Vedi, vedi, è difficile spiegare,
è difficile capire,
se non hai capito già ...

Francesco Guccini

To E. Engeler, E. Specker and J. Waldvogel

[P. Mihăilescu]Universität Paderborn

EFFICIENT "QUASI"- DETERMINISTIC PRIMALITY TEST IMPROVING AKS. DRAFT

PREDA MIHĂILESCU AND ROBERTO M. AVANZI

Abstract. We combine ideas from the seminal paper of Agrawal, Kayal and Saxena [AKS] as improved by Lenstra [Le3] with the particular case sharpening of Berrizbeitia and Qi Cheng and introduce the cyclotomy of rings setting ([Le2], [BovdH] and [Mi]) for the later. Thus we deduce a new variant of the AKS algorithm which:

(i) has run - time $O\left(\log^{4+o(1)}(n)\right)$.
(ii) works on all prime candidates $n > e^{e^{2e}}$.
(iii) is "quasi deterministic", in the sense that it is deterministic under the assumption that some roots of unity can be found in polynomial time, while failing to do so would raise an explicit contradiction to the GRH.

The bottleneck of the algorithm are the *space* requirements.

1. Introduction

Agrawal, Kayal and Saxena surprised the mathematical world in August 2002 with a polynomial deterministic primality proving algorithm. The strikingly beautiful algorithm relays on (essentially) the following theorem:

Theorem 1 (Agraval, Kayal, Saxena)**.** *Let n be a positive integer and r, q be primes such that $(p,n) = 1$ for all primes $p \leq r$, $q | r-1$, $q > 4\sqrt{r}\log(n)$ and $n^{(r-1)/q} \not\equiv 1 \bmod r$. Furthermore, suppose that*

$$(1) \quad (a+x)^n \equiv a + x^n \mod (n, x^r - 1) \quad \forall a \in \mathbb{N}, 1 \leq a \leq 2\sqrt{r} \cdot \log(n).$$

Then n is a prime power.

This magnificent idea essentially solved the complexity theoretical problem of primality proving. Since August numerous specialists are looking out for possible improvements.

Date: Version 2.0 April 23, 2003.

A theoretical "scratch" in the original paper [AKS] is due to the fact that the proof that r can be found in polynomial time relies on a theorem of Fouvry from analytical number theory, which fails to provide effective bounds. Based on this theorem Agrawal et. al. proved the upper bound $r = O(\log n)^6$ while the conjectural and empirically plausible bound is $r = O(\log n)^2$. The problem was soon removed by H.W. Lenstra Jr [Le3]. Lenstra succeeded at the same time to remove the condition that just about any parameter in theorem 1 be prime, except of course for n. We shall state and prove his theorem in a slightly more general setting in the next section. Ulterior joint work of Lenstra and Pomerance continued to improve the provable upper bound on r.

From a practical point of view, both tests (1) and Lenstra's variation thereof need to be performed in extensions of $\mathbb{Z}/(n \cdot \mathbb{Z})$ of *very large degree* $O\big((\log n)^2\big)$. What more is, the number of individual tests (exponentiations in an extension) which need to performed is equally large. These two facts make the first versions of the AKS tests, including Lenstra's improvements, prohibitive even for modestly large integers n, of say 300 decimal digits.

In order to reduce the number of exponentiations to just one, Berrizbeitia [Be] made the following observation: Suppose that a sufficiently large power of 2 divides $n-1$, say $2^k = T || (n-1)$ and $T > (\log n)^2$ and furthermore, that a primitive $T-$th root $a \bmod n$ exists in the sense that $a^T = 1$ but $(a^{T/2} - 1, n) = 1$. Then one may consider the extension $\mathbf{R} = \mathbb{Z}/(n \cdot \mathbb{Z})[X]/(X^T - a)$ with $\xi \in \mathbf{R}$ given by $\xi = X \bmod (X^T - 1)$. If $\mu \in \mathbb{C}$ is a primitive T^2-th root of unity and ι is the natural map $\mathcal{O}(\mathbb{Q}(\mu))/(n \cdot \mathcal{O}(\mathbb{Q}(\mu))) \to \mathbf{R}$ with $\mu \mapsto \xi$, then $\iota\left(\mathcal{O}(\mathbb{Q}(\mu^T))\right) = \mathbb{Z}/(n \cdot \mathbb{Z})$ and $[\mathbb{Q}(\mu) : \mathbb{Q}(\mu^T)] = [\mathbf{R} : \mathbb{Z}/(n \cdot \mathbb{Z})]$. The conjugates of μ over $\mathbb{Q}(\mu^T)$ are $\mu \cdot \mu^{iT}$, for $i = 1, 2, \ldots, T$ and they are all distinct modulo n. Based on this observation, Berrizbeitia shows that if

$$(1 + \xi)^n = 1 + \xi^n \quad \text{as elements of } \mathbf{R}, \tag{2}$$

then $(1 + b\xi)^n = 1 + b^n \xi^n = 1 + b\xi^n$ for all $b \in S = \{a^i : i = 1, 2, \ldots, T\}$. He then adapts the proof of Theorem 1 to deduce that n must be a prime power. Thus, the number of tests is reduced to one (2), but the extension degree does not drop. What more is, the test is only applicable to n such that $T|(n-1)$. The idea is deep and it was slightly generalized by Qi Cheng [QC], who allowed a general prime power $r^k|(n-1)$ - thus increasing the number of special values of n which could be proved by his AKS variant. We do not discuss his additional interesting, yet not relevant in our context, idea of using ECPP in order achieve an all purpose test.

