Notes

on

PRIMES in $\mathcal{P}$

Hokkaido University

Laboratory for Algorithmics

by Thomas Zeugmann

Sapporo, January 2008

These notes deal with the first deterministic, polynomial time algorithm for testing primality which has been found by Agrawal, Kayal and Saxena [1].

We start by recalling some basic facts from group theory. We consider here finite multiplicative groups G and denote the neutral element by 1. We write $|G|$ to denote the cardinality of G.

Fact 1.

(1.1) For every element $a \in G$ we have: The order d of a divides $|G|$.

(1.2) If G is a cyclic group then every subgroup of U of G is also cyclic.

(1.3) If G is a cyclic group and g is any generator for it then we have: $g^i = g^j$ if and only if $|G|$ divides $i - j$.

We also need the following lemmata.

Lemma 1. *Let p be a prime and let $a \in \mathbb{Z}_p^*$, and let d be the order of a. Then we have*

(1) *d divides $p - 1$.*

(2) *If q is a prime such that $q|(p-1)$ but q^2 does not divide $p-1$, then, for $s = (p-1)/q$ we have that*

$$q|d \text{ if and only if } a^s \not\equiv 1 \bmod p \ .$$

Proof. Of course, (1) is a direct consequence of Fact 1 above. But we also provide a direct proof here. Since d is the order of a, we know that $a^d \equiv 1 \bmod p$. Now, suppose $p - 1 = kd + \ell$, where $0 < \ell < d$. Then, by Fermat's Little Theorem and construction, we get

$$1 \equiv a^{p-1} \equiv a^{kd+\ell} \equiv \left(a^d\right)^k a^\ell \equiv a^\ell \not\equiv 1 \bmod p \ ,$$

a contradiction. Thus, we must have $\ell = 0$, and hence $d|(p - 1)$. This proves (1).

For showing (2), we first note that $p-1 = qs$ and that q does not divide s. Next, assume $d|s$. Then we can write $s = ed$, and thus $a^s \equiv 1 \bmod p$. Conversely, if $a^s \equiv 1 \bmod p$, then we must have $s \geq d$. A similar argument as in the proof of Assertion (1) directly yields $d|s$. Summarizing, we have

$$a^s \equiv 1 \bmod p \text{ if and only if } d|s \ .$$

Finally, if q would divide d, then we could conclude $q|s$, too, since $d|s$. But this is impossible, since we know that q does not divide s. Hence, we arrive at q does not divide d if and only if $d|s$ if and only if $a^s \equiv 1 \bmod p$. This proves Assertion (2), and we are done. ∎

Lemma 2. *Let $n \in \mathbb{N}$, $n \geq 2$, and $a \in \mathbb{N}^+$ be such that* $\gcd(n, a) = 1$. *Then we have:*

$$n \text{ is prime if and only if } (X + a)^n \equiv (X^n + a) \bmod n \ .$$

Proof. By the Binomial theorem we have

$$(X + a)^n = \sum_{i=0}^{n} \binom{n}{i} a^i X^{n-i} \ . \tag{1}$$

If n is prime then for all $1 \leq i \leq n - 1$ we get that

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}$$

has a numerator that is divisible by n but its denominator is not. Thus, $n|\binom{n}{i}$ for all $1 \leq i \leq n - 1$. Hence, we have

$$(X + a)^n \equiv X^n + a^n \equiv X^n + a \bmod n \ ,$$

where $a^n \equiv a \bmod n$ is due to Fermat's Little Theorem. This proves the necessity.

For the sufficiency, suppose that n is not prime. Let p be any prime dividing n and let $s \geq 1$ be such that $p^s|n$ but $p^{s+1} \nmid n$. Now, we look at the coefficient with index p in (1), i.e., at

$$\binom{n}{p} \cdot a^p = \frac{n(n-1)\cdots(n-p-1)}{p!} \cdot a^p \ .$$

The numerator is divisible by p^s but not divisible by p^{s+1} and the denominator is divisible by p. Since $\gcd(n, a) = 1$ we also know that p does not divide a and thus $p \nmid a^p$, too. Consequently,

$$\frac{n(n-1)\cdots(n-p-1)}{p!} \cdot a^p$$

is *not* divisible by p^s and thus not by n. So, the coefficient of X^{n-p} is not congruent 0 modulo p. Therefore,

$$(X + a)^n \not\equiv (X^n + a) \bmod p \ ,$$

and the lemma is shown. ∎

The Algorithm

Lemma 2 directly yields a primality test. Let n be any odd number. Then one chooses any $a < n$ with $\gcd(n, a) = 1$. Clearly, if we have chosen an $a < n$ such that $\gcd(n, a) \neq 1$, then we already know that n is not prime. Next, we have to check whether or not all

coefficients of $(X+a)^n$ taken modulo n do vanish except the coefficients of X^n and of a^n. If this is the case, then n is prime; otherwise it is not.

However, this means that we have to check $n+1$ many terms and thus the running time is not polynomial in $\log n$. It is even worse than checking all odd possible factors less than $\sqrt{n}$. So, we need at least one more idea. This idea has been found by Agrawal, Kayal and Saxena. Here is there algorithm.

