UNIVERSITÀ DEGLI STUDI DI PADOVA

FACOLTÀ DI SCIENZE MM. FF. NN.
CORSO DI LAUREA IN MATEMATICA

ELABORATO FINALE

ON SOME POLYNOMIAL-TIME PRIMALITY ALGORITHMS

(ALCUNI ALGORITMI POLINOMIALI DI PRIMALITÀ)

RELATORE: PROF. ALESSANDRO LANGUASCO

DIPARTIMENTO DI MATEMATICA PURA E APPLICATA

LAUREANDA: VALÉRIE GAUTHIER UMAÑA

ANNO ACCADEMICO 2007/2008

Acknowledgments:

My most sincere gratitude to Professor Alessandro Languasco, advisor of this thesis, who in addition to being a fundamental guide in the making of this thesis, was completely engaged and helped me enormously during all the process. I also thank him for all the time that he devoted to me and the great motivation that he transmitted me.
I would like to thank also my parents and my sister for their support and unconditional help.

Introduction

In 1801 Gauss said: *"The problem of distinguishing prime numbers from composite numbers is one of the most fundamental and important in arithmetic. It has remained as a central question in our subject from ancient times to this day, and yet still fascinates and frustrates us all*[1]*"*. This problem has been studied by a lot of great mathematicians and it was not until the last century, that its importance was recognized in applied mathematics. This because of computer's science improvement and its application in cryptography.

We say that an algorithm is a deterministic algorithm if it will be correctly terminated. For example, a primality test is deterministic, if for every integer n, given as an input, the output will be prime if n is prime and composite otherwise. We say that an algorithm is a polynomial time one, if there exists a polynomial g, such that, if the input has m digits, the algorithm stops after $\mathcal{O}(g(m))$ elementary operation. From the definition of primality, $d(n) = 2$, a simple algorithm to check this property is to see whether any integer d between 2 and $\sqrt{n}$ actually divides n. The problem of this test is that if n is very big, the number of elementary operations, would be very big, and we should wait for a long period of time to have a reply. The main idea is to find a certain $\mathcal{P}$ such that: n is prime $\Leftrightarrow$ n has the property $\mathcal{P}$, and such that the condition of $\mathcal{P}$ can be verified in a "short" time.

The goal of this work is to introduce the main polynomial time primality algorithm. In the first chapter we introduce the Fermat pseudoprimes and the Miller-Rabin primality test which computational cost is $\mathcal{O}(\log^5 n)$ bit operations and is deterministic if the Extended Riemann Hypothesis (ERH) is true. Strictly speaking, this is not a primality test but a "compositeness test", since it without assuming ERH, does not prove the primality of a number. In the second part of the first chapter we introduce the H. Lenstra version of the Adleman-Pomerance-Rumely

[1] from Article 329 of Gauss's Disquisitiones Arithmeticae (1801)

primality test, based on Gauss sums. Its running time is bounded by $(\log n)^{c \log \log \log n}$ for some positive constant c. This primality test is deterministic but it only has an "almost" polynomial time. The main reference for this first chapter is Crandall-Pomerance [3].

In August 2002, Agrawal, Kayal and Saxena [1] presented the first deterministic, polynomial-time primality test, called AKS. Even if this primality test is not used in practice, it is very important from a theoretical point of view. In the second chapter we introduce the AKS algorithm and calculate its computational cost. The computational cost of this algorithm is $\mathcal{O}(\log^{21/2+\epsilon} n)$. The main references for this second chapter are [1] and [7].

In the last chapter we introduce another primality test, based on the AKS one. This version done by Lenstra and Pomerance is a deterministic and polynomial test with a computational cost $\widetilde{\mathcal{O}}((\log n)^6)$ (where the notation $\widetilde{\mathcal{O}}(X)$ means a bound $c_1 X (\log X)^{c_2}$ for suitable positive constants c_1, c_2). We also compute its computational cost, and see the main differences between the original AKS primality test and the Lenstra-Pomerance algorithm. The main reference for this last chapter is [9]

Contents

Chapter 1

Two primality tests

1.1 Pseudoprimes

Let $\mathcal{P}$ an easily checkable arithmetic property such that: n is prime $\Rightarrow$ n has the property $\mathcal{P}$. If an integer n has the property $\mathcal{P}$ we say that n is $\mathcal{P}-pseudoprime$. If n doesn't check $\mathcal{P}$ we can conclude that n is composite, otherwise, we are not able to conclude. The main idea is to find such a property (easy to verify) such that the number of pseudoprimes is rare compared to the number of primes, and so if n checks $\mathcal{P}$, we can say that n has a big probability to be a prime.