Cyclotomy of rings, as born in the celebrated primality test of Adleman, Rumely and Pomerace [ARP] and Lenstra's presentation [Le1] at the Bourbaki seminar, and subsequently developed and implemented in [BovdH] and [Mi, Mi1], deals exactly with the situation in which one does not have a sufficient factored part of $n-1$ (the prime 2 is always a factor if n is odd). It allows to build *cyclotomic extensions* of $\mathbb{Z}/(n \cdot \mathbb{Z})$ of degree k such that $n^k - 1$ has a large – in the cyclotomy primality test: $O(\sqrt{n})$ – completely factored part.

The idea of Berrizbeitia can be generalized if one replaces $\mathbb{Z}/(n \cdot \mathbb{Z})$ by an extension $\mathbf{A} \supset \mathbb{Z}/(n \cdot \mathbb{Z})$ of degree k, such that a factored part $m|n^k - 1$ with $m = O(\log^{2+o(1)}(n))$ is known. We encounter in this context the problem solved in the test of [ARP], yet scaled down to mere $O(\log^2(n))$: minimize $\mathrm{ord}_m(n) = |\langle n \bmod m \rangle|$ subject to (essentially) $m > \log^2(n)$. By a celebrated theorem of

Prachar and Odlyzko, used in [ARP], this problem has very satisfactorily solutions in the order of magnitude $\mathrm{ord}_m(n) = O\left(((\log_2(n))^{\log_4(n)}\right)$, where the notation $\log_i(n)$ deviates from the usual and means the i - fold iterated logarithm.

The galois theory of cyclotomic extensions is quite well understood in the context of primality testing. We show in this paper that the idea of Berrizbeitia applied in small cyclotomic extensions leads to the most performing primality proving algorithm currently known. Not only do we reduce the number of tests this way to one for all input integers n, but by forcing the factored part to be a *very smooth* integer and using the chinese remainder theorem in the group ring, we reduce the one AKS in a extension of huge degree, to several few ones in extensions of modic degrees.

Remark 1. *At completion of this paper I was informed that D. Bernstein has also announced a generalization of the idea of Berrizbeitia* [Br], *yielding a* $O(\log^{4+o(1)}(n))$ *test.*

2. Cyclotomic extensions

Since their definition by Lenstra [Le2], cyclotomic extensions have undergone various changes in name and *Gestalt*, over "cyclotomic constellations" [BovdH], "cyclotomic extensions of finite rings" [Mi, Mi1] to "pseudo-fields" [Le3]. Essentially the reader may imagine a cyclotomic extension to be an extension of the ring $\mathbb{Z}/(n \cdot \mathbb{Z})$ which contains a $s-$th root of unity ζ and about which one can prove - without knowing that n is prime - sufficient properties in order to be allowed to work in the extension as if it was a finite field and n were a prime. We shall review here various definitions and important properties of cyclotomic extensions, which will be used in the constructions and proofs underlying our algorithm. The theory of cyclotomy of rings being covered in the works cited above, we refer the reader to the proofs given in the literature for the facts we ennounce here.

In a more formal way, let us start by defining galois extensions of $\mathbb{Z}/(n \cdot \mathbb{Z})$ accroding to Lenstra's [Le2]:

Definition 1. *If G is a group, a ring $\mathbf{R} \supset \mathbb{Z}/(n \cdot \mathbb{Z})$ is called galois extension of $\mathbb{Z}/(n \cdot \mathbb{Z})$ with group G, if, given $t = \#G$, there are t elements $z_1, z_2, \ldots, z_t \in \mathbf{R}$ such that:*

(i) $\mathbf{R} = \prod_{i=1}^{t} (\mathbb{Z}/(n \cdot \mathbb{Z})) \cdot z_i$ *and the map* $\mathbb{Z}/(n \cdot \mathbb{Z}) \to \mathbf{R}$ *is injective,*

(ii) $\det(\sigma(z_i))_{\sigma \in G} \in \mathbb{Z}/(n \cdot \mathbb{Z})^*$.

Note that (ii) implies that the z_i must be $\mathbb{Z}/(n \cdot \mathbb{Z})$ - linear independent. Here are some examples of galois extensions of rings, from [Le2, Mi]:

Examples 1.

(a) *If $\mathbf{R}_i$ is galois over $\mathbb{Z}/(n \cdot \mathbb{Z})$ with group G_i, for $i = 1, 2$ then $\mathbf{R}_1 \otimes_{\mathbb{Z}/(n \cdot \mathbb{Z})} \mathbf{R}_2$ is galois over $\mathbb{Z}/(n \cdot \mathbb{Z})$ with group $G_1 \times G_2$.*

(b) *If n is a prime, $\mathbb{Z}/(n \cdot \mathbb{Z})$ is a galois field $\mathbb{K}$ and a galois extension $\mathbf{R}$ of $\mathbb{K}$ in the sense of field theory is a galois extension of $\mathbb{Z}/(n \cdot \mathbb{Z})$ in the sense of definition 1.*

(c) *Let s be a positive integer with $(n, s) = 1$ and ζ_s a primitive $s-$*th *root of unity in $\mathbb{C}$. The ring $\mathbf{R} = \mathbb{Z}[\zeta_s]/(n \cdot \mathbb{Z}[\zeta_s])$ is galois over $\mathbb{Z}/(n \cdot \mathbb{Z})$ with* *group $G = (\mathbb{Z}/s\cdot\mathbb{Z})^*$. The element $(x \bmod s)$ acts upon $\mathbf{R}$ by raising ζ_s to the power x.*

(d) *Consider example (c) with n a prime and $\mathbb{Z}/(n\cdot\mathbb{Z})$ a galois field. If*

$$H = (\mathbb{Z}/s\cdot\mathbb{Z})^* \,/\, \langle n \bmod s\rangle$$

and $t = \#\langle n \bmod s\rangle$ then

$$\mathbf{R} \;=\; \mathbb{Z}[\zeta_s]/(n\cdot\mathbb{Z}[\zeta_s]) \;\cong\; \prod_{\rho\in H} \mathbb{F}_{p^t} \tag{3}$$

by basic algebraic number theory.