Algorithm AKS

Input: Odd integer $n > 1$

1. `if (` n `is of the form` a^b, $b > 1$ `) output COMPOSITE;`
2. $r := 2$;
3. `while (` $r < n$ `) {`
4. `  if (` $\gcd(n, r) \neq 1$ `) output COMPOSITE;`
5. `  if (` r `is prime ) then`
6. `    let` q `be the largest prime factor of` $r - 1$;
7. `    if (` $q \geq 4\sqrt{r}\log n$ `)`
8. `    and (` $n^{\frac{r-1}{q}} \not\equiv 1 \bmod r$ `) then`
9. `      break;`
10. $r := r + 1$;
11. }
12. `for` $a = 1$ `to` $\lfloor 2\sqrt{r}\log n \rfloor$ `do`
13. `  if (` $(X+a)^n \not\equiv (X^n + a) \bmod (X^r - 1, n)$ `) then`
14. `  output COMPOSITE;`
15. `output PRIME;`

Looking at the algorithm we see that instead of testing the equivalence

$$(X+a)^n \equiv (X^n + a) \bmod n$$

directly, they figured out that it suffices to check

$$(X+a)^n \bmod (n, X^r - 1) \quad \text{and} \quad (X^n + a) \bmod (n, X^r - 1) \ ,$$

where $X^r - 1$ is a suitably chosen polynomial. Suitably chosen means that the degree r can be kept small enough. So the coefficients are still calculated modulo n but the polynomials X^s are taken modulo $(X^r - 1)$. For example, $X^r \equiv 1 \bmod (X^r - 1)$ and thus $X^s \equiv X^{s \bmod r} \bmod (X^r - 1)$.

If n is prime, then the check is clearly satisfied. For the opposite direction, it turned out that one has to perform the check for several values of a. If all these tests are fulfilled then either n is a prime or a prime power. But the case that n is a power of some number can be handled easily.

It remains to show the correctness of the ***Algorithm AKS*** and to analyze its running time. We start with the running time.

1.1. Analyzing the Running Time

In [5] we have already presented the algorithm ***EXP***. This algorithm is easily modified to compute $(X + a)^n \bmod (n, X^r - 1)$ within $O(\log n)$ multiplications of polynomials having degree at most r and coefficients from $\mathbb{Z}_n$.

We continue by going through the algorithm. In line 1, one has to check whether or not $n = a^b$. Obviously, the possible b's can be bounded by $2 \leq b \log n$. For each such b the following computation is performed. If an $a < n$ is given, one can check by fast exponentiation if $a^b < n$ or $a^b = n$ or $a^b > n$. Therefore, we can use *binary search* in $\{1, \ldots, n\}$ to look for an a such that $a^b = n$. Such a binary search needs $O(\log n)$ exponentiations and thus $O((\log n)^2)$ arithmetic operations. Thus, the overall time needed to execute line 1 is $O((\log n)^3)$.

If n is given, a prime $r < n$ is said to be ***n-good*** if r does not divide n and if the biggest prime divisor q of $r - 1$ satisfies

(i) $q \geq 4\sqrt{r} \log n$, and

(ii) $n^{\frac{r-1}{q}} \not\equiv 1 \bmod r$.

Note that the fulfillment of Condition (ii) means that q is a divisor of the order d of n in $\mathbb{Z}_r^*$ (cf. Lemma 1). This means in particular that $q \leq d$. Together with (i) this yields a lower bound for d.

Next, the loop in lines 3 through 11 checks for $r = 2, 3, \ldots$ whether or not $gcd(n, r) \neq 1$ (in this case n is not prime) and then if r is n-good. How many times this loop is executed does depend on

$$\varrho(n) =_{df} \min\{r \mid \gcd(n, r) \neq 1 \text{ or } r \text{ is } n\text{-good or } r = n\} \ .$$

As we shall see below, $\varrho(n) = O((\log n)^6)$. Here, we estimate the running time in dependence of $\varrho(n)$. The gcd computation is done by using the procedure ***ECL*** from [5]. Thus, for one r we need time $O(\log n)$ and thus the overall time is $O(\varrho(n) \log n)$.

For checking primality of r in line 5 one maintains a prime table by the sieve of Eratosthenes up to $2^{\lceil \log r \rceil}$. This needs time $O(\varrho(n) \log\log(\varrho(n)))$.

Using the same table, one can check in line 6 if the greatest prime factor q of $r-1$ satisfies $q \geq 4\sqrt{r}\log n$. For doing this, we have to check all prime factors q' of $r-1$ with $q' < \sqrt{r}$. This clearly requires one division per possible prime factor. Thus the overall time needed here is $O((\varrho(n))^{3/2})$.

In line 8, we apply ***EXP***. Thus the time needed here is $O(\varrho(n)\log n)$. Hence, the overall time needed for executing the loop in lines 3 through 11 is $O((\varrho(n))^{3/2} + \varrho(n)\log n)$.

For the previously computed r, in lines 12, 13, 14 for each a, $1 \leq a \leq 2\sqrt{r}\log n$, one computes $(X+a)^n \bmod (X^r-1, n)$ and compares it with $X^n + a \equiv X^{n \bmod r} + r$. Since a multiplication of polynomials with coefficients from $\mathbb{Z}_n$ of degree less than r takes (in naïve implementation) time $O(r^2)$, the time for one step of fast exponentiation is $O((\varrho(n))^2 \log n)$. Thus, the time needed to execute lines 12, 13, 14 for all a is

$$O\left(\sqrt{\varrho(n)}\log n \cdot (\varrho(n))^2 \log n\right) = O\left((\varrho(n))^{5/2}(\log n)^2\right) \ .$$

Therefore, the running time of ***Algorithm AKS*** is $O((\log n)^k)$ for some constant k provided we can show that $\varrho(n) = O\left((\log n)^6\right)$.

For doing this, we need some more knowledge from number theory. First we define for all real numbers $x > 0$,

$$\pi(x) =_{df} |\{p \mid p \leq x,\ p \text{ is prime}\}| \ .$$

Then, the famous prime number theorem is telling us the following.

Theorem 1 (*Prime Number Theorem*)

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

The proof of the prime number theorem is beyond the scope of this course. Actually, for our purposes we only need a weaker version of the Prime Number Theorem which is also much easier to prove.