1.1.1 Fermat pseudoprimes and Carmichael numbers

Theorem 1.1 (Fermat's little theorem)**.** *If n is prime, then for any integer a, we have*

$$a^n \equiv a (\text{mod } \ n). \tag{1.1}$$

Definition 1.1 (Fermat pseudoprimes)**.** *An odd composite number n, for which*

$$a^n \equiv a (\text{mod } \ n)$$

are called pseudoprimes in base a. And they are denoted by $psp(a)$.

For example, $n = 91 = 7 \times 13$ is $psp(3)$ and $105 = 3 \times 5 \times 7$ is $psp(13)$.

Definition 1.2. *Let $x \in \mathbb{R}$, $x > 0$. We define $P_a(x)$ to be the number of $psp(a)$ not exceeding x.*

x	$P_2(x)$	$\pi(x)$	$\frac{P_2(x)}{\pi(x)}$
10^3	3	168	$(1.79)(10^{-2})$
10^4	22	1229	$(1.79)(10^{-2})$
10^5	78	9592	$(8.13)(10^{-3})$
10^6	245	78498	$(3.12)(10^{-3})$
10^7	750	664579	$(1.12)(10^{-3})$
10^8	2057	5761455	$(3.57)(10^{-4})$
10^9	5597	50847534	$(1.1)(10^{-4})$
10^{10}	14884	455052511	$(3.27)(10^{-5})$
10^{11}	38975	4118054813	$(9.46)(10^{-6})$
10^{12}	101629	37607912018	$(2.70)(10^{-6})$
10^{13}	264239	346065536839	$(7.64)(10^{-7})$

Table 1.1: Cardinality of the $psp(2)$ set below x

This table (based on [11] and [8]), let us make the hypothesis that the number of pseudoprimes in base 2 are significantly smaller than $\pi(x)$. In fact in Crandall-Pomerance [3] we have the following theorem.

Theorem 1.2. *For each fixed integer $a \geq 2$, the number of Fermat pseudoprimes in base a that are less or equal to x is $o(\pi(x))$ as $x \to \infty$. That is, Fermat pseudoprimes are rare compared with primes.*

Hence if for a pair n, a (where $1 < a < n - 1$) the equation (1.1) holds, there is a big probability that n is prime; in fact we call it a "probable prime base a", and we denote it $prp(a)$. We also have that:

Theorem 1.3. *For each integer $a \geq 2$ there are infinitely many Fermat pseudoprimes base a.*

Now let us see what's happen for the integer who are pseudoprimes in more than one base, for example 341 is a pseudoprime in base 2 but not in base 3. Testing the pseudoprimality in different basis, we are going to have a bigger probability to be a prime, this idea motivate the following definition:

Definition 1.3 (Carmichael number)**.** *A composite integer n who is $psp(a)$ for every integer $a < n$ such that $(a, n) = 1$ is called a Carmichael number.*

In 1899 Korselt proved the following result, but he did not exhibit an example of such integer n.

Theorem 1.4 (Korselt criterion). *An integer n is a Carmichael number if and only if n is positive, composite, squarefree, and for each prime p dividing n we have $p-1$ dividing $n-1$.*

In 1910 Robert Daniel Carmichael, gave the smallest example $561 = 3 \times 11 \times 17$, and from that moment on these numbers are called Carmichael numbers. Other examples are: $1105 = 5 \times 13 \times 17$, $1729 = 7 \times 13 \times 19$, $2465 = 5 \times 17 \times 29$.