If $s \in \mathbb{N}$, let Φ_s denote the $s-$th cyclotomic polynomial. The *intrinsic* definition of cyclotomic extension, such as given in [Le2] is:

Definition 2 ([Le2], (4.1))**.** *Let n, s be positive integers. An $s-$th cyclotomic extension $(\mathbf{R}, \sigma, \zeta)$ of $\mathbb{Z}/(n\cdot\mathbb{Z})$ is an $\mathbb{Z}/(n\cdot\mathbb{Z})$-algebra $\mathbf{R}$ together with an automorphism σ of $\mathbf{R}$ and an element $\zeta \in \mathbf{R}$ such that:*

(i) *$\mathbf{R}$ is galois over $\mathbb{Z}/(n\cdot\mathbb{Z})$ with group generated by σ.*
(ii) *$\Phi_s(\zeta) = 0$ and $\sigma\zeta = \zeta^n$.*
(iii) *$\sigma^t = id_{\mathbf{R}}$.*

If these conditions hold, s is the order *and t is the* degree *of the extension $\mathbf{R}$.*

Cyclotomic extensions are rich in equivalent properties [Mi]. The pairs (n, s) for which cyclotomic extensions exist are exceptional and the existence of such pairs is considered as a property of n with respect to s which qualifies n to behave like a prime. A simple property reflecting this fact is the following: an $s-$th cyclotomic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$ exists if and only if

$$r \in \langle n \mod s\rangle, \qquad \text{for all} \quad r \mid n. \tag{4}$$

Next we show some useful models of an $s-$th cyclotomic extension:

Fact 1. *Let n, s be positive integers. Suppose that there is a polynomial $\Psi(x) \in \mathbb{Z}/(n\cdot\mathbb{Z})[X]$ of degree $t = |\langle n \mod s\rangle|$ such that:*

(i) *$\Psi(x) \mid \Phi_s(x)$*
(ii) *if $\mathbf{R} = \mathbb{Z}/(n\cdot\mathbb{Z})[X]/(\Psi_s(X))$ and $\zeta = (X \mod \Psi(X)) \in \mathbf{R}$, then $\Psi(\zeta^{n^i}) = 0$ for $i = 1, 2, \ldots, t$*
.

Then $(\mathbf{R}, \sigma, \zeta)$, where $\sigma(\zeta) = \zeta^n$, is an $s-$th cyclotomic extension.

The next model shows the connection between cyclotomic extensions and the ring of integers of certain subfields of the $s-$th cyclotomic field.

Fact 2. *Let n, s be integers and $G = \langle n \bmod s\rangle \subset \mathbb{Z}/(s\cdot\mathbb{Z})^\times$. Let $\mathbb{K} = \mathbb{Q}(\zeta_s) \subset \mathbb{C}$ be the $s-$th cyclotomic field and $\mathbb{K}_0 = \mathbb{K}^G \subset \mathbb{K}$ be subfield fixed by G. Let $\mathbf{R} \supset \mathbb{Z}/(n\cdot\mathbb{Z})$ be a galois ring of degree $t = \mathrm{ord}_s(m)$.*

(iv) *Suppose there is an homomorphism*

$$\iota : \mathcal{O}(\mathbb{K}) \to \mathbf{R} \quad \textit{such that} \quad \iota\,(\mathcal{O}(\mathbb{K}_0)) = \mathbb{Z}/(n\cdot\mathbb{Z}),$$

and let $\zeta = \iota(\zeta_s) \in \mathbf{R}$ and define $\sigma : \zeta \mapsto \zeta^n$. Then $(\mathbf{R}, \sigma, \zeta)$ is an $s-$th cyclotomic extension.

(v) *If* $(\mathbf{R}, \sigma, \zeta)$ *is an* $s-$th *cyclotomic extension, then there is an homomorphsim* $\iota : \mathcal{O}(\mathbb{K}) \to \mathbf{R}$ *with* $\mathcal{O}(\mathbb{K}_0) = \mathbb{Z}/(n \cdot \mathbb{Z})$ *and we have the commutative diagram:*

$$\tau(\iota(\alpha)) = \iota(\sigma(\alpha)) \quad \textit{for all} \quad \alpha \in \mathcal{O}(\mathbb{K}_1).$$

(vi) *The properties (v), (vi) hold when replacing* $\mathbb{K}_0$ *by some* $\mathbb{K}_0' \subset \mathbb{K}_0$ *and* $\mathbb{K}' \supset \mathbb{K}_0'$ *having group* $Gal\ (\mathbb{K}'/\mathbb{K}_0') = G$.

(vii) *If* $(\mathbf{R}, \sigma, \zeta)$ *and* ι *are like in (v) or like in (vi), then* $\mathbf{R}' = \iota(\mathcal{O}(\mathbb{L}))$ *is a galois extension for any field* $\mathbb{K}_0' \subset \mathbb{L} \subset \mathbb{K}'$. *The ring* $\mathbf{R}'$ *contains Gauss periods length* $l = \frac{|\langle n \bmod s \rangle|}{|G|}$. *It is an instance of a* pseudo - field *in the recent terminology of* [Le3].

