Università degli Studi Roma Tre
Facoltà di Scienze M.F.N.
Corso di Laurea in Matematica

Tesi di Laurea Magistrale in Matematica

Primality Tests in Polynomial Time

Candidato
Alberto Bedodi

Relatore
Prof. Francesco Pappalardi

Anno Accademico 2008-2009
Febbraio 2010

Contents

INTRODUCTION

A prime number is an integer number that it is evenly divisible only by itself and 1. Since ancient times, people have been interested in the properties of this kind of numbers and have tried to find out how they work and how to determine whether a number is prime or not. Euclid, for example, has proved that these numbers are infinite and Gauss stated the the problem of distinguishing prime numbers from composite ones and factorising composite numbers is one of the most important and useful problems in arithmetic.
Besides the fascination they have, prime numbers are also of fundamental importance in mathematics in general, and cryptography in particular: in fact some crypto-systems are based on prime numbers. So it is of great interest to study their different properties, specially those properties that allow one to efficiently determine if a number is prime.
The definition of prime numbers already gives a way of determining if a number n is prime: try dividing n by every number $m \leq \sqrt{n}$, if any m divides n then it is composite, otherwise it is prime. This test is inefficient: it takes $\Omega(\sqrt{n})$ steps to determine if n is prime.
An efficient test should need only a polynomial (in the size of the input equal to $[\log n]$) number of steps.
In this thesis we analyse four efficient deterministic primality tests and a probabilistic one.
The first deterministic algorithm determining whether an input number n is prime or composite and working in polynomial time, is the AKS-Algorithm. This primality test has been created by two young student, together with their professor, in August 2002. The authors of this algorithm sent an article titled *PRIMES is in P* to some experts that immediately appreciated it for its correctness, elegance and simplicity. This article can be found at the following address:

$$\texttt{http}:\texttt{//www.cse.iitk.ac.in/news/primality.html}.$$

The greatness of this algorithm is not only the fact that it solves one of the oldest problems, but is also the fact that it does not use unproved results and that everybody can easily understand it.
In the first chapter of this thesis we deal with this algorithm an we analyse its complexity time that is $\tilde{\vartheta}(\log^{12} n)$. We also give some conjectures that,

if proved, would lead the complexity time to $\tilde{\vartheta}(\log^6 n)$; unfortunately we do not know whether they are true or not.

In the second chapter we deal with a version of the AKS algorithm with an improvement suggested by Lenstra thanks to which the complexity time is $\tilde{\vartheta}(\log^{21/2} n)$.

In the third chapter we analyse Berrizbeitia's algorithm, that works only for a large family of numbers, namely $n \equiv 1 \pmod 4$ and $n \equiv -1 \pmod 4$. In the first case the algorithm runs, in the worst case, at least 2^{11} times faster than the best possible running time for the AKS algorithm. For the case $n \equiv -1 \pmod 4$ we get the same result using 2^9 instead of 2^{11}.

In the forth chapter, which is the most important of the thesis, we present an algorithm created by Lenstra and Pomerance and whose complexity time is $\tilde{\vartheta}(\log^6 n)$. This complexity is not achieved by proving the conjectures of the AKS algorithm.

Finally, in the last chapter, we give a sketch of Bernstein's algorithm that, differently from the others, is not deterministic but probabilistic: that is, if n is composite, the output is COMPOSITE, but if n is prime, the probability that the output is PRIME is at least 1/2. However, since each run of the algorithm is independent, after k runs the probability that we have not yet distinguished if whether n is prime or composite is $< 1/2^k$ which is negligible for large k's.

Chapter 1

THE AKS-ALGORITHM

In this chapter we are going to analyse the AKS-algorithm: a deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

1.1 The idea

The test is based on the following theorem:

Theorem 1.1.1. *Let $a, p \in \mathbb{Z}$ such that* $\gcd(a,p) = 1$. *Then p is prime if and only if*

$$(x-a)^p \equiv (x^p - a) \pmod{p}. \tag{1.1}$$

Proof. We know that

$$(x-a)^p = \sum_{i=0}^{p} \binom{p}{i} (-a)^{p-i} x^i.$$

($\Rightarrow$) If p is prime, for $0 < i < p$, we have $\binom{p}{i} \equiv 0 \pmod{p}$ and, therefore, the coefficient of x^i, for $0 < i < p$, is 0. The coefficient of x^p is $\binom{p}{p}(-a)^0 = 1$. Moreover, from Fermat's Little Theorem, we have that $(-a)^{p-1} \equiv 1 \pmod{p}$ therefore the coefficient of x^0 is $\binom{p}{0}(-a)^p \equiv -a \pmod{p}$.
($\Leftarrow$) If p is composite: let's consider q a factor of p, and let $q^k \mid\mid p$, that means $p = q^k m$ with $\gcd(q,m) = 1$ and $k \geq 1$.
Then,

$$\binom{p}{q} = \frac{p(p-1)\cdots(p-(q-2))(p-(q-1))}{q!} =$$

$$= \frac{mq^k(mq^k-1)\cdots(mq^k-(q-2))(mq^k-(q-1))}{q!}$$

which, dividing both numerator and denominator by q, is equal to

$$\frac{mq^{k-1}(mq^k-1)\cdots(mq^k-(q-2))(mq^k-(q-1))}{(q-1)!}$$

since $q \nmid (mq^k-1),\ldots,(mq^k-(q-2))(mq^k-(q-1))$ we have that

$$q^k \nmid \binom{p}{q}$$

$$\Rightarrow p \nmid \binom{p}{q}.$$

Since $\gcd(a,p)=1$, we have $\gcd(p,a^{p-q})=1$. Then the coefficient of x^q in $(x-a)^p$, given by $(-a)^{p-q}\binom{p}{q}$, is not zero modulo p, while it is zero in x^p-a . So we have that $(x-a)^p-(x^p-a)$ cannot be identically null on $(\mathbb{Z}/p\mathbb{Z})$. ■

This theorem suggests a simple test of primality: given an input p, choose an a and test whether the congruence (1.1) is satisfied. This test is inefficient since it takes time $\Omega(p)$ because it evaluates p coefficients in the worst case. A simple way to reduce the number of coefficients is to evaluate both sides of (1.1) modulo a polynomial of the form x^r-1 for an appropriately chosen small r. In other words, we could test if the following equation is satisfied:

$$(x-a)^p \equiv (x^p-a) \pmod{x^r-1, p}. \tag{1.2}$$

The idea is to verify this congruence for a few values of a. From Theorem 1.1 we know that all primes satisfy the equation (1.2). The problem now is that also some composites p satisfy the equation for a few values of a and r. However we show that for appropriately chosen r if the equation (1.2) is satisfied for several $a's$ then p must be a prime power.
The number of $a's$ and the appropriate r are both bounded by a polynomial in $[\log n]$ and therefore, we get a deterministic polynomial time algorithm for testing primality.
The congruence (1.2) takes $\vartheta(r^2\log^3 p)$ time, using the successive square method to calculate the powers. The algorithm chooses an appropriate r, that is an r whose order is $\vartheta(\log^6 p)$, such that there exists a constant $\delta \geq 0$ such that a prime factor of $r-1$ is at least $r^{\frac{1}{2}+\delta}$; Etienne Fouvry, R.C.Baker and G.Harmann showed, in [18,19], that this r exists. After this, the algorithm verifies the congruence (1.2) for a "small"$(\vartheta(\sqrt{r}\log p))$ number of $a's$. We are going to show that this algorithm determines whether p is prime or not.

1.2 Algebraic preliminaries

In this section we state some algebraic results that will be used in the later proofs.

Proposition 1.2.1. *If p is prime and $h(x)$ is a polynomial of degree d irreducible in $\mathbb{F}_p$, then $\mathbb{F}_p/(h(x))$ is a finite field of order p^d.*

Since now $h(x)$ will be a factor of $\frac{x^r-1}{x-1}$ and the logarithms will be to base 2.

Proposition 1.2.2. *Let $\mathbb{F}$ be a field. The polynomial x^d-1 divides the polynomial x^n-1 if and only if d divides n.*

Proof. ($\Leftarrow$) If $d \mid n$, then, assuming $n = dm$, we have

$$x^n - 1 = x^{dm} - 1 = (x^d-1)(x^{d(m-1)} + \ldots + x^d + 1).$$

Therefore $x^d - 1 \mid x^n - 1$ in $\mathbb{F}$.
($\Rightarrow$) If $n = qd + r$, in $\mathbb{F}[x]$ we have

$$\begin{aligned}(x^n-1) &= x^{qd+r}-1\\ &= x^{qd}x^r - 1\\ &= (x^{qd}-1)x^r + x^r - 1\\ &= (x^d-1)(x^{d(q-1)}+\ldots+x^d+1)x^{n-qd}+x^{n-qd}-1\\ &= (x^d-1)(x^{n-d}+x^{n-2d}+\ldots+x^{n-qd})+(x^{n-qd}-1).\end{aligned}$$

So, if $x^d-1 \mid x^n-1$, it has to be $x^{n-qd}-1=0$, which implies $n-qd=0$ and $qd=n$. Consequently we have $d \mid n$. ■

Lemma 1.2.1. *Let p and r be prime such that $p \neq r$,*

1. *The multiplicative group of any field $\mathbb{F}_{p^t}$ for $t>0$, denoted by $\mathbb{F}^*_{p^t}$ is cyclic.*

2. *Let $f(x)$ be a polynomial with integral coefficients. Then*

$$f(x)^p \equiv f(x^p) \pmod p$$

.

3. *Let $h(x)$ be any factor of x^r-1. Let $m \equiv m_r$ (mod r). Then*

$$x^m \equiv x^{m_r} \pmod{h(x)}$$

.

4. *Let $o_r(p)$ be the order of p modulo r. Then, in $\mathbb{F}_p$, $\frac{x^r-1}{x-1}$ factorises into irreducible polynomials, each of degree $o_r(p)$*

Proof. 1. In order to show that $\mathbb{F}^*_{p^t}$ is cyclic we need to find an element $g \in \mathbb{F}^*_{p^t}$ such that $\{g, g^2, \ldots, g^{p^t-1} = 1\} = \mathbb{F}^*_{p^t}$.
Let $p^t = q$ and suppose $q \geq 3$, otherwise we have a trivial matter, and let's write $q-1 = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. For each $i = 1, \ldots, m$ let's consider $x^{\frac{q-1}{p_i}} - 1 \in \mathbb{F}_q[x]$. There exists an $a_i \in \mathbb{F}^*_q$ that is not a root of $x^{\frac{q-1}{p_i}} - 1$, since this polynomial cannot have more than $\frac{q-1}{p_i}$ distinct roots in $\mathbb{F}^*_q$.
Let $b_i = a_i^{\frac{q-1}{p_i^{\alpha_i}}}$ and $g = b_1 b_2 \cdots b_m$. We want to show that:

(a) ord(b_i)= $p_i^{\alpha_i}$

(b) ord(g)= $q-1$

Then:

(a) $b_i^{p_i^{\alpha_i}} = \; a_i^{\frac{q-1}{p_i^{\alpha_i}}}\Bigg)^{p_i^{\alpha_i}} = a_i^{q-1}$ which is equal to 1 since the order of any element of $\mathbb{F}^*_q$ divides $q-1$. Consequently we have that ord$(b_i)|$ $p_i^{\alpha_i}$. If ord(b_i)< $p_i^{\alpha_i}$, then $b_i^{p_i^{\alpha_i-1}} = \; a_i^{\frac{q-1}{p_i^{\alpha_i}}}\Bigg)^{p_i^{\alpha_i-1}} = a_i^{\frac{q-1}{p_i}} = 1$, but this is impossible since a_i is not a root of $x^{\frac{q-1}{p_i}} - 1$.

(b) We need to show that $g = b_1 b_2 \ldots b_m$ is a generator. Let's suppose that ord(g)< $q-1$, then ord$(g)|$ $q-1$ implies that ord$(g)|$ $\frac{q-1}{p_i}$ for some $i = 1, \ldots, m$.
So we have $g^{\frac{q-1}{p_1}} = b_1^{\frac{q-1}{p_i}} \cdots b_m^{\frac{q-1}{p_i}} = 1$. On the other hand, for any index $i \neq j$, the integer $p_j^{\alpha_j} =$ ord(b_j) divides $\frac{q-1}{p_i}$.
Therefore, $b_j^{\frac{q-1}{p_i}} = 1$ for any $j \neq i$ which means that $b_i^{\frac{q-1}{p_i}} = 1$ since $b_1^{\frac{q-1}{p_i}} \cdots b_i^{\frac{q-1}{p_i}} \cdots b_m^{\frac{q-1}{p_i}} = 1$; but this is impossible since, in this case, $p_i^{\alpha_i}$, which is the period of b_i, should divide $\frac{q-1}{p_i}$.

2. Let's consider $f(x) = a_0 + a_1 x + \ldots + a_d x^d$. We know that the coefficient of x^i in $f(x)^p$ is

$$\sum_{\substack{i_0+\ldots+i_d=p \\ i_1+2i_2+\ldots+di_d=i}} a_0^{i_0} \cdots a_d^{i_d} \frac{p!}{i_0! \cdots i_d!}$$

There are two cases:

(a) $i_k < p$ for any $k = 0, \dots, d$. In this case we have

$$\frac{p!}{i_0! \cdots i_d!} \equiv 0 \pmod{p}$$

(b) There exists j such that $i_j = p$ and, therefore, $i_k = 0$ for any $k \neq j$. In this case we have, from $0i_0 + 1i_1 + \ldots + di_d = 1$, that

$$i = i_j \cdot j = pj.$$

Therefore the coefficient of $x^i (= x^{pj})$ is a_j^p and, from Fermat's Little Theorem, we have

$$a_j^p \equiv a_j \pmod{p}.$$

Thus from these two cases we obtain that:

$$f(x)^p \equiv a_0 x^{p \cdot 0} + a_1 x^{p \cdot 1} + \ldots + a_d x^{p \cdot d} \equiv f(x^p) \pmod{p}.$$

3. We know that $m \equiv m_r \, (mod \; r)$ which means $m = kr + m_r$. Now,

$$\begin{aligned} & x^r \equiv 1 \pmod{x^r - 1} \\ & \quad \Rightarrow x^{kr} \equiv 1 \pmod{x^r - 1} \\ & \quad \Rightarrow x^{kr+m_r} = x^{kr} x^{m_r} \equiv x^{m_r} \pmod{x^r - 1} \\ & \quad \Rightarrow x^m \equiv x^{m_r} \pmod{h(x)}. \end{aligned}$$

4. Let $d = o_r(p)$ and let's suppose that $\frac{x^r-1}{x-1}$ has an irreducible factor, $h(x)$ in $\mathbb{F}_p$ of degree k. Now $\mathbb{F}_[x]/h(x)$ forms a field of size p^k. Let's denote $g(x)$ the generator of the cyclic multiplicative subgroup $(\mathbb{F}_[x]/h(x))^*$. We have:

$g(x)^p \equiv g(x^p) \pmod{p}$ [by fact 2 of the previous lemma]

$g(x)^p \equiv g(x^p) \pmod{p, h(x)}$

$\Rightarrow g(x)^{p^d} \equiv g(x^{p^d}) \pmod{p, h(x)}$ [by induction]

We are going to prove the induction.

Let $g(x)^{p^k} \equiv g(x^{p^k}) \pmod{p, h(x)}$ $(k \geq 1)$.

Then,

$$\begin{aligned} g(x)^{p^{k+1}} &\equiv g(x)^{p^k p} \pmod{p, h(x)} \\ &\equiv (g(x)^{p^k})^p \pmod{p, h(x)} \\ &\equiv (g(x^{p^k}))^p \pmod{p, h(x)} \quad \text{[by the inductive hypothesis]} \\ &\equiv g((x^p)^{p^k}) \pmod{p, h(x)} \quad \text{[by fact 2]} \\ &\equiv g(x^{p^{k+1}}) \pmod{p, h(x)}. \end{aligned}$$

It follows that

$$\begin{aligned} g(x)^{p^d} &\equiv g(x) \pmod{p, h(x)} \\ \Rightarrow g(x)^{p^d-1} &\equiv 1 \pmod{p, h(x)}. \end{aligned}$$

Since the order of $g(x)$ is $(p^k - 1)$, we have that $(p^k - 1) \mid (p^d - 1)$, which implies $k \mid d$.
On the other hand we also have that $h(x) \mid (x^r - 1)$ in $\mathbb{F}_p$, and, then, in the field $\mathbb{F}_p[x]/h(x)$ we have $x^r \equiv 1 \pmod{p, h(x)}$. It follows that the order of x in the field must be r (since r is prime and $x \not\equiv 1$).
Consequently, $r \mid (p^k - 1)$, that is $p^k \equiv 1 \pmod{r}$, and, therefore, $d \mid k$.
Then $k = d = o_r(p)$, which implies the Lemma.

■

In addition to the above algebraic facts, we will need the following two number theoretic facts.

Lemma 1.2.2. [18,19] *Let $P(n)$ denote the greatest prime divisor of n. There exist constants $c > 0$ and n_0 such that, for all $x \geq n_0$*

$$\left| \left\{ p \mid p \text{ is prime}, p \leq x \text{ and } P(p-1) > x^{\frac{2}{3}} \right\} \right| \geq c \frac{x}{\log x}$$

The above lemma is, in fact, known to hold for exponents up to 0.6683.

Lemma 1.2.3. [20] *Let $\pi(n)$ be the number of primes $\leq n$. Then for $n \geq 1$:*

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

1.3 The AKS Algorithms

```
                    AKS ALGORITHM
    Input:  integer $n > 1$.
    if ($n$ is of the form $a^b$, $b > 1$) output $COMPOSITE$;
    $r = 2$
    while ($r < n$){
        if ($\gcd(n, r) \neq 1$) output $COMPOSITE$;
        if ($r$ is prime)
            let $q$ be the largest prime factor of $r - 1$;
            if ($q \geq 4\sqrt{r}\log n$) and ($n^{\frac{r-1}{q}} \not\equiv 1$ mod($r$))
                break;
        $r \quad r + 1$;
    }
    for $a = 1$ to $2\sqrt{r}\log n$
        if (($(x - a)^n \not\equiv (x^n - a)$ (mod $x^r - 1, n$)) output $COMPOSITE$;
    output $PRIME$;
```

Theorem 1.3.1. *The algorithm above returns PRIME if and only if n is prime.*

We are going to prove this theorem through a sequence of lemmas. First note that the algorithm has two loops. The first one, which is a `while` loop, tries to find a prime r such that $r - 1$ has a large prime factor $q \geq 4\sqrt{r}\log n$ such that $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$, which implies that $q \mid o_r(n)$. Let us first bound the number of iterations of this loop.

Theorem 1.3.2. *There exist positive constants c_1 and c_2 for which there is a prime r in the interval $[c_1(\log n)^6, c_2(\log n)^6]$ such that $r - 1$ has a prime factor $q \geq 4\sqrt{r}\log n$ and $q \mid o_r(n)$*

Proof. Let c and $P(n)$ be as given in Lemma 1.2.2. Then the number of prime r's (called *special* primes) between $c_1(\log n)^6$ and $c_2(\log n)^6$ such that $P(r - 1) > (c_2(\log n)^6)^{\frac{2}{3}} > r^{\frac{2}{3}}$ is, for a large enough n,

$$\geq \# \text{ special primes in } [1, \ldots, c_2(\log n)^6] - \# \text{ of primes in } [1, \ldots, c_1(\log n)^6].$$

Using lemma 1.2.2, with $x = c_2(\log n)^6$, and lemma 1.2.3, with $n = c_1(\log n)^6$, we have that this number is

$$\begin{aligned}
&\geq \frac{cc_2(\log n)^6}{\log(c_2(\log n)^6)} - \frac{8c_1(\log n)^6}{\log(c_1(\log n)^6)} \\
&\geq \frac{cc_2(\log n)^6}{(\log c_2 + 6\log\log n)} - \frac{8c_1(\log n)^6}{(\log c_1 + 6\log\log n)} \\
&\geq \frac{cc_2(\log n)^6}{7\log\log n} - \frac{8c_1(\log n)^6}{6\log\log n} \\
&= \frac{(\log n)^6}{\log\log n}\left(\frac{cc_2}{7} - \frac{8c_1}{6}\right)
\end{aligned}$$

Let us choose the constants $c_1 \geq 4^6$ and c_2 such that the quantity in braces, called c_3, is positive. Let $x = c_2(\log n)^6$. We are going to prove that among these primes r there exists at least one such that $q = P(r-1)$ verifies the conditions $q \geq 4\sqrt{r}\log n$ and $q \mid o_r(n)$.
Since $q \geq r^{\frac{2}{3}} = r^{\frac{1}{2}}r^{\frac{1}{6}} \geq \sqrt{r}(4^6(\log n)^6)^{\frac{1}{6}} = 4\sqrt{r}\log n$, the first condition is satisfied.
In order to verify the second condition, let's consider the following product:

$$\prod = (n-1)(n-2)\cdots(n^{x^{\frac{1}{3}}} - 1)$$

We have $x = c_2(\log n)^6$, since $x > q \geq x^{\frac{2}{3}}$ and $r - 1 < x$, the exponent $(r-1)/q$ is in $[1, x^{\frac{1}{3}}]$. This product has $x^{\frac{1}{3}}$ factors less than $n^{x^{\frac{1}{3}}}$, each with no more than $x^{\frac{1}{3}}(\log n)$ prime factors; this implies that the product doesn't have more than $x^{\frac{2}{3}}\log n$ prime factors. In fact, $\nu_2(n) = \vartheta(\log n)$. Since

$$x^{\frac{2}{3}}\log n < \frac{c_3(\log n)^6}{\log\log n},$$

there exists at least a special prime r, that doesn't divide the product $\prod$, for which the second condition is verified. In fact, $o_r(n) \mid (r-1) \Rightarrow (r-1) = ko_r(n)$ and $q \mid (r-1)$ implies that either $q \mid k$ or $q \mid o_r(n)$, but, from $n^{\frac{(r-1)}{q}} \not\equiv 1 \pmod{r}$, we have that $q \mid o_r(n)$. This is the searched r. ∎

Once we know that the `while` loop halts, we are ready to show the following:

Lemma 1.3.1. *If n is prime, the algorithm returns PRIME.*

Proof. The `while` loop cannot return COMPOSITE since $\gcd(n, r) = 1$ for all $r < c_2(\log n)^6$, where c_2 is as in Lemma 1.2.2. By Lemma 1.2.1 (fact 2), supposing $f(x) = (x - a)$ and $p = n$, we have that $(x-a)^n \equiv (x^n - a) \pmod{n}$ which implies that the `for` loop cannot return COMPOSITE (in step 12, however, the condition should be verified also modulo $x^r - 1$, but actually this reduces the polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ and, therefore, it doesn't change the validity of the congruence. Thus, the algorithm will identify n as PRIME. ■

Now let's turn our attention to the case where n is composite.
If n is of the form a^b with $b > 1$ or if in step 4 the algorithm finds a factor of n, then the output is COMPOSITE. Let's suppose that it doesn't happen and the algorithm starts the `for` loop after finding the prime r with the `while` loop. Since n is composite let's call p_i, with $1 \leq i \leq k$, its prime factors. Obviously $n^{lcm_i\{o_r(p_i)\}} \equiv 1 \pmod{r}$ which implies that $o_r(n) \mid lcm_i\{o_r(p_i)\}$ and hence there exists a prime factor p of n such that, since $q \mid o_r(n)$, we have $q \mid o_r(p)$, where q is the largest prime factor of $r-1$.
The `for` loop uses the value of r obtained to do polynomial computations on $l = 2\sqrt{r}\log n$ binomials: $(x-a)$ for $1 \leq a \leq l$. By Lemma 1.2.1 (fact 4) we know that there exists a polynomial $h(x)$, irreducible factor in $\mathbb{F}_p$ of $\frac{x^r-1}{x-1}$, of degree $d = o_r(p)$. Note that

$$(x-a)^n \equiv (x^n - a) \pmod{x^r - 1, n}$$

implies that

$$(x-a)^n \equiv (x^n - a) \pmod{h(x), p}$$

So the identity for each binomial holds in the field $\mathbb{F}_p[x]/(h(x))$. The set of l binomials form a large cyclic group in this field:

Lemma 1.3.2. *In the field $\mathbb{F}_p[x]/(h(x))$, the group generated by the l binomials: $(x-a)$,$1 \leq a \leq l$ that is*

$$G = \{ \prod_{1 \leq a \leq l} (x-a)^{\alpha_a} \,|\, \alpha_a \geq 0, \forall\, 1 \leq a \leq l\},$$

is cyclic and of size $> \binom{d}{l}^l$.

Proof. It is clear that G is a group and, since it is a subgroup of the cyclic group $(\mathbb{F}_p[x]/(h(x)))^*$, it is also cyclic. Now consider the set

$$S = \{ \prod_{1 \leq a \leq l} (x-a)^{\alpha_a} \,|\, \sum_{1 \leq a \leq l} \alpha_a \leq d-1,\, \alpha_a \geq 0, \forall\, 1 \leq a \leq l\}$$

All the elements of S are distinct in $\mathbb{F}_p[x]/(h(x))$: as a matter of fact, the `while` loop ensures that once it halts the final r is such that $r > q > 4\sqrt{r}\log n > l$. Also step 4 of the algorithm checks gcd of r and n. If any of the a's are congruent modulo p, then $p < l < r$ and thus step 4 of the algorithm identifies n as COMPOSITE. Thus none of the a's are congruent modulo p. This implies that all elements of S are distinct in the field $\mathbb{F}_p[x]/(h(x))$ since degree of any element of S is less than d which is the degree of $h(x)$. The size of S is equal to the possibilities we have to choose the α_a. The sum of the α_a can be equal to $0, 1, \ldots, d-1$; an integer k can be obtained as sum of l non negative integers in $\binom{k+l-1}{l-1}$ different ways, so we have $\#S =$

$$\sum_{k=0}^{d-1} \binom{k+l-1}{l-1} = \binom{d+l-1}{l} = \frac{(l+d-1)(l+d-2)\cdots(d)}{l!} > \left(\frac{d}{l}\right)^l .$$

Since S is just a subset of G we get the result. ■

Since $q \mid o_r(p) = d$ and $q > 4\sqrt{r}\log n$ we have $d \geq 4\sqrt{r}\log n$, that is $d \geq 2l$ or, equally, $\frac{d}{l} \geq 2$. Therefore the size of G is greater than 2^l which, since $l = 2\sqrt{r}\log n$, is equal to $n^{2\sqrt{r}}$.
Let $g(x)$ be a generator of G. Clearly, order of $g(x)$ in $\mathbb{F}_p[x]/(h(x))$ is $> n^{2\sqrt{r}}$. We now define a set related to $g(x)$ which will play an important role in the remaining arguments. Let

$$I_{g(x)} = \{m \mid g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}.$$

Now we prove two important properties of $I_{g(x)}$:

Lemma 1.3.3. *The set $I_{g(x)}$ is closed under multiplication.*

Proof. Let $m_1, m_2 \in I_{g(x)}$. So

$$g(x)^{m_1} \equiv g(x^{m_1}) \pmod{x^r - 1, p}$$

and

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}.$$

Also we have, by substituting x^{m_1} in place of x in the second congruence:

$$\begin{gathered} g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^{m_1 r} - 1, p} \\ \Rightarrow g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p} \\ [\text{since } x^r - 1 \mid x^{m_1 r} - 1] \end{gathered}$$

From these, we get

$$\begin{aligned} g(x)^{m_1 m_2} &\equiv (g(x)^{m_1})^{m_2} \pmod{x^r - 1, p} \\ &\equiv g(x^{m_1})^{m_2} \pmod{x^r - 1, p} \\ &\equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}. \end{aligned}$$

Hence $m_1 m_2 \in I_{g(x)}$. ■

The second property of $I_{g(x)}$ that plays a crucial role in our proof is:

Lemma 1.3.4. *Let the order of $g(x)$ in $\mathbb{F}_p[x]/(h(x))$ be o_g and let $m_1, m_2 \in I_{g(x)}$. Then $m_1 \equiv m_2 \pmod{r}$ implies that $m_1 \equiv m_2 \pmod{o_g}$.*

Proof. Since $m_1 \equiv m_2 \pmod{r}$, we have $m_2 = kr + m_1$ for some $k \geq 0$. Since $m_2 \in I_{g(x)}$ we have:

$$\begin{aligned} g(x)^{m_2} &\equiv g(x^{m_2}) \pmod{x^r - 1, p} \\ \Rightarrow g(x)^{m_2} &\equiv g(x^{m_2}) \pmod{h(x), p} \\ \Rightarrow g(x)^{kr+m_1} &\equiv g(x^{kr+m_1}) \pmod{h(x), p} \\ \Rightarrow g(x)^{kr} g(x)^{m_1} &\equiv g(x^{m_1}) \qquad \text{[by Lemma 1.2.1,fact 3]} \\ \Rightarrow g(x)^{kr} g(x)^{m_1} &\equiv g(x)^{m_1} \pmod{h(x), p}. \end{aligned}$$

Now $g(x) \not\equiv 0$ implies that $g(x)^{m_1} \not\equiv 0$ and, hence, we can cancel $g(x)^{m_1}$ from both sides, leaving us with

$$g(x)^{kr} \equiv 1 \pmod{h(x), p}.$$

Therefore,

$$\begin{aligned} kr &\equiv 0 \pmod{o_g} \\ \Rightarrow m_2 &\equiv m_1 \pmod{o_g} \end{aligned}$$

■

The above property implies that there are "few" ($\leq r$) numbers in $I_{g(x)}$ that are less than o_g.
Now we are ready to prove the most important property of our algorithm:

Lemma 1.3.5. *If n is composite, the algorithm returns COMPOSITE.*

Proof. Suppose that the algorithm returns PRIME instead. Thus, the `for` loop ensures that for all $1 \leq a \leq 2\sqrt{r}\log n$ we have,

$$(x - a)^n \equiv (x^n - a) \pmod{x^r - 1, p} \tag{1.3}$$

Notice that $g(x)$ is just a product of powers of l binomials, $(1 \leq a \leq l)$, all of which satisfy equation (1.3). Then,

$$g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}$$

Therefore, $n \in I_{g(x)}$. Also, $p \in I_{g(x)}$, by Lemma 1.2.1 (fact 2), and, trivially, $1 \in I_{g(x)}$. We will now show that the set $I_{g(x)}$ has more than r number that are less than o_g, contradicting Lemma 1.3.4.
Consider the set

$$E = \left\{ n^i p^j \mid 0 \leq i, j \leq \lfloor \sqrt{r} \rfloor \right\}.$$

By Lemma 1.3.3, $E \subseteq I_{g(x)}$. Since $|E| = (1 + [\sqrt{r}])^2 > r$, there are two elements $n^{i_1}p^{j_1}$ and $n^{i_2}p^{j_2}$ in E with $i_1 \neq i_2$ or $j_1 \neq j_2$ such that $n^{i_1}p^{j_1} \equiv$

$n^{i_2}p^{j_2} \pmod{r}$ by pigeon-hole principle. But then by Lemma 1.3.4 we have $n^{i_1}p^{j_1} \equiv n^{i_2}p^{j_2} \pmod{o_g}$. This implies that

$$n^{i_1-i_2} \equiv p^{j_2-j_1} \pmod{o_g}$$

Since $o_g \geq n^{2\sqrt{r}}$ and $n^{|i_1-i_2|}, p^{|j_1-j_2|} < n^{\sqrt{r}}$, the above congruence turns into an equality. Since p is prime, this equality implies that $n = p^k$ for some $k \geq 1$. However, in step 1 of the algorithm, composite numbers of the form p^k for $k \geq 2$ are already detected. Therefore, $n = p$, but this is a contradiction since, by hypothesis, n is composite. Thus, the `for` loop of the algorithm returns COMPOSITE. ■

This completes the proof of the Theorem 1.3.1.