When a number is known to be pseudoprime to several bases, it has more chances to be a Carmichael number, in fact in [11] the result of Pomerance, Selfridge and Wagstaff show us that while only 10% of the $psp(2)$ is below 25×10^9 are Carmichael numbers, 89% of pseudoprimes in bases 2, 3, 5 and 7 simultaneously are Carmichael numbers. Let's see if the Carmichael numbers are finite, in which case we will have an effective primality test.

Definition 1.4. *Let $C(x)$ be the number of Carmichael numbers not exceeding x.*

In 1956 P. Erdös had given an heuristic argument that not only there are infinitely many Carmichael numbers, but there are not as rare as one might expect. He conjectured that for any fixed $\epsilon > 0$, there is a number $x_0(\epsilon)$ such that $C(x) > x^{1-\epsilon}$.

Theorem 1.5. *[Harman] There are infinitely many Carmichael numbers. In particular, for x sufficiently large, $C(x) > x^{0.33}$*

The "sufficiently large" in theorem 1.5 has not been calculated, but probably it is the 96th Carmichael number, 8719309. Now we can ask if we have a "Carmichael number theorem" analog to the "primes number theorem" that give us an asymptotic formula for $C(x)$. Nevertheless there is not even a conjecture of what this formula might be. However, there is a somewhat weaker conjecture.

Conjecture 1.1 (Erdös, Pomerance). *The number $C(x)$ of Carmichael numbers not exceeding x satisfies*

$$C(x) = x^{1-(1+o(1))\log\log\log x/\log\log x} \quad \textit{as } x \to \infty$$

The Fermat's theorem is a first criterion of selection in primality testing, nevertheless we saw that is not so strong. We are going to introduce now an other criterion based on the same idea but this one will allow us to have a better primality test.

1.1.2 Strong pseudoprimes and Miller-Rabin test

Let p be an odd prime number, and a such that $(a, p) = 1$, then by Fermat's little theorem we have $a^{p-1} \equiv 1 (\text{mod } p)$. In particular, if $p = 2m + 1$ we have that:

$$a^{2m} - 1 = (a^m - 1)(a^m + 1) \equiv 0 (\text{mod } p).$$

As p is prime, it must divide one of the two factors. It doesn't divide both because, in this case, it will divide the difference $(a^m + 1) - (a^m - 1) = 2$ and, since p is odd, this is not possible. Thus $a^m \equiv \pm 1 (\text{mod } p)$.
Now let take the decomposition $2^S t + 1$ of p and consider

$$a^{p-1} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1)...(a^{2^{(S-1)}t} + 1),$$

we can do a similar reasoning and we found the following theorem.

Theorem 1.6 (Miller-Rabin). *Suppose that n is an odd prime and $n - 1 = 2^s t$, where t is odd. If a is not divisible by n then*

$$\begin{cases} \textit{either } a^t \equiv (1 \bmod n) \\ \textit{or } a^{2^i t} \equiv -1 (\text{mod } n) \textit{ for some } i \textit{ with } 0 \leq i \leq s - 1. \end{cases} \tag{1.2}$$

Definition 1.5 (Strong pseudoprime). *We say that n is a strong pseudoprime in base a if n is an odd composite number, $n - 1 = 2^s t$, with t odd, and* (1.2) *holds. We denote this property as spsp*(a).

Lets consider some examples: $2047 = 23 \times 89$, $121 = 11^2$ and $781 = 11 \times 71$, are strong pseudoprimes in base 2, 3 and 5, respectively. The least strong pseudoprime simultaneously on bases 2, 3 and 5 is $2315031751 = 151 \times 751 \times 28351$, it is also a Carmichael number, and strong pseudoprime in base 7. Nevertheless the cardinality of strong pseudoprimes in various bases is "small", in [11] we can see that 2315031751 is the only number with this property less than 25×10^9.
In analogy with the probably prime numbers, we can define a "strong probably prime base a" (*i.e.* the natural numbers holding the equation (1.2)) and we denote it by *sprp*(a).