Let p be an odd prime and $k(p) = v_p\left(n^{p-1} - 1\right)$, with v_p the p - adic valuation. If it exists, an $p-$th cyclotomic extension of $\mathbb{Z}/(n \cdot \mathbb{Z})$ may contain also a $p^{k(p)}-$th primitive root of unity; this is in fact true if n is a prime. This leads to the following

Definition 3. *Let* p *be a prime. The* saturation exponent *of* p *is:*

$$k(p) = \begin{cases} v_2(n^2 - 1) & \textit{if } p = 2 \textit{ and } n = -1 \bmod 4 \\ v_p\left(n^{p-1} - 1\right) & \textit{otherwise} \end{cases} \tag{5}$$

Let $m = \prod_i p_i^{e(i)} \in \mathbb{N}$ *be the prime factorization of an integer. The* (n -) saturated order above m *is:*

$$\overline{m} = \prod_i p_i^{\max(e(i), k(p_i))}.$$

An $m-$th *cyclotomic extension* $(\mathbf{R}, \sigma, \zeta)$ *is called* **saturated** *if* $m = \overline{m}$ *and* **subsaturated** *otherwise. If* $e(i) = k(p_i)$ *for all* $p_i | m$, *the extension is* minimal saturated.

Saturated extensions are characterized by the following property:

Theorem 3. *If* $(\mathbf{R}, \sigma, \zeta)$ *is a saturated* $m-$th *extension and* $m' | m^h$ *for some* $h > 0$ *(i.e.* m' *is built up from primes dividing* m*), then* $\mathbf{R}[X]/(X^{m'} - \zeta)$ *is an* $m \cdot m'-$th *cyclotomic extension.*

Since the existence of cyclotomic extensions needs in general to be proved, the meaning of this theorem is that it suffices to prove the existence of minimal saturated extensions; the existence of extension of higher orders above the same radical follows.

Suppose that $\mathbf{R}' \supset \mathbf{R}$ are respectively $m'-$th and $m-$th cyclotomic extensions with $m | m'$ having the same radical and $\mathbf{R}$ is saturated. Then

$$\text{Gal}\ (\mathbb{Q}(\zeta_{m'})/\mathbb{Q}(\zeta_m)) \cong \text{ Gal } (\mathbf{R'}/\mathbf{R}) \cong \langle n^{\text{ord}_m(n)} \bmod m' \rangle.$$

We include finally for completeness the celebrated theorem of analytic number theory which underlies the algorithm of Adleman, Pomerance and Rumeley [ARP].

Theorem 4 (Prachar, Odlyzko, Pomerance)**.** *There exists an effectively computable positive constant* c *such that* $\forall\ N > e^e, \quad \exists\ t > 0$ *satisfying*

$$t < (\log N)^{c \cdot \log \log \log N} \quad \textit{and} \quad \prod_{\{q \in \mathcal{P}, (q-1) | t\}} q^2 > N, \tag{6}$$

where $\mathcal{P} \subset \mathbb{N}$ *is the set of primes. In particular, if we define for such* t *the function* $f(t) = \prod_{\{q \in \mathcal{P}, (q-1) | t\}} q$, *then* $\lambda(f(t)) = O(t^{1/\log_2(t)})$, *where* $\lambda(x) = lcm_{\ p^{e(p)} || x} \left(\varphi(p^{e(p)})\right)$ *is the Carmichael function.*

3. Primality test

We start with some preparatory

Lemma 1 (Lenstra, [Le3]). *Let n be an integer which is not a prime power and $\ell | n$. Furthermore, let M be an integer which is coprime to n and define*

$$\gamma = GCD\{n^i \ell^j - n^{i'} \ell^{j'} : i, j; i', j' \in \mathbb{Z}_{>0} \text{ and } n^i \ell^j \equiv n^{i'} \ell^{j'} \mod M\}.$$

Suppose also that $\langle \ell \bmod M \rangle \subset \langle n \bmod M \rangle$. Then

$$\gamma \leq n^{\sqrt{|\langle n \bmod M \rangle|/3}}. \tag{7}$$

Proof. Apply Minkowski's theorem ... □

We shall consider the situation in which a composite n allows a $s-$th cyclotomic extension $(\mathbf{R}, \sigma, \zeta)$ and are interested in the structure of its reduction modulo eventual primes dividing n. This is given by the following:

Lemma 2. *Let n, s be positive integers and $(\mathbf{R}, \sigma, \zeta)$ be an $s-$th cyclotomic extension of $\mathbb{Z}/(n \cdot \mathbb{Z})$. Suppose that $\ell | n$ is a prime. Let $\mathcal{L} = \mathcal{L}_1 \subset \mathbf{R}$ be a maximal ideal containig ℓ and $\mathcal{L}_{i+1} = \sigma(\mathcal{L}_i)$ for $i = 1, 2, \ldots, t-1$ with $t = |\langle n \bmod s \rangle|$. Then the ideal*

$$(\ell) = \ell \cdot \mathbf{R} = \prod_{i=1}^{t} \mathcal{L}_i$$

$$(\ell) = \ell \cdot \mathbf{R} = \prod_{i=1}^{t} \mathcal{L}_i \tag{8}$$

$$\mathbf{R}' = \bigoplus_{i=1}^{t/u} \mathbb{F}_q = \sum_{i=1}^{t/u} \mathbf{k}_i \quad \textit{with} \quad \mathbf{k}_i \cong \mathbb{F}_q \tag{9}$$

$$= \{\sum_{j=0}^{d-1} a_j \cdot \xi'^j : a_j \in \mathbb{F}_\ell \} \tag{10}$$

if $\alpha_i = \sum_{j=0}^{d-1} a_{i,j} \cdot \xi'^j \in \mathbf{R}'$ for $i = 1, 2$ then $\alpha_1 = \alpha_2$ iff $a_{1,j} = a_{2,j}$ for all $j = 0, 1, \ldots, M-1$.