Theorem 2. *For all $x > 2$ we have*

$$\frac{x}{6\log x} \leq \pi(x) \leq \frac{8x}{\log x} \ .$$

Among all prime numbers $r \leq x$, in particular we are interested in those for which $r-1$ has a large prime factor. We write $P(a)$ to denote the largest prime dividing a. Furthermore, we define

$$\pi^{**}(x) =_{df} |\{r \mid r \text{ is prime}, r \leq x, P(r-1) > x^{2/3}\}|$$

Then, the following theorem holds.

Theorem 3 (*Fouvry's [3] Theorem*) *There are a constant $c > 0$ and a real x_0 such that for all $x \geq x_0$ we have $\pi^{**}(x) \geq c\frac{x}{\log x}$.*

So, for a constant fraction of all primes $r \leq x$ we have $P(r-1) > x^{2/3}$. Now, we are ready to prove the following lemma.

Lemma 4. *There exists an n_0 such that for all $n \geq n_0$ there is a prime r satisfying*

(1) $r \leq 4096 \cdot (\log n)^6$

(2) *either r divides n or r is n-good.*

Proof. We set $y = 4096 \cdot (\log n)^6$ and consider the product

$$\Pi = \prod_{j=1}^{y^{1/3}} (n^j - 1) \ .$$

Since $\Pi < \left(n^{y^{1/3}}\right)^{y^{1/3}} = n^{y^{2/3}}$ and since every prime is greater than or equal to 2 we can estimate the number N of factors in the prime factorization of Π as follows:

$$N < \log\left(n^{y^{2/3}}\right) = y^{2/3} \log n = 256 \cdot (\log n)^5 \ .$$

Therefore, by Theorem 3 there exist a $c > 0$ and an n_0 such that for all $n \geq n_0$ we have

$$\begin{aligned} 256 \cdot (\log n)^5 &< c \cdot \frac{4096 \cdot (\log n)^6}{\log(4096 \cdot (\log n)^6)} \\ &= c \cdot \frac{4096 \cdot (\log n)^6}{12 + 6 \log\log n} \\ &\leq \pi^{**}(4096 \cdot (\log n)^6) \ . \end{aligned}$$

Consequently, for all $n \geq n_0$ there is a prime r such that $r < y$ and $P(r-1) \geq y^{2/3}$ and $r \not| \, \Pi$. This prime obviously fulfills Assertion (1).

Now, if $r|n$ we are done. It remains to show that r is n-good provided it does not divide n. By construction,

$$\begin{aligned} P(r-1) &\geq y^{2/3} = y^{1/2} \cdot y^{1/6} \geq r^{1/2} \cdot y^{1/6} \\ &= \sqrt{r}(4096 \cdot (\log n)^6)^{1/6} \\ &= 4\sqrt{r} \log n \ . \end{aligned}$$

This shows (i) of the definition of n-goodness.

Since $r \not| \Pi$ we directly get $r \not| (n^j - 1)$ for all $1 \leq j \leq y^{1/3}$. Thus, we have $n^j \not\equiv 1 \bmod r$ for all these j. Hence, it suffices to show that

$$\frac{r-1}{q} \in \{1, \ldots, y^{1/3}\} \ .$$

This can be seen as follows.

$$\frac{r-1}{q} \ < \ \frac{r}{q} \ \leq \ \frac{y}{y^{2/3}} \ = \ y^{1/3} \ ,$$

and the lemma is proved. ∎

Thus, we have shown that the ***Algorithm AKS*** is leaving its `while-loop` always with an $r = O\left((\log n)^6\right)$. Putting it all together, we can summarize:

Theorem 5. *The running time of* ***Algorithm AKS*** *is* $O\left((\log n)^{17}\right)$.

1.2. Correctness

Next, we show the correctness ***Algorithm AKS***. All material needed for the correctness proof that we should already know is summarized in the appendix of this lecture. So, please check this appendix.

The main part of original proof of Agrawal, Kayal and Saxena is summarized in the following theorem. Here, we follow Bernstein [2].

Theorem 6. *Assume the following conditions to be satisfied:*

(α) $n \geq 2$ *is an odd natural number,*

(β) $r < n$ *is a prime number such that* $r \not| n$,

(γ) q *is a prime number such that* $q|(r-1)$, $q \geq 4\sqrt{r}\log n$ *and*

(δ) $n^{\frac{r-1}{q}} \not\equiv 1 \bmod n$.

Furthermore, let $L = \lfloor 2\sqrt{r}\log n \rfloor$ *and assume that*

(ε) $\gcd(a, n) = 1$ *for all* a, $1 \leq a \leq L$

(ζ) $(X + a)^n \equiv (X^n + a) \bmod (n, X^r - 1)$ *for all* a, $1 \leq a \leq L$.

Then $n = p^i$ *for a prime number* p *and an* $i \geq 1$.

Proof. The proof is done by a series of lemmata.

Lemma 7. n *possesses a prime factor* p *such that* $q \,|\, \mathrm{ord}_r(p)$.

Proof. By (δ) we have $n^{\frac{r-1}{q}} \not\equiv 1 \bmod n$. This implies that n must have a prime factor p satisfying

$$p^{\frac{r-1}{q}} \not\equiv 1 \bmod r \ . \tag{2}$$

For seeing this, suppose the converse, i.e., all prime factors p of n satisfy

$$p^{\frac{r-1}{q}} \equiv 1 \bmod r \ .$$

Then we can multiply all prime factors and obtain

$$n^{\frac{r-1}{q}} \equiv 1 \bmod r \ ,$$

a contradiction.