Algorithm 1.1 (Strong probable prime test). *Input: An odd number $n > 3$, represented as $n = 1 + 2^s t$, with t odd and an integer a with $1 < a < n - 1$.*
Output: The algorithm returns either "n is sprp(a)" or "n is composite"

```
1. [Odd part of $n-1$] let $b = a^t \bmod n$; if ($b = 1$ or $b = n-1$) return "n is sprp(a)";

2. [Power of 2 in $n-1$]
   for ($j \in [1, s-1]$){
   $b = b^2 \bmod n$;
   if ($b = n-1$) return "n is sprp(a)";
   }
   return "n is composite";
```

Definition 1.6. *Let $\mathcal{S}(x) = \{a(\bmod n) : n \text{ is a strong pseudoprime base } a\}$ and let $S(x) = \#\mathcal{S}(x)$.*

Theorem 1.7. *For each odd composite integer $n > 9$ we have $S(n) \leq \frac{1}{4}\varphi(n)$, where $\varphi(n)$ is Euler's function evaluated at n.*

See the prove of this theorem in [3].

Definition 1.7. *Let n an odd composite number, we will call "witness" a base for which n is not a strong pseudoprime.*

Theorem 1.7 implies that at least 3/4 of all integers in $[1, n-1]$ are witness for n, when n is an odd composite number. By the algorithm 1.1 we can test if n is *spsp*(a), so we can write an algorithm who decide if the given number a is a witness for n. The following algorithm is often referred as "the Miller-Rabin test", it is a probabilistic test based in the algorithm 1.1 but with a random base a.

Algorithm 1.2 (Miller-Rabin Test)**.** *Input: An odd number $n > 3$.*
Output: a witness for n, if a is a witness return (a, YES), otherwise (a, NO);

```
1. [Choose a possible witness] Choose random by an integer $a \in [2, n-2]$; using algorithm
   1.1 we decide whether $n$ is strong probable prime base $a$;

2. [declaration] if ($n$ is a sprp($a$)) return (a,NO);
   return (a,YES);
```

By theorem 1.7, the probability that the Algorithm fails to produce a witness for n is $< 1/4$, so if we repeat the algorithm 1.2 k independent times, the probability for it to fails is $< 1/4^k$. If the output of the k repetition of this algorithm doesn't give a witness, we can only make a conjecture that n is prime, with a probability bigger than $1 - 1/4^k$.

Now, let $W(n)$ be the least of the witnesses for n, we want to know if it exists a bound $B \in \mathbb{N}$ not so large such that for all odd composite number N we have $W(n) \leq B$. In this case, we can make a primality test, repeating algorithm 1.1 for all $2 \leq a \leq B$, and we will have a polynomial, deterministic test. Unfortunately, such B doesn't exist. In 1994 Alford, Granville and Pomerance shown that:

Theorem 1.8. *There are infinitely many odd composite numbers n with*

$$W(n) > (\log n)^{1/(3 \log\log\log n)}.$$

In fact, the number of such composite numbers n up to x is at least $x^{1/(35 \log\log\log x)}$ when x is sufficiently large.

Nevertheless Bach, based on Miller's work, proved that there exist a slowly growing function of n which is always greater than $W(n)$ if the Extended Riemann Hypothesis (ERH) is true:

Theorem 1.9. *Assuming the ERH, $W(n) < 2\log^2 n$ for all odd composite numbers n.*

For the proof, see [3].

Now we are going to introduce the Miller primality test, that is a polynomial deterministic test if the Riemann hypothesis holds, in this case we say that the algorithm is conditioned.

Algorithm 1.3 (Miller primality test)**.** *Input: an odd number $n > 1$.*
Output: The answer to the question: is n prime? The output is "NO" if n is composite, and "YES" if either n is prime or the extended Riemann hypothesis is false.

```
1. [Witness bound ] $W = \min\{\lfloor 2\log^2 n, n-1 \rfloor\}$;

2. [Strong probable prime test] for ($2 \leq a \leq W$) { By algorithm 1.1 decide whether $n$ is
   sprp($a$), if it is return NO; }
   return YES;
```

Using log instead of $\log_2$ to simplify the equation, we have that the running time of the algorithm 1.1 is $\mathcal{O}(\log^3 n)$ and as we have to repeat it at most $\log^2 n$, the computational cost of this primality test is $\mathcal{O}(\log^5 n)$ bit operations.