The theorem of Lenstra announced in the introduction is the following:

Theorem 5 (Lenstra, october 2002). *Let n, d be pairwise coprime positive integers and $\mathbb{Z}/(n \cdot \mathbb{Z}) \subset (\mathbf{R}, \sigma, \zeta)$ a full cyclotomic extension of degree $[\mathbf{R} : \mathbb{Z}/(n \cdot \mathbb{Z})] = d$ and order M, with η a primitive $m-$th root of unity. Suppose that:*

A. *There is a finite set $S \subset \mathbf{R}$ such that $a - b \in \mathbf{R}^\times$ for all distinct $a, b \in S$ and*

$$(1 + a \cdot \eta)^n = \sigma(1 + a \cdot \eta) \quad \textit{for all} \quad a \in S. \tag{11}$$

B. $\binom{d+|S|-1}{|S|} \geq n^{\sqrt{d/3}}$.

Then n is a prime power.

Proof. Lenstra's initial theorem used $S = \{1, 2, \ldots, k\} \subset \mathbb{Z}$. However the proof is similar.

Suppose that n is composite, not a prime power and let $\ell | n$ be a prime. We let $\mathbf{R}' = \mathbf{R} \bmod \ell$, a galois ring. Let $\mathfrak{L} \supset (\ell)$ a maximal ideal of $\mathbf{R}$ containing ℓ; then

$\mathbf{R}/\mathfrak{L} = \mathbb{F}_{\ell^u} = \mathbb{F}_q$ for some $u|d = [\mathbf{R} : \mathbb{Z}/(n \cdot \mathbb{Z})]$ and $\langle p \bmod M \rangle \subset \langle n \bmod M \rangle$. Thus

$$\mathbf{R}' = \bigoplus_{i=1}^{d/u} \mathbb{F}_q = \sum_{i=1}^{d/u} \mathbf{k}_i \quad \text{with} \quad \mathbf{k}_i \cong \mathbb{F}_q \tag{12}$$

$$= \{\sum_{j=0}^{d-1} a_j \cdot \xi'^j : a_j \in \mathbb{F}_\ell \} \tag{13}$$

if $\alpha_i = \sum_{j=0}^{d-1} a_{i,j} \cdot \xi'^j \in \mathbf{R}'$ for $i = 1, 2$ then $\alpha_1 = \alpha_2$ iff $a_{1,j} = a_{2,j}$ for all $j = 0, 1, \ldots, M-1$.

We define the set

$$G = \{\prod_{a \in S} (1 + a \cdot \zeta)^{e(a)} \mod \ell : 0 \leq e(a) \text{ and } \sum_a e(a) \leq m\} \subset \mathbf{R}'.$$

Note that $a - b \in \mathbf{R}^\times$ for all $a, b \in S$. By the previous remark and (10) it follows that $\alpha_{\vec{e}} = \prod_{a \in S} (1 + a \cdot \zeta)^{e(a)} \bmod \ell$ are different for different vectors of exponents $\vec{e}$. Hence the elements of G are pairwise distinct and the bound in th ehypothesis implies $|G| \geq \binom{d+|S|-1}{|S|} \geq n^{\sqrt{d/3}}$.

Let $\sigma_n \in$ Gal $(\mathbf{R}'/\mathbb{F}_p)$ be given by $\zeta' \mapsto \zeta'^n$ and $F = \{\alpha \in \mathbf{R}' : \alpha^n = \sigma_n(\alpha)\}$; it follows from (11) that $1 + a \cdot \xi \in F$ for all $a \in S$, so $F \neq \emptyset$. By multiplicativity, we also have $G \subset F$. If s is defined like in lemma 1, we prove that $|F| = s + 1$. The zero element $0 \in G$, so let $G' = G \setminus \{0\}$, which is a multiplicative group. We prove that $|G'| = s$. Let $H = \langle p \bmod M \rangle$ and $K = \langle n \bmod M \rangle / H = G/H$; let $\mathbf{k}_i = \mathbf{R}/\mathfrak{L}_i$ in (8), with $\mathfrak{L}_i$ being maximal ideals and $\nu \in K$ be such that $\mathfrak{L}_{i+1} = \nu \mathfrak{L}_i$, cyclically. If $\alpha \in \mathbf{R}'$ has the chinese remainder theorem representation $\alpha \equiv \alpha_i \bmod \mathfrak{L}_i$, then K acts on the vector $\vec{\alpha_i}$ by cyclic permutation of the entries: $\nu\alpha \equiv \nu\alpha_i \bmod \mathfrak{L}_{i+1}$. Furthermore, the projections $G_i = G' \bmod \mathfrak{L}_i$ are also multiplicative groups, as one easily verifies by considering $\alpha \in G'$ with $\alpha \equiv \nu^i \alpha_1 \bmod \mathfrak{L}_{\mathfrak{i}}$. Let $t = |G_i|$ be the common order of these multiplicative groups. Then $|G| = t \cdot d/u = s'$. One verifies from the definition of G and s that $\alpha^s = 1$ for all $\alpha \in G'$, so $s'|s$. Reciprocally, let $\beta \in \mathbf{R}'$ have order s; then $\beta \in G$. Indeed, by (8), $p \equiv n^u \bmod M$, so $\beta^{n^u - p} = 1$ and $\sigma_p = \beta^{n^u}$. The claim follows from $\sigma_n = \sigma_p \circ \nu$.

By lemma 1, $|F| = s + 1 \leq n^{\sqrt{|\langle n \bmod M \rangle|/3}} = n^{\sqrt{d/3}}$. But $|G| \geq \binom{d+|S|-1}{|S|} > n^{\sqrt{|\langle n \bmod M \rangle|/3}}$, in contradiction with $G \subset F$. Thus n must be a prime power. □

We are now able to present our main theorem, which adapts Berrizbeitia's idea to cyclotomy:

Theorem 6. *Let n be a positive integer and m be coprime to n and such that*

$$\binom{m + m \cdot \lambda(m)}{m} > n^{\sqrt{m \cdot \lambda(m)/3}}. \tag{14}$$

*Let $\overline{m}$ be the saturated n - order above m and $(\mathbf{A}, \sigma, \zeta)$ be a $\overline{m}-$*th *cyclotomic extension of degree $d_0 = \lambda(m) = [\mathbf{A} : \mathbb{Z}/(n \cdot \mathbb{Z})]$. Let $\mathbf{R} = \mathbf{A}[X]/(X^m - \zeta)$, $\xi = X \bmod (X^m - \zeta) \in \mathbf{R}$ and extend σ to $\mathbf{R}$. If*

$$(1 + \xi)^n = \sigma(1 + \xi), \tag{15}$$

then n is a prime power.