By (β) we know that $r \not| \, n$ and since r is prime we get $\gcd(n, r) = 1$. Hence, $d = \mathrm{ord}_r(p)$ exists and must divide $(r-1)$ (cf. Lemma 1). Thus, we have $kd = r - 1$ for some $k \in \mathbb{N}$. Therefore, $(r-1)/q = (kd)/q \in \mathbb{N}$. Since q is prime this implies $q|k$ or $q|d$. If $q|k$, then $p^{(r-1)/q} \equiv 1 \bmod r$, a contradiction to (2). Thus, we conclude $q|d$ and the lemma is shown. ∎ (Lemma 7)

In the following we shall work extensively with this prime factor p of n as well as with $\mathbb{Z}_p$ and $\mathbb{Z}_p[X]$. If $p = n$, then we are already done. Thus, from now on we assume $p \leq \frac{1}{2}n$.

Next, we observe that

$$p > L \ . \tag{3}$$

For seeing this, suppose the converse, i.e., $p \leq L$. Since p is a prime factor of n, we directly obtain $\gcd(n, p) = p$, a contradiction to (ε).

Consequently, the primality of p together with (3) implies that $\gcd(a, p) = 1$ for all $1 \leq a \leq L$. That is, $1, 2, \ldots, L \in \mathbb{Z}_p^*$ and all pairwise different. Moreover, we can conclude that all polynomials

$$X + a \quad \text{for } 1 \leq a \leq L$$

are pairwise different in $\mathbb{Z}_p[X]$.

Lemma 8. *$(X + a)^n \equiv (X^n + a) \bmod (p, X^r - 1)$ for all a, $1 \leq a \leq L$.*

Proof. By (ζ) we know that

$$(X + a)^n \equiv (X^n + a) \bmod (n, X^r - 1) \text{ for all } a, \ 1 \leq a \leq L \ .$$

Therefore, there are polynomials $f, g \in \mathbb{Z}[X]$ such that

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

Since $p|n$, we have $\ell =: n/p \in \mathbb{Z}$ and thus

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

The latter equality directly yields $(X + a)^n \equiv (X^n + a) \bmod (p, X^r - 1)$ ∎ (Lemma 8)

We can generalize Lemma 8 to exponents of the form n^i, $i \geq 0$.

Lemma 9. *$(X+a)^{n^i} \equiv (X^{n^i}+a) \bmod (p, X^r-1)$ for all a, $1 \leq a \leq L$ and all $i \in \mathbb{N}$.*

Proof. The proof is done inductively. For $i = 0$ the assertion is trivial and for $i = 1$ we have it already shown in Lemma 8. Thus, we assume the induction hypothesis for i and perform the induction step to $i+1$. Let a with $1 \leq a \leq L$ be arbitrarily fixed. By Lemma 8 we have $(X+a)^n \equiv (X^n+a) \bmod (p, X^r-1)$. This means there are polynomials $f, g \in \mathbb{Z}[X]$ such that

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

For X we substitute X^{n^i} and obtain

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

Recall that for any $m \geq 1$ we have

$$(X^m - 1) = (X-1)(X^{m-1} + X^{m-2} + \cdots + X + 1) \ .$$

Substituting X by X^r thus yields

$$(X^{rm} - 1) = (X^r - 1)(X^{r(m-1)} + X^{r(m-2)} + \cdots + X^r + 1) \ .$$

Thus, we see that $(X^r - 1)$ divides $(X^{rn^i} - 1)$ and therefore

$$(X^{n^i}+a)^n \equiv \Big((X^{n^i})^n + a\Big) \equiv (X^{n^{i+1}} + a) \bmod (p, X^r - 1) \tag{4}$$

Finally, the induction hypothesis is

$$(X+a)^{n^i} \equiv (X^{n^i} + a) \bmod (p, X^r - 1)$$

and thus we can raise both sides to the nth power yielding

$$(X+a)^{n^{i+1}} \equiv (X^{n^i} + a)^n \bmod (p, X^r - 1)$$

Now, using (4) and the transitivity of $\equiv$ we arrive at

$$(X+a)^{n^{i+1}} \equiv (X^{n^{i+1}} + a) \bmod (p, X^r - 1)$$

which completes the induction step. ∎ (Lemma 9)

We can generalize even further.

Lemma 10. *$(X+a)^{n^i p^j} \equiv (X^{n^i p^j} + a) \bmod (p, X^r - 1)$ for all a, $1 \leq a \leq L$ and all $i, j \in \mathbb{N}$.*

Proof. Let a number a with $1 \leq a \leq L$ be arbitrarily fixed. By Lemma 9 there is a polynomial $f \in \mathbb{Z}[X]$ such that

$$(X+a)^{n^i} \equiv (X^{n^i} + a) + (X^r - 1) f(X) \bmod p \ .$$

Next, we take the p^jth power on both sides and apply Theorem 18, Assertion (b). Thus, we obtain:

$$\begin{aligned}(X+a)^{n^ip^j} &\equiv \Big((X^{n^i}+a)+(X^r-1)f(X)\Big)^{p^j} \\ &\equiv (X^{n^ip^j}+a)+(X^{p^jr}-1)f(X^{p^j}) \bmod p\end{aligned}$$

Using a similar argumentation as in the proof of (4) we see that (X^r-1) divides $(X^{p^jr}-1)$ and thus, the lemma follows. ∎ (Lemma 10)