1.2 Gauss sums primality test

In this section, we are going to introduce the Adleman-Pomerance-Rumely primality test, based on Gauss sums, whose running time is bounded by $(\log n)^{c \log\log\log n}$ for some positive constant c. We are going to introduce the H. Lenstra version which is less practical, but simpler.

Definition 1.8 (Dirichlet Character to the modulus q)**.** *Suppose q a positive integer and χ is a function from the integers to the complex numbers such that*

1. *For all integers m,n, $\chi(mn) = \chi(m)\chi(n)$.*
2. *χ is periodic modulo q.*
3. *$\chi(n) = 0$ if and only if $gcd(n, q) > 1$.*

Let q be a prime with primitive root g. If ζ is a complex number with $\zeta^{q-1} = 1$, then we can build a character χ to the modulus q via $\chi(g^k) = \zeta^k$ for every integer k (and of course, $\chi(m) = 0$ if m is a multiple of q).

Definition 1.9. *Let $\zeta_n = e^{2\pi i/n}$ (a primitive n-th root of 1), we define $\tau(\chi)$ the Gauss sum by*

$$\tau(\chi) = \sum_{m=1}^{q-1} \chi(m)\zeta_q^m.$$

We have that

$$\tau(\chi) = \sum_{k=1}^{q-1} \chi(g^k)\zeta_q^{g^k} = \sum_{k=1}^{q-1} \zeta^k \zeta_q^{g^k}$$

As $\tau(\chi)$ is a character modulo q, we know that his order is a divisor of $q-1$. Now suppose that p is a prime factor of $q-1$. We wish to build such a character $\chi_{p,q}$ modulus q and of order p. Suppose $g = g_q$ is the least positive root for q, we can build such a character as follows: $\chi_{p,q}(g_q^k) = \zeta_p^k$ for every integer k.

$\chi_{p,q}$ is in fact defined to the modulus q since $\zeta_p^{q-1} = 1$, and it has order p since $\chi_{p,q}(m)^p = 1$ for every nonzero residue $m \bmod q$ and $\chi_{p,q}(g_q) \neq 1$. Let

$$G(p,q) = \tau(\chi_{p,q}) = \sum_{m=1}^{q-1} \chi_{p,q}(m)\zeta_q^m = \sum_{k=1}^{q-1} \zeta_p^k \zeta_q^{g_q^k} = \sum_{k=1}^{q-1} \zeta_p^{k \bmod p} \zeta_q^{g_q^k \bmod q}.$$

The Gauss sum is an element of the ring $\mathbb{Z}[\zeta_p, \zeta_q]$. The elements of this ring can be expressed uniquely as sums $\sum_{j=0}^{p-2} \sum_{k=0}^{q-2} a_{j,k}\zeta_p^j \zeta_q^k$ where each $a_{j,k} \in \mathbb{Z}$. Note that if α is in $\mathbb{Z}[\zeta_p, \zeta_q]$, then the same happens for its complex conjugate $\overline{\alpha}$. We say that two element of this ring are congruent modulo n if the coefficients are congruent modulo n. It's important to note that ζ_p, ζ_q are treated as symbols.

Lemma 1.1. *If p,q are primes with $p|q-1$, then $G(p,q)\overline{G(p,q)} = q$.*

For the proof of this lemma see [3]. The following result can be viewed as an analogue to Fermat's little theorem we have described in the previous section.

Lemma 1.2. *Suppose p, q, n are primes with $p|q-1$ and $gcd(pq, n) = 1$. Then*

$$G(p,q)^{n^{p-1}-1} \equiv \chi_{p,q}(n) (\bmod\ n).$$

Proof. Let $\chi = \chi_{p,q}$. Since n is prime, by the multinomial theorem we have that

$$G(p,q)^{n^{p-1}} = \Big(\sum_{m=1}^{q-1} \chi(m)\zeta_q^m\Big)^{n^p-1} \equiv \sum_{m=1}^{q-1} \chi(m)^{n^{p-1}} \zeta_q^{mn^{p-1}} (\bmod\ n).$$