1.4 Time Complexity Analysis

It is straightforward to calculate the time complexity of the algorithm.

Theorem 1.4.1. *The asymptotic time complexity of the algorithm is $\tilde{\vartheta}(\log^{12} n)$, where $\tilde{\vartheta}(f(n)) = \vartheta(f(n)poly(\log f(n)))$.*

Proof.

- The first step of the algorithm verifies whether n is of the form a^b for some $b > 1$ that means calculating if $\lfloor n^{\frac{1}{b}} \rfloor^b = n$ for some b in the interval $[2, \log n]$. This requires $\vartheta(\log n \frac{\log^3 n}{\log n}) = \vartheta(\log^3 n)$ bit operations.

- As noted in Theorem 1.3.2, the `while` loop makes $r = \vartheta(\log^6 n)$ iterations. Let's now measure the work done in one iteration of the `while` loop.
The first step calculates $\gcd(n, r)$ and takes $poly(\log \log r)$ asymptotic time if the gcd is calculated by using the Euclidean Algorithm. The next two steps, determining whether r is prime and finding q (the greatest prime factor of $r - 1$), would take at most $r^{\frac{1}{2}}poly(\log \log n)$ time in the brute-force implementation.
It takes at most $poly(\log \log n)$, by using the repeated-squares method, to verify if $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$.
Thus, total asymptotic time taken by the `while` loop is: $\tilde{\vartheta}(\log^6 n \cdot r^{\frac{1}{2}}) = \tilde{\vartheta}(\log^9 n)$

- The `for` loop verifies the condition $(x - a)^n \equiv x^n - a \pmod{x^r - 1, n}$ for some a's. This is the crucial step of the algorithm, but, unluckily, it is also the step that takes the most time. If repeated-squares is used, then one iteration of this `for` loop takes $\tilde{\vartheta}(\log n \cdot r \log n)$. The number of iterations of this loop is $\vartheta(r^{\frac{1}{2}} \log n) = \vartheta(\log^4 n)$. Thus, the `for` loop takes asymptotic time $\tilde{\vartheta}(r^{\frac{3}{2}} \log^3 n) = \tilde{\vartheta}(\log^{12} n)$.

Thus, the `for` loop requires the most time and, therefore, the asymptotic time complexity of the AKS algorithm is $\tilde{\vartheta}(\log^{12} n)$. ■

1.5 Improving Time Complexity

Nevertheless, in practice, the algorithm is much faster. In fact, it is possible to prove that many positive primes r are such that $P(r-1) > r^{\frac{2}{3}}$, but it is believed that the number of primes r such that $P(r-1) = \frac{r-1}{2}$ is infinite.

Definition 1.5.1. *If both r and $\frac{r-1}{2}$ are primes, then $\frac{r-1}{2}$ is a Sophie Germain Prime. We will call such r's co-Sophie German Primes.*

The following conjecture gives the density of *Sophie German Primes.* This conjecture has been verified for $r \leq 10^{10}$.

Conjecture 1.5.1. (Sophie-German Prime Density) [21] *The number of co-Sophie German Primes $< x$ is asymptotic to $\frac{Dx}{\log^2 x}$ where D is a constant (estimated to be approximately $0.6601618\ldots$).*

If this conjecture is true, then the `while` loop exits a "suitable" r in $\vartheta(\log^2 n)$:

Lemma 1.5.1. *Assuming the conjecture 1.5.1, there exists "suitable" r in the range $\left[64\log^2 n, c_2 \log^2 n\right]$ for all $n > n_0$, where n_0 and c_2 are positive constants.*

Proof. First of all note that if both r and $q = \frac{r-1}{2}$ are prime, then the only possible orders of n modulo r are $\{1, 2, q, 2q = r-1\}$. But the order of n modulo r can be 1 or 2 for at most $2\log n$ primes r, since (n^2-1) has at most $\log(n^2-1)$ prime factors. Let's leave aside these prime factors of (n^2-1) and consider the other co-Sophie German Primes r for which the order of n modulo r is at least $\frac{r-1}{2}$. We would now like that

$$\begin{aligned} r > \frac{r-1}{2} &\geq 4\sqrt{r}\log n \\ \Rightarrow r &\geq 8\sqrt{r}\log n \\ \Rightarrow \sqrt{r} &\geq 8\log n \\ \Rightarrow r &\geq 64\log^2 n. \end{aligned}$$

Hence we consider the range $\left[64\log^2 n, c_2\log^2 n\right]$ and we show that choosing c_2 large enough, we find at least one desired r in this range. By the conjecture 1.5.1 there are $\frac{Dc_2\log^2 n}{\log^2(64\log^2 n)}$ co-Sophie German Primes less than $c_2\log^2 n$. Out of these, at most $\frac{D64\log^2 n}{\log^2(64\log^2 n)}$ are less than $64\log^2 n$ (again by the conjecture). From the remaining ones, there are at most $2\log n$ primes for which order of

n modulo r is 1 or 2.
Thus we will choose c_2 such that

$$\begin{aligned} & \frac{Dc_2 \log^2 n}{\log^2(c_2 \log^2 n)} > \frac{D64 \log^2 n}{\log^2(64 \log^2 n)} + 2 \log n \\ \text{or,} \quad & \frac{c_2 \log^2 n}{(\log \log n)^2} > \frac{100 \log^2 n}{(\log \log n)^2} \quad \text{[for large enough } n\text{]} \\ \text{or,} \quad & c_2 > 100 \quad \text{[for large enough } n\text{].} \end{aligned}$$

■

This immediately leads us to a heuristic time complexity of $\tilde{\vartheta}(r^{\frac{1}{2}}(\log n)^2)$ for the `while` loop and of $\tilde{\vartheta}(r^{\frac{3}{2}}(\log n)^3)$ for the `for` loop. Therefore, if the conjecture 1.5.1 holds, the time complexity for our algorithm is $\tilde{\vartheta}(\log^6 n)$.

Chapter 2

AKS-Algorithm with Lenstra's variant

The algorithm we are now presenting is a slight variant of the AKS algorithm, made by Lenstra, whose time complexity is $\vartheta(\log^{21/2} n)$.

2.1 Preliminaries

In this section we will use the notation $f(x) \equiv g(x) \pmod{h(x), n}$ to represent the equation $f(x) = g(x)$ in the ring $(\mathbb{Z}/n\mathbb{Z})[x]/(h(x))$.
We will use log for base 2 logarithms, and ln for natural logarithms.
For $r \in \mathbb{N}$, $\varphi(r)$ is *Euler's totient function* giving the number of numbers less than r that are relatively prime to r. It is easy to see that $o_r(a) \mid \varphi(r)$ for any a such that $\gcd(a, r) = 1$.

2.2 The Idea

This algorithm is a primality test based on the following identity for prime numbers which is a generalization of Fermat's Little Theorem:

Lemma 2.2.1. *Let $a \in \mathbb{Z}$,$n \in \mathbb{N}$, $n \geq 2$ and $\gcd(a, n) = 1$. Then n is prime if and only if*

$$(x + a)^n \equiv x^n + a \pmod{n}. \tag{2.1}$$

Proof. See proof of Theorem 1.1.1. ■

As for the previous algorithm, the above identity suggests a simple test for primality: given an input n, choose an a and test whether the congruence (2.1) is satisfied. However, this takes time $\Omega(n)$ because we need to evaluate n coefficients in the worst case.
Therefore, like in the case of the AKS algorithm, we can reduce the number

of coefficients evaluating both sides of the congruence modulo $x^r - 1$ for a chosen small r, which means test if the following equation is satisfied:

$$(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}. \tag{2.2}$$

We know that all primes n satisfy equation (2.2) for all values of a and r.
The problem now is that, just like the case of the previous section, some composites n may also satisfy the equation for a few values of a and r (and indeed they do). However we show that for appropriately chosen r if the equation (2.2) is satisfied for several $a's$ then n must be a prime power.
The number of $a's$ and the appropriate r are both bounded by a polynomial in $[\log n]$ and therefore, we get a deterministic polynomial time algorithm for testing primality.
We will need the following simple fact about the lcm of the first m numbers:

Lemma 2.2.2. *Let* LCM(m) *denote the* lcm *of the first m numbers. For* $m \geq 7$*:*

$$\mathrm{LCM}(m) \geq 2^m$$

2.3 The algorithm and its correctness

```
                    LENSTRA'S VARIANT
     Input: integer $n > 1$.
1.   if ($n = a^b$, for $b > 1$ and $a \in \mathbb{N}$) output $COMPOSITE$;
2.   Find the smallest $r$ such that $o_r(n) > \log^2 n$;
3.   If $1 < \gcd(a, n) < n$ for some $a \leq r$
4.       output $COMPOSITE$;
5.   If $n \leq r$
6.       output $PRIME$;
7.   For $a = 1$ to $[\sqrt{\varphi(r)} \log n]$ do
8.       if $((x+a)^n \not\equiv x^n + a \pmod{x^r - 1, n})$
9.           output $COMPOSITE$;
10.  output $PRIME$.
```

Theorem 2.3.1. *The algorithm above returns* PRIME *if and only if n is prime.*

In the reminder of the section, we establish this theorem through a sequence of lemmas.

Lemma 2.3.1. *If n is prime, the algorithm returns* PRIME.

Proof. If n is prime then steps 1 and 3 can never return COMPOSITE. By Lemma 2.2.1, the `for` loop also cannot return COMPOSITE. Therefore the algorithm will identify n as PRIME either in step 6 or in step 10. ■

The converse of the above lemma requires a little more work. If the algorithm returns PRIME in step 6 then n must be prime since, otherwise, step 3 would have found a nontrivial factor of n and the algorithm would have returned COMPOSITE in step 4. So we only need to consider the case in which the algorithm returns PRIME in step 10; so let's assume this to be the case.

The algorithm has two main steps (step 2 and the `for` loop): step 2 finds an appropriate r, and the `for` loop verifies the equation (2.2) for a number of a's. We are now going to bound the magnitude of the appropriate r.

Lemma 2.3.2. *There exists an $r \leq max\{3, [\log^5 n]\}$ such that $o_r(n) > \log^2 n$.*

Proof. This is trivially true when $n = 2$ since $r = 3$ satisfies all conditions. So let's assume that $n > 2$. Then $[\log^5 n] > 10$ and Lemma 2.2.2 applies. Let $r_1, r_2, \ldots, r_t$ be all numbers such that either $o_{r_i}(n) \leq \log^2 n$ or $r_i \mid n$. Each of these numbers must divide the product

$$n \cdot \prod_{i=1}^{[\log^2 n]} (n^i - 1) < n^{\log^4 n} \leq 2^{\log^5 n}$$

and so does their lcm. By Lemma 2.2.2, though, we know that the lcm of the first $[\log^5 n]$ numbers is greater than $2^{[\log^5 n]}$ and therefore there must exist a number $s \leq [\log^5 n]$ such that $s \notin \{r_1, r_2, \ldots, r_t\}$. If $\gcd(s, n) = 1$ then $o_s(n) > \log^2 n$ and we are done. If $\gcd(s, n) > 1$, then since s does not divide n and $\gcd(s, n) \in \{r_1, r_2, \ldots, r_t\}$,$r = \frac{s}{\gcd(s,n)} \notin \{r_1, r_2, \ldots, r_t\}$ and so $o_r(n) > \log^2 n$. ■

Since $o_r(n) > 1$, there must exist a prime divisor p of n such that $o_r(p) > 1$. We must have both $p > r$ and $\gcd(n, r) = 1$ since, otherwise, either step 4 or step 6 would decide the primality of n. This means $p, n \in \mathbb{Z}_r^*$. Also let $l = [\sqrt{\varphi(r)} \log n]$. The `for` loop verifies l equations. Since the algorithm does not output COMPOSITE in this step, we have:

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$$

for every a, $0 \leq a \leq l$. This implies:

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, p} \tag{2.3}$$

for $0 \leq a \leq l$. By Lemma 2.2.1, we have:

$$(x + a)^p \equiv x^p + a \pmod{x^r - 1, p} \tag{2.4}$$

for $0 \leq a \leq l$. Thus n behaves like prime p in the above equation.

Let's give a name to this property:

Definition 2.3.1. *For polynomial $f(x)$ and number $m \in N$, we say that m is introspective for $f(x)$ if*

$$[f(x)]^m \equiv f(x^m) \pmod{x^r - 1, p}.$$

It is clear, form equations (2.3) and (2.4), that both n and p are introspective for $x + a$ when $0 \leq a \leq l$.
The following lemma shows that introspective numbers are closed under multiplication:

Lemma 2.3.3. *If m and m' are introspective numbers for $f(x)$ then so is $m \cdot m'$.*

Proof. See proof of Lemma 1.3.3, with $g(x) = f(x)$. ■

For a number m, the set of polynomials for which m is introspective is also closed under multiplication:

Lemma 2.3.4. *If m is introspective for $f(x)$ and $g(x)$ then it is also introspective for $f(x) \cdot g(x)$.*

Proof. We have:

$$[f(x) \cdot g(x)]^m \equiv [f(x)]^m \cdot [g(x)]^m \equiv f(x^m) \cdot g(x)^m \pmod{x^r - 1, p}.$$

■

The above two lemmas together imply that every number in the set

$$I = \{n^i \cdot p^j \mid i, j \geq 0\}$$

is introspective for every polynomial in the set

$$P = \{\prod_{a=1}^{l} (x + a)^{e_a} \mid e_a \geq 0\}.$$

We now define two groups based on these sets that will play a crucial role in the proof.
The first group is the set of all residues of numbers in I modulo r. This is a subgroup of $\mathbb{Z}_r^*$ since, as already observed, $\gcd(n, r) = \gcd(p, r) = 1$. Let G be this group and let $|G| = t$. G is generated by n and p modulo r and, since $o_r(n) > 4\log^2 n$ we have $t > 4\log^2 n$.
To define the second group, let $\Phi_r(x) = x^{r-1} + x^{r-2} + \ldots + 1 = \frac{x^r - 1}{x - 1}$ the r^{th} cyclotomic polynomial over $\mathbb{F}_p$. Polynomial $\Phi_r(x)$ divides $x^r - 1$ and factors into irreducible factors of degree $o_r(p)$ (see proof of fact 4 of Lemma1.2.1). Let $h(x)$ be one such irreducible factor. The second group, Γ, is the set of all nonzero residues, modulo $h(x)$ and p, of polynomials in P. This group is generated by elements $x+1, x+2, \ldots, x+l$ in the finite field $\mathbb{F} = \mathbb{F}_p[x]/(h(x))$

and is a subgroup of the multiplicative group $(\mathbb{F}_p[x]/(h(x)))^*$.
The following lemma proves a lower bound on the size of the group Γ. It is a slight improvement on a bound shown by Hendrik Lenstra Jr., which, in turn, improved a bound shown in the AKS algorithm.

Lemma 2.3.5. $|\Gamma| \geq \binom{t+l-2}{t-1}$

Proof. Since $h(x)$ is a factor of the cyclotomic polynomial $\Phi_r(x)$, x is a primitive r^{th} root of unity in $\mathbb{F}$, that means $x^r \equiv 1 \pmod{h(x), p}$.
We now show that any two distinct polynomials of degree less than t in P will map to different elements in Γ. Let $f(x)$ and $g(x)$ be two such polynomials in P. Let $f(x) = g(x)$ in the field $\mathbb{F}$ and let $m \in I$. We have $f(x)^m = g(x)^m$ in $\mathbb{F}$. Since m is introspective for both f and g, we have $f(x^m) \equiv g(x^m) \pmod{x^r - 1, p}$ and, since $h(x) \mid x^r - 1$, we have $f(x^m) = g(x^m)$ in $\mathbb{F}$. This implies that x^m is a root of the polynomial $Q(y) = f(y) - g(y)$ for every $m \in G$. So there will be $|G| = t$ distinct roots of $Q(y)$ in $\mathbb{F}$. However, the degree of $Q(y)$ is less than t by the choice of f and g. This is a contradiction and, therefore, $f(x) \neq g(x)$ in $\mathbb{F}$. Moreover, $i \neq j$ in $\mathbb{F}_p$ for $1 \leq i \neq j \leq l$, since $l = [2\sqrt{\varphi(r)}\log n] < 2\sqrt{r}\log n < r$ and $p > r$. So the elements $x+1, x+2, \ldots, x+l$ are all distinct in $\mathbb{F}$. It 's also possible that there exists $a \leq l$ such that $x + a = 0$ in $\mathbb{F}$ (it happens if $h(x) = x + a$), and this $x + a$ is not in the set Γ. So there are at least $l - 1$ distinct polynomials of degree one in Γ. Therefore, there exist at least $\binom{t+l-2}{t-1}$ distinct polynomials of degree $< t$ in Γ. ■

In case n is not a power of p, the size of Γ can also be upper bounded:

Lemma 2.3.6. *If n is not a power of p, then* $|\Gamma| < \frac{1}{2}n^{2\sqrt{t}}$

Proof. Let's consider the following subset of I:

$$\hat{I} = \{n^i \cdot p^j \mid 0 \leq i, j \leq [\sqrt{t}]\}$$

If n is not a power of p, then the set $\hat{I}$ has $([\sqrt{t}] + 1)^2 > t$ distinct numbers. Since $|G| = t$, at least two numbers in $\hat{I}$ must be equal modulo r. Let m_1 and m_2 be such two number and let $m_1 > m_2$. So, by fact 3 of Lemma 1.2.1, we have:

$$x^{m_1} \equiv x^{m_2} \pmod{x^r - 1}.$$

Let $f(x) \in P$. Then,

$$\begin{aligned} f(x)^{m_1} &\equiv f(x^{m_1}) \pmod{x^r - 1, p} \\ &\equiv f(x^{m_2}) \pmod{x^r - 1, p} \\ &\equiv f(x)^{m_2} \pmod{x^r - 1, p}. \end{aligned}$$

This implies that $f(x)^{m_1} = f(x)^{m_2}$ in the field $\mathbb{F}$. Therefore, $f(x) \in \Gamma$ is a root of the polynomial $Q'(y) = y^{m_1} - y^{m_2}$ in the field $\mathbb{F}$. As $f(x)$ is an arbitrary element of Γ, we have that the polynomial $Q'(y)$ has at least $|\Gamma|$ distinct roots in $\mathbb{F}$. The degree of $Q'(y)$ is $m_1 \leq (np)^{[\sqrt{t}]} < \frac{1}{2}n^{2\sqrt{t}}$ (since $p \mid n$ and $n \neq p$ by hypothesis). This shows $|\Gamma| < \frac{1}{2}n^{2\sqrt{t}}$. ■

We are now ready to prove the correctness of the algorithm:

Lemma 2.3.7. *If the algorithm returns PRIME, then n is prime.*

Proof. Suppose that the algorithm returns PRIME. Lemma 2.3.5 implies that for $t = |G|$ and $l = [2\sqrt{\varphi(r)}\log n]$:

$$\begin{aligned}
|\Gamma| &\geq \binom{t+l-2}{t-1} \\
&\geq \binom{l-1+[2\sqrt{t}\log n]}{[2\sqrt{t}\log n]} \qquad (\text{since } \ t > 2\sqrt{t}\log n) \\
&\geq \binom{2\,[2\sqrt{t}\log n]-1}{[2\sqrt{t}\log n]} \qquad (\text{since } \ l = [2\sqrt{\varphi(r)}\log n] \geq [2\sqrt{t}\log n]) \\
&\geq 2^{[2\sqrt{t}\log n]} \qquad (\text{since } \ 2\sqrt{t}\log n \geq 3) \\
&\geq \frac{(2^{\log n})^{2\sqrt{t}}}{2} = \frac{1}{2}n^{2\sqrt{t}}.
\end{aligned}$$

By Lemma 2.3.6, $|\Gamma| < \frac{1}{2}n^{2\sqrt{t}}$, if n is not a power of p. Therefore $n = p^k$ for some $k > 0$. If $k > 1$, then the algorithm will return COMPOSITE in step 1. Therefore, $n = p$. ■

This completes the proof of Theorem 2.3.1.

2.4 Time Complexity Analysis

Theorem 2.4.1. *The asymptotic time complexity of the algorithm is $\tilde{\vartheta}(\log^{21/2} n)$.*

Proof.

- The first step of the algorithm takes asymptotic time $\tilde{\vartheta}(\log^3 n)$, since the algorithm calculates $[n^{\frac{1}{b}}]$.

- In step 2, we find an r with $o_r(n) > \log^2 n$. This can be done by trying out successive values of r and testing in $n^k \not\equiv 1 \pmod r$ for every $k \leq \log^2 n$. For a particular r, this will involve at most $\vartheta(\log^2 n)$ multiplications modulo r and so will take time $\tilde{\vartheta}(\log^2 n \log r)$. By Lemma 2.3.2 we know that the algorithm only needs to try $\vartheta(\log^5 n)$ different values of r, to find the required one. Thus the total time complexity of step 2 is $\tilde{\vartheta}(\log^7 n)$.

- The third step involves computing the gcd of r numbers. Each gcd computation, with the Euclidean Algorithm, takes time $\vartheta(\log^2 n)$ and, therefore, the time complexity of this step is $\vartheta(r\log^2 n) = \vartheta(\log^7 n)$.

- The time complexity of step 5 is just $\vartheta(\log n)$.
- In the `for` loop (steps 7-8), we need to verify $[\sqrt{\varphi(r)}\log n]$ congruences. Each congruence requires $\vartheta(\log n)$ multiplications of degree r polynomials with coefficients of size $\vartheta(\log n)$. So each congruence can be verified in time $\tilde{\vartheta}(r\log^2 n)$ steps. Thus the time complexity of the `for` loop is $\tilde{\vartheta}(r\sqrt{\varphi(r)}\log^3 n) = \tilde{\vartheta}(r^{\frac{3}{2}}\log^3 n) = \tilde{\vartheta}(\log^{21/2} n)$.

The time of the `for` loop dominates all the others and is, therefore, the time complexity of the algorithm. ■

2.5 Improving Time Complexity

The time complexity of the algorithm can be improved by improving the estimate of r done in Lemma 2.3.2. Of course the best possible scenario would be when $r = \vartheta(\log^2 n)$ and, in that case, the time complexity of the algorithm would be $\tilde{\vartheta}(\log^6 n)$.
In fact, there are two conjectures that support the possibility of such an r. The first conjecture is the following:

Conjecture 2.5.1. (Artin's Conjecture) *Given any number $n \in \mathbb{N}$ that is not a perfect square, the number of primes $r \leq m$ for which $o_r(n) = r - 1$ is asymptotically $A(n) \cdot \frac{m}{\ln m}$ where $A(n)$ is Artin's constant with $A(n) > 0.35$.*

If Artin's Conjecture, which holds under the Generalized Riemann Hypothesis, becomes effective for $m = \vartheta(\log^2 n)$, it shows that there is an $r = \vartheta(\log^2 n)$ with the required properties.
The second one is the **Sophie-German Prime Density Conjecture** (Conjecture 1.5.1) that we have seen in the previous chapter.
If this conjecture holds, we can conclude that $r = \vartheta(\log^2 n)$:
by Conjecture 1.5.1, there must exist at least $\log^2 n$ Sophie-German Primes between $8\log^2 n$ and $c\log^2 n(\log\log n)^2$ for a suitable constant c. For any such prime q, we have that the only possible orders of n modulo q are $\{1, 2, \frac{q-1}{2}, q\}$. Any q for which $o_q(n) \leq 2$ must divide $n^2 - 1$ which has at most $\log(n^2 - 1)$ prime factors, and so the number of such q is bounded by $\vartheta(\log n)$. This implies that there must exist a prime $r = \vartheta(\log^2 n)$ such that $o_r(n) > \log^2 n$.

Chapter 3

Berrizbeitia's Algorithms for a large family of numbers

3.1 Introduction

We are now going to present algorithms that run faster than AKS algorithm and are deterministic primality tests. But they work only for a large family of integers, namely integers $n \equiv 1 \pmod 4$ for which an integer a is given such that Jacobi symbol $\left(\frac{a}{n}\right) = -1$, and the integers $n \equiv -1 \pmod 4$ for which an integer a is given such that $\left(\frac{a}{n}\right) = \left(\frac{1-a}{n}\right) = 1$. The algorithms we present run in $2^{-\min(k,[2\log\log n])}\tilde{\vartheta}(\log n)^6$ time, where $k = \nu_2(n-1)$ is the exact power of 2 dividing $n-1$ when $n \equiv 1 \pmod 4$, and $k = \nu_2(n+1)$ in $n \equiv -1 \pmod 4$. In particular, the running time of these algorithms improves up to $\tilde{\vartheta}(\log n)^4$ if the value of $k \geq [2\log\log n]$. If n is a large enough prime, then we show that the algorithm for the case $n \equiv 1 \pmod 4$ runs, in the worst case, that is when $k = 2$, at least 2^{11} times faster than the best possible running time for the AKS algorithm. This advantage in running time increases with the value of k. For the case $n \equiv -1 \pmod 4$ we get the same result using 2^9 instead of 2^{11}.

In the case $n \equiv 1 \pmod 4$, and assuming an integer a is given such that $\left(\frac{a}{n}\right) = -1$, the two crucial points of our algorithm are:

1. It is enough to verify

$$(1+mx)^n \equiv 1 + mx^n \pmod{n, x^{2^s} - a}$$

where $s = [2\log\log n]$. Since $2^{2(\log\log n)} = (\log n)^2$, then we have $2^s < (\log n)^2$. Since we have seen, in the AKS algorithm, that $r \in [64(\log n)^2, c(\log n)^6]$, then we have that 2^s is at least 64 times smaller than r, then each of these verifications for different values of m are faster than the verification of the analogues step in the AKS algorithm.

2. These verifications only have to be done for $2^{\max(s-k,0)}$ different values of m, where $k = \nu_2(n-1)$, since, as we will see, some of the conjugates of the monomial $1 + mx^n$ in the corresponding finite field, are also monomials satisfying the same congruence. So, each iteration of our test produces $2^{\min(s,k)}$ different monomials satisfying the congruence.

These two facts together allow us to give a more efficient primality test for those numbers and such that its efficiency improves with the value of k up to certain limit ($[2 \log \log n]$).
For number $n \equiv -1 \pmod 4$ we will be able to obtain similar results.

3.2 Notation and Preliminaries

Throughout this chapter by $\log n$ we always mean log to the base 2 and p denotes an odd prime number.

Definition 3.2.1. *Let a be an integer coprime with p. We define The Legendre Symbol $\left(\frac{a}{p}\right)$ by the formula*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 : & \text{if there is an integer } x \text{ such that } x^2 \equiv a \pmod p \\ -1 : & \text{otherwise.} \end{cases}$$

This symbol has the following properties:

1. If ab is coprime with p, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

The Legendre Symbol can be extended multiplicatively to the *Jacobi Symbol* replacing p with an odd number m. That is, if $m = p_1 \cdots p_k$ and $\gcd(a,m) = 1$, then $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$. The Jacobi Symbol also satisfies property (1) of the Legendre Symbol above. Most important, it the Quadratic Reciprocity Law which is:
Let m, n be odd and coprime numbers. Then,

1. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

2. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{2}}$

3. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

As a reference for the proof of the quadratic reciprocity law we give [2].
Let $\mathbb{F}_p$ denote the finite field with p elements. We are now going to recall some facts about the theory of finite field that we shall employ.

Fact 1: Let K and E be finite fields containing $\mathbb{F}_p$. Let $q = |K|$ and suppose $K \subseteq E$. Then, $[E : \mathbb{F}_p] = [E : K][K : \mathbb{F}_p]$.

Now let K be a finite extension of $\mathbb{F}_p$ with $q = |K|$. Let K^* be the multiplicative group and g a generator of K^*.

Lemma 3.2.1. *For an element α of K, the following are equivalent*

1. $x^2 - \alpha^l$ *is irreducible over K for every odd integer l.*
2. $x^2 - \alpha$ *is irreducible over K.*
3. $\alpha = g^t$ *for some odd integer t.*
4. $\alpha^{\frac{q-1}{2}} = -1$.

