3.7 The AKS Primality Test

MILLER reduced the quest for an **efficient deterministic** primality test to the extended RIEMANN hypothesis. In August 2002 the three Indian mathematicians Manindra AGRAWAL, Neeraj KAYAL und Nitin SAXENA surprised the scientific community with a complete proof that relied on an astonishingly simple deterministic algorithm. It immediately was baptized "AKS primality test". The fastest known version costs $\mathrm{O}(\log(n)^6)$.

Proposition 13 (Basic criterion) *Let $a, n \in \mathbb{Z}$ be coprime, $n \geq 2$. Then the following statements are equivalent:*

(i) *n is prime.*

(ii) *$(X+a)^n \equiv X^n + a \pmod{n}$ in the polynomial ring $\mathbb{Z}[X]$.*

Proof. From the binomial theorem we have

$$(X+a)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} X^i$$

in $\mathbb{Z}[X]$.

"(i) $\Longrightarrow$ (ii)": If n is prime, then $n | \binom{n}{i}$ for $i = 1, \ldots, n-1$, hence $(X+a)^n \equiv X^n + a^n \pmod{n}$. By FERMAT's theorem $a^n \equiv a \pmod{n}$.

"(ii) $\Longrightarrow$ (i)": If n is composite, then we choose a prime $q|n$, and k with $q^k|n$ and $q^{k+1} \not| n$. Then $q \neq n$ and

$$q^k \not| \binom{n}{q} = \frac{n \cdots (n-q+1)}{1 \cdots q}.$$

Hence the coefficient of X^q in $(X+a)^n$ is $\neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. ◇

Remarks

1. Looking at the absolute term in (ii) we see that the basic criterion generalizes FERMAT's theorem.

2. Consider the ideal $\mathfrak{q}_r := (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$ for $r \in \mathbb{N}$. If n is prime, then $(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}_r}$. This shows:

Corollary 1 *If n is prime, then in the polynomial ring $\mathbb{Z}[X]$*

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}_r}$$

for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ and all $r \in \mathbb{N}$.

Applying the basic criterion as a primality test in a naive way would cost about $\log_2 n$ multiplications of polynomials in $\mathbb{Z}/n\mathbb{Z}[X]$ using the binary power algorithm. But these multiplications become more and more expensive, in the last step we have to multiply two polynomials of degree about $\frac{n}{2}$ for an expense of size about n. The corollary bounds the degrees by $r-1$, but its condition is only necessary, not sufficient.

The sticking point of the AKS algorithm is a converse of the corollary that says that we need to try only "few" values of a, however sufficiently many, for a suitable fixed r:

Proposition 14 (AKS criterion, H. W. LENSTRA**'s version)** *Let n be an integer ≥ 2. Let $r \in \mathbb{N}$ be coprime with n. Let $q := \operatorname{ord}_r n$ be the order of n in the multiplicative group $\mathbb{M}_r = (\mathbb{Z}/r\mathbb{Z})^\times$. Furthermore let $s \geq 1$ be an integer with $\gcd(n,a) = 1$ for all $a = 1, \ldots, s$ and*

$$\binom{\varphi(r)+s-1}{s} \geq n^{2d\cdot\lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor}$$

for each divisor $d|\frac{\varphi(r)}{q}$. Assume

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}} \quad \text{for all } a = 1, \ldots s$$

with the ideal $\mathfrak{q} = \mathfrak{q}_r = (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$. Then n is a prime power.

We reproduce the proof by D. BERNSTEIN, breaking it up into a series of lemmas and corollaries.

Lemma 5 *For all $a = 1, \ldots s$ and all $i \in \mathbb{N}$*

$$(X+a)^{n^i} \equiv X^{n^i} + a \pmod{\mathfrak{q}}.$$

Proof. We reason by induction over i. In

$$(X+a)^n = X^n + a + n \cdot f(X) + (X^r - 1) \cdot g(X)$$

we substitute $X \mapsto X^{n^i}$ in $\mathbb{Z}[X]$:

$$(X+a)^{n^{i+1}} \equiv (X^{n^i} + a)^n = X^{n^i \cdot n} + a + n \cdot f(X^{n^i}) + (X^{n^i \cdot r} - 1) \cdot g(X^{n^i})$$

$$\equiv X^{n^{i+1}} + a \pmod{\mathfrak{q}},$$

since $X^{n^i r} - 1 = (X^r)^{n^i} - 1 = (X^r - 1)(X^{r\cdot(n^i-1)} + \cdots + X^r + 1)$ is a multiple of $X^r - 1$. $\diamond$

Now let $p|n$ be a prime divisor. *Claim*: n is a power of p.

