An elliptic variant of the AKS primality test

(with J.-M. Couveignes, T. Ezome)

R. Lercier

DGA/CELAR & University of Rennes — France
Reynald.Lercier (at) m4x.org

IRMAR

June 2009

Outline

Outline

AKS primality test

Theorem

n is prime if and only if $(x+1)^n = x^n + 1 \bmod n$ in $\mathbb{Z}[x]$

Elegant. . . but it involves storing n coefficients !

AKS algorithm (mainly) performs this test

- modulo $x^d - 1$ for d s.t. $o_d(n) > \log^2 n$,
- not only for $x+1$, but for

$$x + a, \ \ a = 1, \ldots, \lfloor \sqrt{\varphi(d)} \log n \rfloor$$

.

That is,

$$(x+a)^n \equiv x^n + a \bmod (n, x^d - 1).$$

AKS improvements (in a nutshell)

We have $d \leqslant \max\{3, \lceil \log^5 n \rceil\}$,

this yields a $\tilde{O}(\log^{21/2} n)$ complexity [see AKS paper].

Roughly, we might distinguish two lines of improvements.

- Lenstra-Pomerance: Replace $x^d - 1$ by "irreducible polynomials" of degree $\simeq \log^2 n$

  $\rightarrow \tilde{O}(\log^6 n)$ complexity.

- Berritzbeitia-Cheng: Make use of "degree friendly" $\mathbb{Z}/n\mathbb{Z}$ automorphism, $x \mapsto \zeta x$, when $d \mid n-1$, to restrict AKS to the *only* test $(x+1)^n \equiv x^n + 1$.

$$\rightarrow \tilde{O}(\log^4 n) \text{ complexity} \quad (\text{if } \exists d \simeq \log^2 n \text{ s.t. } d | n-1)\,.$$

The later was improved by [Avanzi-Mihailescu] and (indep.) [Bernstein] to the case $d | n^k - 1$ for some k.

A (rather long) proof that $n = 1\,000\,045\,187$ is prime
(with Berritzbeitia-Cheng's variant)

Step 1. $d = 1109$ divides $n - 1$. Set $n - 1 = d \,.\, m$

Step 2. $\alpha = 2$ is a unit mod n :

$$2 \,.\, 500022594 = n + 1 \,.$$

Step 3. $\xi = \alpha^m \bmod n = 562098320$ is of exact order d :

$$\begin{aligned}
\xi - 1 &= 562098319 \text{ is a unit mod } n \\
\xi^2 - 1 &= 955016771 \text{ is a unit mod } n \\
\xi^3 - 1 &= 225452510 \text{ is a unit mod } n \\
&\vdots \\
\xi^{d-1} - 1 &= 766633118 \text{ is a unit mod } n \\
\xi^d - 1 &= 0
\end{aligned}$$

Let $R = \mathbb{Z}/1000045187\mathbb{Z}$ and $S = R[x]/(x^d - 2)$.

A proof that $n = 1\,000\,045\,187$ is prime (cont.)

$(1, x, x^2, \ldots, x^{d-1})$ is a R-basis of S. We define an R automorphism

$$\sigma : S \to S \text{ by setting } \sigma(x) = \zeta x\,.$$

Step 4. $\theta = x - 1 \bmod (n, x^d - \alpha)$ is a unit in S [$x^d - 1 = \alpha - 1$ and $\alpha - 1$ is a unit] and we check that

$$\theta^n = \xi x - 1 \bmod n.$$

$$\begin{aligned}
(x-1)^2 &= x^2 + 1000045185\,x + 1 \bmod (n, x^d - \alpha)\,,\\
&\vdots\\
(x-1)^{500022593} &= 456910923\,x^{1108} + \ldots \bmod (n, x^d - \alpha)\,,\\
(x-1)^{1000045186} &= 562098319\,x^{1108} + \ldots \bmod (n, x^d - \alpha)\,,\\
(x-1)^{1000045187} &= 562098320\,x - 1 \bmod (n, x^d - \alpha)\,,\\
&= \xi\,x - 1 \bmod (n, x^d - \alpha)\,.
\end{aligned}$$

A proof that $n = 1\,000\,045\,187$ is prime (cont.)

We have now enough equations to prove that n is a prime...

Let p a prime factor of n, and $a = \theta \bmod p$.