Proof. (1) ⇒ (2) is trivial. Now let's prove (2) ⇒ (3). Since g is a generator, then $\alpha = g^t$ for some t. Let's suppose that t is not odd, that is $t = 2m$. Then $x^2 - \alpha = x^2 - g^{2m} = (x - g^m)(x + g^m)$ is reducible. But it is a contradiction, so we have that t is odd. (3) ⇒ (4) is obtained by noticing that $g^{\frac{q-1}{2}} = -1$ since g is a generator. Hencen $\alpha^{\frac{q-1}{2}} = (g^t)^{\frac{q-1}{2}} = (-1)^t$ which is equal to -1 since t is odd. Finally, to show (4) ⇒ (1) let's suppose that $x^2 - \alpha^l$ with l odd integer is reducible. Then, there is $\beta \in K$ such that $\beta^2 = \alpha^l$. So $(\alpha^{\frac{q-1}{2}})^l = \beta^{q-1} = 1$, but if $\alpha^{\frac{q-1}{2}} = -1$ and l is odd, then we should have $(\alpha^{\frac{q-1}{2}})^l = -1$. Thus, we have a contradiction. ∎

Lemma 3.2.2. *Let $q = |K|$. Assume $q \equiv 1 \pmod 4$. If $x^2 - a$ is irreducible over K and θ is a root of $x^2 - a$, then $x^2 - \theta$ is irreducible over $K(\theta)$.*

Proof. Note that $|K(\theta)| = q^2$. By Lemma 3.2.1 it is enough to prove that $\theta^{\frac{q^2-1}{2}} = -1$. Note that since $q \equiv 1 \pmod 4$ then $\frac{q+1}{2} = t$ is odd. Also, since $x^2 - a$ is irreducible over K, then $a^{\frac{q-1}{2}} = -1$. Hence,

$$\theta^{\frac{q^2-1}{2}} = ((\theta^2)^{\frac{q+1}{2}})^{\frac{q-1}{2}} = (-1)^t = -1$$

(we have used the fact that $\theta^2 = a$ being θ a root of $x^2 - a$). ∎

Corollary 3.2.1. *If $|K| = q \equiv 1 \pmod 4$ and $a \in K$ is such that $a^{\frac{q-1}{2}} = -1$, then the polynomial $x^{2^s} - a$ is irreducible over K for all $s \geq 1$.*

Proof. Let's proceed inductively on s.
If $s = 1$, then $x^{2^s} - a = x^2 - a$ is irreducible over K by Lemma 3.2.1 (4 implies 2).
Now let's suppose that for all K such that $|K| = q \equiv 1 \pmod 4$ and $a \in K$ such that $x^2 - a$ is irreducible, then $x^{2^{s-1}} - a$ is irreducible.
Then we have $[\mathbb{F}_p[\sqrt{a}] : \mathbb{F}_p] = 2$. Moreover, by Lemma 3.2.2 we have that x^2-

$\sqrt{a}$ is irreducible over $\mathbb{F}_p[\sqrt{a}]$ which implies, using the inductive hypothesis, that $x^{2^{s-1}} - \sqrt{a}$ is irreducible over $\mathbb{F}_p[\sqrt{a}]$. Thus, we have $[\mathbb{F}_p(x^{2^{s-1}} - \sqrt{a}) : \mathbb{F}_p[\sqrt{a}]] = 2^{s-1}$. Let ρ be a root of $x^{2^{s-1}} - \sqrt{a}$, then $\mathbb{F}_p(x^{2^{s-1}} - \sqrt{a})$ is equal to $\mathbb{F}_p[\sqrt{a}, \rho]$ which, since $\rho^{2^{s-1}} = \sqrt{a}$, is equal to $\mathbb{F}_p[\rho]$. So by Fact 1 we have $[\mathbb{F}_p[\rho] : \mathbb{F}_p] = 2^s$ from which we can understand that $\deg f_\rho = 2^s$.
Moreover, we know that $\rho^{2^s} = a$ which means that ρ is a root of $x^{2^s} - a$. Thus we must have $f_\rho = x^{2^s} - a$ that, by definition, is irreducible over K. ■

We can now establish the following proposition

Proposition 3.2.1. *1. If $p \equiv 1 \pmod 4$ and $\left(\frac{a}{p}\right) = -1$, then $x^{2^s} - a$ is irreducible over $\mathbb{F}_p$.*

2. If $p \equiv 3 \pmod 4$ and $\left(\frac{a}{p}\right) = \left(\frac{1-a}{p}\right) = -1$, then $x^{2^s} - 2x^{2^{s-1}} + a$ is irreducible over $\mathbb{F}_p$

Proof. The first assertion is a particular case of the Corollary 3.2.1 since $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod p$. In order to prove (2) let $\theta_1 = 1 + \sqrt{1-a}$. Since $\left(\frac{1-a}{p}\right) = -1$ then $\mathbb{F}_p(\theta)$ has degree over 2 over $\mathbb{F}_p$. Hence, it has $p^2 = q$ elements, so $q \equiv 1 \pmod 4$. Moreover,

$$\theta_1^{\frac{p^2-1}{2}} = (\theta_1^{p+1})^{\frac{p-1}{2}} = ((1+\sqrt{1-a})(1-\sqrt{1-a}))^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} = -1.$$

(We have used property 2 of the Legendre Symbol to state that $\theta_1^{p+1} = \theta_1(1^p + (1-a)^{\frac{p}{2}}) = \theta_1(1 + (1-a)^{\frac{p-1}{2}+\frac{1}{2}}) = \theta_1(1 + (-1)(1-a)^{\frac{1}{2}}) = \theta_1(1 - \sqrt{1-a})$.
Corollary 3.2.1 implies that $x^{2^{s-1}} - \theta_1$ is irreducible over $\mathbb{F}_p(\theta_1)$. A root θ of this polynomial satisfies, $(x^{2^{s-1}} - \theta_1)(x^{2^{s-1}} - \theta_1^p) = 0$ which is equal to

$$x^{2^s} - (\theta_1 + \theta_1^p)x^{2^{s-1}} + \theta_1^{p+1} = x^{2^s} - 2x^{2^{s-1}} + a$$

which belongs to $\mathbb{F}_p[x]$. So we have $[\mathbb{F}_p(\theta) : \mathbb{F}_p(\theta_1)] = 2^{s-1}$. Moreover we know that $[\mathbb{F}_p(\theta_1) : \mathbb{F}_p] = 2$. So we can conclude, by Fact 1, that $[\mathbb{F}_p(\theta) : \mathbb{F}_p] = 2^{s-1} \cdot 2 = 2^s$, which means that the polynomial $x^{2^s} - 2x^{2^{s-1}} + a$ must be irreducible over $\mathbb{F}_p$. ■

3.3 Algorithm for the case $n \equiv 1 \pmod 4$

Let's now suppose $n \equiv 1 \pmod 4$. Let $k = \nu_2(n-1)$. So $k \geq 2$. Let a be an integer such that $\left(\frac{a}{n}\right) = -1$.

Note for example that if $n = h2^k + 1$ and $h \not\equiv 0 \pmod 3$, then

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)(-1)^{\frac{n-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{n}{3}\right)(-1)^{\frac{h2^k}{2}} =$$
$$= \left(\frac{n}{3}\right) = \begin{cases} 0 & \text{if} \quad n \equiv 0 \pmod 3 \\ 1 & \text{if} \quad n \equiv 1 \pmod 3 \\ -1 & \text{if} \quad n \equiv 2 \pmod 3 \end{cases}$$

but we have $n = h2^k + 1$ which implies that $n \not\equiv 1 \pmod 3$. Thus, in this case, we have that n is either a multiple of 3 or $\left(\frac{3}{n}\right) = -1$. It follows that the algorithm that we are now going to see, is deterministic for numbers of that form.
Finally let $s = \lceil 2 \log\log n \rceil = [2 \log\log n] + 1$. Note that $(\log n)^2 < 2^s < 2(\log n)^2$.
Let's now see the **Algorithm 1**:

```
                         CASE 1: $n \equiv 1 \pmod 4$

     Let $k = \nu_2(n-1)$, $s = \lceil 2\log\log n \rceil$.
     Input: integers $n, a$ such that $n \equiv 1 \pmod 4$, $\left(\frac{a}{n}\right) = -1$.
1.   Let $A = a^{\frac{n-1}{2^k}}$. If $A^{2^{k-1}} \not\equiv -1 \pmod n$, output $COMPOSITE$;
2.   If $k > (1/2)\log n$, output $PRIME$ ;
3.   If $n = d^e$ for some positive integers $d$ and $e$ with $e > 1$, output $COMPOSITE$ ;
4.   $m = 1, S = \{1\}, S' = \{1\}$;
5.   While ($|S| < 2^{\max(s-k,0)}$){
6.        While ($m^{2^k} \pmod n \in S'$){
7.             $m$    $m + 1$;
8.        }
9.        If $m > |S|2^k + 1$, output $COMPOSITE$;
10.      If $\gcd(m, n) > 1$, output $COMPOSITE$;
11.      If $\gcd(m^{2^k} - s', n) > 1$ for some $s'^{\in S'}$, output $COMPOSITE$;
12.      $S$    $S \bigcup \{m\}$;
13.      $S'$    $S' \bigcup \{m^{2^k} \pmod n\}$
14.  }
15.  If $(1 + mx)^n \not\equiv (1 + mx^n) \pmod{n, x^{2^s} - a}$, output $COMPOSITE$;
16.  Output $PRIME$.
```

Where:
Steps (1) and (2) verify properties of the Legendre Symbol and Proth's Theorem.
Step (3) verifies that n is not a perfect power.
Steps (4)-(14) generate a set S of cardinality $2^{\max(s-k,0)}$
Steps (15) and (16) verify the congruence for all $m \in S$.

The rest of this section is devoted to the proof of the following two results:

Theorem 3.3.1. *The algorithm above returns PRIME if and only if n is prime (as long as $n > 100$).*

Theorem 3.3.2. *The running time of the algorithm is $\tilde{\vartheta}(2^{-\min(s,k)}(\log n)^6)$. Note that this is $\tilde{\vartheta}((\log n)^6)$ if $k = 2$ and is $\tilde{\vartheta}((\log n)^4)$ if $k \geq s$.*

Let's prove these theorems through the proofs of a series of lemmas.

Lemma 3.3.1. *If n is prime ($n > 100$), the algorithm returns PRIME.*

Proof. Step (1) of the algorithm cannot return COMPOSITE because $A^{2^{k-1}} = a^{\frac{n-1}{2} \cdot 2^{k-1}} = a^{n-1}$ and, by property 2 of the Legendre Symbol, we know that if n is prime, then $-1 = \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$, so $A^{2^{k-1}} \not\equiv 1$ can never occur. Step (3) cannot return COMPOSITE because n is not a perfect power.
Now we show that Steps (4)-(14) do not return COMPOSITE. First note that if $k \geq s$ then the algorithm does not enter the **while** loop, hence these steps cannot return COMPOSITE in this case. So we may assume $k < s$. In this case, the algorithm generates the set S, that is, a sequence of integers m_i with $i = 1, \ldots, 2^{s-k}$ and $m_1 = 1$. Since n is prime, the number of solutions of $x^{2k} = 1$ in $\mathbb{F}_n$ is at most 2^k. It follows that $m_2 \leq 2^k + 1$. Inductively, using this same reasoning, we deduce that $m_t \leq (t-1)2^k + 1$. Note that $t-1$ is the cardinality of the set S at that stage of the algorithm. It follows that under the assumption that n is prime, $m > |S|2^k + 1$ cannot occur. Besides, since the greatest m_i is m_{s-k} and $m_{s-k} \leq (2^{s-k}-1)2^k+1$ then it follows that each $m_i \leq (2^{s-k} - 1)2^k + 1 < 2^s < 2(\log n)^2 < n$ (this last inequality certainly occurs if $n > 100$). Hence, in the algorithm, $\gcd(m, n) > 1$ cannot occur. Finally, since $m_i^{2^k} \not\equiv m_j^{2^k} \pmod{n}$ for all $j < i$ (otherwise $m_i \quad m_{i+1}$), then $\gcd(m^{2^k} - s', n) > 1$ cannot occur. This concludes the analysis for these steps.
For Step (15), since $(1+mx)^n \equiv 1+mx^n \pmod{n}$, then $(1+mx)^n \equiv 1+mx^n$ $(\bmod\ n, x^{2^s} - a)$, so this step does not return COMPOSITE. ■

We assume from now on that the output of the algorithm is PRIME.

Lemma 3.3.2. *Suppose that the algorithm has passed Step (1), that is, it has verified $A^{2^{k-1}} \not\equiv -1 \pmod{n}$. Then we have*

1. *$\nu_2(d-1) \geq k$ for all divisors of n.*

2. *There is a prime divisor p of n for which $\nu_2(p-1) = k$. For such prime p, $\left(\frac{a}{p}\right) = -1$*

Proof. 1. It is enough to prove it for prime divisors d of n. The hypothesis implies $A^{2^{k-1}} \not\equiv -1 \pmod{d}$, whence $\mathrm{ord}_d(A) = 2^k$ which implies that $2^k \mid d - 1$ and, therefore, $\nu_2(d-1) \geq k$.

2. If every prime divisor q of n were to satisfy $\nu_2(q-1) > k$, then so would the product, that is n, but it cannot occur. Let p be a prime divisor of n satisfying $\nu_2(p-1) = k = \nu_2(n-1)$. Let $t = \frac{p-1}{2^k}$. Since k is the exact power of 2 dividing $p-1$, then t is odd. Hence,

$$\left(\frac{A}{p}\right) \equiv A^{\frac{p-1}{2}} \equiv (A^t)^{2^{k-1}} \equiv (-1)^t \equiv -1 \pmod p$$

where we have used the fact that, from Step (1) of the algorithm, $A^{2^{k-1}} \equiv -1 \pmod n$ and $p \mid n$. Since $A = a^{\frac{n-1}{2^k}}$ and $\frac{n-1}{2^k}$ is odd, then we get $\left(\frac{a}{p}\right) = -1$.

■

Let's now recall a theorem which is important in number theory

Theorem 3.3.3. [Proth] *If p is a Proth number, namely a number of the form $k2^n + 1$ with k odd and $k < 2^n$, then if for some integer a*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

then p is prime.
Moreover, if p is a quadratic nonresidue modulo a then the converse is also true, and the test is conclusive. Such an a may be found by iterating a over small primes and computing the Jacobi Symbol until: $\left(\frac{a}{p}\right) = -1$.

Form this Theorem we can deduce the following Lemma:

Lemma 3.3.3. *If the algorithm returns PRIME at Step (2), then n is prime*

Now we assume that n has passed Step (2) (so $k \leq 1/2 \log n$). We let p be a prime divisor of n satisfying $\nu_2(p-1) = k = \nu_2(n-1)$. Since $\left(\frac{a}{p}\right) = -1$, then by Proposition 3.2.1, the polynomial $x^{2^s} - a$ is irreducible over $\mathbb{F}_p$. Let θ be a root of the polynomial in an algebraic closure C of $\mathbb{F}_p$, let $K = \mathbb{F}_p(\theta)$ and K its multiplicative group. Every $\alpha \in K^*$ is $\alpha = f(\theta)$ for some unique non-zero polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $t < 2^s$. Let m be an integer. We denote by r_m the multiplicative homomorphism of K^* consisting in raising to the m-th power. We denote by σ_m the linear map of K defined by $\sigma_m(\alpha) = f(\theta^m)$, where $f(x)$ is the unique polynomial just mentioned.

Lemma 3.3.4. *For an integer m the following are equivalent:*

1. *θ^m is a root of $\mathrm{irr}_\theta(x) = x^{2^s} - a$.*
2. *$a^m = a$ (in $\mathbb{F}_p$)*
3. *$\sigma_m(h(\theta)) = h(\theta^m)$ for all $h(x) \in \mathbb{F}_p[x]$.*

4. $\sigma_m \in \mathrm{Gal}(K/\mathbb{F}_p)$.

Proof. Note that, since θ is a root of $x^{2^s} - a$, we have $\theta^{2^s} = a$.
It is clear that (1) implies (2) since $a = (\theta^m)^{2^s} = a^m$. To see that (2) implies (3), let's consider $h(x) = f(x) + (x^{2^s} - a)p(x)$ where $\deg f(x) < 2^s$. By definition of σ_m we have:

$$\begin{aligned}\sigma_m(h(\theta)) &= \sigma_m(f(\theta) + (\theta^{2^s} - a)p(x)) = \sigma_m(f(\theta)) = \\ &= f(\theta^m) = h(\theta^m) - (a^m - a)p(\theta^m) = \\ &= h(\theta^m) :\end{aligned}$$

To prove that (3) implies (4) note that, since σ_m is clearly a linear map over $\mathbb{F}_p$, we only have to prove that it is multiplicative, and this i trivial. Finally, (4) implies (1) is also evident: just note that $\sigma_m(\theta) = \theta^m$ is a conjugate of θ over $\mathbb{F}_p$, hence, it must be a root of $\mathrm{irr}_\theta(x)$. ■

In particular, since $a^n \equiv a \pmod{n}$ and, therefore, modulo p, this lemma implies that $\sigma_n \in \mathrm{Gal}(K/\mathbb{F}_p)$, so it must be a power of the Frobenius automorphism $\sigma_p^i = \sigma_{p^i}$. The idea will be to show that, under certain conditions that are met if the algorithm outputs prime in the last step, this implies that $n = p^i$. We still need quite a few observations before reaching that conclusion.
Write $n = p^l d$. Then, from $a^n = a$ and $a^{p^l} = a$ it is easy to see that $a = a^{p^l d} = (a^{p^l})^d = a^d$. So σ_d is also an automorphism. Moreover, so is $\sigma_{d^i}\sigma_{p^j}$ for all $i, j \geq 0$. More generally if m_1 and m_2 satisfy the equivalent conditions of the previous lemma then so does $m_1 m_2$ and it is also easy to verify that $\sigma_{m_1 m_2} = \sigma_{m_1} \circ \sigma_{m_2}$. Similarly, if m_1 and $m_1 m_2$ satisfy the conditions, then so does m_2. On the other hand, if m satisfies any of the equivalent conditions of the previous lemma, then the product $\sigma_m r_{-m}$ is also a multiplicative homomorphism of K^* since it is a product of homomorphisms. It follows that

$$G_m = \ker(\sigma_m r_{-m}) = \{f(\theta) \in K^* \mid f(\theta^m) = f(\theta)^m\}$$

is a subgroup of K^*, hence cyclic, generated by, say, $g_m(\theta)$. We are now going to analyse the properties of these cyclic groups. First note that if $\alpha \in G_m$ then $\alpha^m = f(\theta)^m = f(\theta^m) = \sigma_m(\alpha)$

Lemma 3.3.5. *Suppose m_1 and m_2 satisfy any of the equivalent conditions of Lemma 3.3.4 then,*

1. *For all $i \geq 0$, $G_{p^i} = K^*$.*

2. $G_{m_1} \cap G_{m_2} \subseteq G_{m_1 m_2}$.

3. $|G_{m_i}|$ *divides* $m_i^{2^s} - 1$. *In particular* $\gcd(m_i, |G_{m_i}|) = 1$.

4. $G_{m_1 m_2} \cap G_{m_1} \subseteq G_{m_2}$.

Proof. 1. That $G_1 = K^*$ is trivial. Let $\alpha \in K^*$, then $\sigma_{p^i}(\alpha) = \sigma_p^i(\alpha) = \alpha^{p^i}$, since σ_p is the Frobenius automorphism.

2. Let $\alpha \in G_{m_1} \cap G_{m_2}$. Then, $\sigma_{m_1}(\alpha) = \alpha^{m_1}$ and $\sigma_{m_2}(\alpha) = \alpha^{m_2}$. It follows that

$$\sigma_{m_1 m_2}(\alpha) = \sigma_{m_1}(\sigma_{m_2}(\alpha)) = \sigma_{m_1}(\alpha^{m_2}) = (\sigma_{m_1}(\alpha))^{m_2} = (\alpha^{m_1})^{m_2} = \alpha^{m_1 m_2}.$$

This implies $\alpha \in G_{m_1 m_2}$.

3. Let α be a generator of G_{m_i} . By part 2 of this lemma $\alpha \in G_{m_i^{2^s}}$. On the other hand, since σ_{m_i} is an automorphism of K then $\sigma_{m_i}^{2^s}$ is the identity. So we have $\alpha^{m_i^{2^s}} = \sigma_{m_i^{2^s}}(\alpha) = \sigma_{m_i}^{2^s}(\alpha) = \mathrm{id}(\alpha) = \alpha$. So $\alpha^{m_i^{2^s}-1} = 1$. Hence $|G_{m_i}| = \mathrm{ord}(\alpha)$ divides $m_i^{2^s} - 1$. In particular $\gcd(m_i, |G_{m_i}|) = 1$.

4. Let $\alpha \in G_{m_1 m_2} \cap G_{m_1}$. Then

$$(\alpha^{m_2})^{m_1} = \alpha^{m_1 m_2} = \sigma_{m_2}(\sigma_{m_1}(\alpha)) = \sigma_{m_2}(\alpha^{m_1}) = (\sigma_{m_2}(\alpha))^{m_1}.$$

By part 3 of this lemma, we know that m_1 is coprime with $|G_{m_1}|$, which means that there is an integer t such that $tm_1 \equiv 1 \pmod{|G_{m_1}|}$. Raising both sides of the equality to this t, we obtain $(\alpha^{m_2})^{m_1 t} = (\sigma_{m_2}(\alpha))^{m_1 t}$. Note that $\sigma_{m_2}(\alpha)$ has the same order than α. Hence $\alpha^{m_2} = \sigma_{m_2}(\alpha)$.

■

Write $n = p^l d$ where d is coprime with p. From the previous lemma we can deduce the following result:

Corollary 3.3.1. *For all $i, j \geq 1$, $G_n \subseteq G_{p^i} G_{d^j}$*

Proof. $G_n = G_{dp^l} = G_{dp^l} \cap G_{p^l} \subseteq G_d \subseteq G_{d^i} = G_{d^i} \cap G_{p^j} \subseteq G_{d^i p^j}$. ■

Corollary 3.3.2. *If m_1 and m_2 satisfy any of the equivalent conditions of Lemma 3.3.4, then $\sigma_{m_1} = \sigma_{m_2}$ implies $|G_{m_1} \cap G_{m_2}|$ divides $m_1 - m_2$.*

Proof. Let $\alpha \in G_{m_1} \cap G_{m_2}$. Then $\alpha^{m_1} = \sigma_{m_1}(\alpha) = \sigma_{m_2}(\alpha) = \alpha^{m_2}$, thus $\alpha^{m_1 - m_2} = 1$. Since $G_{m_1} \cap G_{m_2}$ is a cyclic group, then $|G_{m_1} \cap G_{m_2}|$ must divide $m_1 - m_2$. ■

The lemma we are going to see, is very important since it shows how to obtain $2^{\min(k,s)}$ monomials in G_n from one iteration in Step (15) of the algorithm. This is the reason why the complexity of the algorithm improves as k grows.

Lemma 3.3.6. *1. Suppose $k < s$. If for some integer m, we have $(1 + m\theta) \in G_n$, then $(1 + mA^i\theta) \in G_n$ for $i = 1, 2, \dots, 2^k$.*

2. Suppose $k \geq s$. Let $B = A^{2^{k-s}}$. If $(1 + \theta) \in G_n$, then $(1 + B^i\theta) \in G_n$ for $i = 1, 2, \dots, 2^s$.

Proof. 1. Since G_n is a group, then $(1 + m\theta) \in G_n$ implies $(1 + m\theta)^{p^i} = (1 + m\theta^{p^i}) \in_n$. The elements θ^{p^i} are the Galois conjugates of θ in $\mathbb{F}_p[\theta]$. Since $\theta^{2^s} = A$, then the conjugates are of the form $\theta\zeta$, where $\zeta^{2^s} = 1$. Since $k \leq s$, every A^i satisfies $(A^i)^{2^s} = 1$. So the A^i are among the possible values for ζ. In particular, $(1 + mA^i\theta) \in G_n$.

2. Same as in (1) by noting that B is a primitive 2^s-th root of 1 in $\mathbb{F}_p$.

■

Lemma 3.3.7. *If the algorithm outputs prime at Step (16), then $|G_n| \geq 2^{2^s}$.*

Proof. Assume first that $k < s$.
Again we denote by m_i, with $i = 1, \dots 2^{s-k}$, the sequence of elements of the set S generated by the algorithm in Steps (4)-(14). We claim that m_iA^j for $i = 1, 2, \dots, 2^{s-k}$ and $j = 1, 2, \dots, 2^k$ are all different and non-zero in $\mathbb{F}_p$. To see this, recall that A has order 2^k in $\mathbb{F}_p$. Hence, A^j is non-zero in $\mathbb{F}_p$ for all j and they are all different for $j = 1, \dots, 2^k$. The algorithm verifies $\gcd(m_i, n) = 1$ which implies that all the m_iA^j are non-zero in $\mathbb{F}_p$. Let's suppose $m_iA^j = m_{i'}A^{j'}$ in $\mathbb{F}_p$. Raising to the 2^k-th power, we get $m_i^{2^k} = m_{i'}^{2^k}$ in $\mathbb{F}_p$, but since in Step (11) the algorithm verified that $m_i^{2^k} - m_{i'}^{2^k}$ is coprime with n, then we must have $i = i'$ whence we deduce that $j = j'$. So we have 2^s different non-zero elements of $\mathbb{F}_p$. Denote them by t_r for $r = 1, \dots, 2^s$. In Step (15) the algorithm verifies that $(1 + m_i\theta) \in G_n$ for each $i = 1, \dots, 2^{s-k}$. It follows from the previous lemma that $(1 + t_r\theta) \in G_n$ for $r = 1, 2 \dots, 2^s$.
If, on the other hand, $k > s$, then the algorithm verifies that $(1 + \theta) \in G_n$, and, again, using the previous lemma, we get $(1 + B^r\theta) \in G_n$ for $r = 1, \dots, 2^s$. So in both cases we obtain 2^s different monomials in G_n. To simplify we will always denote them as $(1 + t_r\theta) \in G_n$ for $r = 1, \dots, 2^s$. Since G_n is a group, it contains the set T defined as

$$T = \left\{ \prod_{r=1}^{2^s} (1 + t_r\theta)^{\epsilon_r} \mid \epsilon_r \in \mathbb{Z}^+, \sum \epsilon_r < 2^s \right\}.$$

Every element of T is of the form $f(\theta)$ for some $f(x)$ of degree less than 2^s. Since all t_r are different in $\mathbb{F}_p$ then the polynomials $f(x)$, corresponding to the different choices of ϵ_i, are different in $\mathbb{F}_p[x]$. Since the degrees are less than 2^s, then the corresponding elements of S are different.
T properly contains the set

$$T_1 = \left\{ \prod_{r=1}^{2^s} (1 + t_r\theta)^{\epsilon_r} \mid \epsilon_r \in \{0, 1\}, \sum \epsilon_r < 2^s \right\}.$$

In this set, we have 2^{2^s} choices for ϵ_r, but one of these, the one such that $\epsilon_r = 1$ for all r, cannot be considered because $\sum \epsilon_r$ must be less than 2^s. So the cardinality of T_1 is $2^{2^s} - 1$. Hence, T has at least 2^{2^s} elements. Therefore, $|G_n| \geq 2^{2^s}$. ■

We are now ready to complete the proof of Theorem 3.3.1.

Proof. of Theorem 3.3.1
It remains to prove that if the algorithm outputs prime in the last step, then n is prime. Assume n has more than one prime divisor. Hence, $n = p^l d$ where $\gcd(d, p) = 1$ and $d > 1$. We know that $\sigma_{p^i}\sigma_{d^j} \in \mathrm{Gal}(K/\mathbb{F}_p)$ for all $i, j \geq 0$. Since $\mathrm{Gal}(K/\mathbb{F}_p)$ has order 2^s, it follows from the pigeon hole principle that there exist two different pairs (i_1, j_1) and (i_2, j_2) with $0 \leq i_1, j_1, i_2, j_2 \leq [\sqrt{2^s}]$ such that $\sigma_{p^{i_1}d^{j_1}} = \sigma_{p^{i_2}d^{j_2}}$. It follows from Corollary 3.3.2 that

$$|G_{p^{i_1}d^{j_1}} \cap G_{p^{i_2}d^{j_2}}| \quad \text{divides} \quad p^{i_1}d^{j_1} - p^{i_2}d^{j_2}$$

Hence, from Corollary 3.3.1 we obtain

$$|G_n| \quad \text{divides} \quad p^{i_1}d^{j_1} - p^{i_2}d^{j_2}.$$

Note that $p^{i_1}d^{j_1} - p^{i_2}d^{j_2} < n^{[\sqrt{2^s}]} \leq n^{\sqrt{2^s}}$. Also note that from $s = \lceil 2 \log\log n \rceil$ we can easily deduce that $2^s > (\log n)^2$ that is $\sqrt{2^s} > \log n$ which means $2^{\sqrt{2^s}} > n$ from which we can conclude that $2^{2^s} > n^{\sqrt{2^s}}$. Moreover we know, from Lemma 3.3.7, that $|G_n| > n^{\sqrt{2^s}}$. So we obtain $p^{i_1}d^{j_1} = p^{i_2}d^{j_2}$. But this is not possible because p and d are coprime and $(i_1, j_1) \neq (i_2, j_2)$. Hence $d = 1$. So, $n = p^l$. Since n has passed Step (13) of the algorithm (n cannot be a non trivial perfect power), we conclude that $l = 1$ which means $n = p$. ■

Analysis of Complexity:

Proof. of Theorem 3.3.2

Step (1) involves the calculation of $a^{\frac{n-1}{2}} \pmod{n}$ which takes $\tilde{\vartheta}((\log n)^2)$ time using the fast Fourier tranform.

Step (3), as in the case of the AKS algorithm with Lenstra's variant, takes $\tilde{\vartheta}((logn)^3)$.

Steps (4)-(14): If $k \geq s$ the algorithm does not enter the **while** loop, so in this case this step has no cost.
When $k < s$, every integer m that the algorithms deals with, is less than 2^s. For each of these integers m, it computes $m^{2^k} \pmod{n}$. It follows that the algorithm calculates m^{2^k} for at most 2^s different values of m (in practice

much less than this). This involves $k2^s \leq s2^s$ modular multiplications modulo n. Using the fast Fourier transform, these computations take at most $\tilde{\vartheta}((\log n)^3)$. On the other hand, the algorithm in these Steps computes less than $2^{2^{(s-k)}}$ gcd's. This takes $2^{2^{(s-k)}}\tilde{\vartheta}((\log n)) = 2^{-2k}\tilde{\vartheta}((\log n)^5)$ time.