We enlarge the ideal $\mathfrak{q} = (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$ to $\hat{\mathfrak{q}} := (p, X^r - 1) \trianglelefteq \mathbb{Z}[X]$. Then the identity from Lemma 5 holds also $\bmod\ \hat{\mathfrak{q}}$, and since we now calculate $\bmod\ p$, we even have:

Corollary 2 *For all $a = 1, \ldots s$ and all $i, j \in \mathbb{N}$*

$$(X + a)^{n^i p^j} \equiv X^{n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Let $H := \langle n, p \rangle \leq \mathbb{M}_r$ be the subgroup generated by the residue classes $n \bmod r$ and $p \bmod r$. Let

$$d := \#(\mathbb{M}_r / H) = \frac{\varphi(r)}{\#H}.$$

From $q = \operatorname{ord}_r n \mid \#H$ we have $d \mid \frac{\varphi(r)}{q}$. Hence d satisfies the precondition of Proposition 14. For the remainder of the proof we fix a complete system of representants $\{m_1, \ldots, m_d\} \subseteq \mathbb{M}_r$ of $\mathbb{M}_r/H$. Corollary 2 then extends to

Corollary 3 *For all $a = 1, \ldots s$, all $k = 1, \ldots, d$, and all $i, j \in \mathbb{N}$*

$$(X^{m_k} + a)^{n^i p^j} \equiv X^{m_k n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Proof. We use the same trick as in Lemma 5 and substitute $X \mapsto X^{m_k}$ in $\mathbb{Z}[X]$:

$$(X + a)^{n^i p^j} = X^{n^i p^j} + a + p \cdot f(X) + (X^r - 1) \cdot g(X) \text{ in } \mathbb{Z}[X],$$

$$(X^{m_k} + a)^{n^i p^j} = X^{m_k n^i p^j} + a + p \cdot f(X^{m_k}) + (X^{m_k \cdot r} - 1) \cdot g(X^{m_k}),$$

and from this the proof is immediate. $\diamond$

The products $n^i p^j \in \mathbb{N}$ with $0 \leq i, j \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ are bounded by

$$1 \leq n^i p^j \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor}.$$

The number of such pairs $(i, j) \in \mathbb{N}^2$ is $(\lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor + 1)^2 > \frac{\varphi(r)}{d}$, and all $n^i p^j \bmod r$ are contained in the subgroup H with $\#H = \frac{\varphi(r)}{d}$. Hence there are different $(i, j) \neq (h, l)$ with

$$n^i p^j \equiv n^h p^l \pmod{r}.$$

We even have $i \neq h$—otherwise $p^j \equiv p^l \pmod{r}$, hence $p | r$. Thus we have shown the first part of the following lemma:

Lemma 6 *There exist i, j, h, l with $0 \leq i, j, h, l \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ and $i \neq h$ such that for $t := n^i p^j$, $u := n^h p^l$, the congruence $t \equiv u \pmod{r}$ is satisfied, and $|t - u| \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} - 1$, as well as*

$$(X^{m_k} + a)^t \equiv (X^{m_k} + a)^u \pmod{\hat{\mathfrak{q}}}$$

for all $a = 1, \ldots, s$ and all $k = 1, \ldots d$.

Proof. The latter congruence follows from $X^t = X^{u+cr} \equiv X^u \pmod{X^r - 1}$, hence

$$(X^{m_k} + a)^t \equiv X^{m_k t} + a \equiv X^{m_k u} + a \equiv (X^{m_k} + a)^u \pmod{\hat{\mathfrak{q}}},$$

for all a and k. $\diamond$

Now r and n are coprime, and p is a prime divisor of n, thus $X^r - 1$ has no multiple zeroes in an algebraic closure of $\mathbb{F}_p$. Hence it has r distinct zeroes, and these are the r-th roots of unity $\bmod\, p$. They form a cyclic group by Proposition 2. Let ζ be a generating element, that is a primitive r-th root of unity. For one of the irreducible divisors $h \in \mathbb{F}_p[X]$ of $X^r - 1$ we have $h(\zeta) = 0$. Let

$$K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X] \cong \mathbb{Z}[X]/\hat{\hat{\mathfrak{q}}}$$

with the ideal $\hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$. Thus we have an ascending chain of ideals

$$\mathfrak{q} = (n, X^r - 1) \hookrightarrow \hat{\mathfrak{q}} = (p, X^r - 1) \hookrightarrow \hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$$

and a corresponding chain of surjections

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/\mathfrak{q} \longrightarrow \mathbb{F}_p[X]/(X^r - 1) \longrightarrow K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X].$$

Lemma 7 *With the notations of Lemma 6 we have in K:*

(i) $(\zeta^{m_k} + a)^t = (\zeta^{m_k} + a)^u$ *for all* $a = 1, \ldots, s$ *and all* $k = 1, \ldots d$.