Proof. The extension $\mathbf{A}$ being saturated, it follows by theorem 3 that $\mathbf{R}$ is cyclotomic and $\text{Gal}(\mathbf{R}/\mathbf{A}) = \text{Gal}(\mathbb{K}/\mathbb{L}) = \mathbb{Z}/(m\cdot\mathbb{Z})$. Let $\rho = \zeta^{\overline{m}/m} \in \mathbf{R}$ and $S = \{\rho^i : 0 \le i < m\}$. Since $(\rho^i - \rho^j)|m$ and $(m,n) = 1$, it follows that $a - b \in \mathbf{A}^\times$ for any distinct $a, b \in S$ and we have $|S| = m$. We let $d_0 = \lambda(m) = [\mathbf{A} : \mathbb{Z}/(n\cdot\mathbb{Z})]$ and $d = [\mathbf{R} : \mathbb{Z}/(n\cdot\mathbb{Z})] = m\cdot d_0$.

In order to apply theorem 5, we have to show that (15) implies $(1+\zeta^i\xi)^n = \sigma(1+\zeta^i\cdot\xi)$ for $i = 1, 2, \ldots, m-1$. Let $\tau = \sigma^{d_0}$ be a generator of $G = \text{Gal}(\mathbf{R}/\mathbf{A})$, then $\tau\xi/\xi = \xi^{n^{d_0}-1}$; by definition, $\left((n^{d_0}-1)/\overline{m}, m\right) = 1$, so $\tau\xi/\xi$ is a primitive $m-$th root of unity (remember that ξ is one of order $m\cdot\overline{m}$). Since τ generates a group of order m, it follows that $S = \{\tau^i(1+\xi)\}$. We assume, without restriction of generality, that $\tau\xi = \zeta\xi$. The statement now follows by galois theory:

$$\begin{aligned}(1+\zeta^i\cdot\xi)^n &= (\tau(1+\xi))^n = \tau\left((1+\xi)^n\right)\\ &= \tau\sigma(1+\xi) = \sigma\tau(1+\xi) = \sigma(1+\zeta^i\cdot\xi).\end{aligned}$$

The claim of the theorem follows now by applying theorem 5 to the extension $\mathbf{R}$ with degree $d|m\cdot\lambda(m)$ and using the lower bound on the binomial coefficient in the hypothesis. □

We show how to work in smaller extensions rather then $\mathbf{R}$. Let $m = \prod p^{e(p)}$ be like in the previous theorem, $M = m\cdot\overline{m}$, $l = \text{ord}_m(n)|\lambda(m)$ and $\mathcal{M} = \{p \in \mathcal{P} : p|m\}$. Finally, let $\mu = \mu_M \in \mathbb{C}$ be a primitive $M-$th root of unity. For each $p \in \mathcal{M}$ we define:

$$\begin{array}{rcllrcl}\mathbf{R}_p &=& \mathbf{A}[X]/(X^{p^{e(p)}} - \zeta) &,& \xi_p &=& X \mod X^{p^{e(p)}} - \zeta \in \mathbf{R}_p,\\ (16)\mathbf{N}_p &=& \mathbf{N}_{\mathbf{R}/\mathbf{R}_p} \in G &,& h(p) &=& m/p^{e(p)};\\ \mathbb{K} &=& \mathbb{Q}(\mu) &,& \mathbb{K}_p &=& \mathbb{Q}(\mu^{h(p)}).\end{array}$$

Note that $\mathbf{R}_p \subset \mathbf{R}$ and $\xi_p = \xi^{h(p)}$, which allows the definition of the norms $\mathbf{N}_p$. The isomorphism $\text{Gal}(\mathbb{K}/\mathbb{K}_p) \cong \text{Gal}(\mathbf{R}/\mathbf{R}_p)$ is a usefull consequence of the definition 2 of cyclotomic extensions. Since $\text{Gal}(\mathbf{R}/\mathbb{Z}/(n\cdot\mathbb{Z})) = \langle n \bmod M\rangle$, where $M = m\cdot\overline{m}$, it follows that $\text{Gal}(\mathbf{R}/\mathbf{R}_p) = \langle n^{m\cdot l/h(p)} \bmod M\rangle$ and $\mathbf{N}_p = \sum_{i=0}^{h(p)-1} \sigma^{i\cdot m\cdot l/h(p)}$. In $\text{Gal}(\mathbb{K}/\mathbb{K}_p)$ we have

$$\mathbf{N}_m = \sum_{i=0}^{h(p)-1} \sigma_{i\cdot M/h(p)},$$

where $\sigma_x \in \text{Gal}(\mathbb{K}/\mathbb{Q})$ maps $\mu \mapsto \mu^x$. Note that the factor $m\cdot l/h(p)$ is now replaced by $M/h(p)$, for obvious reasons.

We claim that the $N = \{\mathbf{N}_p : p \in \mathcal{M}\} \subset \mathbb{Z}[G]$ is a set of coprime elements of the group ring. This can be easily verified by considering the isomorphism $\mathbb{Z}[G] \cong \mathbb{Z}[X]/(X^m - 1)$ and showing that the polynomials which are images of $\mathbf{N}_p$ are coprime in the ring $\mathbb{Z}[X]/(X^m-1)$. There is thus a linear combination $\sum_p \theta_p\cdot\mathbf{N}_p = 1$ with $\theta_p \in \mathbb{Z}[G]$. Furthermore, the norms $\mathbf{N}_p$ act, by equality of the galois group, also on $\mathbf{R}$ and the embedding $\iota : \mathcal{O}(\mathbb{K}) \to \mathbf{R}$ commutes with G.