First,

$$a^{n^k} = \sigma^k(a) \bmod (p, x^d - \alpha)\ \forall k \in \mathbb{N}.$$

Second, the reduction of σ modulo a prime ideal of S/pS is an automorphism of a finite field, and we can further prove $\exists\ z \in \mathbb{N}$ s.t.

$$a^p = \sigma^z(a) \bmod (p, x^d - \alpha)\,.$$

And thus, for k, $l \in \mathbb{N}$,

$$a^{n^k p^l} = \sigma^{k+zl}(a).$$

A proof that $n = 1\,000\,045\,187$ is prime (cont.)

We want to show that the order of a in S/pS is rather large.

Let $h(x)$ be one of the irreducible factor of $x^d - \alpha \bmod p$,
let $b = a \bmod (p, h(x))$, let $q = n/p$, then

- the reduction $\langle a \rangle \longrightarrow \langle b \rangle$, $a \mapsto b$ is a bijection,
- $\#\langle a \rangle$ divides $p^{\deg h} - 1$,
- p and n are relatively prime to $\#\langle a \rangle$,
- and thus, for i and j in $\mathbb{Z}$,

$$a^{p^i q^j} = \sigma^{i(1-z)+j}(a) \bmod (p, h(x)).$$

A proof that $n = 1\,000\,045\,187$ is prime (cont.)

There exist four integers i, i', j and j' in $\{0, 1, \ldots, \lfloor\sqrt{d}\rfloor\}$ s. t.

$$(i, j) \neq (i', j') \text{ and } i(1-z) + jz = i'(1-z) + j'z \bmod d\,.$$

Exponentiations by $q^i p^j$ and $q^{i'} p^{j'}$ act similarly on a,

$$q^i p^j = q^{i'} p^{j'} \bmod \#\langle a\rangle. \tag{1}$$

Both integers $q^i p^j$ and $q^{i'} p^{j'}$ are $\leqslant n^{\lfloor\sqrt{d}\rfloor}$. Thus, if

$$n^{\lfloor\sqrt{d}\rfloor} \leqslant \#\langle a\rangle\,,$$

then Eq. (1) is an equality between integers and n is a power of p.

A proof that $n = 1\,000\,045\,187$ is prime (cont.)

For every subset $\mathcal{S}$ of $\{0, 1, \ldots, d-1\}$, let

$$a_{\mathcal{S}} = \prod_{k \in \mathcal{S}} (\zeta^k x - 1) \bmod (p, x^d - a) = \prod_{k \in \mathcal{S}} \sigma^k(a).$$

This is a power of a, because every $\sigma^k(a)$ is.

Degree considerations show that if

$$\mathcal{S}_1,\ \mathcal{S}_2 \subset \{0, 1, \ldots, d-1\},\ \mathcal{S}_1 \neq \mathcal{S}_2,$$

then

$$a_{\mathcal{S}_1} \neq a_{\mathcal{S}_2} \bmod p\,.$$

So, the order of a is at least $2^d - 1$.

A proof that $n = 1\,000\,045\,187$ is prime (end)

We have

$$2^d \simeq 6.9\,10^{333} > 10^{306} \simeq n^{\lfloor\sqrt{d}\rfloor}$$

and none of $n^{1/2}$, $n^{1/3}$, $\ldots$, $n^{1/29}$ are integers, so

$$n = p = 1\,000\,045\,187 \text{ is a prime.}$$

Outline

Some notations

- Let $E/\mathbb{F}_q$ be an elliptic curve given by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,.$$

- If A is a point in $E(\mathbb{F}_q)$, we denote by $\tau_A : E \longrightarrow E$ the translation by A. We set $x_A = x \circ \tau_{-A}$ and $y_A = y \circ \tau_{-A}$.
- If A, B and C are three pairwise distinct points in $E(\mathbb{F}_q)$, we define

$$\Gamma(A, B, C) = \frac{y(C - A) - y(A - B)}{x(C - A) - x(A - B)}\,.$$

- We define a function $u_{A,B} \in \mathbb{F}_q(E)$ by $u_{A,B}(C) = \Gamma(A, B, C)$.

  It has degree two with two simple poles, at A and B.