By Fermat's little theorem, $n^p - 1 \equiv 1 (\bmod\ p)$, so that $\chi(m)^{n^{p-1}} = \chi(m)$. Letting n^{-1} denote a multiplicative inverse of n modulo q, we have

$$\sum_{m=1}^{q-1} \chi(m)^{n^{p-1}} \zeta_q^{mn^{p-1}} = \sum_{m=1}^{q-1} \chi(m)\zeta_q^{mn^{p-1}} = \sum_{m=1}^{q-1} \chi(n^{-(p-1)})\chi(mn^{p-1})\zeta_q^{mn^{p-1}}.$$

As $\chi(n^p) = \chi(n)^p = 1$, and mn^{p-1} runs over a residue system $(\bmod\ q)$ as m does, we have

$$\sum_{m=1}^{q-1} \chi(m)^{n^{p-1}} \zeta_q^{mn^{p-1}} = \chi(n) \sum_{m=1}^{q-1} \chi(mn^{p-1})\zeta_q^{mn^{p-1}} = \chi(n)G(p,q).$$

Hence we have that

$$G(p,q)^{n^{p-1}} \equiv \chi(n)G(p,q)(\bmod\ n).$$

Letting q^{-1} be a multiplicative inverse of q modulo n and multiplying this last displayed equation by $q^{-1}\overline{G(p,q)}$, by lemma 1.1 we have the desired result. □

In some cases the congruence can be replaced by an equality, as we can see in the following lemma.

Lemma 1.3. *If m, n are natural numbers with m not divisible by n and $\zeta_m^j \equiv \zeta_m^k (\bmod\ n)$, then $\zeta_m^j = \zeta_m^k$.*

For the proof of this lemma see [3].

Definition 1.10. *Suppose p, q are distinct primes. If $\alpha \in \mathbb{Z}[\zeta_p, \zeta_q] \setminus \{0\}$, where*

$$\alpha = \sum_{i=0}^{p-2} \sum_{k=0}^{q-2} a_{i,k} \zeta_p^i \zeta_q^k,$$

denote by $c(\alpha)$ the greatest common divisor of the coefficients $a_{i,k}$. Further, let $c(0) = 0$.

Let's see now the deterministic Gauss sum primality test.

Algorithm 1.4 (Gauss sums primality test)**.** *Input: $n \in \mathbb{Z}$.*
Output: The algorithm decide whether n is prime or composite, returning "n is prime" or "n is composite" in the appropriate case.

```
1. [ Initialize ] $I = -2$;

2. [Preparation] $I = I + 4$;
   Find the prime factors of $I$ by trial division, if $I$ is not squarefree, go to [Preparation];
   Let $F = \prod_{(q-1)|I} q$, if $F \leq n$ go to [Preparation]; note that $F$ is squarefree and $F > \sqrt{n}$;
   If $n$ is a prime factor of $I \cdot F$, return "n is prime" ;
   If $gcd(n, I \cdot F) > 1$, return "n is composite";
   For (prime $q|F$) find the least positive root $g_q$ for $q$.

3. [Probable prime computation ]
   For (prime $p|I$) factor $n^{p-1} - 1 = p^{s_p} u_p$ where $p$ does not divide $u_p$;
   For (primes $p, q$ with $p|I, q|F, p|q-1$)
   {       Find the first positive integer $w(p,q) \leq s_p$ with

                 $G(p,q)^{p^{w(p,q)u_p}} \equiv \zeta_p^j (\bmod\ n)$ for some integer $j$,

           If no such number is found, return "n is composite" .
   }
```

```
4. [Maximal order search]
   For (prime $p|I$) set $w(p)$ equal to the maximum of $w(p,q)$ over all primes $q|f$ with $p|q-1$,
   and set $q_0(p)$ equal to the least such prime $q$ with $w(p) = w(p,q)$;
   For (primes $p, q$ with $p|I$, $p|F$, $p|q-1$) find an integer $l(p,q) \in [0, p-1]$ with
   $G(p,q)^{p^{w(p)}u_p} \equiv \zeta_p^{l(p,q)} (\bmod\ n)$;

5. [Coprime check]
   For (prime $p$ with $p|I$)
   {$H = G(p, q_0(p))^{p^{w(p)-1}u_p} \bmod\ n$;
   for $(0 \leq j \leq p-1)\{$
   if(gcd$(n, c(H - \zeta_p^j)) > 1)$ (with notation from definition 1.10) return “n is composite”;
   }
   }

6. [Divisor search]
   l(2)=0;
   For (odd prime $q|F$) use the Chinese Remainder Theorem to build an integer $l(q)$ with

       $l(q) \equiv l(p,q) (\bmod\ p)$ for each prime $p|q-1$.

   Use the Chinese remainder theorem to construct an integer $l$ with

       $l \equiv g_q^{l(q)} (\bmod\ q)$ for each prime $q|F$

   For $(i \leq j < I)$, if $l^j \bmod\ F$ is a nontrivial factor of $n$, return “n is composite”;


   Return “n is prime”;
```

