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 the largest prime divisor of $n-1$. Assume that $n$ has no prime divisor smaller than $s$; then $\frac{n^{r-1}}{r} \equiv 0 \pmod{r}$, and that $(x-b)^n \equiv x^n - b$ in the ring $(\mathbb{Z}/n)[x]/(x^r - 1)$ 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 $p^{\frac{n^{r-1}}{r}} \equiv 0 \pmod{r} \notin \{0, 1\}$. (Otherwise $p^{\frac{n^{r-1}}{r}} \equiv 1 \pmod{r} \in \{0, 1\}$ for every prime divisor $p$ of $n$; so $\frac{n^{r-1}}{r} \notin \{0, 1\}$; contradiction.)

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

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

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

$G$ has at least $(q^{s+1} - 1)/q \geq n^{2/\sqrt{\varphi(d)}}$ elements: namely, all $(x-1)^{e_1} \cdots (x-s)^{e_s} \equiv h \mod q$ 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 $(x-1)^{e_1} \cdots (x-s)^{e_s} \equiv (x-1)^{f_1} \cdots (x-s)^{f_s} \mod h$, then $(x-1)^{e_1} \cdots (x-s)^{e_s} \equiv (x-1)^{f_1} \cdots (x-s)^{f_s}$; but $p \geq s$, so $x-1, \ldots, x-s$ are distinct irreducible polynomials in $(\mathbb{Z}/p)[x]$, so $(e_1, \ldots, e_s) = (f_1, \ldots, f_s)$.)

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

By hypothesis $(x-b)^n \equiv x^n - b \pmod{x^r - 1}$ for $1 \leq b \leq s$. Thus $g^n \equiv (x-1)^{e_1} \cdots (x-s)^{e_s} \equiv (x^n - 1)^{e_1} \cdots (x^n - s)^{e_s} \equiv g(x^n) \pmod{x^r - 1}$. Define $T$ as the set of positive integers $c$ such that $g^c \equiv g(x^c) \pmod{x^r - 1}$. Then $n \in T$. Furthermore, $g^1 = g(x^1)$, 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 $g(x^f)^f \equiv g(x^{ef}) \pmod{x^{ef} - 1}$ so $g(x^f)^f \equiv g(x^{ef}) \pmod{x^{ef} - 1}$; if also $g^f \equiv g(x^f) \pmod{x^r - 1}$ then $g^f \equiv g(x^f)^f \equiv g(x^{ef})$. Thus every product $n^p p^l$ is in $T$.)

\textbf{Date:} 20020808.
1991 Mathematics Subject Classification. Primary 11Y16.
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 \( t \equiv u \pmod{r} \), 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 \( g^t \equiv g^u \pmod{g \pmod{h}} \); in other words, \( t \equiv u \pmod{h} \). But \( t \) and \( u \) are positive integers bounded by \( n^{i+j} \leq n^{2\lfloor \sqrt{r} \rfloor} \), which is at most the order of \( g \pmod{h} \), so \( t = u \). In other words, \( n^{i-k} = p^{i-k} \). Hence \( n \) is a power of \( p \).