Step (15): This is the part of the computation that will determine the complexity of the algorithm. It involves $2^{\max(s-k,0)}$ iterations, where by iteration we mean the computation of $(1+mi_x)^n \text{mod}(n, x^{2^s} - a)$. Using fast exponentiation, each iteration takes at most $2\log n$ multiplications in the field K. Using the fast Fourier transform, each of of these involves $\vartheta(2^s s)$ modular multiplications, and, likewise, each of these takes $\tilde{\vartheta}(\log n)$ time. We must add that the reduction modulo $x^{2^s} - a$ is necessary after multiplications of elements in K, but these are done with 2^s modular multiplications, which does not affect complexity. So each iteration takes $\tilde{\vartheta}((\log n)^4)$. Hence this step takes

$$2^{\max(s-k,0)}\tilde{\vartheta}((\log n)^4) = 2^{-\min(s,k)}\tilde{\vartheta}((\log n)^6),$$

and so does the algorithm. ■

3.4 Algorithm for the case $n \equiv -1 \pmod 4$

Throughout this section we assume that $n \equiv -1 \pmod 4$, and $k = \nu_2(n+1)$. In particular $k \geq 2$. We assume that an integer a is given such that $\left(\frac{a}{n}\right) = \left(\frac{1-a}{n}\right) = -1$. . Note for example that, just like we have seen in the previous section, if $n = h2^k - 1$ and $h \not\equiv 0 \pmod 3$ then n is either a multiple of 3 or $\left(\frac{3}{n}\right) = \left(\frac{1-3}{n} = -1\right)$. It follows that the algorithm we are now going to see is deterministic for numbers of that form. Further we let $t = \lceil \log\log n \rceil + 1$, noting that $t = s + 1$. Hence we have $2(\log n)^2 < 2^t < 4(\log n)^2$. Let's now see the proposed **Algorithm 2**:

```
                    CASE 2: $n \equiv -1 \pmod 4$

     Let $k = \nu_2(n+1)$, $t = \lceil 2\log\log n \rceil + 1$.
     Input:  integers $n, a$ such that $n \equiv -1 \pmod 4$, $\left(\frac{a}{n}\right) = \left(\frac{1-a}{n}\right) = -1$.
1.   If $a^{\frac{n-1}{2}} \not\equiv -1 \pmod n$, output COMPOSITE;
2.   If $(1+\sqrt{1-a})^n \not\equiv 1 - \sqrt{1-a} \pmod n$, output COMPOSITE ;
3.   If $k > (1/2)\log n$, outputPRIME;
4.   If $n = d^e$ for some positive integers $d$ and $e$ with $e > 1$, output COMPOSITE ;
5.   For $m = 1$ to $2^{\max(t-k,0)}${
6.        If $\gcd(m,n) > 1$, output COMPOSITE;
7.   }
8.   For $m = 1$ to $2^{\max(t-k-1,0)}${
9.        If $(1+mx)^n \not\equiv (1+mx^n) \pmod{n, x^{2^{t+1}} - 2x^{2^t} + a}$, output COMPOSITE;
10.  }
11.  Output PRIME.
```

Where:
Steps (1), (2) and (3) verify properties of the Legendre Symbol, the Frobenius automorphism and Lucas-type Theorem.
Step (4) verifies that n is not a perfect power.
Steps (5), (6) and (7) find a sequence of m_i's.
Steps (8)-(11) find elements in G_n.

Let's now see two theorems that are analogous to Theorem 3.3.1 and Theorem 3.3.2 respectively:

Theorem 3.4.1. *The algorithm above returns prime if and only if n is prime (assuming $n > 25$).*

Theorem 3.4.2. *The running time of the algorithm is $\tilde{\vartheta}(2^{-\min(s,k)}(\log n)^6)$.*

In the rest of this section we will prove a series of lemmas that will let us prove these theorems.

Lemma 3.4.1. *If n is prime, the algorithm returns PRIME.*

Proof. Steps (1)-(3) cannot output COMPOSITE: in the first place because of the properties of the Legendre Symbol, and secondly because of the properties of the Frobenius automorphism. The rest proceeds as in the case $n \equiv 1 \pmod 4$ except that in the **for** loop of Steps (5)-(7) we only need $n > 25$ to make sure that $2^{-\max(t-k,0)} < n$. ■

We now assume that the output of the algorithm is PRIME.

Lemma 3.4.2. *Let $n, a, 1-a$ as in the input of the algorithm, and $k = \nu_2(n+1)$. Suppose $a^{\frac{n-1}{2}} \equiv -1 \pmod n$ and that $(1+\sqrt{1-a})^n \equiv 1-\sqrt{1-a} \pmod n$. Then,*

1. *Every prime divisor q of n satisfies either*

   a $q \equiv 1 \pmod{2^{k+1}}$ or

   b $q \equiv -1 \pmod{2^k}$

   It satisfies **a** *if and only if* $\left(\frac{1-a}{q}\right) = \left(\frac{a}{q}\right) = 1$.
   It satisfies **b** *if and only if* $\left(\frac{1-a}{q}\right) = \left(\frac{a}{q}\right) = -1$.

2. *There exists a prime divisor p of n such that $\nu_2(p+1) = \nu_2(n+1) = k$. For such p,* $\left(\frac{1-a}{p}\right) = \left(\frac{a}{p}\right) = -1$.

Proof. 1. Let q be a prime divisor of n. We first note that $\left(\frac{a}{q}\right) = 1$ if and only if $q \equiv 1 \pmod 4$. To show this, let's recall that, since $n \equiv -1 \pmod 4$, then $\frac{n-1}{2}$ is odd. Hence, $\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)^{\frac{n-1}{2}} = \left(\frac{a^{\frac{n-1}{2}}}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$. where we have used property 1 of Jacobi Symbol for the last equality. We now claim that $(1+\sqrt{1-a})^{\frac{n^2-1}{2}} \equiv -1 \pmod 4$. This is true since

$$(1+\sqrt{1-a})^{\frac{n^2-1}{2}} = ((1+\sqrt{1-a})^{n+1})^{\frac{n-1}{2}} = ((1-\sqrt{1-a})(1+\sqrt{1-a}))^{\frac{n-1}{2}} = \\ = a^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

Now suppose $\left(\frac{1-a}{q}\right) = 1$. Then, $\mathbb{F}_q(\sqrt{1-a}) = \mathbb{F}_q$. Since $(1+\sqrt{1-a})^{\frac{n^2-1}{2}} \equiv -1 \pmod n$ then $(1+\sqrt{1-a})^{\frac{n^2-1}{2}} = -1$ in $\mathbb{F}_q$. But $\nu_2(n+1) = k$ implies $\nu_2(n^2-1) = k+1$. So the element $(1+\sqrt{1-a})^{\frac{n^2+1}{2^{k+1}}}$ has order 2^{k+1} in $\mathbb{F}_q$, which means $2^{k+1} \mid q-1$ and, therefore, $q \equiv 1 \pmod{2^{k+1}}$. In particular, $\left(\frac{a}{q}\right) = 1$ according to what we have just noted. Suppose now that $\left(\frac{1-a}{q}\right) = -1$. Then $\mathbb{F} = \mathbb{F}_q(\sqrt{1-a})$ has q^2 elements. Again, $(1+\sqrt{1-a})^{\frac{n^2-1}{2}} = -1$ in $\mathbb{F}$, so

$$(1+\sqrt{1-a})^{\frac{n^2-1}{2}} = ((1+\sqrt{1-a})^{n-1})^{\frac{n+1}{2}} = \left(\frac{(1+\sqrt{1-a})^n}{(1+\sqrt{1-a})}\right)^{\frac{n+1}{2}} = \left(\frac{1-\sqrt{1-a}}{1+\sqrt{1-a}}\right)^{\frac{n+1}{2}} = -1.$$

Note that in $\mathbb{F}_q(\sqrt{1-a})$, the element $\beta = (\frac{1-\sqrt{1-a}}{1+\sqrt{1-a}}) = (1+\sqrt{1-a})^{q-1}$ lies in the unique subgroup of $\mathbb{F}^*$ of order $q+1$. $\beta^{\frac{n+1}{2^k}}$ has order 2^k, so $2^k \mid q+1$ which means that $q \equiv -1 \pmod{2^k}$. Also, $\left(\frac{a}{q}\right) = -1$ as noted.

2. Since $\left(\frac{1-a}{n}\right) = -1$ then there must be a prime divisor of n such that $\left(\frac{1-a}{q}\right) = -1$ So, as we have just seen, we have $q \equiv -1 \pmod{2^k}$. If all primes satisfying $\left(\frac{1-a}{q}\right) = -1$ satisfy $q \equiv -1 \pmod{2^{k+1}}$, then by part 1, n would satisfy $n \equiv \pm 1 \pmod{2^{k+1}}$. But, $\nu_2(n+1) = k$ implies that this is not possible. So there is $p \mid n$ such that $\nu_2(p+1) = k$. For such p, which is congruent to $-1 \pmod 4$, we must have $\left(\frac{a}{p}\right) = -1$ Hence, we also must have $\left(\frac{1-a}{p}\right) = -1$ since we have just proved that $\left(\frac{1-a}{p}\right) = 1$ implies $\left(\frac{1-a}{n}\right) = 1$.

■

Corollary 3.4.1. *If the algorithm outputs PRIME in Step (3), then n is prime.*

Proof. It is deduced easily from the previous Lemma by noting that $k > 1/2 \log n$ is the same as $k > \log n^{1/2}$ which implies that $2^k > 2^{\log n^{1/2}} = n^{1/2} = \sqrt{n}$. So if n is composite, then there exists a prime divisor q such that $q < \sqrt{n} < 2^k$, but this implies that q can't be congruent to 1 modulo 2^{k+1} and not even to -1 modulo 2^k which is a contradiction with the previous Lemma. Therefore, n is prime. ■

Assume now that n has passed Steps (1)-(3) of the algorithm, and let p the prime divisor of n for which $\nu_2(p+1) = k$. We let $\mathbb{F} = \mathbb{F}_p(\sqrt{1-a})$ and $K = \mathbb{F}_p(\theta)$ where θ is a root of the polynomials $x^{2^{t+1}} - 2x^{2^t} + a = \operatorname{irr}_\theta(x)$ which is irreducible by Proposition 3.2.1. We also note that $K = \mathbb{F}(\theta)$ and θ is a root of $x^{2^t}(1 + \sqrt{1-a})$ or $x^{2^{t+1}} - (1 - \sqrt{1-a})$, which are both irreducible over $\mathbb{F}$. For simplicity we will assume θ is a root of the first of these two polynomials. The roots of the other one are also roots of $\operatorname{irr}_\theta(x)$. Let σ_m defined, as in the case $n \equiv 1 \pmod 4$, by $\sigma_m(f(\theta)) = f(\theta^m)$ when $\deg f(x) < 2^s$.
Now we need the following Lemma:

Lemma 3.4.3. *For an integer m the following are equivalent:*

1. *θ^m is a root of $\operatorname{irr}_\theta(x) = x^{2^{t+1}} - 2x^{2^t} + a$.*
2. *$(1 + \sqrt{1-a})^m = 1 \pm \sqrt{1-a}$ in $\mathbb{F}$.*
3. *$\sigma_m(h(\theta)) = h(\theta^m)$ for all $h(x) \in \mathbb{F}_p[x]$.*
4. *$\sigma_m \in \operatorname{Gal}(K/\mathbb{F}_p)$.*

The proof of this lemma is quite similar to that given for Lemma 3.3.4.

When σ_m is an automorphism we let

$$G_m = \{\alpha \in K \ : \ \sigma_m(\alpha) = \alpha^m\}.$$

Then G_m is a cyclic subgroup of K^*. Now write $n = p^l d$, where $\gcd(p, d) = 1$. As in the case $n \equiv 1 \pmod 4$, from the above lemma we can deduce that $\sigma_{p^i d^j} \in \mathrm{Gal}(K/\mathbb{F}_p)$ for all $i, j \geq 0$. Moreover we carry over Lemma 3.3.5, Corollary 3.3.1 and Corollary 3.3.2 in this new environment.
Let

$$\alpha = (1 + \sqrt{1-a})^{\frac{n^2-1}{2^{k+1}}}.$$

We now have the following lemma which is analogous to Lemma 3.3.6.

Lemma 3.4.4. *Let* $\beta = \alpha^{2^{\max(k+1-t,0)}}$. *If* $(1 + m\theta) \in G_n$ *for some* $m \neq 0$ *in* $\mathbb{F}_p$*, then* $(1 + m\beta^i\theta) \in G_n$ *for* $i = 1, \ldots, 2^{\min(k+1,t)}$.

Proof. . Proceed as in the proof of Lemma 3.3.6 noting that the conjugates of θ over the field $\mathbb{F}$ are of the form $\theta\zeta$ where $\zeta^{2^t} = 1$. The powers of β are among the latter. ■

Now, like in the previous case, we are going to estimate the size of G_n using the following lemma:

Lemma 3.4.5. *If the algorithm outputs PRIME in the last step, then* $|G_n| > 2^{2^t}$.

Proof. In Steps (5)-(7) the algorithm verifies that every integer less than $2^{\max(t-k,0)}$ is coprime with n, hence they are all different and non-zero in $\mathbb{F}_p$. Let $\gamma_{ij} = m_i\beta^j$ for $i = 1, 2, \ldots, 2^{\max(t-k-1,0)}$ and $j = 1, 2, \ldots, 2^{\min(k+1,t)}$. There are 2^t $\gamma_{i,j}$'s. We claim that they are all different and non-zero in $\mathbb{F}$. Suppose $m_i\beta^j = m_{i'}\beta^{j'}$. Then $\frac{m_i}{m_{i'}} = \beta^{j'-j}$. Note that all the powers of β are in $\mathbb{F} - \mathbb{F}_p$ except for $\beta^{2^{\min(k+1,t)}}$ and $\beta^{2^{min(k,t-1)}}$. which belong to $\mathbb{F}_p$. Then we get either $\beta^j = \beta^{j'}$, in which case $m_i = m_{i'}$ leading to $i = i'$, or, $\beta^{j-j'} = -1$, in which case $m_i = -m_{i'}$. So we have $m_i + m_{i'} = 0$ in $\mathbb{F}_p$. But this is impossible since $m_i + m_{i'}$ and the algorithm verified that these were coprime with n. Thus, we get our claim.
Next, since the algorithm verified in Step (9) that $(1 + m_i\theta) \in G_n$ for each i, it follows from the previous lemma that each of the $(1 + \gamma_{ij}\theta) \in G_n$. Therefore G_n contains 2^t different monomials over $\mathbb{F}$, and, as in the case $n \equiv 1 \pmod 4$, we get the result. ■

We are now ready for the proofs of the main theorems of this section:

Proof. of Theorem 3.4.1
Again this proceeds along the lines of the proof of Theorem 3.3.1. The only difference is that now $\mathrm{Gal}(K/\mathbb{F}_p)$ has order 2^{t+1} and G_n has at least 2^{2^t} elements. The fact that $2^{2^t} > n^{\sqrt{2^{t+1}}}$ is easily derived from $2^{2^s} > n^{\sqrt{2^s}}$, keeping in mind that $t = s + 1$. ■

Analysis of Complexity:

Proof. of Theorem 3.4.2
The proof is similar to the proof of Theorem 3.3.2. We note that the cost of Steps (5)-(7) is $\tilde{\vartheta}((\log n)^3)$, which is less than the cost of Steps (4)-(14) of the algorithm in the previous case, because the number of gcd's computed is much less in this one. However, this fact doesn't lead to an improvement of time complexity since the steps which determining it are Steps (8)-(11). In the following Remark we compare the speed of this algorithm with the one we have seen for case $n \equiv 1 \pmod 4$, obtaining, in this way, the proof. ∎

Remark 1: *We note that the same polynomial used in this algorithm could have been used in the algorithm for number* $n \equiv 1 \pmod 4$, *with no additional hypothesis on* a. *To see this, notice that if* $\left(\frac{a}{n}\right) = -1$ *and* $\left(\frac{1-a}{n}\right) = 1$, *then* $\left(\frac{a^{-1}}{n}\right) = -1$ *and*

$$\left(\frac{1-a^{-1}}{n}\right) = \left(\frac{-a^{-1}(1-a)}{n}\right) = \left(\frac{a^{-1}}{n}\right) = -1.$$

So the pair $a, 1-a$ *is achieved at most at the cost of computing* a^{-1}. *Hence, by Proposition 3.2.1 the polynomial* $x^{2^{t+1}} - 2x^{2^t} - a$ *is irreducible. However the algorithm we presented for numbers* $n \equiv 1 \pmod 4$ *runs about four times faster than the one we presented for* $n \equiv -1 \pmod 4$. *This happens because, even if the number of operations performed by both algorithms is the same, the degree of the polynomial used in the second case, is four times the degree of the polynomial used in the first one.*

3.5 Weakly Conditioned and Unconditioned Tests

3.5.1 Case 1: $n \equiv 1 \pmod 4$.

Let $n \equiv 1 \pmod 4$. Let $k = \nu_2(n-1)$, obviously $k \geq 2$. This time we assume integers a and u are such that $1 \leq u \leq k$ and $a^{\frac{n-1}{2^u}} \equiv -1 \pmod n$. Note that if $u = 1$ then we obtain the case we have already analysed. At the other hand, if $u = k$ we can conclude that such an a always exists: $a = -1$. Hence we will refer to this latter case as the *unconditioned* one. We are going to see a deterministic primality test for all such numbers. The complexity of this test will depend also on u. The optimal performance occurs when $u = 1$; on the contrary $u = k$ is the worst case we can obtain.
First of all, let's note that if $n = h2^k + 1$ is prime, and $h \not\equiv 0 \pmod 5$ then either $5^{\frac{n-1}{2}} \equiv -1 \pmod n$ or $5^{\frac{n-1}{4}} \equiv -1 \pmod n$ or n is a multiple of 5. This fact has been used to produce a deterministic primality test for numbers of that form provided $k > \log n$ (see [4]). Combining this observation with the one we have done in the Section where we dealt with this case, we can deduce that every number of the form $n = h2^k + 1, h \not\equiv 0 \pmod{15}$ is either a multiple of 3 or 5, or can be tested using $a = 3$ or $a = 5$ and $u = 1$ or

$u = 2$. Again we let $s = \lceil 2 \log\log n \rceil$.
We now present the algorithm in the form of a theorem. We don't give a proof of this theorem since it can be deduced as in the section where we dealt with this case: we will only enumerate some facts.

Theorem 3.5.1. *Let $n \equiv 1 \pmod 4$. Let $k = \nu_2(n-1)$. Let $s = \lceil 2\log\log n \rceil$. Let a and u be integers, $1 \leq u \leq k$ and such that $a^{\frac{n-1}{2^u}} \equiv -1 \pmod n$. Let S be a set of integers, $|S| = 2^{\max(s-k+2(u-1),0)}$ such that for any pair m, m' of different elements of S, $\gcd(m^{2^{k+1-u}} - m'^{2^{k+1-u}}, n) = 1$ and such that every element of S is coprime with m. Suppose also that for every $m \in S$ we have $(1+mx)^n \equiv (1+mx^n) \pmod{n, x^{2^{s+2(u-1)}} - a}$ and that n in not a non trivial perfect power. Then n is prime.*

Proof. Sketch Let $r = s+u-1$. Let $f(x) = x^{2^{s+2(u-1)}} - a = x^{2^{r+u-1}} - a$.

1. The equation $a^{\frac{n-1}{2}} \equiv -1 \pmod n$ implies that every prime divisor q of n satisfies $\nu_2(q-1) \geq k-u+1$.
2. There is a prime p dividing n such that $\nu_2(p-1) \leq k$.
   Let p be such a prime and θ a root of $f(x)$ in an algebraic closure of $\mathbb{F}_p$.
3. $2^r \leq [K : \mathbb{F}_p] \leq 2^{r+u-1}$.
4. $\sigma_n \in \mathrm{Gal}(K/\mathbb{F}_p)$. G_n is a cyclic subgroup of K^*.
   Suppose $n = p^l d$
5. $\sigma_d \in \mathrm{Gal}(K/\mathbb{F}_p)$. $G_n \subseteq G_{p^i d^j}$ for all $i, j \geq 0$.
6. There are integers i_1, i_2, j_1, j_2 such that $0 \leq i_1, i_2, j_1, j_2 \leq \sqrt{2^{n+u-1}}$, $(i_1, j_1) \neq (i_2, j_2)$ and such that $\sigma_{p^{i_1} d^{j_1}} = \sigma_{p^{i_2} d^{j_2}}$.
7. $|G_n|$ divides $p^{i_1} d^{j_1} - p^{i_2} d^{j_2}$.
8. From the fact $2^{2^s} > n^{\sqrt{2^s}}$ it is easily deduced that for all $v \geq 0$, $2^{s+v} > n^{\sqrt{2^{s+2v}}}$. In particular, $2^{2^r} > n^{\sqrt{2^{r+u-1}}}$.
9. From the fact $(1+m\theta) \in G_n$ for all $m \in S$ we deduce, just like we have done in the section where we dealt with this case, that G_n contains 2^r different monomials over $\mathbb{F}_p$. Hence, $|G_n| \geq 2^{2^r}$.
10. From items 6, 7, 8 and 9 we can deduce that $d = 1$ so $n = p^l$.
11. Since n is not a non trivial perfect power then we must have $n = p$.

■

Corollary 3.5.1. *If n, k, a, u are as in the previous theorem then the primality of n can be determined in $2^{2(u-1)} 2^{\max(s+2(u-1)-k,0)} \tilde{\vartheta}((\log n)^4)$ time.*

Proof. As in the analysis of complexity of the previous sections. ■

To be more precise about this result A_u the algorithm associated to Theorem 3.5.1 and $C(A_u)$ its complexity. Corollary 3.5.1 implies that $C(A_u) \approx 2^{4(u-1)}C(A_1)$ if $k \leq 2^s$ and $C(A_u) \approx 2^{2(u-1)}C(A_1)$ if $k \geq 2^{s+2(u-1)}$.
Even more precise, $C(A_u) \approx 2^{4(u-1)}2^{-\min(\max(k-s,0),2(u-1))}C(A_1)$.
Note also that in the *unconditioned* case $(u = k)$ the complexity is $2^{4(k-1)}\tilde{\vartheta}((\log n)^6)$ which is polynomial time only for values of k not too large.

3.5.2 Case 2: $n \equiv -1 \pmod 4$.

First of all let's note the following:

Remark 2: *If b, c are given integers such that $\left(\frac{b^2+c^2}{n}\right) = -1$ then $a = (bc^{-1})^2 + 1$ satisfies $\left(\frac{a}{n}\right) = \left(\frac{1-a}{n}\right) = -1$. This is easy to verify noting that $\left(\frac{-1}{n}\right) = -1$ since $n \equiv -1 \pmod 4$. Alternatively, we could replace the polynomial in the algorithm by the polynomial $x^{2^{t+1}} - 2bx^{2^t} + (b^2 + c^2)$, which is also irreducible in $\mathbb{F}_p$ under the assumption $(b^2 + c^2)^{\frac{n-1}{2}} \equiv -1 \pmod n$ and $(x + iy)^n \equiv (x - iy) \pmod n$.*

Like we have seen for the case $n \equiv 1 \pmod 4$, similarly, when $n \equiv -1 \pmod 4$ we have the following theorem, that we state without proof for the same reason.

Theorem 3.5.2. *Let $n \equiv -1 \pmod 4$ and let $k = \nu_2(n + 1)$. Also let $s = \lceil 2 \log\log n \rceil$ and $t = s + 1$. Let $\alpha \in \mathbb{Z}[i]$ and u a positive integer, $1 \leq u \leq k + 1$ and such that $\alpha^{\frac{n^2-1}{2^u}} \equiv -1 \pmod n$. Suppose that every positive integer less or equal than $2^{\max(s-k+2(u-1),0)+1}$ is coprime with n.
Suppose also that for every $m \leq 2^{\max(s-k+2(u-1),0)}$ we have $(1 + mx)^n \equiv (1+mx^n) \pmod{n, x^{2^{t+2u-1}} - \alpha}$ and that n is not a non trivial perfect power. Then, n is prime.*

Corollary 3.5.2. *If n, k, α, u are as in the previous theorem, then the primality of n can be determined in $2^{2u}2^{\max(s+2(u-1)-k,0)}\tilde{\vartheta}((\log n)^4)$ time. In other words, if we call these tests B_u, then $C(B_u) \approx 4C(A_u)$.*

3.6 Conclusions and Conjecture

In practice, it is clearly desirable to apply **Algorithm 1** or **Algorithm 2** when possible.
In the worst case $(\nu_2(n - 1) = k = 2)$, **Algorithm 1** runs at least 2^{11} times faster than the best possible running time of the AKS algorithm for primes n large enough. Hence, the worst case of **Algorithm 2** runs 2^9 times faster than the best possible case of AKS. This occurs because the

main step of **Algorithm 1** executes at most $2^{s-2} \leq \frac{(\log n)^2}{4}$ iterations, each of which consists in multiplying polynomials of degree at most $(\log n)^2$. In contrast, in the best possible case AKS executes $8(\log n)^2$ multiplications of polynomials of degree at least $64(\log n)^2$. When k is large the difference in the performance improves dramatically.
For implementation, if no integer a satisfying $\left(\frac{a}{n}\right) = -1$ is known a priori, then a search for such an a within a reasonable range should be implemented. In addition, if this fails to produce such an a, then a search for a small value of u would be useful.
Note that if $k > 1/2 \log n$ then **Algorithm 1** and **Algorithm 2** run in $\tilde{\vartheta}((\log n)^2)$ time. Also, while k increases from 2 to $[2 \log \log n]$ the running time improves up to $\tilde{\vartheta}((\log n)^4)$. But when k varies from $[2 \log \log n]$ to $[1/2 \log n]$ there is no more improvement in the speed of our algorithm. Here we believe one should attempt to sharpen the algorithms because the order of the group G_n can be proven to increase together with k, in such a way that it forces s, that is the smallest solution of $|G_n| > n^{2^{s/2}}$, to decrease. To be precise we formulate the following conjecture:

Conjecture 3.6.1. **Algorithm 1** *and* **Algorithm 2** *can be modified in such a way that while k increases from 2 to* $(1/2) \log n$ *the complexity of both algorithms decreases from* $\tilde{\vartheta}((\log n)^6)$ *to* $\tilde{\vartheta}((\log n)^2)$.

Chapter 4

Lenstra and Pomerance

The algorithm we are now going to present is a deterministic primality test that decides, in time $\tilde{\vartheta}(\log^6 n)$, whether an input integer n is prime or not.

4.1 Introduction

We have seen that the AKS algorithm with Lentra's variant works in time $\tilde{\vartheta}(\log^{21/2} n)$ and we have argued that the true run time of this algorithm may reasonably be conjectured to equal $\tilde{\vartheta}(\log^6 n)$. Lenstra and Pomerance's algorithm, that we are now going to analyse, achieves the same run time not by proving their conjectures, but by modifying their algorithm. Both the AKS algorithm and this one perform computations in a suitable ring extension of the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n; if d denotes the degree of the extension, the problem of obtaining a small run time exponent boils down to providing a good upper bound for the smallest d that can be used. In the AKS algorithm we have used the ring $(\mathbb{Z}/n\mathbb{Z})[x]/(x^d-1)$, and Agrawal *et al.* found that the problem of accurately estimating the least usable value for d leads to an unsolved problem in analytic number theory. Therefore, in this algorithm we select our ring extension from a much wider class, for which estimating d becomes feasible. The ring extensions of $\mathbb{Z}/n\mathbb{Z}$ that we use shall be referred to as *pseudofields*.

4.2 Pseudofields

Definition 4.2.1. *A pseudofield is a pair (A, α) consisting of a ring A and an element $\alpha \in A$, such that for some integer $n > 1$, some integer $d > 0$, and some ring automorphism σ of A, the following conditions are satisifed:*

$$\text{char} A = n, \tag{4.1}$$

$$\#A \leq n^d, \tag{4.2}$$

$$\sigma\alpha = \alpha^n, \tag{4.3}$$

$$\sigma^d\alpha = \alpha, \tag{4.4}$$

$$\sigma^{d/l}\alpha - \alpha \in A^* \quad \text{for each prime number } l \text{ dividing } d. \tag{4.5}$$

4.2.1 Algebraic properties of pseudofields

We are now going to see the basic algebraic properties of pseudofields.
First let's state the following condition: for a ring A, an element $\alpha \in A$, and a ring automorphism σ of A, we will have occasion to refer to:

$$\sigma\alpha \quad \text{belongs to the subring of } A \text{ generated by } \alpha. \tag{4.6}$$

This condition is implied by condition (4.3), if n is a positive integer.

Lemma 4.2.1. *Let A be a ring, let $\alpha \in A$, let $\mathbb{Z}_{>0}$, and let σ be a ring automorphism of A such that* (4.4)*,*(4.5) *and* (4.6) *are satisfied. Then, for any $i, j \in \mathbb{Z}$ with $i \not\equiv j \pmod{d}$ one has $\sigma^i\alpha - \sigma^j\alpha \in A^*$.*

Proof. Let $h \in \mathbb{Z}$,$h \notin d\mathbb{Z}$, and let $I = (\sigma^h\alpha - \alpha)$ be the A-ideal generated by $(\sigma^h\alpha - \alpha)$. The set $B = \{\beta \in A : \sigma^h\beta \equiv \beta \pmod{I}\}$ is a subring of A. Since, obviously, $\sigma^h\alpha \equiv \alpha \pmod{I}$, we have $\alpha \in B$ and, by (4.6), $\sigma\alpha \in B$; that is, choosing $\beta = \sigma\alpha$, we have $\sigma^{h+1}\alpha \equiv \sigma\alpha \pmod{I}$, which implies that $\sigma(\sigma^h\alpha - \alpha)$ belongs to I, and, therefore, $\sigma I \subseteq I$. On the other hand, since σ^d maps $\sigma^h\alpha - \alpha$ to itself, we actually have $\sigma I = I$, so for all $m \in \mathbb{Z}$ one has $\sigma^m I = I$.
It follows that the set $H = \{m \in \mathbb{Z} : \sigma^m\alpha \equiv \alpha \pmod{I}\}$ is a subgroup of $\mathbb{Z}$. It contains d and h, where $h \notin d\mathbb{Z}$, so we have $H = d'\mathbb{Z}$ where d' is a divisor of d with $1 \leq d' < d$. Choose a prime number l that divides d/d'. Then $d/l \in d'\mathbb{Z} = H$, so $\sigma^{d/l}\alpha - \alpha \in I$. Thus by (4.5) the ideal I contains a unit, and therefore $I = A$. This implies $\sigma^h\alpha - \alpha \in A^*$. Now let $i, j \in \mathbb{Z}$,$i \not\equiv j \pmod{d}$. Then the integer $i - j$ does not belong to $d\mathbb{Z}$, so by the result just proved we have $\sigma^{i-j}\alpha - \alpha \in A^*$. Applying σ^j we find $\sigma^i\alpha - \sigma^j\alpha \in A^*$, as required. ■

Lemma 4.2.2. *Let A be a ring, let $k \in \mathbb{Z}_{\geq 0}$, and let $\alpha_1, \alpha_2, \ldots, \alpha_k \in A$ be such that $\alpha_i - \alpha_j \in A^*$ whenever $1 \leq i < j \leq k$. Then for each $g \in A[x]$ which vanishes at $\alpha_1, \alpha_2, \ldots, \alpha_k$, we have $g \in A[x] \cdot \prod_{i=1}^k (x - \alpha_i)$*

Proof. Let $I_i = A[x] \cdot (x - \alpha_i)$, for $1 \leq i \leq k$. For $i \neq j$, the unit $\alpha_i - \alpha_j$ can be written as $-(x-\alpha_i)+(x-\alpha_j)$, so $I_i + I_j = A[x]$ that means that I_i and I_j are co-prime, which implies that $\prod_{i=1}^k I_i = \bigcap_{i=1}^k I_i$. From $x \equiv \alpha_i \pmod{I_i}$ we obtain $g \equiv g(\alpha_i) \pmod{I_i}$ for each $g \in A[x]$, so if each $g(\alpha_i)$ vanishes, then we have $g \in \bigcap_{i=1}^k I_i = \prod_{i=1}^k I_i = A[x] \cdot \prod_{i=1}^k (x - \alpha_i)$, as required. ■

The following result summarizes the technical information on pseudofields that we shall need.