Let $\omega_p = \mathbf{N}_p(1+\xi) = \iota(\mathbf{N}_p(1+\mu)) \in \mathbf{R}_p$. The polynomials $\mathbf{N}_p(1+\mu)$ have small coefficients in μ and can be computed symbolically, over $\mathbb{Q}$ and then mapped into $\mathbf{R}_p$.

Theorem 7. *Let n, m be odd integers such that the premises of theorem 6 hold, except for (15). for $p \in \mathcal{M}$ we let $\omega_p = \mathbf{N}_p(1+\xi) \in \mathbf{R}_p$, with $\mathbf{N}_p, \mathbf{R}_p$ defined above.*

If

$$\omega_p^n = \tau(\omega_p) \quad \textit{for all} \quad p \in \mathcal{M}, \tag{17}$$

then n is a prime power.

Proof. We have to show that (17) implies (15). Indeed,

$$\begin{aligned}(1+\xi)^n &= (1+\xi)^{n\sum_p \theta_p \cdot \mathbf{N}_p} = \prod_p (\mathbf{N}_p(1+\xi))^{n\theta_p} \\ &= \prod_p \omega_p^{n\theta_p} = \prod_p \sigma(\omega_p)^{\theta_p} = \prod_p \left(\sigma(1+\xi)^{\theta_p \mathbf{N}_p}\right) \\ &= \sigma\left(\prod_p (1+\xi)^{\theta_p \mathbf{N}_p}\right) = \sigma(1+\xi).\end{aligned}$$

□

We finally show that m satisfying (14) can be small, as a consequence of the theorem 4.

Lemma 3. *There is a $m = O\left((\log(n))^{2+o(1)}\right)$ which satisfies (14). Furthermore, such m has the number of factors $\omega(m) < 2 \cdot \log\log n$.*

Proof. We let $d = \lambda(m)$ and note that Stirling's formula implies $\binom{m+dm}{m} \sim (d+1)^m \cdot e^m$ and rigorously, if $m > d > 10$ then $\binom{m+dm}{m} > (5(d+1)/2)^m$, so the condition (14) is satisfied for $\lambda(m) > 10$ if

$$\sqrt{3m/d} \cdot \log\left(5 \cdot (1+d)/2\right) > \log n. \tag{18}$$

But by theorem 4, we can choose m such that $d = \lambda(m) = O(m^{o(1)})$ and thus $m > O(\log(n))^{2/(1-o(1))}$, which confirms the claim. The bound on the number of factors is trivial, yet useful. □

4. Algorithm and run time

We can now finally give in Table 1 an overview of the algorithm, using the notation introduced above. Let n be an odd positive integer to be tested for primality.

The consistency of this algorithm follows from the way it was defined.

The run - time estimate is based on lemma 3. Let m b chosen by this theorem and such that (14) holds. Let $\mathcal{M}$ be its set of prime factors and $t = |\mathcal{M}|$ the cardinality of this set, so $t < \log_2(n)$. For each prime $p \in \mathcal{M}$ we have to perform a test (17), i.e. an exponentiation in the extension $\mathbf{R}_p$, which has degree $\lambda(m) \cdot p^{e(p)} < \lambda^2(m)$, by construction. We shall write $M(n,h)$ for the time for a multiplication with in a ring of characteristic n and degree h. Since the time for the construction of the working extensions is nevertheless dominated by the tests of (17), we have the following run - time estimate:

$$\begin{aligned}(19) T(n) &< t \times \log(n) \times M(n, \lambda^2(m)) < \log(n) \cdot \log\log(n) \cdot M(n, \log^{o(1)}(n)) \\ &= O\left(\log^{2+o(1)}(n)\right),\end{aligned}$$

for people who *believe* in *"soft Oh"* - run - time estimates. For more practical oriented people, it is suggestive to remark that T is well estimated by $O(\log\log n)^k$ Selfridges, for some $k < 5$. In particular, the run - time of our algorithm only differs

Algorithm `Efficient AKS`

1) Find a highly composite m with $m = O\left(\log^{2+o(1)}(n)\right)$, such that (14) holds. Let $\overline{m}$ be the n - saturated order above m. Check that n is not a prime power and $(m, n) = 1$.
2) Construct a (working) cyclotomic extension with degree $[\mathbf{A} : \mathbb{Z}/(n \cdot \mathbb{Z})] = \mathrm{ord}_m(n)$. If this does not succeed, declare n composite or GRH false and stop.
3) Find a primitive $\overline{m}-$th root of unity $\zeta \in \mathbf{A}$. If this does not succeed, declare n composite or GRH false and stop.
4) For each prime $p \in \mathcal{M}$, let $\mathbf{R}_p, \xi_p, \mathbf{N}_p, \mathbb{K}, \mathbb{K}_p$ be defined in (16). Compute $\mathbf{N}_p(1+\mu) \in \mathbb{K}_p$ and let $\omega_p = \iota\left(\mathbf{N}_p(1+\mu)\right) \in \mathbf{R}_p$.
5) For each prime $p \in \mathcal{M}$, test that
$$\omega_p^n = \tau_p(\omega_p).$$
Stop, declaring n composite, if any of these tests fails.
6) Declare n prime and stop.

Table 1

from the one of probabilistic primality tests by a value which is negligible in "soft - Oh" estimates, *a soft*, yet certainly noticeable difference.