Correctness :

Clearly the declaration of prime and composite in step [Preparation] is correct. By the lemma 1.2 the declaration in step [Probable prime computation] is also true. In step [Coprime check] if the *gcd* is not 1, it is clear that n is composite, so algorithm's reply is correct. For sure in step [Divisor search], the declaration of composite is true. What remains to prove is: if n is composite, it has to stop in one of these steps, if not it will be declared prime at the end of the algorithm.

To prove this, suppose n is a composite number with least prime factor r, and suppose n has survived steps 1-5. We will need two claims:

Claim 1:

$$p^{w(p)} | (r^{p-1} - 1) \text{ for each prime } p|I. \tag{1.3}$$

For each prime $p|I$, (1.3) implies there are integers a_p, b_p with

$$\frac{r^{p-1} - 1}{p^{w(p)} u_p} = \frac{a_p}{b_p}, \qquad b_p \equiv 1 (\text{mod } p). \tag{1.4}$$

Let a be such that $q \equiv a_p(\text{mod } p)$ for each prime $p|I$.

Claim 2:

$$r \equiv l^a (\text{mod } F). \tag{1.5}$$

Thus, if n is composite, and it has survived steps 1-5, since $F \geq \sqrt{n} \geq r$ and $F \neq r$, we have that r is equal to the least positive residue of $l^a(\text{mod } F)$. So that the proper factor r of n will be discovered in step [Divisor search] and the algorithm will declare n composite as desired. We can conclude now that the algorithm is deterministic. Let's now prove the two claims:

Proof of claim 1: is clear that (1.3) is true if $w(p) = 1$, so assume $w(p) \geq 2$. Suppose some $l(p, q) \neq 0$. Then by lemma 1.3: $G(p, q)^{p^{w(p)u_p}} \equiv \zeta_p^{l(p,q)} \not\equiv 1(\text{mod } n)$, and the same is true mod r. Let h the multiplicative order of $G(p, q)$ modulo r, so that $p^{w(p)+1}|h$. But lemma 1.2 implies that $h|p(r^{p-1} - 1)$, so that $p^{w(p)}|r^{p-1} - 1$, as claimed. Now suppose that each $l(p, q) = 0$. Then from the step [Coprime check] we have:

$$G(p, q_0)^{p^{w(p)}u_p} \equiv 1(\text{mod } r), \quad G(p, q_0)^{p^{w(p)-1}u_p} \not\equiv \zeta_p^j(\text{mod } r)$$

for all j. Moreover, letting h be the multiplicative order of $G(p, q_0)$ modulo r, we have $p^{w(p)}|h$. Also, since $G(p, q_0)^m \equiv \zeta_p^j(\text{mod } r)$ for some integers m, j we get $\zeta_p^j = 1$. Lemma 1.2 then implies that $G(p, q_0)^m \equiv 1(\text{mod } r)$ so that $h|r^{p-1} - 1$ and $p^{w(p)}|h$. This complete the proof of claim 1.

