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

Consider the products $n^i p^j$ with $0 \leq i \leq \lfloor\sqrt{r}\rfloor$ and $0 \leq j \leq \lfloor\sqrt{r}\rfloor$. Note for future reference that $n^i p^j \leq n^{2\lfloor\sqrt{r}\rfloor}$. There are $(\lfloor\sqrt{r}\rfloor+1)^2 > r$ pairs (i,j) here, 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 $x^t = x^u$ in $\mathbf{F}_p[x]/(x^r-1)$, so $(x+b)^t = x^t + b = x^u + b = (x+b)^u$ 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 $\prod_b(x+b)^{e_b}$ 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 $|t-u| \leq n^{2\lfloor\sqrt{r}\rfloor} \leq \binom{q+\#S-1}{\#S} \leq \#G$, and $g^t = g^u$, 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. □

Date: 20020820.
1991 *Mathematics Subject Classification.* Primary 11Y16.

Theorem 2 (Manindra Agrawal, Neeraj Kayal, Nitin Saxena, Hendrik W. Lenstra, Jr.)**.** *Let n and r be positive integers. Let S be a finite set of integers. Assume that n is a primitive root modulo r; that $\gcd\{n, b-b'\} = 1$ for all distinct $b, b' \in S$; that $\binom{\varphi(r)+\#S-1}{\#S} \geq n^{\lfloor\sqrt{r}\rfloor}$; 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. If $n = 1$ then n is a power of a prime, so assume that $n \geq 2$. Let p be a prime divisor of n. Note for future reference that $\varphi(r) > 1$. (Otherwise $n \leq n^{\lfloor\sqrt{r}\rfloor} \leq \binom{\varphi(r)+\#S-1}{\#S} = \binom{\#S}{\#S} = 1$, contradiction.)

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

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

Find an irreducible polynomial h in $\mathbf{F}_p[x]$ dividing the rth cyclotomic polynomial Φ_r. Observe that any polynomial $g \in \mathbf{F}_p[x]$ such that $g(x^{n^a}) = 0$ in $\mathbf{F}_p[x]/h$ for all $a \geq 0$ must be divisible by Φ_r. (If $c \in \{0,1,\ldots,r-1\}$ and $\gcd\{r,c\} = 1$ then, by hypothesis, $c \equiv n^a \pmod{r}$ for some a, so $g(y^c) = g(y^{n^a})$ in $\mathbf{F}_p[y]/(y^r-1)$, so $g(y^c) = 0$ in the field $\mathbf{F}_p[y]/h(y)$. The powers y^c are distinct in $\mathbf{F}_p[y]/h(y)$, so g is divisible by $\prod_c (x - y^c) = \Phi_r$ in $(\mathbf{F}_p[y]/h(y))[x]$, hence in $\mathbf{F}_p[x]$.)

Note that $x+b \in (\mathbf{F}_p[x]/h)^*$. (If $x+b = 0$ in $\mathbf{F}_p[x]/h$ then $x^{n^a}+b = (x+b)^{n^a} = 0$ in $\mathbf{F}_p[x]/h$ for all a, so Φ_r divides $x+b$; but $\deg\Phi(r) = \varphi(r) > 1$.)

Define G as the subgroup of $(\mathbf{F}_p[x]/h)^*$ generated by $\{x+b : b \in S\}$. Then $g^{tp^{\lfloor\sqrt{r}\rfloor}} = g^{up^{\lfloor\sqrt{r}\rfloor}}$ for all $g \in G$; pth powering is invertible in $\mathbf{F}_p[x]/h$, so $g^t = g^u$.

G has at least $\binom{\varphi(r)+\#S-1}{\#S}$ elements: specifically, all products $\prod_{b\in S}(x+b)^{e_b}$ with $\sum_b e_b \leq \varphi(r)-1$. (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 $\prod_b(x+b)^{e_b}$ are distinct in $\mathbf{F}_p[x]$. Now assume that two products $e = \prod_b(x+b)^{e_b}$ and $f = \prod_b(x+b)^{f_b}$ are the same in $\mathbf{F}_p[x]/h$. Then $e^{n^a} = \prod_b(x+b)^{n^a e_b} = \prod_b(x^{n^a}+b)^{e_b} = e(x^{n^a})$ in $\mathbf{F}_p[x]/h$ for all $a \geq 0$; similarly $f^{n^a} = f(x^{n^a})$ in $\mathbf{F}_p[x]/h$; so $e(x^{n^a}) = f(x^{n^a})$ in $\mathbf{F}_p[x]/h$. Thus Φ_r divides $e-f$. Both e and f have degree smaller than $\varphi(r) = \deg\Phi(r)$, so $e = f$ in $\mathbf{F}_p[x]$.)

G is a finite multiplicative subgroup of a field, so it has an element g of order $\#G$. But $|t-u| \leq n^{\lfloor\sqrt{r}\rfloor} \leq \binom{\varphi(r)+\#S-1}{\#S} \leq \#G$, and $g^t = g^u$, 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. $\square$

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 moderately large integer. A theorem of Fouvry from analytic number theory implies that a suitable r exists on the scale of $(\log n)^6$, with s on the scale of $(\log n)^4$.

(For readers who care about ease of run-time analysis: Carl Pomerance points out that one can use a theorem of Goldfeld, older and simpler than the theorem of Fouvry, if 6 and 4 are replaced by substantially larger numbers. As an alternative, Lenstra has a generalization of Theorem 1 and Theorem 2, allowing many more r's at some expense in speed; one can very easily prove that r and s suitable for Lenstra's generalization exist on the scale of $(\log n)^5$.)

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.

(For readers who care about speed: A suitable r and s are conjectured to exist on the scale of $(\log n)^2$, with $q = (r-1)/2$. One can easily choose r and s to minimize the time spent checking the conditions $(x+b)^n = x^n + b$. The time is essentially linear in $rs(\lg n)^2$. The minimum value of $rs(\lg n)^2$ is conjectured to be $(0.017\ldots + o(1))(\lg n)^6$ with Theorem 2, or $(2.25\ldots + o(1))(\lg n)^6$ with Theorem 1. In contrast, in the algorithm stated by Agrawal, Kayal, and Saxena, the value of $rs(\lg n)^2$ is conjectured to be $(1024 + o(1))(\lg n)^6$; the Agrawal-Kayal-Saxena paper imposes the unnecessarily strong conditions $q \geq 4\sqrt{r}\lg n$ and $s \geq 2\sqrt{r}\lg n$.)

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`