Proposition 4.2.1. *Let A be a ring, let $\alpha \in A$, and let the integers $n \in \mathbb{Z}_{>0}$, $d \in \mathbb{Z}_{>0}$ and let the ring automorphism σ of A satisfy* (4.1), (4.2), (4.4), (4.5) *and* (4.6). *Then we have:*

(a) *for each $\beta \in A$ there are unique $a_0, a_1, \ldots, a_{d-1} \in (\mathbb{Z}/n\mathbb{Z})$ with $\beta = \sum_{i=0}^{d-1} a_i\alpha^i$;*

(b) *we have $\#A = n^d$, and σ^d equals the identity;*

(c) *the polynomial $f = \prod_{i=0}^{d-1}(x - \sigma^i\alpha)$ belongs to the subring $(\mathbb{Z}/n\mathbb{Z})[x]$ of $A[x]$;*

(d) *the ring homomorphism $(\mathbb{Z}/n\mathbb{Z})[x] \to A$ sending x to α is surjective, and its kernel is generated by the polynomial f from* **(c)***;*

(e) *if $I \subset A$ is an ideal, then we have $\sigma I \subset I$ if and only if there exists a divisor m of n such that $I = mA$;*

(f) *for each prime factor p of n there exists a unique residue class $(i \bmod d)$ such that for all $\beta \in A$ we have $\beta^p \equiv \sigma^i\beta \pmod{pA}$.*

Proof. Let's denote $\ : (\mathbb{Z}/n\mathbb{Z})[x] \to A$ the unique homomorphism which sends x to α as in **(d)**. This homomorphism maps each $g \in (\mathbb{Z}/n\mathbb{Z})[x]$ to $g(\alpha)$. Let's now suppose $g \in \ker(\ )$, then for each $i \in \mathbb{Z}$, we have $g(\sigma^i\alpha) = \sigma^i(g(\alpha)) = \sigma^i(\ (g)) = 0$ and, by Lemma 4.2.1, we have that $\sigma^i\alpha - \sigma^j\alpha \in A^*$ for $i \not\equiv j \pmod d$; so, applying Lemma 4.2.2, we obtain that $g \in A[x]f$, where f is as in **(c)**. Let $\tilde{\ }$ be the restriction of $\ $ to $(\mathbb{Z}/n\mathbb{Z}) + (\mathbb{Z}/n\mathbb{Z})x + \ldots + (\mathbb{Z}/n\mathbb{Z})x^{d-1}$. Since each non-zero $g \in A[x]f$ has degree at least d, this implies

$$\ker(\ ) \cap ((\mathbb{Z}/n\mathbb{Z}) + (\mathbb{Z}/n\mathbb{Z})x + \ldots + (\mathbb{Z}/n\mathbb{Z})x^{d-1}) = \{0\},$$

so that $\ker(\tilde{\ }) = (0)$ and, therefore, this restriction is injective. Moreover, we know that there are n^d elements is $((\mathbb{Z}/n\mathbb{Z}) + (\mathbb{Z}/n\mathbb{Z})x + \ldots + (\mathbb{Z}/n\mathbb{Z})x^{d-1})$ and, from (4.2), we also know that $\#A \leq n^d$; so, since $\tilde{\ }$ is injective, it must be surjective as well and we must have $\#A = n^d$. This proves **(a)**, the firs statement of **(b)**, and the surjectivity in **(d)**. Since each element of A can be expressed in α, the second statement of **(b)** follows from (4.4). Applying **(a)** to $\beta = \alpha^d$, one finds $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}/n\mathbb{Z}$ for which the polynomial $g = x^d - \sum_{i=0}^{d-1} a_ix^i = x^d - \alpha^d$ belongs to $\ker(\ )$; hence $g \in A[x]f$, and comparing degrees and leading coefficients one finds $g = f$. This implies **(c)**. We have $\ker(\ ) = A[x]f \cap (\mathbb{Z}/n\mathbb{Z})[x] = (\mathbb{Z}/n\mathbb{Z})[x]f$, the latter equality because f is a monic polynomial in $(\mathbb{Z}/n\mathbb{Z})[x]$. This proves the remaining assertion of **(d)**.

The "if"-part of **(e)** is clear. For the "only if"-part, let I be an ideal of A with $\sigma I \subset I$, and let $\bar{A}$ be the ring A/I. From $\sigma I \subset I$ it follows that σ induces a ring homomorphism $\bar{\sigma} : \bar{A} \to \bar{A}$. From **(b)** one sees that $\bar{\sigma}^d$ is the identity on $\bar{A}$, so $\bar{\sigma}$ is an automorphism of $\bar{A}$. Put $m = \text{char}\bar{A}$. Then m divides n,

and we have $mA \subset I$, so from **(a)** we see $\#\bar{A} = \#A/I \leq \#A/mA = m^d$, with the equality if and only if $mA = I$. We claim that (4.1), (4.2), (4.4), (4.5) and (4.6), with $\bar{A}$, m, d, $\bar{\sigma}$ and $\bar{\alpha} \equiv \alpha \pmod{I}$ in the roles of A, n, d, σ and α, are satisfied. We have just proved (4.2); (4.1) is true by definition; (4.4), (4.5) and (4.6) follow from the corresponding properties of A, n, d, σ and α. Hence, applying **(b)** to this new situation, we find $\#\bar{A} = m^d$, so that $mA = I$. This proves **(e)**.
To prove **(f)**, we replace, for notational convenience, n and A by p and A/pA, so that we may assume $n = p$. Let $\phi : A \to A$ be the ring homomorphism that maps each $\beta \in A$ to β^p, and let $g \in (\mathbb{Z}/n\mathbb{Z})[x]$ be such that $\sigma\alpha = g(\alpha)$. If $\rho : A \to A$ is any homomorphism with $\sigma\rho = \rho\sigma$, then we have $\sigma(\rho\alpha) = \rho(\sigma\alpha) = \rho(g(\alpha)) = g(\rho\alpha)$. Applying this to $\rho = \phi$ and to $\rho = \sigma^i$, where $i \in \mathbb{Z}$, we obtain $\sigma(\phi\alpha) = g(\phi\alpha)$ and $\sigma(\sigma^i\alpha) = g(\sigma^i\alpha)$ and therefore $\sigma(\phi\alpha) \equiv \sigma(\sigma^i\alpha) \pmod{\phi\alpha - \sigma^i\alpha)A}$. Hence, for any $i \in \mathbb{Z}$, the ideal $I = (\phi\alpha - \sigma^i\alpha)A$ satisfies $\sigma I \subset I$, so by **(e)** and the fact that n is prime, we have that $I = A$ or $I = nA$; since $A = A/pA$ with $p = n$, $nA = nA/nA = 0$. So we have that $\phi\alpha - \sigma^i\alpha$ is either a unit or 0. From $\prod_{i=0}^{d-1}(\phi\alpha - \sigma^i\alpha) = f(\phi\alpha) = \phi(f(\alpha)) = \phi(\prod_{i=0}^{d-1}(\alpha - \sigma^i\alpha)) = \phi(0) = 0^p = 0$, we see that not all $\phi\alpha - \sigma^i\alpha$ can be units, so at least one of them is 0. Then we have $\phi\alpha = \sigma^i\alpha$, so $\phi = \sigma^i$ by **(a)**. The uniqueness of i mod d follows from Lemma 4.2.1. This completes the proof. ■

Proposition 4.2.2. *Let (A, α) be a pseudofield and let n, d be as in the definition. Then there is a unique monic polynomial $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ with the property that there is a ring isomorphism $(\mathbb{Z}/n\mathbb{Z})[x]/(f) \cong A$ that maps the coset $x \pmod{f}$ to α. In addition, the degree of this polynomial equals d.*

Proof. Since (4.3) implies (4.6), Proposition 4.2.1 applies. The existence of f follows from 4.2.1**(d)**. No two distinct monic polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ generate the same ideal, so f is unique. From 4.2.1**(c)** we deduce $\deg f = d$. This completes the proof. ■

The polynomial f from the above proposition and its degree d are called the *characteristic polynomial* and the *degree* of the pseudofield, respectively. The proposition implies that each element of A can in a unique way be written as $g(\alpha)$, where $g \in (\mathbb{Z}/n\mathbb{Z})[x]$ satisfies $\deg g < d$. This implies that equality holds in (4.2). It also implies that, as a ring, A is generated by α, so that the automorphism σ of A is uniquely determined by (4.3); we refer to it as the *Frobenius automorphism* of the pseudofield.

Finite fields yield pseudofields, as explained in the following result.

Proposition 4.2.3. *Let p be a prime number, let A be a ring of characteristic p, and let $\alpha \in A$. Then (A, α) is a pseudofield if and only if A is a finite field satisfying $A = \mathbb{F}_p(\alpha)$. In addition, if (A, α) is a pseudofield, and σ denotes its Frobenius automorphism, then for all $\beta \in A$ we have $\sigma\beta = \beta^p$.*

Proof. j

DA RIVEDERE UN PO'!!!!!!

For the "if"-part let's assume that A is a finite field with $A = \mathbb{F}_p(\alpha)$. Let $d = [A : \mathbb{F}_p]$ and let's define $\sigma : A \to A$ by putting $\sigma\beta = \beta^p$ for every $\beta \in A$. Now (4.1), (4.2), (4.3) and (4.4) are obvious. Moreover, if l is a prime number dividing d, then $\sigma^{d/l}$ is not the identity, so by $A = \mathbb{F}_p(\alpha)$ we have $\sigma^{d/l}\alpha \neq \alpha$; since A is a field, this implies (4.5).
To prove the "only if"-part and the last statement of the proposition, let's assume that (A, α) is a pseudofield. Let d be the degree and σ the Frobenius automorphism. Since p is prime, the map $A \to A$ sending each β to β^p is a ring homomorphism. It agrees with σ on α, so by 4.2.1**(a)** on all of A, which is the last statement of our proposition. To prove that A is a field, we let $\beta \in A$, and we prove that β equals 0 or is a unit. Put $I = A\beta$. From $\sigma\beta = \beta^p$ we see that $\sigma I \subset I$, so by 4.2.1**(e)** and the fact that p is prime, we have $I = A$ or $I = pA = 0$. In the first case β is a unit, in the second case it equals 0. Thus, A is a field. By 4.2.1**(a)**, it is finite, and we have $A = \mathbb{F}_p(\alpha)$. This completes our proof. ∎

4.2.2 Primality testing with pseudofields

We are now going to see that, for the purpose of primality testing, pseudofields can play the role that the rings $(\mathbb{Z}/n\mathbb{Z})[x]/(x^d - 1)$ play in the AKS algorithm with Lenstra's variant.

Lemma 4.2.3. *Let R be a ring, and let G be a finite subgroup of R^* such that for each $\beta \in G$, $\beta \neq 1$ we have $\beta - 1 \in R^*$. Then G is cyclic.*

Proof. We may clearly assume $R \neq \{0\}$, so that we can choose a maximal ideal M of R. Let γ be the natural group homomorphism $\gamma : R^* \to (R/M)^*$. For each $\beta \in G$, $\beta \neq 1$, the unit $\beta - 1$ does not belong to M, so that $\beta \notin \ker(\gamma)$. Hence the restriction of γ to G is injective, and G is isomorphic to its image in $(R/M)^*$. Since any finite subgroup of the multiplicative group of a field is cyclic, then G is cyclic. ∎

Let (A, α) be a pseudofield, and denote n, d and σ its characteristic, its degree and its Frobenius automorphism, respectively. We let p be a prime divisor of n, and put $R = A/pA$. We shall simply write α for the image of α in R, and σ for the automorphism of R induced by σ. Note that conditions (4.1), (4.2), (4.4), (4.5) and (4.6), with R, α, p, d and σ in the role of A, α, n, d and σ, are satisfied, so that Proposition 4.2.1 can be used. As we have seen in the proof of Proposition 4.2.3, by 4.2.1**(e)** applied to $I = R\beta$ we have that

$$\text{if } \beta \in R \text{ satisfies } \sigma\beta \in R\beta, \text{ then } \beta = 0 \text{ or } \beta \in R^*. \tag{4.7}$$

We put

$$G = \{\beta \in R : \beta \neq 0,\ \sigma\beta = \beta^n\}.$$

For any $\beta \in G$, we have $\sigma\beta = \beta^n \in R\beta$, so $\beta \in R^*$ by (4.7). Since G is finite, closed under multiplication and contains 1, it is a subgroup of R^*. Moreover, for any $\beta \in G$, $\beta \neq 1$, we have $\sigma\beta = \beta^n \equiv 1 \bmod R \cdot (\beta - 1)$, so $\sigma(\beta - 1) \in R \cdot (\beta - 1)$ and, again by (4.7), $\beta - 1 \in R^*$. Thus, Lemma4.2.3 implies

$$G \text{ is a cyclic subgroup of } R^*. \tag{4.8}$$

Lemma 4.2.4. *If $\#G > n^{\sqrt{d/3}} - 1$, then n is a power of p.*

We will not deal with the proof of this lemma.

Proposition 4.2.4. *Let (A, α) be a pseudofield of degree d with Frobenius automorphism σ, and let $n = \mathrm{char} A$. Suppose that for each $a = 1, 2, \ldots, \left[(d/3)^{1/2}(\log n)/\log 2\right]$ we have $\alpha^n + a = (\alpha + a)^n$. Suppose also that we have $d > (\log n)^2/\left(3 \cdot (\log 2)^2\right)$, and that n has a prime factor greater than $(d/3)^{1/2}(\log n)/\log 2$. Then n is a power of a prime number.*

Proof. Let's write $B = [(d/3)^{1/2}(\log n)/\log 2]$. When $d = (\log n)^2/3 \cdot (\log 2)^2$ we have $B = \left(\frac{(\log n)^2}{9 \cdot (\log 2)^2}\right)^{1/2} \cdot \log n/\log 2 = \frac{\log^2 n}{3 \cdot (\log 2)^2} = d$ and therefore, $d > (\log n)^2/\left(3 \cdot (\log 2)^2\right)$ implies $d > B$.
We apply the results that we have just seen to a prime factor p of n that satisfies $p > B$. Since (A, α) is a pseudofield, we know, by condition (4.3), that $\sigma\alpha = \alpha^n$, from which we can deduce that the element α of $R = A/pA$ belongs to the subgroup G of R^*. From $\sigma(\alpha + a) = \sigma\alpha + a = \alpha^n + a = (\alpha + a)^n$ for $a = 1, 2, \ldots, B$ and from 4.2.1**(a)**,which implies each $\alpha + a \neq 0$, we see that $\alpha + 1, \alpha + 2, \ldots, \alpha + B$ also belong to G. For each proper subset S of $\{1, 2, \ldots, B\}$, the element $\prod_{a \in S}(\alpha + a)$ also belongs to G. There are $2^{B+1} - 1$ such sets S, and we claim that they give rise to 2^{B+1} different elements of G. To prove this, note that by $p > B$ the polynomials $x + a$, $a = 0, 1, \ldots, B$ are distinct in $\mathbb{F}_p[x]$, and that by unique factorization in $\mathbb{F}_p[x]$ the polynomials $\prod_{a \in S}$, with S as above, are pairwise distinct. By $d > B$, all these polynomials have degrees smaller than d, so by 4.2.1**(a)** (applied to R) they give rise to $2^{B+1} - 1$ different elements $\prod_{a \in S}(\alpha + a)$ of G, as asserted.
It follows that we have

$$\#G \geq 2^{B+1} - 1 > 2^{(d/3)^{1/2}(\log n)/\log 2} - 1$$

since $2 = e^{\log 2}$, we have

$$2^{(d/3)^{1/2}(\log n)/\log 2} - 1 = e^{\log n^{\sqrt{d/3}} \cdot (\log 2/\log 2)} - 1 = n^{\sqrt{d/3}} - 1.$$

Thus we have

$$\#G > n^{\sqrt{d/3}} - 1.$$

Applying 4.2.4 we conclude that n is a power of p. ■

4.3 Algorithmic aspects of pseudofields

Proposition 4.2.2 shows that a pseudofield is, up to isomorphism, determined by its characteristic n and its characteristic polynomial f. We shall, for algorithmic purposes, always assume a pseudofield to be specified by the pair (n, f), the polynomial f being represented by its vector of coefficients; this applies in particular when a pseudofield forms part of the input or output of an algorithm. The pseudofield represented by (n, f) equals $((\mathbb{Z}/n\mathbb{Z})[x]/(f), x \bmod f)$, and its elements are represented as polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ of degree smaller than the degree d of the pseudofield. It is well-known that there are algorithms that, given n, f, and two elements of $(\mathbb{Z}/n\mathbb{Z})[x]/(f)$, compute the sum and the product of this two elements within time $\tilde{\vartheta}(d \log n)$ [see 14].

As a consequence, testing the equality $\alpha^n + a = (\alpha + a)^n$ from Proposition 4.2.4 for a single value of a in $\mathbb{Z}/n\mathbb{Z}$ can be done in time $\tilde{\vartheta}\left(d(\log n)^2\right)$, and for about $(d/3)^{1/2}(\log n)/\log 2$ values of a in time $\tilde{\vartheta}((d^{1/2}\log n)^3)$. This time bound will equal the required time bound $(\tilde{\vartheta}((\log n)^6))$ if we use a pseudofiled for which the degree d is, as a function of n, not too much larger than the lower bound $(\log n)^2/(3 \cdot (\log 2)^2)$ from Proposition 4.2.4. Thus, we are faced with the problem of constructing a pseudofield of given characteristic and approximately given degree. In order to solve this problem, we are now going to introduce some definitions.

Definition 4.3.1. *Let $n \in \mathbb{Z}, n > 1$. By a period pair for n we mean a pair (r, q) of integers with the properties*

$$r \text{ is a prime not dividing } n, \tag{4.9}$$

$$q \mid r - 1 \text{ with } q > 1, \tag{4.10}$$

$$\text{the multiplicative order of } n^{(r-1)/q} \text{ modulo } r \text{ equals } q. \tag{4.11}$$

(4.11) implies that $n^{(r-1)/q} \not\equiv 1 \pmod{r}$. Further,

Definition 4.3.2. *A period system for n is a finite set P of period pairs for n such that*

$$\gcd(q, q') = 1 \text{ whenever } (r, q), (r', q') \in P, (r, q) \neq (r', q'), \tag{4.12}$$

and the degree of P is $\prod_{(r,q)\in P} q$.

4.3.1 Gaussian Periods

In this section we let n be an integer with $n > 1$. Let r be a prime number not dividing n, and define $\Phi_r = \sum_{i=0}^{r-1} \in (\mathbb{Z}/n\mathbb{Z})[x]$. The element $(x \bmod \Phi_r)$ of the ring $(\mathbb{Z}/n\mathbb{Z})[x]/(\Phi_r)$ is denoted by ζ_r, and that ring itself by $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. We have $\zeta_r^r = 1 \neq \zeta_r$, so ζ_r is an element of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^*$ of order r. From $\deg \Phi_r = r-1$, we know that $\nu \in (\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ means that $\nu = a_0 + a_1\zeta_r + \ldots + a_{r-2}\zeta_r^{r-2}$ with $a_0, \ldots, a_{r-2} \in \mathbb{Z}/n\mathbb{Z}$; this implies that $\{1, \zeta_r, \ldots, \zeta_r^{r-2}\}$ generate $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. Thus, also $\{1, \zeta_r, \ldots, \zeta_r^{r-2}, \zeta_r^{r-1}\}$ generate this ring and, since $1 = -(\zeta_r + \ldots + \zeta_r^{r-1})$ we see that the elements ζ_r^i, $1 \leq i \leq r-1$, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$.

For each $a \in \mathbb{Z}, a \notin r\mathbb{Z}$, the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ has a unique automorphism mapping ζ_r to ζ_r^a; we write σ_a for this automorphism. The set Δ of all automorphism of the form σ_a is a group under composition, and the map $\sigma_a \to a \pmod r$ is a group isomorphism $\Delta \cong \mathbb{F}_r^*$. We can conclude that Δ is cyclic of order $r-1$, and that, for $\tau \in \Delta$, the elements $\tau\zeta_r = \zeta_r^a$ with $1 \leq a \leq r-1$, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$.

Next let q be a positive integer dividing $r-1$. Then $\Delta^q = \{\tau^q : \tau \in \Delta\}$ is a subgroup of index q of Δ. The subset $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q} = \{\beta \in (\mathbb{Z}/n\mathbb{Z})[\zeta_r] : \rho\beta = \beta \ \forall \rho \in \Delta^q\}$ is the set of all the elements of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ which are invariant under all $\rho \in \Delta^q$ and is a subring of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. An element $\omega = \sum_{\tau\in\Delta} a_\tau \cdot \tau\zeta_r$, with each $a_\tau \in \mathbb{Z}/n\mathbb{Z}$, belongs to this subring if and only if $\rho\omega = \omega \ \forall\rho \in \Delta^q$. We have $\rho\omega = \sum_{\tau\in\Delta} a_\tau \cdot \rho\tau\zeta_r$. Let's call $\delta = \rho\tau$, then we have $\rho\omega = \sum_{\delta\in\Delta} a_{\delta\rho^{-1}} \cdot \delta\zeta_r$. Since both $\delta\zeta_r$ and $\tau\zeta_r$, with $\tau, \delta \in \Delta$, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$, we have $\omega = \rho\omega$ if and only if $a_{\delta\rho^{-1}} = a_\delta$ which is the same as $a_\tau = a_{\tau\rho}$ for all $\tau \in \Delta, \rho \in \Delta^q$.

Note that if $\tau_1, \tau_2 \in \Delta$ and $\tau_1\Delta^q = \tau_2\Delta^q$ then $a_{\tau_1} = a_{\tau_2}$.

We know that $[\Delta : \Delta^q] = \{\tau_1\Delta^q, \tau_2\Delta^q, \ldots, \tau_q\Delta^q\}$ which means that $\forall\, \tau \in \Delta, \exists!\, i\ \exists!\, \rho$ such that $\tau = \tau_i\rho$. So we have

$$\omega = \sum_{\tau\in\Delta} a_\tau \cdot \tau\zeta_r = \sum_{i=1}^{q} \sum_{\tau\in\tau_i\Delta^q} a_\tau \cdot \tau\zeta_r = \sum_{i=1}^{q} \sum_{\rho\in\Delta^q} a_{\tau_i\rho} \cdot \tau_i\rho\zeta_r = \sum_{i=1}^{q} a_{\tau_i} \sum_{\rho\in\Delta^q} \tau_i\rho\zeta_r$$
$$= \sum_{i=1}^{q} a_{\tau_i} \cdot \tau_i \left(\sum_{\rho\in\Delta^q} \rho\zeta_r \right)$$

If we put $\eta_{r,q} = \sum_{\rho\in\Delta^q} \rho\zeta_r$, then $\sum_{i=1}^{q} a_{\tau_i} \cdot \tau_i(\eta_{r,q}) = 0$ means $\omega = 0$, but this implies that all the coefficients are equal to 0, since the elements $\tau\zeta_r$ form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ over $\mathbb{Z}/n\mathbb{Z}$. Therefore, the elements $\tau\eta_{r,q}$, with τ ranging over a set of coset representatives for Δ modulo Δ^q, form a basis for $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}$ over $(\mathbb{Z}/n\mathbb{Z})$; in particular we have $\#(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q} = n^q$.

Definition 4.3.3. *The elements $\tau\eta_{r,q}$ are called Gaussian periods of degree q and conductor r.*

We have, for example, $\eta_{r,r-1} = \eta_r$ and $\eta_{r,1} = -1$. Let's write

$$f_{r,q} = \prod_{\tau\Delta^q\in\Delta/\Delta^q} (y - \tau\eta_{r,q}).$$

This is a monic polynomial in y of degree q with $f_{r,q}(\eta_{r,q}) = 0$. Its coefficients, which belong to $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$, are invariant under all $\rho \in \Delta$, so they belong to $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^1} = (\mathbb{Z}/n\mathbb{Z}) \cdot \eta_{r,1} = \mathbb{Z}/n\mathbb{Z}$. Thus, we have $f_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[y]$.

Proposition 4.3.1. *Let $n \in \mathbb{Z}, n > 1$, let r be a prime number not dividing n, and let q be a divisor of $r-1$ with the property that the element $(n^{(r-1)/q} \bmod r)$ of $\mathbb{F}_r^*$ has order q.*
Let the notation $\zeta_r, \sigma_a, \Delta, \eta_{r,q}, f_{r,q}$ be as just defined. Then we have:

(a) *if n is prime, then in the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ we have $\eta_{r,q}^n = \sigma_n \eta_{r,q}$;*

(b) *if in the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ we have $\eta_{r,q}^n = \sigma_n \eta_{r,q}$, then $\big((\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}, \eta_{r,q}\big)$ is a pseudofield of characteristic n and degree q, with characteristic polynomial $f_{r,q}$.*

Proof. To prove **(a)**, let's suppose that n is prime. Then the map from $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ sending each β to β^n is a ring homomorphism, and since it agrees with σ_n on ζ_r it coincides with σ_n on all of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. This implies **(a)**.
To prove **(b)**, let the group homomorphism $\gamma : \mathbb{F}_r^* \to \mathbb{F}_r^*$ sending each x to $x^{(r-1)/q}$. Then $\ker(\gamma) = \mathbb{F}_r^{*^q}$ which is a subgroup of index q of $\mathbb{F}_r^*$, and therefore, we have $\#\ker(\gamma) = (r-1)/q$. So we have $\#(\mathbb{F}_r^*/\mathbb{F}_r^{*^q}) = q$ and this group is cyclic since it is the quotient of two cyclic groups. We know, by Fundamental Theorem of Homomorphism, that $(\mathbb{F}_r^*/\mathbb{F}_r^{*^q}) \simeq \Im(\gamma)$ which is the unique subgroup of $\mathbb{F}_r^*$ of order q. Moreover, we have $\gamma((n \bmod r)\mathbb{F}_r^{*^q}) = n^{(r-1)/q} \bmod r$ which, therefore, belongs to $\Im(\gamma)$ and, by hypothesis, has order q. Thus, $(\mathbb{F}_r^*/\mathbb{F}_r^{*^q})$ is generated by $(n \bmod r)\mathbb{F}_r^{*^q}$. Let's now consider the isomorphism $\theta : \mathbb{F}_r^* \to \Delta$ which maps $n \pmod r$ to σ_n. We have just seen that $(\mathbb{F}_r^*/\mathbb{F}_r^{*^q}) =< (n \bmod r)\mathbb{F}_r^{*^q} >$, so we can deduce, by considering the images of θ, that Δ/Δ^q is generated by $\sigma_n\Delta^q$.
Let's write, for brevity, $A = (\mathbb{Z}/n\mathbb{Z})[\zeta_r]^{\Delta^q}$ and let's define the ring homomorphism $\phi : (\mathbb{Z}/n\mathbb{Z})[y] \to A$ by $\phi(g) = g(\eta_{r,q})$. The image of ϕ is the subring of A generated by $\eta_{r,q}$. Let's denote S this subring. From $\sigma_n\eta_{r,q} = \eta_{r,q}^n$ it follows that S is mapped to itself by σ_n. Since A is invariant for Δ^q, all the elements of Δ^q act as the identity on A, and since $\sigma_n\Delta^q$ generates Δ/Δ^q, then S is mapped to itself by *all* $\tau \in \Delta$. Hence, in addition to $\eta_{r,q}$ it contains all $\tau\eta_{r,q}$ which is a basis for A, so we have $S = A$; in other words, ϕ is surjective. We know that $f_{r,q}(\eta_{r,q}) = 0$; this implies that the kernel of ϕ contains the $(\mathbb{Z}/n\mathbb{Z})[y]$-ideal generated by $f_{r,q}$.
Let's note that, since $\#A = n^q$, then $\ker(\phi)$ has index n^q in $(\mathbb{Z}/n\mathbb{Z})[y]$ because $(\mathbb{Z}/n\mathbb{Z})[y]/\ker(\phi) \simeq A$ by Fundamental Theorem of Homomorphism that can be applied for the surjectivity of ϕ; besides we know that $\#((\mathbb{Z}/n\mathbb{Z})[y]/(h(y))) = n^{\deg(h)}$ and, since $\deg(f_{r,q}) = q$, we have $\#((\mathbb{Z}/n\mathbb{Z})[y]/(f_{r,q}))) = n^q$. Thus we can deduce that both $\ker(\phi)$ and the $(\mathbb{Z}/n\mathbb{Z})[y]$-ideal generated by $f_{r,q}$ have index n^q in $(\mathbb{Z}/n\mathbb{Z})[y]$, so they must be equal. Thus, ϕ induces a ring isomorphism $(\mathbb{Z}/n\mathbb{Z})[y] \cong A$.

We prove that $A, \alpha = \eta_{r,q}, n, d = q$ and σ equal to the restriction of σ_n to A, satisfy conditions (4.1)-(4.5).