Moreover, Theorem 19 is telling us, in particular, that there is an irreducible polynomial $h \in \mathbb{Z}_p[X]$ with $\deg(h) = \mathrm{ord}_r(p)$ dividing $X^r - 1$. Thus, Lemma 10 directly implies

$$(X+a)^{n^ip^j} \equiv (X^{n^ip^j}+a) \bmod (p, h(X)) \ . \tag{5}$$

Furthermore, by Theorem 15, we know that the structure $\mathbb{F} =_{df} \mathbb{Z}_p[X]/h(X)$ is a finite field (of order $p^{\deg(h)}$). Thus, in $\mathbb{F}$ we can rewrite Equation (5) simply as

$$(X+a)^{n^ip^j} = X^{n^ip^j} + a \ . \tag{6}$$

Next, we consider all pairs (i,j) with $0 \le i,j \le \lfloor\sqrt{r}\rfloor$. Note that there are more than r such pairs . Thus, by the pigeonhole principle there must be tow different pairs (i,j) and (k,ℓ) such that

$$n^ip^j \equiv n^kp^\ell \bmod r \ .$$

We set $t := n^ip^j$ and $u := n^kp^\ell$. Without loss of generality we can assume that $t \le u$. By (6) we have $(X+a)^t = X^t + a$ and $(X+a)^u = X^u + a$. Furthermore, $t \equiv u \bmod r$ by construction and thus

$$X^t \equiv X^u \bmod (X^r - 1) \ .$$

Since $h(X)$ divides $X^r - 1$ we also have $X^t \equiv X^u \bmod (p, h(X))$ and hence $X^t = X^u$ in $\mathbb{F}$. Consequently, we can conclude

$$(X+a)^t = X^t + a = X^u + a = (X+a)^u \text{ in } \mathbb{F} \ .$$

But the latter equation means

$$(X+a)^{u-t} = 1 \text{ in } \mathbb{F} \ . \tag{7}$$

Now, we aim to show that $t = u$. Suppose we have already shown it. Then, we know that

$$n^ip^j = n^kp^\ell \text{ and therefore } p^{j-\ell} = n^{k-i} \ .$$

If $i = k$ then also $j = \ell$, a contradiction to $(i,j) \neq (k,\ell)$. Hence, n is a power of p and we are done.

Therefore, we finally show $t = u$. This proof is done indirectly. Suppose the converse, i.e., $t \neq t$. So, we have $t < u$ and thus $u - t \geq 1$. Consider the multiplicative subgroup G of $\mathbb{F}^*$ generated by the polynomials $(X + a)$, $a = 1, \ldots, L$.

Claim 1. $|G| < (1/2)n^{2\sqrt{r}} - 1$.

Equation (7) is true for polynomials $(X + a)$ and $u - t \geq 1$. Thus, the assumptions of Lemma 20 are fulfilled and we conclude $|G| \leq u - t \leq u - 1$. Taking into account that $p \leq n/2$ and that $k, \ell \leq \sqrt{r}$, we can estimate u as follows:

$$u = n^k p^\ell \leq n^k \left(\frac{p}{2}\right)^\ell \leq \left(\frac{n^2}{2}\right)^{\sqrt{r}} < \frac{1}{2} \cdot n^{2\sqrt{r}} \ .$$

Consequently, $|G| \leq u - 1 < (1/2)n^{2\sqrt{r}} - 1$ and Claim 1 is shown.

Claim 2. $|G| \geq (1/2)n^{2\sqrt{r}} - 1$.

It suffices to show that $|G| \geq 2^L - 1$, since then

$$2^L = 2^{\lfloor 2\sqrt{r} \log n \rfloor} \geq 2^{2\sqrt{r} \log n - 1} = \frac{1}{2} n^{2\sqrt{r}} \ .$$

For any subset $M \subset \{1, \ldots, L\}$ we define the polynomial $p_M(X) = \prod_{a \in M}(X + a)$. By definition, p_M is a polynomial from G and $\deg(p_M) < L$. There are $2^L - 1$ possibilities to choose M and thus there are $2^L - 1$ many polynomials p_M. These polynomials are all different over $\mathbb{Z}_p[X]$, since they have different roots (cf. (3). Since $\deg(h) = \mathrm{ord}_r(p) \geq L$, these polynomials are also all different over $\mathbb{Z}_p[X]/h(X)$. Consequently, $|G| \geq 2^L - 1$. This proves Claim 2.

Together, Claim 1 and 2 yield a contradiction, and we can thus conclude $u = t$. As seen above $u = t$ implies $n = p^i$ for some $i \geq 1$. Thus, the theorem follows. ∎

Theorem 11. *Algorithm AKS returns* `PRIME` *if and only if* n *is prime.*

Proof. Sufficiency. Let n be a prime number. Then n is not of the form a^b, $b > 1$, and hence the condition in line 1 will never happen. The tests in line 4 will always return $\gcd(n, r) = 1$. Furthermore, it does not matter why the `while-loop` is finished, by Lemma 2 we know that the test in line 13 cannot be fulfilled for all a with $n \not| a$. If $n|a$, then we have $a \equiv 0 \bmod n$ and the test is also not fulfilled. Hence, the algorithm reaches line 15 and outputs `PRIME`.

Necessity. It suffices to show that n is indeed prime if the Algorithm AKS returns in line 15 `PRIME`. We distinguish the following cases.

Case 1. The `while-loop` in lines 3 through 11 is executed to its end.

Then, after leaving the `while-loop` the variable `r` has value n. By the test in line 4 we have that for all $r < n$ the condition $\gcd(r, n) = 1$ has been verified. Thus, for all $r < n$ we get $r \not| n$, and thus n is prime.

Case 2. The `while-loop` in lines 3 through 11 is left via the `break` in line 9.

Then the variable `r` has a value $r < n$. Now, we observe

(β) $r < n$ and r is prime (checked in line 5),

(γ) the largest prime factor q of $r-1$ satisfies $q \geq 4\sqrt{r}\log n$ (checked in line 7),

(δ) $n^{\frac{r-1}{q}} \not\equiv 1 \bmod r$ (checked in line 8).

Furthermore, for all a, $1 \leq a \leq L = \lfloor 2\sqrt{r}\log n \rfloor$ we have:

(ε) $\gcd(a,n) = 1$. This is true, since $L < 4\sqrt{r}\log n \leq q < r$ (checked in line 7). Hence, in all previous executions of the `while-loop` in line 4 it has been checked whether or not $\gcd(n,a) \neq 1$. If this test would have been fulfilled ones, then the algorithm would have returned `COMPOSITE`.