Ingredient 1: Some simple elliptic functions

We can prove the following identities (with Taylor expansions at poles).

$$\begin{aligned}
\Gamma(A,B,C) &= \Gamma(B,C,A) = -\Gamma(B,A,C) - a_1 \\
&= -\Gamma(-A,-B,-C) - a_1\,, \\
u_{A,B} + u_{B,C} + u_{C,A} &= \Gamma(A,B,C) - a_1\,,
\end{aligned}$$

$$\begin{aligned}
u_{A,B}u_{A,C} &= x_A + \Gamma(A,B,C)u_{A,C} + \Gamma(A,C,B)u_{A,B} \\
&\quad + a_2 + x_A(B) + x_A(C)\,, \\
u_{A,B}^2 &= x_A + x_B - a_1 u_{A,B} + x_A(B) + a_2\,.
\end{aligned}$$

Ingredient 2: Residue fields of divisors on elliptic curves

Let E be an elliptic curve defined over $\mathbb{F}_q$.

- Assume $E(\mathbb{F}_q)$ contains a cyclic subgroup $\mathcal{T}$ of order d (plus some milde technical conditions).
- Let $I : E \to E'$ be the degree d cyclic isogeny with kernel $\mathcal{T}$, the quotient $E'(\mathbb{F}_q)/I(E(\mathbb{F}_q))$ is isomorphic to $\mathcal{T}$.
- Take A in $E'(\mathbb{F}_q)$ such that A mod $I(E(\mathbb{F}_q))$ generates this quotient.
- The fiber $\mathcal{P} = I^{-1}(A) = \sum_{T \in \mathcal{T}}[B + T]$ is an irreducible divisor.

  The d geometric points above A are defined on a degree d extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$ (and permuted by Galois action).

$\mathbb{F}_{q^d}$ is the residue extension of $\mathbb{F}_q(E)$ at $\mathcal{P}$.

Elliptic Normal Basis

For $k \in \mathbb{Z}/d\mathbb{Z}$, we set

$$u_k = \mathfrak{a} u_{kT,(k+1)T} + \mathfrak{b}.$$

($\mathfrak{a}$ and $\mathfrak{b}$, constants chosen such that $\sum u_k = 1$).

Lemma (A normal basis)

The system $\Theta = (u_k(B))_{k \in \mathbb{Z}/d\mathbb{Z}}$ is a $\mathbb{F}_q$ normal basis of $\mathbb{F}_{q^d}$.

Proof

Let λ_k in $\mathbb{F}_q$ such that $\sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k(B) = 0$.

Let us consider the function $f = \sum_{k\in\mathbb{Z}/d\mathbb{Z}} \lambda_k u_k$.

- It cancels not only at B, but at $B+T$ with $T \in \mathcal{T}$ (because f is defined over $\mathbb{F}_q$).
- And f has d poles, the points in $\mathcal{T}$.
- Let us assume $f \neq 0$, then $(f) = (f)_0 - (f)_\infty$ with
$$(f)_0 = \sum_{T\in\mathcal{T}} [B+T] \text{ and } (f)_\infty = \sum_{T\in\mathcal{T}} [T].$$
- So, $\sum_{T\in\mathcal{T}} (B+T) - (T) = d\,B = 0_E$. This is impossible, $\Rightarrow f = 0$.
- Taylor expansions at poles show that all λ_k's are equal.
- Since $\sum u_k = 1$, all λ_k's are thus null.

A fast multiplication algorithm

$$\begin{aligned}\overrightarrow{\iota} &= (\iota_i)_{0\leqslant i\leqslant d-1} \text{ s.t. } x(B) = \textstyle\sum_{0\leqslant k\leqslant d-1} \iota_k\theta_k.\\ \vec{x}_R &= (x(R+kT))_{0\leqslant k\leqslant d-1}, \quad \vec{u}_R = (u_0(R+kT))_{0\leqslant k\leqslant d-1}.\end{aligned}$$

Lemma

The multiplication tensor for normal elliptic basis of type Θ is

$$\vec{\alpha},\vec{\beta} \mapsto (\mathfrak{a}^2\overrightarrow{\iota}) \star \Big((\vec{\alpha}-\sigma(\vec{\alpha})) \diamond (\vec{\beta}-\sigma(\vec{\beta}))\Big) +$$
$$\overrightarrow{u_R}^{(-1)} \star \Big((\vec{u}_R\star\vec{\alpha}) \diamond (\vec{u}_R\star\vec{\beta}) - (\mathfrak{a}^2\vec{x}_R) \star \Big((\vec{\alpha}-\sigma(\vec{\alpha})) \diamond (\vec{\beta}-\sigma(\vec{\beta}))\Big)\Big)$$

Remark: $\star$ is the convolutional product, $\diamond$ is the component-wise product.