Conditions (4.1), (4.2) and (4.3) are clearly satisfied. Since A is invariant for Δ^q, we have that $\rho\alpha = \alpha$ for all $\alpha \in A$, $\rho \in \Delta^q$. From $\sigma_n^q \in \Delta^q$ we know that we can choose $\rho = \sigma_n^q$, from which we deduce condition (4.4).

We are now going to prove condition (4.5). Since $\sigma_n \Delta^q$ generates the group Δ/Δ^q of order q, we may rewrite the definition of $f_{r,q}$ as

$$f_{r,q} = \prod_{i=0}^{q-1} (y - \eta_{r,q}) \,.$$

Therefore, calculating the derivative $f'_{r,q} = \mathrm{d}f_{r,q}/\mathrm{d}y$, we have

$$f'_{r,q} = \sum_{j=0}^{q-1} \left(\prod_{\substack{i=0 \\ i \neq j}}^{q-1} (y - \sigma^i \eta_{r,q}) \right)$$

and, separating the case $j = 0$, we have

$$f'_{r,q} = \prod_{i=1}^{q-1} (y - \sigma^i \eta_{r,q}) + \sum_{j=1}^{q-1} \left(\prod_{\substack{i=0 \\ i \neq j}}^{q-1} (y - \sigma^i \eta_{r,q}) \right) .$$

The second term of this addition is a sum such that, in the case $f'_{r,q}(\eta_{r,q})$, any addend is a product in which the factor with $i = 0$ is equal to 0 and, therefore, this sum is equal to 0. Thus,

$$f'_{r,q}(\eta_{r,q}) = \prod_{i=1}^{q-1} (\eta_{r,q} - \sigma^i \eta_{r,q}).$$

So to prove (4.5) it will suffice to prove $f'_{r,q}(\eta_{r,q}) \in A^*$.

Let p be a prime number dividing n.

Taking the isomorphism $(\mathbb{Z}/n\mathbb{Z})[y]/(f_{r,q}) \cong A \subseteq (\mathbb{Z}/n\mathbb{Z})[x]/(\frac{x^r-1}{x-1})$ modulo p, we see that the ring $\mathbb{F}_p[y]/(f)$, where $f = f_{r,q} \pmod p \in \mathbb{F}_p[x]$, is isomorphic to a subring of $\mathbb{F}_p[x]/(g)$, where $g = \sum_{i=0}^{r-1} x^i$. Since g divides $x^r - 1$, where r is a prime number different from p, we have that g is squarefree in the ring $\mathbb{F}_p[x]$ and, therefore, $\gcd(g, \mathrm{d}g/\mathrm{d}x) = 1$ in the ring $\mathbb{F}_p[x]$. From Lemma 4.3.1, stated and proved below, it follows that we have $\gcd(f, \mathrm{d}f/\mathrm{d}y) = 1$ in the ring $\mathbb{F}_p[y]$. Thus, there are $u, v \in \mathbb{F}_p[y]$ with $uf + v\mathrm{d}f/\mathrm{d}y = 1$. Lifting u, v to $(\mathbb{Z}/n\mathbb{Z})[y]$, we obtain $u_p, v_p, w_p \in (\mathbb{Z}/n\mathbb{Z})[y]$ such that $u_p f_{r,q} + v_p f'_{r,q} = 1 + p w_p$. Since they are polynomials in $(\mathbb{Z}/n\mathbb{Z})[y]$ we can apply ϕ to u_p, v_p, w_p; so we have $\phi(u_p f_{r,q} + v_p f'_{r,q}) = \phi(1 + p w_p)$ which is $\phi(u_p f_{r,q}) + \phi(v_p f'_{r,q}) - \phi(p w_p) = 1$. We know that $\phi(h) = h(\eta_{r,p})$ for all $h \in (\mathbb{Z}/n\mathbb{Z})[y]$ and, therefore, we have $u_p(\eta_{r,q}) \cdot f_{r,q}(\eta_{r,q}) + v_p(\eta_{r,q}) \cdot$

$f'_{r,q}(\eta_{r,q}) - p \cdot w_p(\eta_{r,q}) = 1$, but we also know that $f_{r,q}(\eta_{r,q}) = 0$. So we get, for each prime number p dividing n, an identity in A of the form $v_p(\eta_{r,q}) \cdot f'_{r,q}(\eta_{r,q}) - p \cdot w_p(\eta_{r,q}) = 1$. Take the product over p, repeating the pth identity just as many times as p occurs in n. On the right, we get 1. On the left, the only term that does not have a factor $f'_{r,q}(\eta_{r,q})$ is divisible by n and is therefore 0. Hence, 1 is divisible by $f'_{r,q}$ in A, so that the latter element is a unit, as required. The formula we gave for $f_{r,q}$ shows that it is indeed the characteristic polynomial for the pseudofield. ■

Lemma 4.3.1. *Let p be a prime number, and let $f, g \in \mathbb{F}_p[x]$ be non-zero polynomials for which the ring $\mathbb{F}_p[x]/(f)$ is isomorphic to a subring of $\mathbb{F}_p[x]/(g)$. Suppose also $\gcd(g, \mathrm{d}g/\mathrm{d}x) = 1$. Then we have $\gcd(f, \mathrm{d}f/\mathrm{d}x) = 1$.*

Proof. A non-zero polynomial $h \in \mathbb{F}_p[x]$ satisfies $\gcd(h, \mathrm{d}h/\mathrm{d}x) = 1$ if and only if h is squarefree in the ring $\mathbb{F}_p[x]$, and if and only if there is no non-zero nilpotent element in the ring $\mathbb{F}_p[x]/(h)$. Thus, $\gcd(g, \mathrm{d}g/\mathrm{d}x) = 1$ implies that there is no non-zero nilpotent element in $\mathbb{F}_p[x]/(g)$. From the trivial observation that if a ring has no non-zero nilpotent element, then the same is true for a subring, it follows that the subring of $\mathbb{F}_p[x]/(g)$ that is isomorphic to $\mathbb{F}_p[x]/(f)$ has no non-zero nilpotent element and, therefore, $\mathbb{F}_p[x]/(f)$ neither. Thus, $\gcd(f, \mathrm{d}f/\mathrm{d}x) = 1$. ■

4.3.2 The algorithm

Algorithm A. We next describe an algorithm that, given an integer $n > 1$, which may or may not be prime, and a period system P for n satisfying $n > \prod_{(r,q)\in P} q$, attempts to construct a pseudofield of characteristic n and degree $\prod_{(r,q)\in P} q$.

Step 1. For all $(r, q) \in P$ in succession, do the following. Compute $\eta_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ as well as all of its conjugates $\tau\eta_{r,q}$, and form the product of the q polynomials $y - \tau\eta_{r,q}$ in the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r][y]$; the result is $f_{r,q}$, which has coefficients in the subring $\mathbb{Z}/n\mathbb{Z}$ of $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$. If n is not known to be prime, compute by an nth powering in the ring $(\mathbb{Z}/n\mathbb{Z})[y]/(f_{r,q})$ the unique polynomial $g_{r,q} \in (\mathbb{Z}/n\mathbb{Z})[y]$ satisfying $y^n \equiv g_{r,q}$ (mod $f_{r,q}$) and $\deg()g_{r,q} < q$, and test whether in the ring $(\mathbb{Z}/n\mathbb{Z})[\zeta_r]$ we have $g_{r,q}(\eta_{r,q}) = \sigma_n\eta_{r,q}$; if this test fails, declare n composite and halt.

Step 2. [If the algorithm arrives at this point then, as we are going to prove below, for each $(r, q) \in P$ the pair $(n, f_{r,q})$ specifies a pseudofield.] Applying the algorithm of A.1.5 at most $\#P - 1$ times, either find a prime factor of n that is at most $\prod_{(r,q)\in P} q$, or construct the repeated tensor product of the $\#P$ pseudofields specified by the pairs $(n, f_{r,q})$ for $(r, q) \in P$. In the former case, declare n composite and halt, and in the latter case return the tensor product computed by the algorithm and halt. This completes the description of Algorithm A.

Proposition 4.3.2. *Algorithm A, on input n, P satisfying $n > \prod_{(r,q)\in P} q$, runs in time*

$$\tilde{\vartheta}\left(\left(\prod_{(r,q)\in P} q + \sum_{(r,q)\in P} qr\right)\log n\right) \quad \text{or} \quad \tilde{\vartheta}\left(\left(\prod_{(r,q)\in P} q + \sum_{r,q\in P} q(r+\log n)\right)\log n\right)$$

according as n is or is not known to be prime, and either correctly declares n composite or constructs a pseudofield of characteristic n and degree $\prod_{(r,q)\in P} q$.

Proof. We first prove the correctness of the algorithm. By $f_{r,q}(\eta_{r,q}) = 0$, the congruence $y^n \equiv g_{r,q} \pmod{f_{r,q}}$ in Step 1 implies $g_{r,q}(\eta_{r,q}) = \eta_{r,q}^n$. Thus, by Proposition 4.3.1(a), the condition $g_{r,q}(\eta_{r,q}) = \sigma_n \eta_{r,q}$ is necessary for n to be prime, and the algorithm is correct if it halts in Step 1. If it passes Step 1, then by Proposition 4.3.1(b) there is, for each $(r,q) \in P$, a pseudofield od characteristic n with characteristic polynomial $f_{r,q}$. Hence by A.1.5 the algorithm constructs the desired tensor product, or it finds a prime factor of n that is at most $\prod_{(r,q)\in P} q$; in the latter case, n is composite because $n > \prod_{(r,q)\in P} q$. This proves the correctness of the algorithm.
The run time of Step 1 is dominated by the computation of the polynomials $f_{r,q}$ and, if n is not known to be prime, the polynomials $g_{r,q}$ and their values at $\eta_{r,q}$. The computation of $f_{r,q}$, if done by means of ALGORITHM 10.3 from [15] , runs in time $\tilde{\vartheta}(qr\log n)$. The computation of $g_{r,q}$ involves $\vartheta(\log n)$ multiplications in the ring $(\mathbb{Z}/n\mathbb{Z})[y]/(f_{r,q})$ and can therefore be performed in time $\tilde{\vartheta}(q\cdot(\log n)^2)$. The computation of $g_{r,q}(\eta_{r,q})$ runs in time $\tilde{\vartheta}(qr\log n)$. By A.1.5, Step 2 runs in time $\tilde{\vartheta}(\log n \cdot \prod_{(r,q)\in P} q)$. ■

We can now state the following result which is an immediate corollary of this proposition:

Proposition 4.3.3. *There is an algorithm that, given an integer n with $n > 1$ and a period system P for n satisfying $n > \prod_{(r,q)\in P} q$, either correctly declares n composite or constructs a pseudofield of characteristic n and degree $\prod_{(r,q)\in P} q$, and that runs in time*

$$\tilde{\vartheta}\left(\left(\prod_{(r,q)\in P} q + \sum_{r,q\in P} q(r+\log n)\right)\log n\right).$$

In addition, if n is prime, then it is not declared composite, so that the algorithm returns a pseudofiled; whence by Proposition 4.2.3, its characteristic polynomial is irreducible in $\mathbb{F}[x]$. This leads to the following resutl:

Proposition 4.3.4. *There is an algorithm that, given a prime number p and a period system P for p satisfying $p > \prod_{(r,q)\in P} q$, constructs a monic irreducible polynomial $f \in \mathbb{F}_p[x]$ with $\deg f = \prod_{(r,p)\in P} q$, and taht runs in time*

$$\tilde{\vartheta}\left(\left(\prod_{(r,q)\in P} q + \sum_{(r,q)\in P} qr\right)\log p\right).$$

4.4 The continuous Frobenius problem

The famous Frobenius postage problem asks for the largest number which is not in the additive semigroup generated by a set of coprime positive integers. We are now going to see a new result of Bleichenbacher [17] that might be considered a continuous version of this problem.

Theorem 4.4.1. *Suppose S is an open subset of the positive reals that is closed under addition, and such that $1 \notin S$. Then for any number $t \in (0,1]$, we have $\int_{S\cap(0,t)} \mathrm{d}x/x \leq t$.*

Proof. If S is an open subset of the positive reals, let

$$M(S) = \int_S \frac{\mathrm{d}x}{x}.$$

Let S be as in the hypothesis of the proposition, and first suppose that $S_t := S \cap (0,t)$ is a finite union of open intervals; that is, for some positive integer n,

$$S_t = \bigcup_{i=1}^{n} (a_i, b_i),$$

where

$$t \geq b_1 \geq a_1 \geq \cdots \geq b_n \geq a_n \geq 0. \tag{4.13}$$

Let $\mathbf{a}= (a_1, \ldots, a_n)$, $\mathbf{b}= (b_1, \ldots, b_n)$. We claim that the condition that 1 is not in the additive semigroup generated by S_t is equivalent to the assertion: for each vector $\mathbf{h}\in (\mathbb{N}_{\geq 0})^n$,

$$\mathbf{h}\cdot\mathbf{b} > 1 \text{ implies } \mathbf{h}\cdot\mathbf{a} \geq 1. \tag{4.14}$$

Let's suppose that $\mathbf{h}\cdot\mathbf{b} > 1$ implies $\mathbf{h}\cdot\mathbf{a} \geq 1$.
If $x \in< S_t >$ then $x = \sum_{i=1}^n c_i s_i$ where, for all $i = 1, \ldots, n$, $a_i < s_i < b_i$ and $c_i \in N$, that means $\sum_{i=1}^n c_i a_i < x < \sum_{i=1}^n c_i b_i$. Let's now suppose $1 \in< S_t >$, then we have $\sum_{i=1}^n a_i c_i < 1 < \sum_{i=1}^n b_i c_i$; so choosing $\mathbf{h}= (c_1, \ldots, c_n)$ we obtain $\mathbf{h}\cdot\mathbf{a} < 1 < \mathbf{h}\cdot\mathbf{b}$ which is a contradiction.
Now let's suppose that $1 \notin< S_t >$.
Let $\bar{a}_\epsilon = (a_1 + \epsilon, \ldots, a_n + \epsilon)$ and $\bar{b}_\epsilon = (b_1 - \epsilon, \ldots, b_n - \epsilon)$ and $f : \mathbb{R}^n \to \mathbb{R}$ which maps a vector $\mathbf{x}= (x_1, \ldots, x_n)$ to $\sum_{i=1}^n h_i x_i = \mathbf{h}\cdot\mathbf{x}$. This function

is continuous, so we have that if $f(a) < 1 < f(b)$ then there exists ϵ small enough for which $f(a_\epsilon) < 1 < f(b_\epsilon)$. Now let $c_\epsilon = [a_1+\epsilon, b_1-\epsilon] \times \ldots \times [a_n+\epsilon, b_n-\epsilon]$ which is convex and let's consider the restriction of f to c_ϵ which is continuous. By an important analytical theorem, we know that $f(a_\epsilon) < 1 < f(b_\epsilon)$ implies that there exists $s \in c_\epsilon$ such that $f(s) = \sum_{i=1}^n h_i s_i = 1$ that is $1 \in< S_t >$ which is a contradiction.
We have so proved that $1 \notin< S_t > \Leftrightarrow \mathbf{h} \cdot \mathbf{b} > 1$ implies $\mathbf{h} \cdot \mathbf{b} \geq 1$ as required. So it is never the case that $\mathbf{h} \cdot \mathbf{a} < 1 < \mathbf{h} \cdot \mathbf{b}$.
Suppose now that we fix the vector $\mathbf{b}$ and assume that

$$t \geq b_1 > b_2 > \cdots > b_n > 0. \tag{4.15}$$

Consider the set $\mathbf{A}_b$ of vectors $\mathbf{a} \in (\mathbb{R}_{>0})^n$ for which (4.13) and (4.14) hold. If we have that there exists i for which $1/n \in (a_i, b_i)$ with $n \in \mathbb{N}$ then we have $a_i < \frac{1}{n} < b_i$ that means $n \cdot a_i < 1 < n \cdot b_i$; let's choose $\mathbf{h}= n\cdot\, \mathbf{e}_i$ where $\mathbf{e}_i$ is the i-th standard basis vector in $\mathbb{R}^n$, then we have $\mathbf{h} \cdot \mathbf{a} < 1 < \mathbf{h} \cdot \mathbf{b}$ which is impossible. So no interval (a_i, b_i) with $\mathbf{a} \in \mathbf{A}_b$ can contain the reciprocal of an integer; therefore, we have each $a_i \geq b_i/2$. For any vector $\mathbf{a}$ with each $a_i \geq b_i/2$, if $\mathbf{h} \cdot \mathbf{b} \geq 2$, then $\mathbf{h} \cdot \mathbf{a} \geq 1$ Thus, the set $\mathbf{A}_b$ is defined by the conditions $b_i \geq a_i \geq b_i/2$ and (4.14) for the finite set of integer vectors $\mathbf{h}$ with $1 < \mathbf{h} \cdot \mathbf{b} < 2$. We conclude that $\mathbf{A}_b$ is a compact subset of $(\mathbb{R}_{>0})^n$, so there is a choice of the vector $\mathbf{a}$ which maximizes $M(S_t)$ for the given vector $\mathbf{b}$. Call this maximum value $\mathbf{M}_b$ and assume that $\mathbf{a}$ is fixed at a choice which produces this maximum.
Since empty intervals are allowed, that is, it is possible that $a_i = b_i$, it is clear that if some coordinates of $\mathbf{b}$ are deleted to form a shorter vector $\mathbf{b}'$ then $\mathbf{M}_{b'} \leq \mathbf{M}_b$. Thus, by possibly replacing $\mathbf{b}$ with a shorter vector, we may assume that each $a_i < b_i$. We are now going to see that we may assume that each $a_{i-1} > b_i$ for $2 \leq i \leq n$. Let's suppose some $a_{i-1} = b_i$. We may then consolidate the two intervals (a_i, b_i),(a_{i-1}, b_{i-1}) into one interval (a_i, b_{i-1}). Indeed, if not, then now 1 is representable by a sum of members of $S_t \cup b_i$. This sum must involve b_i since $1 \notin < S_t >$. Let the coefficient of b_i be a positive integral m. Now, if $m = 1$, then we have at least another number in the sum since $b_i < 1$. Let's replace b_i in the sum with $b_i + \epsilon$, for a suitable small $\epsilon > 0$, and then replace another member $x \in S_t$ of the sum with $x - \epsilon$. If ϵ is small enough, both $b_i + \epsilon$ and $x - \epsilon$ belong to S_t, and we have represented 1 as a sum of members of S_t, which is impossible. So we have $m \geq 2$. In this case, however, we can replace $m \cdot b_i$ with the sum $(m-1) \cdot (b_i + \frac{\epsilon}{m-1}) + (b_i - \epsilon)$ whose members, for a suitable ϵ, belong to S_t. So we can represent 1 as a sum of members of S_t which is impossible as well. Therefore, the consolidation of the two abutting intervals continues to enjoy the property that 1 is not in the additive semigroup generated by the intervals.
Hence, we may assume that $a_{i-1} > b_i$ for $2 \leq i \leq n$. Thus, we may assume

that the vector $\mathbf{a}$ satisfies

$$t \geq b_1 > a_1 > \cdots > b_n > a_n > 0. \tag{4.16}$$

$$\begin{aligned} H_0 &= \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} < 1\}, \\ H_1 &= \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} = 1\}, \\ H_2 &= \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} > 1\}. \end{aligned}$$

Since each $a_i > 0$, it follows that H_0, H_1 are finite sets.

We are now going to show that H_1 is nonempty. Suppose not. Let $\mathbf{u}= (1, 1, \ldots, 1) \in (\mathbb{N}_{\geq 0})^n$. We claim that if $\epsilon > 0$ is small enough, then the pair ($\mathbf{a}-\epsilon\mathbf{u}$, $\mathbf{b}$) still satisfies (4.14) and (4.16). This would create a choice for S_t with strictly larger $M(S_t)$, a contradiction, thus showing that H_1 is nonempty.

It is clear that we may choose $\epsilon > 0$ small enough so as to preserve the condition (4.16). For $\mathbf{h}\in H_0$ we have $\mathbf{h} \cdot \mathbf{b} \leq 1$, so that the vectors in H_0 do not pose a problem for condition (4.14), and, since H_1 is assumed empty, H_1 also does not pose a problem. There are only finitely many $\mathbf{h}\in H_2$ with $\mathbf{h} \cdot \mathbf{a} \leq 2$. We may choose $\epsilon > 0$ small enough so that $\mathbf{h} \cdot (\mathbf{a} - \epsilon\mathbf{u}) \geq 1$ for all such $\mathbf{h}$. Finally, if $\mathbf{h} \cdot \mathbf{a} > 2$, then if we choose $\epsilon < a_n/2$ we have $\mathbf{h} \cdot (\mathbf{a} - \epsilon\mathbf{u}) = \sum_{i=1}^{n} h_i \cdot (a_i - a_n/2)$ where each member of the sum is greater than $h_i \cdot a_i/2$ from which we can deduce that $\mathbf{h} \cdot (\mathbf{a} - \epsilon\mathbf{u}) > \frac{1}{2}\mathbf{h} \cdot \mathbf{a} > 1$. Hence, as claimed, if $\epsilon > 0$ is small enough, the pair ($\mathbf{a} - \epsilon\mathbf{u}$, $\mathbf{b}$) still satisfies (4.14) and (4.16), providing a contradiction which shows that H_1 is nonempty.

Let $\mathbf{h}\in H_1$. For notational convenience, let $a_{n+1} = b_{n+1} = 0$. And let $\mathbf{e}_k$ be the k-th standard basis vector in $\mathbb{R}^n$. For $k = 1, \ldots, n$, since $\mathbf{h} \cdot \mathbf{a} = 1$ and $a_k > a_{k+1}$, we have

$$\mathbf{h} \cdot \mathbf{a} - a_k + a_{k+1} < 1.$$

Suppose that $h_k > 0$. Let $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k + \mathbf{e}_{k+1}$ in the case that $k < n$, and let $\mathbf{h}' = \mathbf{h} - \mathbf{e}_k$ in the case that $k = n$. Note that $\mathbf{h}' \cdot \mathbf{a} = \mathbf{h} \cdot \mathbf{a} - a_k + a_{k+1} < 1$ so we have $\mathbf{h}' \in H_0$. Hence, from (4.14), we have that $\mathbf{h}' \cdot \mathbf{b} \leq 1$. That is,

$$\mathbf{h} \cdot \mathbf{b} - b_k + b_{k+1} \leq 1.$$

Using that $\mathbf{h} \in H_1$, we get that

$$\mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) = \mathbf{h} \cdot \mathbf{b} - 1 \leq b_k - b_{k+1}$$

Thus, we have

$$h_k\mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \leq h_k(b_k - b_{k+1}) \tag{4.17}$$

an equality that clearly continues to hold even if $h_k = 0$.

Let $\mathbf{v}\in \mathbb{R}^n$ and let x such that $b_{i-1} < a_i + xv_i < b_i \,\forall i$ and then let

$$f_{\mathbf{v}}(x) = M \quad \left. \bigcup_{i=1}^{n}(a_i + xv_i, b_i)\right) .$$

Note that, using a famous analytic theorem, we have

$$f'_{\mathbf{V}}(x) = \sum_{i=1}^{n} -\frac{1}{a_i + xv_i} \cdot v_i$$

from which we see that $f'_{\mathbf{V}}(0) = -\mathbf{v} \cdot m(\mathbf{a})$ where $m(\mathbf{a})= (1/a_1, \ldots, 1/a_n)$. Note too that by the maximality of $\mathbf{a}$, if the vector $\mathbf{a} + x\mathbf{v}$ satisfies (4.14) and (4.16) for all x in some interval $[0, \epsilon)$ with $\epsilon > 0$, then $f'_{\mathbf{V}}(0) \leq 0$, that is, $\mathbf{v}{\cdot}m(\mathbf{a}){\geq} 0$. We now show that this event occurs whenever $\mathbf{h} \cdot \mathbf{v} \geq 0$ for all $\mathbf{h}{\in} H_1$. Suppose that this condition holds. Let's now suppose that we have $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) < 1 < \mathbf{h}' \cdot \mathbf{b}$ for some $\mathbf{h}' \in (\mathbb{N}_{\geq 0})^n$ and let's see that this leads us to a contradiction. Since $\mathbf{h} \cdot \mathbf{b} \leq 1$ for all $\mathbf{h} \in H_0$, we have $\mathbf{h}' \notin H_0$. If $\mathbf{h}' \in H_1$, then $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) = 1 + x\mathbf{h}' \cdot \mathbf{v}\ \forall x \geq 0$, where $\mathbf{h}' \cdot \mathbf{v}$ is greater than 0 by hypothesis, and $x \geq 0$ by construction, so we have $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) \geq 1$ which is a contradiction. Thus, we have $\mathbf{h}' \notin H_1$. If $\mathbf{h} \in H_2$, since $\mathbf{h} \cdot \mathbf{a} > 1$, we may choose $\epsilon > 0$ small enough, such that, for all $\mathbf{h} \in H_2$ and all $x \in [0, \epsilon)$, we have $\mathbf{h} \cdot (\mathbf{a} + x\mathbf{v}) > 1$ which is a contradiction. Therefore, $\mathbf{h}' \notin H_2$. It follows that for $\epsilon > 0$ small enough, if $\mathbf{h} \cdot \mathbf{v} \geq 0$ for all $\mathbf{h} \in H_1$, then $\mathbf{a} + x\mathbf{v}$ satisfies (4.14) and (4.16) for $0 \leq x \leq \epsilon$, and so $\mathbf{v} \cdot m(\mathbf{a}) \geq 0$.
We now apply a result of Farkas

Lemma 4.4.1. (J. Farkas) *Suppose A is an $n \times u$ real matrix and $\mathbf{m} \in \mathbb{R}^n$. Then the inequalities $A\mathbf{v} \geq 0$, $\mathbf{m} \cdot \mathbf{v} < 0$ are unsolvable for a vector $\mathbf{v} \in \mathbb{R}^n$ if and only if there is a vector $\mathbf{p} \in \mathbb{R}^u$ with $\mathbf{p} \geq 0$ and $\mathbf{p}^T A = \mathbf{m}$.*

(Saying that a vector is ≥ 0, we mean that each entry of it is ≥ 0). We apply this lemma to the matrix A whose rows are the u vectors in H_1 and to the vector $\mathbf{m} = m(\mathbf{a})$. Now,

$$A\mathbf{v} = \begin{pmatrix} h_{1_1} & \cdots & h_{1_n} \\ h_{2_1} & \cdots & h_{2_n} \\ \vdots & \ddots & \vdots \\ h_{u_1} & \cdots & h_{u_n} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} h_{1_1}v_1 + \ldots + h_{1_n}v_n \\ \vdots \\ h_{u_1}v_1 + \ldots + h_{u_n}v_n \end{pmatrix} = \begin{pmatrix} \mathbf{h}_1 \cdot \mathbf{v} \\ \mathbf{h}_2 \cdot \mathbf{v} \\ \vdots \\ \mathbf{h}_u \cdot \mathbf{v} \end{pmatrix}$$

Where h_{j_i} is the i-th entry of $\mathbf{h}_j$ and $\mathbf{h}_j \in H_1$. Therefore, $A\mathbf{v} \geq 0$ if and only if $\mathbf{h}_j \cdot v \geq 0$ for all $\mathbf{h}_j \in H_1$, which, as we have just seen, implies $\mathbf{m} \cdot \mathbf{v} \geq 0$. Thus, the lemma implies that there is a vector $\mathbf{p} \in \mathbb{R}^u$ with $\mathbf{p} \geq 0$ and $\mathbf{p}^T A = \mathbf{m}$. Say $\mathbf{p} = (p_1, \ldots, p_u)$ and $H_1 = \{\mathbf{h}_1, \ldots, \mathbf{h}_u\}$. We have

$$(\mathbf{p}^T A)_i = \sum_{j=1}^{n} p_j h_{j_i} = 1/a_i = \mathbf{m}_i \qquad \text{for } 1 \leq i \leq n.$$

Take 4.17 applied to $\mathbf{h}_j$, multiply it by p_j, and sum over j. For $k = 1, \ldots, n$, we have,

$$\sum_{j=1}^{u} p_j h_{j_k} \sum_{i=1}^{n} h_{j_i}(b_i - a_i) \leq \sum_{j=1}^{u} p_j h_{j_k}(b_k - b_{k+1}) = (1/a_k)(b_k - b_{k+1}).$$

Multiplying corresponding inequalities by a_k and summing over k, we get

$$\begin{aligned}\sum_{k=1}^{n} a_k \sum_{j=1}^{u} p_j h_{j_k} \sum_{i=1}^{n} h_{j_i}(b_i - a_i) &\leq \sum_{k=1}^{n}(b_k - b_{k+1}) \\ &= b_1 - b_{n+1} \\ &= b_1 \qquad \text{since} \quad b_{n+1} = 0\end{aligned} \tag{4.18}$$

The left side of (4.18) is

$$\begin{aligned}\sum_{j=1}^{u} p_j \sum_{k=1}^{n} a_k h_{j_k} \sum_{i=1}^{n} h_{j_i}(b_i - a_i) &= \mathbf{a} \cdot \mathbf{h}_j \sum_{j=1}^{u} p_j \sum_{i=1}^{n} h_{j_i}(b_i - a_i) \\ &= \sum_{j=1}^{u} p_j \sum_{i=1}^{n} h_{j_i}(b_i - a_i) \\ &= \sum_{i=1}^{n}(b_i - a_i) \sum_{j=1}^{u} p_j h_{j_i} = \sum_{i=1}^{n}(b_i - a_i)/a_i.\end{aligned}$$

Thus, (4.18) implies that

$$\sum_{i=1}^{n}((b_i/a_i) - 1) \leq b_1 \tag{4.19}$$

However,

$$M((a_i, b_i)) = \int_{a_i}^{b_i} \frac{\mathrm{d}x}{x} = \log(b_i/a_i) < (b_i/a_i) - 1$$

Hence, by (4.19),

$$\mathbf{M}_b = \sum_{i=1}^{n} \log(b_i/a_i) < \sum_{i=1}^{n}(b_i/a_i) - 1 < b_1 \leq t$$

Since $\mathbf{M}_b < t$ for each choice of $\mathbf{b}$ satisfying (4.15), it remains to handle the case of S_t being the union of infinitely many disjoint open intervals. If $S_t(n)$ is the union of n of these disjoint open intervals with $S_t(n) \subset S_t(n+1)$ and $\bigcup S_t(n) = S_t$, we have $M(S_t(n)) < t$ for each n, and $M(S_t) = \lim_{n\to\infty} M(S_t(n)) \leq t$. This concludes the proof of the theorem. ■

4.5 The existence of period systems

The following two sections develop some tools from analytic number theory which will be used to prove our final auxiliary result: the existence of period systems.