(ζ) $(X+a)^n - (X^n + a) \equiv 0 \bmod (X^r - 1, n)$ (checked in the loop of lines 12 through 14).

Therefore, n, r, and q satisfy the assumptions of Theorem 6. Consequently, we get that $n = p^i$ for a prime number p and an $i \in \mathbb{N}^+$. Finally, the test in line 1 ensures that $i = 1$, and thus n is prime. ∎

References

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES in P, Manuscript 2002,
`http://www.cse.iitk.ac.in/users/manindra/primality.ps` or
`http://www.cse.iitk.ac.in/news/primality.pdf`

[2] D.J. BERNSTEIN, Proving primality after Agrawal-Kayal-Saxena, 2003,
`http://cr.yp.to/papers.html#aks`

[3] E. FOUVRY, Théorème de Brun-Titchmarsch: application au théorème de Fermat. *Invent. Math* **79** (1985), 383 – 407.

[4] I. NIVEN AND H.S. ZUCKERMAN (1960), *An Introduction to the Theory of Numbers.* John Wiley and Sons, New York.

[5] T. ZEUGMANN (2008) Course Notes on Complexity and Cryptography, TCS Technical Report, Series B, TCS-TR-B-08-03, Division of Computer Science, Hokkaido University, January, 2008.

1.3. Appendix

Within this appendix we summarize the basic material needed for a proper understanding of the Agrawal, Kayal, Saxena algorithm.

Let R be a commutative ring with 1. Then we define

$$R[x] = \text{the set of all polynomials with coefficients from } R \ .$$

That is, if $f \in R[x]$ then we can write $f(x) = \sum_{i=0}^{m} a_i x^i$, where $a_i \in R$ for $i = 0, \ldots, m$. The ***degree*** of polynomial is defined to be the largest i such that the coefficient a_i of x^i satisfies $a_i \neq 0$, where 0 denotes the neutral element with respect to addition in the ring R. We write $\deg(f)$ to denote the degree of the polynomial f. The degree of the zero polynomial is defined to be $-\infty$.

Next, we define addition and multiplication of polynomials. Let $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$. Then we define

$$(f+g)(x) = \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i =_{df} \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i \ ,$$

where $a_i = 0$ for all $i > m$ and $b_i = 0$ for all $i > n$. Furthermore, we set

$$(f \cdot g)(x) = \left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n} b_i x^i \right) =_{df} \sum_{k=0}^{m+n} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k \ .$$

Note that $R[x]$ is also ring with 1. If a ring R has no divisors of 0, then we call R an ***integral domain***. If R is an integral domain, then $R[x]$ is an integral domain, too. The latter assertion allows the following corollary.

Corollary 12. *If R is an integral domain, then* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Moreover, the following holds.

Theorem 13. *Let R be an integral domain with 1, and let $f, h \in R[x]$ such that $h \neq 0$. Then there exists uniquely determined polynomials $q, r \in R[x]$ such that*

(i) $f(x) = q(x)h(x) + r(x)$,

(ii) $\deg(r) < \deg(h)$.

Polynomials are very useful for constructing finite fields. As we already know, $\mathbb{Z}_p$ is field provided p is prime. To see how finite fields of order p^α, $\alpha \geq 2$, are constructed, we need the following definition.

Definition 1. *Let R be an integral domain with 1. A polynomial $h \in R[x]$ with $h(x) \neq 0$ is said to be **irreducible** if $h(x) = f(x) \cdot g(x)$ implies $\deg(f) = 0$ or $\deg(g) = 0$ for all $f, g \in \mathbb{Z}_p[x]$.*

That is, an irreducible polynomial allows only a trivial decomposition into factors. We can also characterize irreducible polynomials in the following way.

Definition 2. *Let R be an integral domain with 1, and let $f \in R[x]$. An element $a \in R$ is said to be a **root** of f if $f(a) = 0$.*

Then we have the following theorem.

Theorem 14. *Let R be an integral domain with 1, let $f \in R[x]$ and let a be a root of f. Then f is divisible by $(x - a)$.*

Proof. By Theorem 13 there exists a polynomial $q \in R[x]$ and an $r \in R$ such that $f(x) = q(x)(x - a) + r$. But $f(a) = 0 = (a - a) + r$. Therefore, we have $r = 0$. ∎

An immediate consequence of Theorem 14 is the following. If $a_1, \ldots, a_k$ are pairwise different roots of f then f is divisible by $(x - a_1) \cdots (x - a_k)$.

Thus, an irreducible polynomial does not have any root in the underlying integral domain with 1.

Next, we turn our attention to $\mathbb{Z}_p[x]$, where p is prime. Then one can easily generalize the definition of congruence to polynomials. That is, we write $f \equiv g \bmod h$ if h divides $f - g$, where $f, g, h \in \mathbb{Z}_p[x]$. Then we denote by $\mathbb{Z}_p[x]/h(x)$ the set of all polynomials with coefficients from $\mathbb{Z}_p$ that are reduced modulo $h(x)$. We should prove the following theorem as an exercise.

Theorem 15. *Let p be a prime and let $h \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $d \geq 1$. Then $\mathbb{Z}_p[x]/h(x)$ is a finite field of order p^d.*

We often denote any finite field of order n by $\mathbb{F}_n$. Next, we exemplify the construction of a finite field having p^d many elements, where p is prime and $d \geq 2$. As a matter of fact, all finite fields are either isomorphic to some $\mathbb{Z}_p$ or to some $\mathbb{Z}_p[x]/h(x)$. Thus, our constructions also provides a very efficient way to perform calculations in any finite field.