Complexities

Theorem

To every couple (q, d) with q a prime power and $d \geqslant 2$ an integer s.t. $d_q \leqslant \sqrt{q}$, one can associate a normal basis $\Theta(q, d)$ of the degree d extension of $\mathbb{F}_q$ such that the following holds:

- *There exists an algorithm that multiplies two elements given in $\Theta(q, d)$ at the expense of $\tilde{O}(d \log q)$ elementary operations.*

This can be easily extend to a result without any restriction on q and d.

Remark: Here d_q is such that

- $v_\ell(d_q) = v_\ell(d)$ if ℓ is prime to $q-1$, $v_\ell(d_q) = 0$ if $v_\ell(d) = 0$,
- $v_\ell(d_q) = \max(2v_\ell(q-1)+1, 2v_\ell(d))$ if ℓ divides both $q-1$ and d.

Outline

Our approach

Using normal elliptic basis extensions,

- we can find an elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$ with a $d \simeq \log^2 n$ torsion part and construct from it a degree d elliptic extension of $\mathbb{Z}/n\mathbb{Z}$.

  $\longrightarrow$ Lentra-Pomerance arguments transpose to this case.

- elliptic extensions come, by construction, with a "degree friendly" $\mathbb{Z}/n\mathbb{Z}$ automorphism, $B \mapsto B + T$ on E.

  $\longrightarrow$ Berritzbeitia-Cheng arguments transpose too.

This yields a $\tilde{O}(\log^4 n)$ primality test, but no more deterministic (we have to find a curve E).

Elliptic AKS criterion

Theorem (Elliptic AKS criterion)

Let $n \geqslant 2$ be an integer and let E be an elliptic curve over $R = \mathbb{Z}/n\mathbb{Z}$. Let $T \in E(R)$ be a section of exact order d where d is an integer relatively prime to $2n$.

Let E' be the quotient $E/\langle T \rangle$ given by Vélu's formulae. Let $A \in E(R)$ be a section that does not cross the kernel of the dual isogeny.

Assume that,

$$(\theta_0)^n = \theta_1 \,.$$

Assume further that

$$2^{\frac{d-1}{2}} \geqslant n^{\sqrt{d}}.$$

Then n is a prime power.

Example I

We consider here a primality test for $n = 1009$.

We first notice that

$$d_{\min} = \lceil 4(\log_2 n)^2 + 2 \rceil = 401\,.$$

A quick search among maximal quadratic imaginary orders $\mathcal{O}$ (for decreasing fundamental discriminants) yields

$$d = 479 \text{ for } -\Delta = -148\,.$$

In truth, we have

$$52^2 + 3^2\,148 = 4\,n\,,$$

and the corresponding elliptic curve has got $n + 1 - 52$ $(= 2 \times 479)$ points.

Example II

The Hilbert class polynomial associated to $-\Delta = -148$ is

$$H_{-148}(X) = X^2 - 3966018380107200\,X - 7898242515936467904000000\,.$$

One of its roots mod n is $j_E = 353$, and one can check that the point $T = (296, 432)$ is of order d on the elliptic curve

$$E \ : y^2 + xy = x^3 + 364\,x + 907.$$

Similarly, we can check that the point $M = (726, 695)$ is of order 958. Vélu's formulae yield then the quotient elliptic curve,

$$E/\langle T\rangle \ : y^2 + xy = x^3 + 130\,x + 233\,.$$

We choose $A = (383, 201)$, a point of order d on $E/\langle T\rangle$. We can check also that the image of M by the isogeny is equal to $N = (321, 344)$, a point of order 2.

Example III

We can now define, without any ambiguity, a normal elliptic basis

$$\Theta = (\theta_k)_{k \in \mathbb{Z}/d\mathbb{Z}} .$$

A final computation yields

$$\theta_0^{1009} = \theta_{91} .$$