In Section 4.5.1 we review some results concerning the distribution of primes

in residue classes, and give a somewhat weaker, but effective version of the Bombieri-Vinogradov inequality. (See [5] for a similar result.) We also introduce our major tool, a theorem of Deshouillers and Iwaniec [6]. While weaker than Fouvry's theorem, this result is effective in principle.
In Section 4.5.2 we show that there are many primes r with certain constraints on the primes in $r-1$. For this we refer to a paper of Balog [7]. This paper uses the same theorem of Fouvry as in the case of the AKS algorithm, and also the Bombieri-Vinogradov theorem. To achieve effectively computable estimates, we use instead the Deshouillers-Iwaniec result and the effective Bombieri-Vinogradov inequality from Section 4.5.1.
We will only enunciate the results without dealing with the proofs.

4.5.1 The distribution of primes in residue classes

For a natural number q, an integer a coprime to q, and a real number x, let $\pi(x,q,a)$ denote the number of primes $p \leq x$ with $p \equiv a \pmod q$. Also, let

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \ \ p \text{ prime }, k \geq 1 \\ 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

the von Mangoldt's function.
Now let

$$(x,q,a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \Lambda(n), \qquad \theta(x,q,a) = \sum_{\substack{p \leq x, p \text{ prime} \\ p \equiv a \pmod q}} \log p.$$

Now let $\mathrm{li}(x) = \int_0^x \frac{1}{\ln y} \mathrm{d}y$. For a fixed $\epsilon > 0$, we have the asymptotic relations:

$$\pi(x,q,a) \sim \frac{\mathrm{li}(x)}{\varphi(q)} \quad \text{and} \quad (x,q,a) \sim \frac{x}{\varphi()q}$$

as $x \to \infty$, where error estimates may be explicity calculated. For q large we have either ineffective estimates or inequalities. In this section we record some effective inequalities for $\pi(x,q,a)$ that are valid in large ranges for q.

Lemma 4.5.1. [Brun-Titchmarsh inequality] *If $x > q$ we have*

$$\pi(x,q,a) \leq \frac{2x}{\varphi(q)\log(x/q)}.$$

This form of the lemma is due to Montgomery and Vaughan [8]. Note that the inequality gives an upper bound for $\pi(x,q,a)$ that is of the expected order of magnitude, namely $x/(\varphi(q)\log x)$, if $q < x^{1-\epsilon}$. When q is of order of magnitude x^α, the upper bound provided by the lemma is presumably too large by a factor $2/(1-\alpha)$.

Lemma 4.5.2. [effective Bombieri-Vinogradov inequality] *There are absolute, effectively computable positive numbers c_6, c_7 such that for all numbers $x \geq 3$, there is an integer set $S(x) \subset [(\log x)^{1/2} \exp((\log x)^{1/2})]$ of cardinality 0 or 1, such that for each number $Q \in [x^{1/3} \log x, x^{1/2}]$,*

$$\sum_{q \leq Q}{}' \max_{2 \leq y \leq x} \max_{\gcd(a,q)=1} \left| \quad (y, q, a) - \frac{y}{\varphi(q)} \right| \leq c_6 x^{1/2} Q (\log x)^5 + c_6 x \exp\left(-c_7 (\log x)^{1/2}\right),$$

where the dash indicates that if $S(x) = \{s_1\}$, then no q in the sum is divisible by s_1.

For the proof see [9].

Lemma 4.5.3. *With the same notation and hypothesis as in Lemma 4.5.2, we have*

$$\sum_{q \leq Q}{}' \max_{\gcd(a,q)=1} \left| \pi(x, q, a) - \frac{\mathrm{li}(x)}{\varphi(q)} \right| \leq c_{12} x^{1/2} Q (\log x)^5 + c_{12} x \exp\left(-c_7 (\log x)^{1/2}\right),$$

where c_7 is as in Lemma 4.5.2 and $c_1 2$ is an absolute, effectively computable number.

Lemma 4.5.4. [Deshouillers-Iwaniec] *For each integer m with $m \geq 3$ there is an effectively computable integer x_m and absolute and effectively computable positive numbers $c_{13} c_{14}$ with the following property. For arbitrary numbers x, Q with $x \geq x_m$, and $x^{1/2} \leq Q \leq x^{1-1/m}$, and for an arbitrary integer a with $0 < |a| < x^{1/m}$, we have*

$$\pi(x, q, a) \leq \frac{(4/3 + c_{13}/m) x}{\varphi \log(x/q)}$$

for almost all integers $q \in [Q, 2Q]$ with $\gcd(q, a) = 1$, the number of exceptions being less than $Q x^{-c_{14}/m}$.

4.5.2 Sieved primes

In this section we give a lower bound for the distribution of primes r with $r - 1$ free of prime factors in some given set. As we have already said, for the proof we refer to [7]. Before stating this result we present the following lemma:

Lemma 4.5.5. *We have for any real number $t > 1$ that*

$$\sum_{d<t} \frac{1}{\varphi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log t + \nu + \vartheta \left(\frac{\log(2t)}{t} \right),$$

where ζ is the Riemann zeta-function *and where $\nu = \sum_u \mu^2(u)(\gamma - \log u)/(u\varphi(u))$ with $u \mid d$, $\mu(u)$ the* Möbius function *(that is $(-1)^k$ if u is a squarefree and has k distinct prime factors, and 0 otherwise) and γ is the* Euler-Mascheroni constant.

Proposition 4.5.1. *For each integer $m \geq 4$, there are effectively computable positive numbers X_m, δ_m, with X_m an integer, satisfying the following property. If $x \geq X_m$ and Q is a set of primes in the interval $(1, x^{1/2}]$ with*

$$\sum_{q \in Q} \frac{1}{q-1} \leq \frac{3}{11} - \frac{1}{m},$$

then there are at least $\delta_m x/(\log x)^2$ primes $r \leq x$ such that every prime factor q of $r-1$ satisfies $q \leq x^{1/2}$ and $q \notin Q$.

4.5.3 The existence of period systems

We are now ready to prove the existence of period systems.
Also in this section some proofs will not be given.
Let's first show that there are many period pairs for n.

Proposition 4.5.2. *Let n be an integer, $n > 1$, and let w, y be real numbers. Each prime number r satisfies at least one of the following conditions:*

(i) *the element $(n \bmod r)$ of $\mathbb{F}_r$ is either zero or has multiplicative order at most w.*

(ii) *There is an integer m composed of primes at most y with $m \mid r-1$ and $m > w$.*

(iii) *There is an integer q with $q > y$ and $q^2 \mid r-1$.*

(iv) *There is a prime q such that $q > y$ and $\gcd(r, q)$ is a period pair for n.*

Proof. If $(n \bmod r)$ does not belong to F_r^* then **(i)** holds. So let's suppose $(n \bmod r) \in F_r^*$, and let m be the order of $(n \bmod r)$ in F_r^*. Then m divides $r-1$, so if $m \leq w$, then **(i)** holds. Thus, let's suppose $m > w$. If m has no prime factor exceeding y, then **(ii)** holds. Suppose therefore that q is a prime factor of m with $q > y$; then q equals the order of $(n^{m/q} \bmod r)$. If q divides $(r-1)/m$, then **(iii)** holds. If q does not divide $(r-1)/m$, then the element $(n^{(r-1)/q} \bmod r) = (n^{m/q} \bmod r)^{(r-1)/m}$ has order q, and **(iv)** holds. ■

Definition 4.5.1. *The Dickman-de Bruijn function $\rho(u)$ is a continuous function that satisfies the delay differential equation*

$$u\rho'(u) + \rho(u-1) = 0$$

with initial conditions $\rho(u) = 1$ for $0 \leq u \leq 1$.

From [10] we can state

$$\log \rho(u) = -u \cdot \log(u \log u) + \vartheta(u) \quad \text{for} \quad u \geq 2. \tag{4.20}$$

Lemma 4.5.6. *Let x, u, v be real numbers with $x \geq 20$, $1 \leq v \leq u \leq \sqrt{(\log x) \log\log x}$, and put $y = x^{1/u}$, $w = y^v$. The number of prime numbers $r \leq x$ satisfying 4.5.2* ***(ii)*** *is at most*

$$\vartheta \left(u\pi(x) \left(\frac{\rho(v)}{\log(2v)} + \rho(u) \right) \right)$$

Proof. This is Theorem 2 from [11]. ■

Proposition 4.5.3. *For all sufficiently large integers n, if x is a real number such that $x \geq (\log n)^{1+1/1800}$, then the number of prime numbers $r \leq x$ for which there does not exist a period pair (r, q) for n satisfying*

$$q \text{ is prime}, \qquad q > x^{1/(\log\log x)^2}$$

is at most $x/(\log x)^3$.

Proof. By Proposition 4.5.2, we only need to show that when n is a sufficiently large integer and x is a real number with $x \geq (\log n)^{1+1/1800}$, the number of primes $r \leq x$ satisfying one of Proposition 4.5.2**(i)**-**(iii)**, with $w = x^{1/\log\log x}$ and $y = x^{1/(\log\log x)^2}$, is at most $x/(\log x)^3$. We prove this by showing that the number of such primes r is $o(x/(logx)^3$ as $n \to \infty$. If the prime r satisfies 4.5.2**(i)**, then either $r \mid n$ or $r \mid n^m - 1$ for some integer m in $[1, w]$. Since the number of distinct prime divisors of an integer $k > 2$ is evidently smaller than $(\log k)/\log 2$, the number of primes r satisfying Proposition 4.5.2**(i)**, is smaller than

$$\frac{\log n}{\log 2} + \sum_{m \leq w} m \cdot \frac{\log n}{\log 2} \leq w^2 \cdot \frac{\log n}{\log 2} \leq x^{1800/1801+o(1)} = o(x/(\log x)^3)$$

as $n \to \infty$.
To estimate the number of primes $r \leq x$ satisfying Proposition 4.5.2**(ii)** we apply Lemma 4.5.6 with $v = \log\log x$ and $u = v^2$; using (4.20) we can say that, as $n \to \infty$, this number is at most

$$x/(\log x)^{(1+o(1))\log\log\log x} = o(x/(\log x)^3).$$

The number of integers r with $1 < r \leq x$ satisfying Proposition 4.5.2**(iii)** is clearly at most $\sum_{q>y} x/q^2 < x/(y-1) = o(x/(\log x)^3)$ as $n \to \infty$. ■

Let $\epsilon = 1/150$, let n be an integer $n \geq 20$, and let x, u be real numbers with

$$x \geq (\log n)^{1+\epsilon/12} = (\log n)^{1+1/1800}, \qquad u = (\log\log x)^2$$

For a prime r, let $Q(r)$ denote the set of prime divisors q of $r - 1$ with

$$x^{1/u} < q \leq x^{1/2} \quad \text{and} \quad (r, q) \text{ is a period pair for } n.$$

Further, let Q denote the union of the sets $Q(r)$ over all primes $r \leq x$. We are interested in Q since each subset S of it corresponds to at least one period system for n with degree $\prod_{q \in S} q$.

Proposition 4.5.4. *For all sufficiently large integers n and for all real numbers $x \geq (\log n)^{1+\epsilon/12}$, we have*

$$\sum_{q \in Q} \frac{1}{q} > \frac{3-\epsilon}{11}$$

.

Proof. Let

$A = \{\text{prime } r \leq x\text{: prime } q \mid r-1 \text{ implies } q \leq x^{1/2} \text{ and } q \notin Q\}$

$B = \{\text{prime } r \leq x\text{: prime } q \mid r-1 \text{ implies } q \leq x^{1/u} \text{ or } (r,q) \text{ is not a period pair for } n\}$ Clearly $A \subset B$. We use Proposition 4.5.1, with "m" of that result being the current $11 = /\epsilon = 1650$; let $\delta = \delta_{1650}$. Suppose n is so large that Proposition 4.5.1 and 4.5.3 hold for all $x \geq (\log n)^{1+\epsilon/12}$. If $\sum_{q \in Q} 1/q \leq (3-\epsilon)/11$, then Proposition 4.5.1 implies that $\#A \geq \delta x/(\log x)^2$. And so $\#B \geq \delta x/(\log x)^2$. But Proposition 4.5.3 implies that $\#B \leq x/(\log x)^3$. These two inequalities for $\#B$ are incompatible for large n.
From this contradiction we deduce the proof. ■

With n, x, u as above, let N be an integer for which

$$6u \log x \leq N \leq \exp(2(\log x)^{3/5}(\log\log x)^{-3/2}). \qquad (4.21)$$

For a bounded interval I, let $|I|$ denote the length of I.

Proposition 4.5.5. *For an integer N satisfying* (4.21) *and for $i = 1, 2, \ldots, N$, let*

$$I_i = [x^{(i-1)/N}, x^{i/N}), \quad M_i = x^{i/N}/i^2,$$

and

$$k_i = \begin{cases} 0, & \text{if } \#(I_i \cap Q) < M_i \\ \min\{\#(I_i \cap Q),\ \lfloor |I_i|/\log(x^{i/N}) \rfloor\}, & \text{otherwise.} \end{cases}$$

For $i \leq N/u$, $\#(I_i \cap Q) = 0$, and for each $i = 1, 2, \ldots, N$, then $k_i = 0$ or $k_i \geq M_i$.

Proof. Note that all primes $q \in Q$ have $q > x^{1/u}$, so it follows that $\#(I_i \cap Q) = 0$ for $i \leq N/u$. For the second assertion, we thus may assume that $u > 1$. Note that for $i > 1$ we have

$$\frac{|I_i|}{\log(x^{i/N})} = \frac{x^{i/N}(1 - x^{-1/N})}{(i/N)\log x} > \frac{x^{i/N}(\log x)/(2N)}{(i/N)\log x} \geq M_i,$$

where we use $x^{-1/N} = \mathrm{e}^{-(\log x)/N} < 1 - (\log x)/(2N)$, which holds from (4.21). ■

Proposition 4.5.6. *For an integer N satisfying* (4.21) *and intervals I_i and integers k_i defined in Proposition 4.5.5, let Q_i denote the set of the least k_i primes in $I_i \cap Q$. If n is sufficiently large we have*

$$\sum_{i=1}^{N} \sum_{q \in Q_i} \frac{1}{q} > \frac{3}{11} - \frac{\epsilon}{10}.$$

Proof. The double sum here may be smaller than the sum $\sum_{q \in Q} \frac{1}{q}$ in Proposition 4.5.4, the possible difference between them coming from two sources: intervals I_i with $0 < \#(I_i \cap Q) < M_i$ and intervals I_i with $\#(I_i \cap Q) > \lfloor |I_i| / \log(x^i/N) \rfloor$. By Proposition 4.5.5 we only need to consider indices $i > N/u$. We thus may assume that $u > 1$. The sum of $1/q$ for primes q in intervals I_i with $\#(I_i \cap Q) < M_i$ is at most

$$\sum_{i > N/u} \frac{M_i}{x^{(i-1)/N}} = \sum_{i > N/u} \frac{x^{1/N}}{i^2} < \frac{2u}{N} x^{1/N} \leq \frac{1}{3 \log x} \mathrm{e}^{1/(6u)} < \frac{1}{\log x},$$

by the first inequality in (4.21). Thus, this contribution is $o(1)$ as $n \to \infty$, so is negligible.

The sum of $1/q$ for the largest $\#(I_i \cap Q) - \lfloor |I_i| / \log(x^{i/N}) \rfloor$ primes q in an interval I_i with $\#(I_i \cap Q) > \lfloor |I_i| / \log(x^{i/N}) \rfloor$ is estimated as follows. By the prime number theorem (see [12]), the total number of primes in I_i is

$$L_i + \vartheta(E(x^{i/N})),$$

where

$$L_i = \int_{x^{(i-1)/N}}^{x^{i/N}} \frac{\mathrm{d}t}{\log t} \qquad \text{and} \qquad E(z) = z / \exp(c_{16} (\log z)^{3/5} (\log \log z)^{-1/5}),$$

with c_{16} an effective positive constant. As before, we may assume $i > N/u$. Note that

$$0 \leq L_i - \frac{|I_i|}{\log(x^{i/N})} \leq \frac{|I_i|}{\log(x^{(i-1)/N})} - \frac{|I_i|}{\log(x^{i/N})} = |I_i| \frac{N}{i(i-1) \log x}.$$

Further,

$$|I_i| = x^{(i-1)/N} (x^{1/N} - 1) < 2x^{i-1/N} \frac{\log x}{N}, \tag{4.22}$$

so that

$$L_i - \frac{|I_i|}{\log(x^{i/N})} < \frac{2x^{(i-1)/N}}{i(i-1)} = \vartheta(M_i).$$

Further, for $N/u < i < N$,

$$E(x^{i/N}) \leq \frac{x^{i/N}}{\exp(c_{16} u^{-3/5} (\log x)^{3/5} (\log \log x)^{-1/5})} = \frac{x^{i/N}}{\exp(c_{16} (\log x)^{3/5} (\log \log x)^{-7/5})},$$

so that from the upper bound for N in (4.21), $E(x^{i/N}) = \vartheta(M_i)$. Thus, the contribution in Proposition 4.5.4 from primes in I_i with $\#(I_i \cap Q) > \lfloor |I_i| / \log(x^{i/N}) \rfloor$ is

$$\vartheta\left(\sum_{N/u<i\leq N} \frac{M_i}{x^{(i-1)/N}}\right),$$

a sum we have seen to be negligible. ■

Proposition 4.5.7. *For an integer N satisfying* (4.21) *an integer k_i defined in Proposition 4.5.5, let $S(i)$ be the image of the interval*

$$(x^{(i-1)/N}, x^{(i-1)/N} + k_i \log(x^{i/N}))$$

under the natural logarithm map. If n is sufficiently large, then

$$\sum_{i=1}^{N} \int_{S(i)} \frac{\mathrm{d}t}{t} > \frac{3}{11} - \frac{\epsilon}{9}.$$

Proof. Since $\sum_{q\in Q_i} 1/q \leq k_i / x^{(i-1)/N}$, it follows from Proposition 4.5.6 that for n sufficiently large,

$$\sum_{i=1}^{N} \frac{k_i}{x^{(i-1)/N}} > \frac{3}{11} - \frac{\epsilon}{10}. \tag{4.23}$$

Further, if $S(i) \neq \emptyset$, that is, if $k_i > 0$, then

$$\int_{S(i)} \frac{\mathrm{d}t}{t} = \log \quad \frac{\log(x^{(i-1)/N}) + k_i \log(x^{i/N})}{\log(x^{(i-1)/N})}\Bigg).$$

Now, $\log(a + b) > \log(a) + b/a - (b/a)^2$ when $a, b > 0$, so that if $a > \mathrm{e}$ and $0 < b < a$,

$$\log\left(\frac{\log(a+b)}{\log a}\right) > \frac{b}{a \log a} - \frac{2}{\log a}\left(\frac{b}{a}\right)^2 = \frac{b}{a \log a}\left(1 - \frac{2b}{a}\right).$$

Hence,

$$\begin{aligned}\int_{S(i)} \frac{\mathrm{d}t}{t} &> \frac{k_i \log(x^{i/N})}{x^{(i-1)/N} \log(x^{(i-1)/N})} \quad 1 - \frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}}\Bigg) \\ &> \frac{k_i}{x^{(i-1)/N}} \quad 1 - \frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}}\Bigg).\end{aligned}$$

Note that, using (4.21), (4.22) and the definition of k_i,

$$\frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}} \leq \frac{2|I_i|}{x^{(i-1)/N}} < \frac{4 \log x}{N} < \frac{1}{u},$$

so that
$$\int_{S(i)} \frac{\mathrm{d}t}{t} > \frac{k_i}{x^{(i-1)/N}}(1-u^{-1}).$$
Thus, the proposition follows from (4.23) for sufficiently large n. ■

We are now ready for our main result concerning with the existence of period systems:

Proposition 4.5.8. *There is an effectively computable positive integer c_5 such that, for each integer $n > c_5$ and each integer $D > (\log n)^{46/25}$, there exists a period system P for n consisting of pairs (r,q) with*
$$r < D^{6/11}, \qquad q < D^{3/11}, \qquad q \text{ prime},$$
and with degree d satisfying $D \le d < D + D/\exp((\log D)^{3/5}(\log\log(3D))^{-3/2})$. In particular, $d \in [D, 2D)$.

Proof. Let $\epsilon = 1/150$, let n be an integer so large that Proposition 4.5.7 holds, and let D be an integer satisfying
$$D > (\log n)^{11/6+\epsilon} = (\log n)^{46/25}.$$
Let $x = D^{6/11\epsilon/4}$ so that $x > (\log n)^{1+1/1800}$, let $u = (\log\log x)^2$, and let integer N satisfy (4.21). Let $D' = D\exp(2u(\log x)/N)$ and let S be the additive semigroup generated by
$$\bigcup_{i=1}^{N} \frac{1}{\log D'} S(i),$$
where $S(i)$ is as in Proposition 4.5.7. Note that if $S(i) \neq \emptyset$ we have $x^{(i-1)/N} \le x^{1/2}$, so that
$$\frac{\log(x^{i/N})}{\log D'} \le \left(\frac{1}{2}+\frac{1}{N}\right)\frac{\log x}{\log D} = \left(\frac{1}{2}+\frac{1}{N}\right)\left(\frac{6}{11}-\frac{\epsilon}{4}\right) < \frac{3}{11}-\frac{\epsilon}{9}$$
for sufficiently large n; that is, $S(i)/\log D' \subset (0, 3/11-\epsilon/9)$. We suppose that n is so large.
Thus, from Proposition 4.5.7 and the fact that the intervals $S(i)$ are disjoint, we have
$$\int_{S\cap(0,3/11-\epsilon/9)} \frac{\mathrm{d}t}{t} \ge \sum_{i=1}^{N}\int_{S(i)/\log D'} \frac{\mathrm{d}t}{t} = \sum_i \int_{S(i)} \frac{\mathrm{d}t}{t} > \frac{3}{11}-\frac{\epsilon}{9}.$$
It thus follows from Theorem 4.4.1 that $1 \in S$. Hence, there is a finite subset F of $\bigcup_i S(i)$ and positive integers $\kappa(f)$ for each $f \in F$ such that
$$\sum_{f\in F} \kappa(f) f = \log D'.$$

Let $F_i = F \cap S(i)$ for $i = 1, 2, \dots, N$, and let

$$\kappa_i = \sum_{f \in F_i} \kappa(f).$$

Then, using $S(i) = \emptyset$ for $i \le N/u$ from Proposition 4.5.5,

$$\begin{aligned}\sum_{i=1}^{N} \kappa_i = \sum_i \sum_{f \in F_i} \kappa(f) &\le \sum_i \frac{1}{\log(x^{(i-1)/N})} \sum_{f \in F_i} \kappa(f) f \\ &< \frac{1}{\log(x^{1/u-1/N})} \sum_{f \in F} \kappa(f) f = \frac{\log D'}{(1/u - 1/N)\log x} < 2u,\end{aligned} \tag{4.24}$$

where the last inequality holds when n is sufficiently large. If $S(i) \neq \emptyset$, then Proposition 4.5.5 implies that $k_i \ge M_i$, so that $k_i > x^{1/u}/N^2 > 2u > \kappa_i$. Thus, for each i with $\kappa_i > 0$ there are at least κ_i distinct primes in Q_i. Label the least such primes $q_{1,i}, q_{2,i}, \dots, q_{\kappa_i,i}$ and let

$$d = \prod_{i=1}^{N} \prod_{j=1}^{\kappa_i} q_{j,i}.$$

If $r_{j,i} \le x$ is a prime with $q_{j,i} \in Q(r_{j,i})$ then

$$P = \{(r_{j,i}, q_{j,i}) \, : \, i = 1, \dots, N, \; j = 1, \dots, \kappa_i\}$$

is a period system for n with degree d. We have

$$\begin{aligned}|\log D' - \log d| &= \left| \sum_{f \in F} \kappa(f) f - \sum_{i=1}^{N} \sum_{j=1}^{\kappa_i} \log(q_{j,i}) \right| = \left| \sum_{i=1}^{N} \left(\sum_{f \in F_i} \kappa(f) f - \sum_{j=1}^{\kappa_i} \log(q_{j,i}) \right) \right| \\ &< \sum_i \kappa_i \left(\log(x^{i/N}) - \log(x^{(i-1)/N}) \right) = \frac{\log x}{N} \sum_i \kappa_i \\ &< \frac{2u \log x}{N},\end{aligned} \tag{4.25}$$

using (4.24). Thus,

$$D = D' \exp(-2u(\log x)/N) < d < D' \exp(2u(\log x)/N) < D(1 + 6u(\log x)/N).$$

By choosing N near the upper end of the interval in (4.21), we have proved the Proposition. ■

4.5.4 Algorithm for existence of period system

We now proceed with a straightforward transformation of Proposition 4.5.8 into an algorithm for constructing period systems.
This algorithm takes as input an integer $n > 1$ and an integer $D > 0$, and searches for a period system P for n with the properties listed in Proposition 4.5.8.

Algorithm 3:

Step 1. Using a modified version of the sieve of Eratosthenes, sieving with prime powers rather than just with primes, compute the prime factorization of all integers in $[1, 2D)$.

Step 2. For each prime number $r < D^{6/11}$ not dividing n, in increasing order, determine the set $Q(r)$ of prime factors q of $r - 1$ that satisfy

$$q < D^{3/11}, \qquad n^{(r-1)/q} \not\equiv 1 \pmod r, \qquad q \notin \bigcup_{r' < r} Q(r').$$

Put $Q = \bigcup_r Q(r)$ and, for each $q \in Q$, put $r_q = r$ if $q \in Q(r)$.

Step 3. If there is some integer in $[D, 2D)$ that is squarefree and composed solely of primes from Q, let d be the least such integer, let P be the set of all pairs (r_q, q), with q ranging over the prime factors of d, return P, and halt. If no such integer exists, pronounce failure and halt.

4.6 The primality test

In this section we will see that there exists a deterministic algorithm that decides whether an integer n is prime or not. We will also see that it works in the desired time.
Now we see some results that will lead to the claimed algorithm.
In the following Proposition the constant c_5 is as in Proposition 4.5.8.

Proposition 4.6.1. *The algorithm above, on input of integers $n > 1$ and $D > 0$, successfully computes a period system for n with the properties listed in Proposition 4.5.8 if and only if such a period system exists, which is the case if $n > c_5$ and $D > (\log n)^{46/25}$; the run time of the algorithm is $\tilde{\vartheta}(D + D^{6/11} \log n)$.*

Proof. The "if and only if" statement is clear from the algorithm, the second assertion is immediate from Proposition 4.5.8, and proof of the run time estimate is entirely straightforward. ∎

We are now going to describe the algorithm:

Algorithm 4:
Given an integer $n > 1$, this algorithm decides whether or not n is prime.

Step 1. If $n \leq c_5$, find by trial division the least prime p dividing n, declare n prime or composite according as $n = p$ or $n \neq p$, and halt.

Step 2. Using the algorithm of [13], determine the largest $k \in \mathbb{Z}$ for which there exists $m \in \mathbb{Z}$ with $n = m^k$. If $k > 1$, declare n composite and halt.

Step 3. Using standard algorithms for computing elementary functions (cf. [14]), compute an integer D satisfying

$$D_2 < \max\Big((\log n)^2/(3 \cdot (\log 2)^2), (\log n)^{46/25}\Big) < D.$$

Next, using **Algorithm 3**, construct a period system P for n with the properties listed in Proposition 4.5.8. Put $d = \prod_{(r,q)\in P} q$.

Step 4. Using standard algorithms for computing elementary functions (cf. [14]), compute an integer b satisfying

$$b - 1 < (d/3)^{1/2}(\log n)/\log 2 < b + 1,$$

and test by trial division whether n has a divisor among $2, 3, \ldots, \max\{d, b\}$. If it does, let p be the least such divisor, declare n prime or composite according as $n = p$ or $n \neq p$, and halt.

Step 5. Using **Algorithm A** of Proposition 4.3.3, either declare n composite and halt, or construct a pseudofield (A, α) of characteristic n and degree d.

Step 6. For $a = 1, 2, \ldots, b$, test the equality $\alpha^n + a = (\alpha + a)^n$ in A. If all of these are valid, declare n prime and halt. If at least one fails to be valid, declare n composite and halt.

We are now ready to state the following:

Theorem 4.6.1. *There exists, for some effectively computable real number c_0, a deterministic algorithm that, given an integer n with $n > 1$, decides whether or not n is prime, and does so in time at most $(\log n)^6 \cdot (2 + \log\log n)^{c_0}$.*

Proof. We prove that the algorithm above has the properties claimed in the Theorem, that is, it terminates within time $\tilde{\vartheta}((\log n)^6)$, correctly declaring n prime or composite.
Step 1 runs in time $\vartheta(1)$, and by [13], Step 2 runs in time $\tilde{\vartheta}(\log n)$. If the algorithm halts during one of these two steps, it is clearly correct. Assume otherwise, so that one has $n > c_5$ and n is not a proper power. The first

part of Step 3 runs in time $\vartheta(\log n)$, and from $D > (\log n)^{46/25}$ and $D = \vartheta((\log n)^2)$ it follows, by Proposition 4.6.1, that the second part of Step 3 successfully computes a period system in time $\tilde{\vartheta}((\log n)^{23/11})$. We have $d = \vartheta((\log n)^2)$, and from $d \geq 2^{\#P}$ one obtains $\#P = \vartheta(\log(2 \log n))$. Step 4 runs in time $\tilde{\vartheta}((\log n)^3)$ because $b = \vartheta((\log n)^2)$. If the algorithm halts in Step 4, it is clearly correct. Suppose otherwise. Then we have $n > d$, so by Proposition 4.3.3 and the inequalities in Proposition 4.5.8, Step 5 runs in time $\tilde{\vartheta}((\log n)^3)$. As we argued in the section where we dealt with algorithmic aspects of pseudofields, the test in Step 6 can be done in time $\tilde{\vartheta}((d^{1/2} \log n)^3)$, which is $\tilde{\vartheta}((\log n)^6)$. Since n passed Step 4, it has a prime divisor greater than $(d/3)^{1/2}(\log n)/\log 2$, so Proposition 4.2.4 implies that, if n passes the test in Step 6, it is a prime power; not being a proper power, it must be prime. If n does not pass the test in Step 6, then by Proposition 4.2.3 (with n in the role of p and $\alpha + a$ in the role of β) it cannot be a prime number.