5. Practical considerations

The estimate (18) is used best if one first evaluates the right - hand side for a fixed highly composite m: let $g(m) = \sqrt{3m/\lambda(m)} \cdot \log\left(2(1+\lambda(m))\right)$. By (18) and its application (14), it follows that given value of m is sufficient for proving primality if $n < \exp(f(m))$. For example,

$$\lambda(m) = 60 \quad \text{for} \quad m = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61 \sim 7.0 \cdot 10^9. \tag{20}$$

and $n < \exp(f(m))$ for numbers with 30000 decimal digits; the maximal extension degree may be $\lambda(m) \cdot P = 60 \cdot 61 = 3660$. The number of tests is $|\mathcal{M}| = 8$. It is clear by now that the new test out beats the cyclotomy test, which is currently the best performing general primality test. Note also that this example is tight: removing the largest prime $61|m$ from the list of tests results in a reduction of the size of the target numbers n by a factor of ~ 8. More than that, using smaller λ then 60 leads to more restriction in the size of n. For $\lambda(m) = 180$, we can test numbers of more then 500000 decimal digits using 10 tests in extensions of degree up to 32500.

Note that the relevant value for a fixed test number n is $\mathrm{ord}_m(n)|\lambda(n)$, rather then $\lambda(m)$ itself. Certainly, the d - dependent part $g_1(d) = \log(5(d+1)/2)/\sqrt{d}$ in (18) is a falling functions and one is motivated to reduce the degree d bellow its maximal value $\lambda(m)$. This allows for more delicate optimizations in dependence of n.

5.1. **Certification.** It is often practical if large computations as the ones occuring in a primality test can be certified, in the sense that a verifier can convince himself of the validity of the test without having to perform all the operations which were necessary in the first run. Certification has, in primality testing, a precisely defined signification and it is not likely that a very poorly randomized test as the present one (randomness intervenes oly in the construction of the working extension $\mathbf{A}$) may allow certification in this sense.

We propose an idea which is easily realized and can confirm the fact that a full test has been performed. We consider the central tests $\omega_p^n = \sigma(1+\omega_p)$, in $\mathbf{R}_p$. Since the Galois group $G_p =$ Gal $(\mathbf{R}_p/\mathbf{A}) \cong \mathbb{Z}/(p^{e(p)} \cdot \mathbb{Z})$, we must have $\omega_p^{n^{\lambda(m)\cdot p^{e(p)}}-1} = 1$ and thus $\omega_p^{\frac{n^{\lambda(m)\cdot p^{e(p)}}-1}{p^{k(p)+e(p)}}} = \xi_p^a$ for some $a \in \mathbb{N}$. Consequently, $\varpi = \xi_p^{-a'} \cdot \omega_p$, for some explicitly computable a', is a $p^{k(p)+e(p)}-$th power in $\mathbf{R}_p$. The computations made for veriying (15) can be extended to the computation of a solution of $y^{p^{k(p)+e(p)}} = \varpi, \ y \in \mathbf{R}_p$. Since it is virtually impossible to find such a solution without performing the necessary exponentiation, by merely checking $y^{p^{e(p)}} = \varpi$, the verifier may gain a high confidence about the performed proof. He saves thus a factor of $O(\log(n))$ of the operation. Of course, information about the working extension $\mathbf{A}$ needs to be shared to. Note that the proposed "certification" provides *high confidence*, yet not a *formal proof* of the test having been performed.

Acknowledgments: I thank Francois Morain for valuable discussions on the further developments on the AKS algorithm, his insistence that I read the reuslts of Berrizbeitia and Qi Cheng - leading to the present paper - and his quick test implementation in support of these results.

References

[AdLe] L. M. Adleman, H. W. Lenstra, Jr.: "Finding irreducible polynomials over finite fields", Proc. 18-th Ann. ACM Symp. on Theory of Computing (STOC) 1986, pp. 350-355

[AKS] M. Agrawal, N. Kayal and N. Saxena: "Primes is in P", http://www.cse.iitk.ac.in/news/primality.pdf (2002)

[ARP] L. M. Adleman, C. Pomerance, R. S. Rumely: "On distinguishing prime numbers from composite numbers", Annals of Mathematics **117**, p. 173-206 (1983).

[Br] D. Bernstein: *Proving primality in essentially quartic expected time*, http://cr.yp.to/papers.html#quartic (2003).

[Be] P. Berrizbeitia: "Sharpening 'primes in P' for a large family of numbers", http://lanl.arxiv.org/abs/math.NT/0211334 (2002)

[BovdH] W. Bosma and M. van der Hulst: "Primality proving with cyclotomy", Thesis, Universiteit van Amsterdam 1990.

[Le1] H.W.Lenstra Jr.: "Primality Testing Algorithms (after Adleman, Rumely and Williams)", Seminaire Bourbaki # 576, Lectures Notes in Mathematics, **vol 901**, pp 243-258

[Le2] H.W.Lenstra Jr.: "Galois Theory and Primality Testing", in "Orders and Their Applications, Lecture Notes in Mathematics, **vol 1142**, (1985) Springer Verlag

[Le3] H. W. Lenstra Jr.: seminar lectures in Leiden and Oberwolfach, fall 2002.

[Mi] P. Mihăilescu: "Cyclotomy of rings and primality testing", Thesis ETH Nr. 12278, Zürich 1998.

[Mi1] P. Mihăilescu: *Cyclotomy primality proving - recent developments*, Proceedings of the Third International Symposium ANTS III, Portland, Oregon, Lecture Notes in Computer Science **vol. 1423** (1998), pp. 95-111.

[QC] Qi Cheng: "Primality Proving via One Round ECPP and One Iteration in AKS", http://lanl.arxiv.org/abs/math.NT/030179v1 (2003)

(R. Avanzi) Experimentelle Mathematik, Universität Essen
E-mail address, P. Mihăilescu: preda@upb.de
E-mail address, R. Avanzi: mocenigo@exp-math.uni-essen.de