(ii) *If* $G \le K^\times$ *is the subgroup generated by the* $\zeta^{m_k} + a \neq 0$, *then* $g^t = g^u$ *for all* $g \in \bar{G} := G \cup \{0\}$.

Proof. (i) follows from Lemma 6 using the homomorphism $\mathbb{Z}[X] \longrightarrow K$, $X \mapsto \zeta$ with kernel $\hat{\hat{\mathfrak{q}}} \supseteq \hat{\mathfrak{q}}$.

(ii) is a direct consequence from (i). $\diamond$

The $X + a \in \mathbb{F}_p[X]$ for $a = 1, \ldots s$ are pairwise distinct irreducible polynomials since $p > s$ by the premises of Proposition 14. Thus also all products

$$f_e := \prod_{a=1}^{s} (X + a)^{e_a} \quad \text{for } e = (e_1, \ldots, e_s) \in \mathbb{N}^s$$

are distinct in $\mathbb{F}_p[X]$. We consider their images under the map

$$\begin{array}{rcl} \Phi\colon \mathbb{F}_p[X] & \longrightarrow & K^d, \\ f & \mapsto & (f(\zeta^{m_1}), \ldots, f(\zeta^{m_d})). \end{array}$$

Lemma 8 *The images* $\Phi(f_e) \in K^d$ *of the* f_e *with* $\deg f_e = \sum_{a=1}^{s} e_a \le \varphi(r) - 1$ *are pairwise distinct.*

Proof. Assume $\Phi(f_c) = \Phi(f_e)$. By Corollary 3 for $k = 1, \ldots, d$

$$f_c(X^{m_k})^{n^i p^j} = \prod_{a=1}^{s} (X^{m_k} + a)^{n^i p^j c_a} \equiv \prod_{a=1}^{s} (X^{m_k n^i p^j} + a)^{c_a}$$

$$= f_c(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}}$$

and likewise

$$f_e(X^{m_k})^{n^i p^j} \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}},$$

a forteriori mod $\hat{\hat{\mathfrak{q}}}$. Applying Φ to the left-hand sides yields

$$f_c(X^{m_k n^i p^j}) \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\hat{\mathfrak{q}}}}.$$

Thus for the difference $g := f_c - f_e \in \mathbb{F}_p[X]$ we have $g(X^{m_k n^i p^j}) \in h\mathbb{F}_p[X]$ for all $k = 1, \ldots, d$. Let $b \in [1 \ldots r-1]$ be coprime with r, hence represent an element of $\mathbb{M}_r$. Then b is contained in one of the cosets $m_k H$ of $\mathbb{M}_r/H$. Thus there exist k, i, and j with $b \equiv m_k n^i p^j \pmod{r}$. Hence

$$g(X^b) - g(X^{m_k n^i p^j}) \in (X^r - 1)\mathbb{F}_p[X] \subseteq h\mathbb{F}_p[X],$$

hence $g(X^b) \in h\mathbb{F}_p[X]$, and $g(\zeta^b) = 0$. Thus g has the $\varphi(r)$ different zeroes ζ^b in K. But the degree of g is $< \varphi(r)$. Hence $g = 0$, and $f_c = f_e$. $\diamond$

Corollary 4

$$\#\bar{G} \geq \binom{\varphi(r) + s - 1}{s}^{1/d} \geq |t - u| + 1.$$

Proof. There are $\binom{\varphi(r)+s-1}{s}$ options for choosing the exponents $(e_1, \ldots, e_s)$ as in Lemma 8. Since all $\Phi(f_e) \in \bar{G}^d$, we conclude

$$\#\bar{G}^d \geq \binom{\varphi(r) + s - 1}{s} \geq n^{2d \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor}$$

by the premises of Proposition 14, hence

$$\#\bar{G} \geq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} \geq |t - u| + 1$$

by Lemma 6. $\diamond$

Now we can complete the proof of Proposition 14: Since $g^t = g^u$ for all $g \in \bar{G} \subseteq K$, the polynomial $X^{|t-u|}$ has more than $|t - u|$ zeroes in K. This is possible only if $t = u$. By the definition of t and u (in Lemma 6) n is a power of p.

This proves Proposition 14. $\diamond$