j} \le n^{2\lfloor\sqrt{r}\rfloor}$, which is at most the order of $g \bmod h$, so $t = u$. In other words, $n^{i-k} = p^{j-\ell}$. Hence n is a power of p. $\square$

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

E-mail address: djb@cr.yp.to