Example 1. We take $p = 3$ and $d = 2$. That is, we want to construct a finite field having 9 elements and provide the multiplication table for it. Thus, we need a polynomial h of degree 2 which is irreducible over $\mathbb{Z}_3$. For that purpose we can take the polynomial $h(x) = x^2 - x + 2$ which is irreducible over $\mathbb{Z}_3$, since $f(0) \equiv 2 \bmod 3$, $f(1) \equiv 2 \bmod 3$, and $f(2) \equiv 1 \bmod 3$. Now, the elements of $\mathbb{F}_9$ can be expressed as $a\vartheta + b$, where $a, b \in \mathbb{Z}_3$, using an element ϑ satisfying $\vartheta^2 - \vartheta + 2 = 0$. That is, we obtain the 9 elements: $0,\ 1,\ 2,\ \vartheta,\ 2\vartheta,\ \vartheta + 1,\ \vartheta + 2,\ 2\vartheta + 1$, and $2\vartheta + 2$. The computation with these elements is performed in the same way as computations with polynomials $\bmod (\vartheta^2 - \vartheta + 2)$ thereby reducing the coefficients modulo 3. Thus, we obtain the following multiplication

table:

$\cdot$	1	2	ϑ	2ϑ	$\vartheta+1$	$\vartheta+2$	$2\vartheta+1$	$2\vartheta+2$
1	1	2	ϑ	2ϑ	$\vartheta+1$	$\vartheta+2$	$2\vartheta+1$	$2\vartheta+2$
2	2	1	2ϑ	ϑ	$2\vartheta+2$	$2\vartheta+1$	$\vartheta+2$	$\vartheta+1$
ϑ	ϑ	2ϑ	$\vartheta+1$	$2\vartheta+2$	$2\vartheta+1$	1	2	$\vartheta+2$
2ϑ	2ϑ	ϑ	$2\vartheta+2$	$\vartheta+1$	$\vartheta+2$	2	1	$2\vartheta+1$
$\vartheta+1$	$\vartheta+1$	$2\vartheta+2$	$2\vartheta+1$	$\vartheta+2$	2	ϑ	2ϑ	1
$\vartheta+2$	$\vartheta+2$	$2\vartheta+1$	1	2	ϑ	$2\vartheta+2$	$\vartheta+1$	2ϑ
$2\vartheta+1$	$2\vartheta+1$	$\vartheta+2$	2	1	2ϑ	$\vartheta+1$	$2\vartheta+2$	ϑ
$2\vartheta+2$	$2\vartheta+2$	$\vartheta+1$	$\vartheta+2$	$2\vartheta+1$	1	2ϑ	ϑ	2

As an example, we provide the computation of the entry in row $2\vartheta+2$ and column $2\vartheta+1$. We multiply the polynomials $2\vartheta+2$ and $2\vartheta+1$, reduce the result modulo $\vartheta^2-\vartheta+2$, and the coefficients modulo 3. Thus, we obtain:

$$\begin{aligned}(2\vartheta+2)(2\vartheta+1) &= 4\vartheta^2+2\vartheta+2+4\vartheta+2\\ &= \vartheta^2+2\end{aligned}$$

and

$$\begin{array}{l}(\vartheta^2+2)\colon(\vartheta^2-\vartheta+2) \quad = 1\\ \underline{\vartheta^2-\vartheta+2}\\ \vartheta\end{array}$$

Thus, the remainder is ϑ as already displayed in the multiplication table.

Corollary 16. *If $\mathbb{F}$ is a finite field, then its multiplicative group $\mathbb{F}^*$ is cyclic.*

Again, the proof is left as an exercise.

Moreover, the following property of polynomials from $\mathbb{Z}_p[x]$ is needed for proving ***Algorithm AKS*** to be correct. In order to prove this property, we also have to recall the multinomial theorem.

Theorem 17 (Multinomial Theorem)

$$(x_1+x_2+\cdots+x_k)^n = \sum_{\substack{n_1+\cdots+n_k=n\\ n_i\geq 0}} \binom{n}{n_1,n_2,\ldots,n_k} x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}.$$

Proof. We present here an informal proof only. First observe that each of the summands on the right hand side is a result of different ways of choosing x_i's from the product on the left hand side. This is obvious, since there are n factors in the product and we choose one x_i from each factor. But still, before we can go any further, we have to clarify what the ***multinomial coefficient***

$$\binom{n}{n_1,n_2,\ldots,n_k}$$

is supposed to denote. For finding the intuitive meaning, recall that the binomial coefficient $\binom{n}{n_1}$ expresses the number of different ways to split n in two parts of size n_1 and $n-n_1$, i.e., setting $n_2 = n - n_1$, then we have $n_1 + n_2 = n$. So, it looks to be a good idea to set

$$\binom{n}{n_1, n_2} = \binom{n}{n_1} = \frac{n!}{n_1! n_2!}$$

Now, the generalization is fairly obvious. The multinomial coefficient

$$\binom{n}{n_1, n_2, \ldots, n_k}$$

is the number of ways of splitting n into k parts of sizes $n_1, n_2, \ldots, n_k$, i.e., $n_1 + n_2 + \cdots + n_k = n$. Next, we try to find a simple formula for it. We start with n objects and choose n_1 of them for the first part. This gives us $\binom{n}{n_1}$ choices. For the second part we choose n_2 from the remaining $n - n_1$ objects. For this we have $\binom{n-n_1}{n_2}$ choices. For the third part we choose n_3 from the remaining $n - n_1 - n_2$ objects, etc. Hence the total number of choices we have is

$$\begin{aligned}
\binom{n}{n_1, n_2, \ldots, n_k} &= \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} \\
&= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!} \cdots \\
&\quad \cdots \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!} \\
&= \frac{n!}{n_1! n_2! \cdots n_k!}
\end{aligned}$$

Thus, we have collected evidence for Theorem 17 to be true. The formal proof is left as an exercise.

Theorem 18. *Let p be a prime and let $f \in \mathbb{Z}_p[x]$. Then we have*

(a) $f(x)^p \equiv f(x^p) \bmod p$, *and*

(b) $f(x)^{p^j} \equiv f(x^{p^j}) \bmod p$ *for all* $j \geq 0$.