This concludes the proof of this important result. ■

Chapter 5

Bernstein's RP Algorithm

In this chapter we give a sketch of an RP algorithm. This algorithm is a modification of AKS given by Bernstein, following up on ideas of Berrizbeitia, as developed by Qi Cheng.

5.1 Introduction

First of all let's define the RP class:

Definition 5.1.1. *In complexity theory, RP ("randomized polynomial time") is the complexity class of problems for which a probabilistic Turing machine exists with these properties:*

1. *It always runs in polynomial time in the input size.*

2. *If the correct answer is NO, it always returns NO.*

3. *If the correct answer is YES, then it returns YES with probability at least 1/2 (otherwise, it returns NO).*

Next we describe an algorithm belonging to the RP class that distinguishes primes from composites and provides a proof within $\vartheta((\log n)^{4+0(1)})$ steps. The only drawback is that this is not guaranteed to work. Each time one runs the algorithm the probability that it reports back is, by definition of RP class, $\geq 1/2$, but each run is independent, so after 100 runs the probability that one has not yet distinguished whether the given integer is prime or composite is $< 1/2^{100}$, which is negligible. In practice this algorithm makes the original AKS algorithm irrelevant, for if we run the "witness" test, which is an RP algorithm for compositeness, half of the time and run this RP algorithm for primality the other half, then a number n is, in practice, certain to yield its secrets faster (in around $\vartheta((\log n)^{4+o(1)})$ steps) than by the original AKS algorithm.

5.2 A characterization of the primes

Definition 5.2.1. *For a given monic polynomial $f(x)$ with integer coefficients of degree $d \geq 1$ and positive integer n, we say that $\mathbb{Z}[x]/(n, f(x))$ is an almostfield with parameters $(e, v(x))$ if*

(a) *Positive integer e divides $n^d - 1$,*

(b) $v(x)^{n^d-1} \equiv 1 \bmod (n, f(x))$, *and*

(c) $v(x)^{(n^d-1)/q}$ *is a unit in $\mathbb{Z}[x]/(n, f(x))$ for all primes q dividing e.*

If n is prime and $f(x) \pmod n$ is irreducible, then $\mathbb{Z}[x]/(n, f(x))$ is a field; moreover any generator $v(x)$ of the multiplicative group of elements of this field satisfies **(b)** and **(c)** for any e satisfying **(a)**.

Theorem 5.2.1. [Bernstein] *For given integer $n \geq 2$, suppose that $\mathbb{Z}[x]/(n, f(x))$ is an almostfield with parameters $(e, v(x))$ where $e > (2d \log n)^2$. Then n is prime if and only*

- *n is not a perfect power*
- $(t-1)^{n^d} \equiv t^{n^d} - 1 \bmod (n, f(x), t^e - v(v))$ *in $\mathbb{Z}[x, t]$*

Proof. Write $N = n^d$ and $v = v(x)$. If n is a perfect power, then n is composite. If n is prime, then the second condition holds by the Child's Binomial Theorem . So we may henceforth assume that n is not a perfect power and is not prime, and we wish to show that $(t-1)^{n^d} \not\equiv t^{n^d} - 1 \bmod (n, f(x), t^e - v(x))$. Let p be a prime dividing n and $h(x)$ an irreducible factor of $f(x) \pmod p$, so that $\mathbb{F} = Z[x]/(p, h(x))$ is isomorphic to a finite field. Let $P = |F| = p^{\deg h}$, and note that since $p < n$ and $\deg h \leq \deg f$, hence $P < N$.
Let $\zeta \equiv v^{(N-1)/e} \bmod (p, h(x))$ so that ζ is an element of order e in $\mathbb{F}$. To see this, note that $\zeta^e \equiv v^{N-1}$ (mod $()p, h(x))$ by **(b)**; whereas if ζ had order m, a proper divisor of e, then let q be a prime divisor of e/m so that $1 \equiv \zeta^{e/q} \equiv v^{(N-1)/q} \bmod (p, h(x))$, contradicting **(c)**.
The polynomials of the form $\prod_{i=0}^{e-1}(\zeta^i t - 1)^{a_i}$ in $\mathbb{F}[t]$ are distinct, and so those of degree $\leq e-1$ are distinct in $\mathbb{F}[t]/(t^e - v)$.
Now $t^N = t^{N-1}t \equiv v^{(N-1)/e}t \bmod (t^e - v)$, so that $t^N \equiv \zeta t \bmod (p, h(x), t^e - v)$. Thus our second criterion implies that $(t-1)^N \equiv \zeta t - 1 \bmod (p, h(x), t^e - v)$. Moreover replacing t by $\zeta^i t$ gives $(\zeta^i t - 1)^N \equiv \zeta^{i+1} t - 1 \bmod (p, h(x), t^e - v)$ for any integer $i \geq 0$ (since $(\zeta^i t)^e - v = t^e - v$), and thus $(t-1)^{N^i} \equiv \zeta^i t - 1 \bmod (p, h(x), t^e - v)$ by a suitable induction argument. Note that $(t-1)^{N^e} \equiv (t-1) \bmod (p, h(x), t^e - v)$.
Therefore for proper subsets I of $\{0, 1, \ldots, e-1\}$ the powers $(t-1)^{\sum_{i \in I} N^i} \equiv \prod_{i \in I}(\zeta^i t - 1) \bmod (p, h(x), t^e - v)$ all have degree $\leq e-1$ and so are distinct polynomials, and thus there are at least $2^e - 1$ distinct powers of $(t-1)$ mod

$(p, h(x), t^e - v)$.
Now e is the order of an element of $\mathbb{F}^*$, which is a cyclic group of order $P-1$, and so $P-1$ is a multiple of e. Therefore $v^{(P-1)/e}$ is an e-th root of 1 in $\mathbb{F}$, so must be a power of ζ, say ζ^l. Arguing as done earlier, but now with N and ζ replaced by P and ζ, we see that $(t-1)^{P^j} \equiv \zeta^{jl}t - 1 \bmod (p, h(x), t^e - v)$. Combining these results we obtain that $(t-1)^{N^iP^j} \equiv \zeta^{i+jl}t - 1 \bmod (p, h(x), t^e - v)$ for all integers i, j.
There are more than e pairs of integers (i, j) with $0 \leq i, j \leq [\sqrt{e}]$, and so there exist two numbers of the form $i + jl$ (with i and j in this range) that are congruent modulo e, say $i + jl \equiv I + Jl \pmod e$. Therefore if $u := N^iP^j$ and $U := N^IP^J$, then $(t-1)^u \equiv \zeta^{i+jl}t - 1 = \zeta^{I+Jl}t - 1 \equiv (t-1)^U \bmod (p, h(x), t^e - v)$. We will show that $t-1$ is a unit $\bmod (p, h(x), t^e - v)$ so that we can deduce that there are no more than $|U - u| < (NP)^{\sqrt{e}} - 1 < N^{2\sqrt{e}} - 1$ distinct powers of $(t-1) \bmod (p, h(x), t^e - v)$, and thus $2^e < N^{2\sqrt{e}}$, contradicting the hypothesis.
Now $v(x) \neq 1$ in $\mathbb{F}$ by **(c)**, so that $t-1$ is not a factor of $t^e - v(x)$ in $\mathbb{F}[t]$; in other words $t-1$ is a unit in the ring $\mathbb{F}[t]/(t^e - v(x)$, that is $\bmod (p, h(x), t^e - v)$. ■

5.3 Running this primality test in practice

We will show that if n is prime, then an almostfield may be found rapidly in random polynomial time.

Finding the almostfield: Assume that n is prime. By the inclusion-exclusion formula one can prove that there are $(1/d)\sum_{l|d}\mu(d/l)n^l$ irreducible polynomials modulo n of degree d, where μ is the Möbius function that we have seen in Lemma 4.5.5. The biggest term here is the one with $l = d$: in fact $1/d\mu(1)n^d = n^d/d$; that is, roughly $1/d$ of the polynomials of degree d are irreducible. Thus selecting degree d polynomials at random we should expect to find an irreducible one in $\vartheta(d)$ selections. Verifying f is irreducible can be done by checking, via the Euclidean algorithm, that $x^{n^d} - x \equiv 0 \bmod (n, f(x))$ and $x^{n^{d/q}} - x$ is a unit in $\mathbb{Z}[x]/(n, f(x))$ for all primes q dividing d. Once we have found f we know that $\mathbb{Z}[x]/(n, f(x))$ is a field. The elements of $\mathbb{Z}[x]/(n, f(x))$ can be represented by the polynomials $v(x)$ modulo n of degree $< d$. The proportion of these that satisfy **(b)** and **(c)** is $\prod_{p|e}(1 - 1/p) > 1/2 \ln\ln e$, and so selecting such $v(x)$ at random we should expect to find $v(x)$ satisfying **(b)** and **(c)** in $\vartheta(d)$ selections.

Verifying primality conditions: The main part of the running time comes in verifying that $(t-1)^{n^d} \equiv t^{n^d} - 1 \bmod (n, f(x), t^e - v(x))$, which will take $d \log n$ steps, each of which will cost $\vartheta(de(\log n)^{1+o(1)})$ bit operations, giving a total time of $\vartheta(d^2e(\log n)^{2+o(1)})$ bit operations. The conditions $d \geq 1, e > (2\log n)^2$ imply that the running time cannot be better than $\vartheta((\log n)^{4+o(1)})$, and we will indicate in the next section how to find d and e so that we obtain this running time.

5.4 More analytic number theory

To find an almostfield when n is prime we need to find d and e for which e divides $n^d - 1$ and with d and e satisfying certain conditions. Constructions typically give e as a product of primes p which do not divide n and for which $p-1$ divides d, since then p divides $n^d - 1$ by Fermat's Little Theorem, and thus e divides $n^d - 1$.

However, to ensure that e is large, for instance $e > (2d\log n)^2$ as required in the hypothesis of Bernstein's result, we need to use the ideas of analytic number theory. Our general construction looks as follows: for given $z < y$, with $z \geq \epsilon y$ for fixed $\epsilon > 0$, let d be the least common multiple of the integers up to z and e be the product of all primes $p \leq y$ such that all prime power divisors q^a of $p-1$ are $\leq z$. Note that $d = \exp(z+o(z))$ by the prime number theorem and $e = \prod_{p\leq y} p / \prod_{p\in P} p$, where P is the set of primes $p \leq y$ for which $p-1$ has a prime power divisor q^a which is $> z$.

If $p \in P$ write $p-1 = kq^a$ with $q^a > z$, so that $k < y/z \leq 1/\epsilon$. Now the number of $q^a \in (z, y)$ with $a \geq 2$ is $\vartheta(\sqrt{y})$, and so there are $\vartheta(\sqrt{y}/\epsilon)$ values of $p \in P$ for which $p-1$ has a prime divisor q^a with $a \geq 2$.

In our first construction we take $y = 4z$, so that if $a = 1$, then we have a prime pair of the form $q, kq+1$ with $k < 4$, and so $k = 2$. For this we use again Conjecture 1.5.1 which is a bound on the number of prime pairs of the form $q, 2q+1$ telling us that the q's of this form with $q \leq x$ are less than $2cx/(\log x)^2$ where c is a constant.

Therefore $|P| = \vartheta(y/(\log y)^2)$ and so $e = \exp(y + o(y))$ by the prime number theorem. If we take $y = (4+\epsilon)\log\log n$, then we get $e > (2d\log n)^2$ as required, and the values of d and e can, in practice, be found quickly. However, by the previous section the running time will be $\vartheta((\log n)^{8+\vartheta(\epsilon)})$, so we need to choose d and e slightly differently.

This time we take $z = \epsilon y$ with $y = (2+3\epsilon)\log\log n$. We need the generalization of Conjecture 1.5.1:

Lemma 5.4.1. *There exists an absolute constant $c > 0$ such that there are $\leq c(k/\phi(k))(x/(\log x)^2)$ primes $q \leq x$ for which $kq+1$ is also prime, for all even integers k and all $x \geq 2$.*

In this case, corresponding to each prime $p \in P$ with $a = 1$, we have a prime pair $q, kq+1$ with $k \leq 1/\epsilon$ and $q \leq y/k$. For given $k \leq 1/\epsilon$ there are $\leq cy/(\log(\epsilon y))^2$ such prime pairs, by Conjecture 1.5.1 with $x = y/k$, since $\phi(k) \geq 1$. Therefore $|P| = \vartheta(y/(\epsilon(logy)^2) + \sqrt{y}/\epsilon) = o(y/\log y)$, so the product of the primes in P is $\leq y^{|P|} = \exp(o(y))$. Thus $e = \exp(y + o(y))$ by the prime number theorem, and so $e > (2d \log n)^2$ as required; but now the running time will be $\vartheta((\log n)^{4+\vartheta(\epsilon)})$, and letting $\epsilon \to 0$ we get the desired result.

Appendix A

Tensor Product

A.1 Preliminaries

In this section we are going to see some important results about Tensor Products. For general properties of tensor products, see [1, Chapter XVI].

Proposition A.1.1. *Let A_1 be free over R, with basis $\{v_i\}_{i\in I}$. Then every element of $A_1 \otimes A_2$ has a unique expression of the form*

$$\sum_{i\in I} y_i \otimes v_i, \qquad y_i \in A_2$$

with almost all $y_i = 0$.

Proof. see [1]. ■

Corollary A.1.1. *Let A_1,A_2 be free over R, with bases $\{v_i\}_{i\in I}$ and $\{w_j\}_{j\in J}$ respectively. Then $A_1 \otimes A_2$ is free, with basis $\{v_i \otimes w_j\}$. We have*

$$\dim(A_1 \otimes A_2) = (\dim A_1)(\dim A_2).$$

Proof. Immediate form the proposition ■

Tensor products can be used to construct "large" psudofields out of small ones, in the following manner:

Proposition A.1.2. *Let (A_1, α_1) and (A_2, α_2) be pseudofields with* char A_1 =char $A_2 = n$*, and suppose that the degrees d_1, d_2 of these pseudofields satisfy $d_1 > 1, d_2 > 1$, and* $\gcd(d_1, d_2) = 1$*. Then the tensor product $(A_1 \otimes_{\mathbb{Z}/z\mathbb{Z}} A_2, \alpha_1 \otimes \alpha_2)$ is a pseudofield of characteristic n and degree d_1d_2.*

Proof. We need to check that $A = A_1 \otimes_{\mathbb{Z}/z\mathbb{Z}} A_2$, $\alpha = \alpha_1 \otimes \alpha_2$, n, $d = d_1d_2$ and $\sigma = \sigma_1 \otimes \sigma_2$ satisfy conditions from (4.1) to (4.5). By Proposition 4.2.1(a), each A_i is a free $\mathbb{Z}/n\mathbb{Z}$-module with basis $1, \alpha_i, \ldots, \alpha_i^{d_i-1}$, so from Corollary A.1.1 we see that A is a free $\mathbb{Z}/n\mathbb{Z}$- module with basis $(\alpha_1^i \otimes \alpha_2^j)_{0\leq i<d_1, 0\leq j<d_2}$.

This implies both (4.1) and (4.2). We have, $\sigma(\alpha) = \sigma_1(\alpha_1) \otimes \sigma_2(\alpha_2) = \alpha_1^n \otimes \alpha_2^n = \alpha^n$, which is (4.3). Each $\sigma_i^{d_i}$ is the identity on A_i, so σ_d is the identity on A, which implies (4.4). Finally, to prove (4.5), let l be a prime number dividing d. Then l divides exactly one of d_1 and d_2; by symmetry we may assume it divides d_2. Let k be a prime number dividing d_1. By $\sigma_1\alpha_1 = \alpha_1^n$, The A_1-ideal $A_1\alpha_1$ is mapped to itself by σ_1 and, therefore, contains $\sigma_1^{d_1/k}\alpha_1 - \alpha_1$; applying (4.5) to A_1 we obtain that this element is a unit of A_1, so α_1 must be a unit of A_1 as well. Since d/l is divisible by d_1, we have $\sigma_1^{d/l}\alpha_1 = \alpha_1 \in A_1^*$. Since d/l is not divisible by d_2, Lemma 4.2.1 implies $\sigma_2^{d/l}\alpha_2 - \alpha_2 \in A_2^*$. It follows that the element $\sigma^{d/l}\alpha - \alpha = (\sigma_1^{d/l}\alpha_1) \otimes (\sigma_2^{d/l}\alpha_2) - \alpha_1 \otimes \alpha_2 = \alpha_1 \otimes (\sigma_2^{d/l}\alpha_2 - \alpha_2)$ is a product of two units, and therefore belongs to A^*. This completes the proof. ■

We are now going to address the problem of designing an algorithm that, given two pseudofields A_i, α_i as in Proposition A.1.2, computes their tensor product. For the general context of our algorithm one may consult [16] Let R be a commutative ring, let $m \in \mathbb{Z}$, $m \geq 0$, and write S for the ring $R[t]/(t^{m+1})$, where t denotes a polynomial variable. The elements $1, t, \ldots, t^m$ form a basis for S over R, in the sense that every element of S has a unique representation of the form $\sum_{i=0}^{m} a_i t^i$, with each $a_i \in R$. The elements $\sum_{i=0}^{m} a_i t^i$ with $a_0 = 0$ form the ideal tS of S, and the elements with $a_0 = 1$ form a subgroup of the group S^* of units of S; we write $1 + tS$ for this subgroup.

We define the maps $D : S \to tS$ and $L : 1 + tS \to tS$ by

$$D \ \sum_{i=0}^{m} a_i t^i \Bigg) = \sum_{i=0}^{m} i a_i t^i \qquad (a_i \in R),$$

$$L(u) = D(u) \cdot u^{-1} \qquad (u \in 1 + tS).$$

Now, let $u = \sum_{i=0}^{m} a_i t^i$ and $v = \sum_{j=0}^{m} b_j t^j$ and let's calculate $D(u \cdot v)$

$$\begin{aligned}
D(u \cdot v) =& D\left(\sum_{i=0}^{m} a_i t^i \cdot \sum_{j=0}^{m} b_j t^j\right) = D\left(\sum_{i=0}^{m}\sum_{j=0}^{m} a_i t^i \cdot b_j t^j\right) = \\
=& D\left(\sum_{i,j=0}^{m} a_i b_j t^{i+j}\right) = \sum_{i,j=0}^{m} (i+j) \cdot a_i b_j t^{i+j} = \\
=& \sum_{i,j=0}^{m} j \cdot a_i b_j t^{i+j} + \sum_{i,j=0}^{m} i \cdot a_i b_j t^{i+j} = \\
=& \sum_{i=0}^{m} a_i t^i \cdot \sum_{j=0}^{m} j b_j t^j + \sum_{j=0}^{m} b_j t^j \cdot \sum_{i=0}^{m} i a_i t^i = \\
=& u \cdot \sum_{j=0}^{m} j b_j t^j + v \cdot \sum_{i=0}^{m} i a_i t^i = u \cdot D(v) + v \cdot D(u).
\end{aligned}$$

From this equality we can deduce that

$$\begin{aligned}
L(uv) =& D(uv) \cdot (uv)^{-1} = (uD(v) + vD(u))(uv)^{-1} = \\
=& (uu^{-1}D(v)v^{-1}) + (vv^{-1}D(u)u^{-1}) = \\
=& L(u) + L(v)
\end{aligned}$$

which means that L is a group homomorphism from the multiplicative group $1 + tS$ to the additive group tS.
For a monic polynomial $g = x^k + \sum_{i=1}^{k} b_i x^{k-i} \in R[x]$, we write $\hat{g}$ for the image of $1 + \sum_{i=1}^{k} b_i t^i$ in S, which belongs to $1 + tS$. Evidently, we have $\widehat{(gh)} = \hat{g} \cdot \hat{h}$ for any two monic polynomials $g, h \in R[x]$.
The *Hadamard product* $*$ is the operation defined on S by

$$\left.\sum_{i=0}^{m} a_i t^i\right) * \left.\sum_{i=0}^{m} b_i t^i\right) = \sum_{i=0}^{m} a_i b_i t^i,$$

for $a_i, b_i \in R$. In the following result we use the definitions just given for the ring $R = \mathbb{Z}/n\mathbb{Z}$.

Proposition A.1.3. *Let the hypotheses and notation be as in Proposition* A.1.2. *Moreover, write f_1, f_2, f for the characteristic polynomials of the pseudofields $(A_1, \alpha_1), (A_2, \alpha_2)$, and $(A_1 \otimes_{\mathbb{Z}/n\mathbb{Z}} A_2, \alpha_1 \otimes \alpha_2)$, respectively. Then for any non-negative integer m we have the identity*

$$L(\widehat{f}) = -L(\widehat{f_1}) * L(\widehat{f_2})$$

in $t(\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$.

Proof. Let the notation $A, \alpha, d, \sigma_1, \sigma_2, \sigma$ be as in the proof of the previous Proposition. We view A_1 and A_2 as subrings of A, identifying α_1 with $\alpha_1 \otimes 1$ and α_2 with $1 \otimes \alpha_2$, so that $\alpha = \alpha_1\alpha_2$. It suffices to prove the identity in $tA[t]/(t^{m+1})$. From $f = \prod_{i=0}^{d-1}(x - \sigma^i\alpha)$ we obtain $\widehat{f} = \prod_{i=0}^{d-1}(1 - (\sigma^i\alpha)t)$. From $L(1 - (\sigma^i\alpha)t) = -(\sigma^i\alpha)t/(1(\sigma^i\alpha)t) = -\sum_{j=1}^{m}(\sigma^i\alpha)^j t^j$ we thus obtain

$$L(\widehat{f}) = \sum_{i=0}^{d-1} L(1 - (\sigma^i\alpha)t) = -\sum_{j=1}^{m} \left. \sum_{i=0}^{d-1}(\sigma^i\alpha)^j \right) t^j.$$

Likewise, we have

$$L(\widehat{f_1}) = -\sum_{j=1}^{m} \left. \sum_{i=0}^{d_1-1}(\sigma_1^i\alpha_1)^j \right) t^j, \qquad L(\widehat{f_2}) = -\sum_{j=1}^{m} \left. \sum_{i=0}^{d_2-1}(\sigma_2^i\alpha_2)^j \right) t^j.$$

The identity to be proved now follows from

$$\sum_{i=0}^{d-1}(\sigma^i\alpha)^j = \left. \sum_{i=0}^{d_1-1}(\sigma_1^i\alpha_1)^j \right) \cdot \left. \sum_{i=0}^{d_2-1}(\sigma_2^i\alpha)^j \right)$$

for all $j \geq 1$, which is a consequence of $\sigma^i\alpha = (\sigma_1^i\alpha_1) \cdot (\sigma_2^i\alpha_2)$ and the fact that the orders d_1 and d_2 of σ_1 and σ_2 are coprime. ■

Proposition A.1.4. *For positive integers n, m, let $S_{n,m}$ denote the ring $(\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$.*

(a) *Let n and m be positive integers such that each prime factor of n exceeds m. Then the map $L : 1 + tS_{n,m} \quad tS_{n,m}$ is a group isomorphism.*

(b) *There is an algorithm that, given positive integers n and m, and an element $u \in 1 + tS_{n,m}$, computes the element $L(u)$ of $tS_{n,m}$ in time $\tilde{\vartheta}(m \log n)$.*

(c) *There is an algorithm that, given positive integers n and m, and an element $s \in tS_{n,m}$, either computes a prime factor of n that is at most m or correctly decides that no such prime factor exists, and in the latter case computes the element $L^{-1}(s)$ of $1 + tS_{n,m}$, all in time $\tilde{\vartheta}(m \log n)$.*

Proof. **(a)** Since each prime factor of n exceeds m, we have $i \in (\mathbb{Z}/n\mathbb{Z})^*$ for $i = 1, \ldots, m$, so D restricts to a group automorphism of $tS_{n,m}$. For the same reason, there are well-defined maps $\log : 1 + tS_{n,m} \quad tS_{n,m}$ and $\exp : tS_{n,m} \quad 1 + tS_{n,m}$ with

$$\log(1 - x) = -\sum_{i=1}^{m} x^i/i, \qquad \exp(x) = \sum_{i=0}^{m} x^i/i!$$

for $x \in tS_{n,m}$. It is well known that log and exp are inverse group isomorphisms. An easy computation shows $L = D \circ \log$. It follows that L is an isomorphism, with inverse $exp \circ D^{-1}$.

(b) In [14, Section 8] one finds an algorithm that computes $L(u)$ by means of $\tilde{\vartheta}(m)$ ring operations in $\mathbb{Z}/n\mathbb{Z}$; this particular algorithm does not depend on the condition, in [14, Section 8], that the field Q of rational numbers be contained in the coefficient ring. By [15, sections 8.3 and 9.1], each ring operation in $\mathbb{Z}/n\mathbb{Z}$ can be done in time $\tilde{\vartheta}(\log n)$.

(c) We describe an algorithm with the stated properties. Using the extended Euclidean algorithm, see [15, Corollary 11.10], one attempts to compute $i^{-1} \in= n\mathbb{Z}$ for $i = 1, 2, \ldots, m$; this can only fail if among those i a prime factor of n is found, in which case the algorithm halts. Suppose it does not fail. Then one computes $D^{-1}(s)$ directly from the definition of D by means of m multiplications in $\mathbb{Z}/n\mathbb{Z}$, and next one uses the algorithm from [14, Section 9] to compute $L^{-1}(s) = \exp(D^{-1}(s))$ using $\tilde{\vartheta}(m)$ ring operations in $\mathbb{Z}/n\mathbb{Z}$; inspection of this algorithm shows that the condition from [14, Section 9] that Q be contained in the coefficient ring may be replaced by the weaker condition that multiplicative inverses of each of $i = 1, 2, \ldots, m$ be available; this condition is satisfied in the present case.

■

Proposition A.1.5. *There is an algorithm with the following property. Given an integer n and two pseudofields of characteristic n and of coprime degrees d_1, d_2 greater than 1, it either finds a prime factor of n that is at most $d_1 d_2$ or it constructs the tensor product of the two given pseudofields, and it does so in time $\tilde{\vartheta}(d_1 d_2 \log n)$.*

Proof. The following algorithm has the stated properties. Let f_1, f_2 be the characteristic polynomials of the two given pseudofields. Put $m = d_1 d_2$ and $S = (\mathbb{Z}/n\mathbb{Z})[t]/(t^{m+1})$, and compute $\widehat{f_1}, \widehat{f_2} \in 1 + tS$ from the definition of $\widehat{f}$. Next compute $L(\widehat{f_1})$ and $L(\widehat{f_2})$ by means of the algorithm of Proposition A.1.4(b), and compute $L(\widehat{f_1}) * L(\widehat{f_2})$ by $d_1 d_2$ multiplications in $\mathbb{Z}/n\mathbb{Z}$. Finally, apply the algorithm of Proposition A.1.4(c) to $s = -L(\widehat{f_1}) * L(\widehat{f_2})$; this either yields a prime factor of n that is at most $m = d_1 d_2$, or it finds $L^{-1}(s) \in 1 + tS$; in the latter case, the characteristic polynomial of the tensor product is the unique monic polynomial $f \in (\mathbb{Z}/nZ)[X]$ of degree $d_1 d_2$ that satisfies $\widehat{f} = L^{-1}(s)$. This completes the description of the algorithm. It is correct by Proposition A.1.3, and Proposition A.1.4 readily implies that it runs in time $\tilde{\vartheta}(d_1 d_2 \log n)$. ■

References

1. S.Lang, *Algebra*, revised third edition, Springer-Verlag, New York 2002.

2. K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, Berlin and New York, 2nd edition, 1990.

3. F. Proth.*Théorèmes sur les nombres premiers.* Comptes Rendus Acad. des Sciences, Paris 87:926, 1878.

4. P. Berrizbeitia and T.G. Berry. *Biquadratic Reciprocity and a Lucasian Primality Test.* Preprint availabel from http://www.ldc.usb.ve/'berry/preprints.html

5. N. M. Timofeev, *The Vinogradov-Bombieri theorem* (in Russian), Mat. Zametki 38 (1985), 801-809, 956.

6. J.-M. Deshouillers and H. Iwaniec, *On the Brun-Titchmarsh theorem on average*, in Topics in classical number theory (G. Halàsz, ed.), Vol. I, (Budapest, 1981), 319-333, Colloq. Math. Soc. Jànos Bolyai, 34, North-Holland, Amsterdam, 1984.

7. A. Balog, *$p + a$ without large prime factors*, in Seminar on number theory, 1983-1984 (Talence, 1983/1984), Exp. No. 31, 5 pp., Univ. Bordeaux I, Talence, 1984.

8. H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika 20 (1973), 119-134.

9. H. Davenport, Multiplicative number theory, Second edition (revised by H. L. Montgomery), Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980.

10. N. G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, J. Indian Math. Soc. (N.S.) 15 (1951), 25-32.

11. C. Pomerance and I. E. Shparlinski, *Smooth orders and cryptographic applications*, Algorithmic Number Theory (Sydney, 2002), 338-348, Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002.

12. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, UK, 1995.

13. D. J. Bernstein, H. W. Lenstra, Jr., and J. Pila, *Detecting perfect powers by factoring into coprimes*, Math. Comp. 76 (2007), 385-388.

14. D. J. Bernstein, *Fast multiplication and its applications*, in J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, 325-384, MSRI Publications 44, Cambridge U. Press, New York, 2008.

15. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 1999.

16. A. Bostan, P. Flajolet, B. Salvy, and É. Schost, *Fast computation of special resultants*, J. Symbolic Comput. 41 (2006), 1-29.

17. D. Bleichenbacher, *The continuous postage problem*, unpublished manuscript, 2003

18. Étienne Fouvry. *Théorème de Brun-Tichmarsh: application au théorème de Fermat.* Invent. Math., 79(2):383-407, 1985.

19. R. C. Baker and G. Harman. *The Brun-Titchmarsh Theorem on average.* In Proceedings of a conference in Honor of Heini Halberstam, Volume 1, pages 39-103, 1996.

20. T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, 1997.

21. G. H. Hardy and J. E. Littlewood. *Some problems of Partitio Numerorum III: On the expression of a number as a sum of primes.* Acta Mathematica, 44:1-70, 1922.