Proof. Let $f \in \mathbb{Z}_p[x]$; then we can write $f(x) = \sum_{i=0}^{k} a_i x^i$, where all $a_i \in \mathbb{Z}_p$. Then we can express $f(x)^p \bmod p$ as follows:

$$f(x)^p \bmod p = \sum_{i=0}^{pk} b_i x^i \ ,$$

where, by the multinomial theorem,

$$b_i = \sum_{\substack{i_0+\cdots+i_k=p \\ i_1+2i_2+\cdots+ki_k=i}} \frac{p!}{i_0! \cdots i_k!} \cdot a_0^{i_0} \cdots a_k^{i_k} \bmod p$$

Clearly, $p!/(i_0! \cdots i_k!)$ is divisible by p provided none of the i_s is equal to p. So, these summands are all congruent 0 mod$p$. If some $i_s = p$, then, by $i_0 + \cdots + i_k = p$ we can conclude $i_j = 0$ for all $j \neq s$. This and $i_1 + 2i_2 + \cdots + ki_k = i$ additionally implies $si_s = i$, i.e., $sp = i$ and thus $s = i/p$. Hence, in this case we have $p!/(i_0! \cdots i_k!) = 1$ and $b_i a_s^p \equiv a_s \bmod p$ by Fermat's Little Theorem. Putting it all together yields

$$\begin{aligned} f(x)^p &\equiv \sum_{s=0}^{k} b_{sp} x^{sp} \\ &\equiv \sum_{s=0}^{k} a_s (x^p)^s \\ &\equiv f(x^p) \bmod p \ . \end{aligned}$$

This proves (a).

Assertion (b) follows from (a) by a simple induction. ∎

For the correctness prove of ***Algorithm AKS*** we further need the decomposition of a very special polynomial, i.e., of the polynomial $X^r - 1$.

In the following, we use $\mathrm{ord}_n(z)$ to denote the order of z in $\mathbb{Z}_n^*$. Next, we provide the wanted decomposition of $X^r - 1$.

Theorem 19. *Let p and r be primes such that $p \neq r$. Then, in $\mathbb{Z}_p[x]$ we have*

$$\frac{x^r - 1}{x - 1} = x^{r-1} + x^{r-2} + \cdots + x + 1 = h_1(x) \cdots h_s(x) \ ,$$

where for all $i = 1, \ldots, s$, all polynomials $h_i \in \mathbb{Z}_p[x]$ are irreducible and $\deg(h_i) = \mathrm{ord}_r(p)$.

Proof. Note that $s = (r-1)/\mathrm{ord}_r(p)$. We set $q(x) = x^{r-1} + x^{r-2} + \cdots + x + 1$. Let $h \in \mathbb{Z}_p[x]$ be an irreducible factor of q with $k = \deg h \geq 1$. We show that $k = d = \mathrm{ord}_r(p)$.

First, we show that $\deg(h) \leq \mathrm{ord}_r(p)$.

Note that $\mathbb{F} = \mathbb{Z}_p[x]/h(x)$ is a finite field of order p^k (cf. Theorem 15). By Corollary 16 we know $\mathbb{F}^*$ is cyclic. Thus, there is a generator $g \in \mathbb{F}^*$. By Theorem 18 we have in $\mathbb{Z}_p[x]$ and thus in F, too,

$$g(x)^{p^d} = g(x^{p^d}) \ . \tag{8}$$

Furthermore, $x^r - 1$ is a multiple of $h(x)$ and thus we have $x^r = 1$ in $\mathbb{F}$. Since $d = \mathrm{ord}_r(p)$ we also have $p^d \equiv 1 \bmod r$. Thus, $p^d = mr + 1$ for some $m \in \mathbb{Z}$. Consequently, $x^{p^d} = x^{mr+1} = x$ in $\mathbb{F}$. By (8) we therefore conclude

$$g(x)^{p^d} = g(x^{p^d}) = g(x) \text{ and thus } g(x)^{p^d - 1} = 1 \text{ in } \mathbb{F} \ .$$

So, $p^d - 1$ must be a multiple of $p^k - 1$ (the order of g in $\mathbb{F}$). Hence, $k \leq d$.

Next, we show that $\mathrm{ord}_r(p) \leq \deg(h)$. In $\mathbb{F}$ we have $x^r = 1$. Since r is prime, the order of x in $\mathbb{F}^*$ is thus r. Hence, r must divide $|\mathbb{F}^*| = p^k - 1$. Consequently, $p^k \equiv 1 \bmod r$ and thus k is a multiple of d. ∎

Finally, we also need the following properties of groups.

Lemma 20. *Let G be a cyclic group and let $g_1, \ldots, g_m$ be elements from G, and let 1 be the neutral element of G. Let G' be the subgroup generated by $g_1, \ldots, g_m$. Then we have:*

If there is a $t \geq 1$ such that $g_i^t = 1$ for all $i = 1, \ldots, m$ then $|G'| \leq t$.

Proof. By Fact 1 at the beginning of these notes, we already know that every subgroup of a cyclic group is cyclic, too. Thus, G' is cyclic and has a generator g. Since $g \in G'$ there are indices $i_1, \ldots, i_m$ such that

$$g = g_1^{i_1} \cdots g_m^{i_m} \ .$$

Furthermore, we can calculate

$$g^t = \left(g_1^{i_1} \cdots g_m^{i_m}\right)^t = g_1^{i_1 \cdot t} \cdots g_m^{i_m \cdot t} = 1^{i_1} \cdots 1^{i_m} = 1 \ .$$

Thus t is a multiple of $|G'|$ and since $t \geq 1$ we also have $t \geq |G'|$. Hence, the lemma follows. ∎