Proof of claim 2: By definition of $\chi_{p,q}$ and l we have

$$G(p, q)^{p^{w(p)}u_p} \equiv \zeta^{l(p,q)} = \zeta^{l(q)} = \chi_{p,q}(l)(\text{mod } r)$$

for every pair of primes p, q with $q|F, p|q-1$. Thus, from (1.4) and Lemma 1.2

$$\chi_{p,q}(r) = \chi_{p,q}(r)^{b_p} \equiv G(p,q)^{(r^{p-1}-1)b_p} = G(p,q)^{p^{w(p)}u_p a_p} \equiv \chi_{p,q}(l)^{a_p} = \chi_{p,q}(l^a) (\text{mod } r).$$

Hence by Lemma 1.3 we have that $\chi_{p,q}(r) = \chi_{p,q}(l^a)$.

The product of characters $\chi_{p,q}$ for p prime, and $p|I$ and $p|q-1$, is a character χ_q of order $\prod_{p|q-1} p = q-1$, as $q-1|I$ and I is squarefree. Bur a character mod q of order $q-1$ is one-to-one on $\mathbb{Z}/q\mathbb{Z}$, so as

$$\chi_q(r) = \prod_{p|q-1} \chi_{p,q}(r) = \prod_{p|q-1} \chi_{p,q}(l^a) = \chi_q(l^a).$$

This way we have that $r \equiv l^a (\text{mod } q)$. Since this hold for each prime $q|F$ and F is squarefree, it follows that (1.5) holds.

Computational cost:

The running time is bounded by a fixed power of I, by the following result from Crandall-Pomerance [3]

Theorem 1.10. *Let $I(x)$ be the least positive squarefree integer I such that the product of the primes p with $p-1|I$ exceeds x. Then there is a positive number c such that $I(x) < ln(x)^{c \log\log\log x}$ for all $x > 16$.*

The reason for assuming $x > 16$ is to ensure that the triple-logarithm is positive.

Thus the running time is bounded by $(\log n)^{c \log\log\log n}$ for some positive constant c. Since the triple log function grows so slowly, this running-time bound is “almost” $\log^{\mathcal{O}(1)}$, and so is “almost” polynomial time.

With some extra work we can extend the Gauss sums primality test to the case where I is not assumed squarefree. This extra degree of freedom allows for a faster test. There are several ways to improve the running time of this test in practice, but the main one is to use Jacobi sums instead of Gauss sums. In fact the Gauss sums $G(p,q)$ are in the ring $\mathbb{Z}[\zeta_p, \zeta_q]$. Doing arithmetic in this ring modulo n requires dealing with vectors with $(p-1)(q-1)$ coordinates, each one being a residue modulo n. Let's define the Jacobi sum $J(p,q)$ as follows

$$J(p,q) = \sum_{m=1}^{q-2} \chi_{p,q}(m^b(m-1)).$$

This sum lies in the much smaller ring $\mathbb{Z}[\zeta_p]$, and so doing arithmetic with this sums is much faster that with the Gauss ones.

We have seen in this first chapter two different primality tests used in practice. The first one is conditioned to the ERH, and the second one is deterministic, but its time is “almost” polynomial. In August 2002, Agrawal, Kayal and Saxena [1] presented the first deterministic, polynomial-time primality test, called AKS. Even if this primality test is not used in practice, it is very important from a theoretical point of view. In the following chapter we are going to introduce this primality test and calculate its computational cost.

Chapter 2

The Agrawal-Kayal-Saxena primality test

In this chapter we will use $\log(x)$ to denote logarithm in base 2, to simplify the equations.

We saw in the introduction that the main idea is to find a certain property $\mathcal{P}$ of the prime numbers such that:

$$n \text{ is prime} \Leftrightarrow n \text{ has the property } \mathcal{P}.$$

And such that the condition of $\mathcal{P}$ can be verified in a "short" time. The AKS is based on the following theorem:

Theorem 2.1. *An integer $n \geq 2$ is prime $\Leftrightarrow$ $(x+a)^n \equiv x^n + a \pmod{n}$.*

Proof. Since $(x+a)^n - (x^n+a) = \sum_{1 \leq j \leq n-1} \binom{n}{j} x^j a^{n-j}$, we have that $(x+a)^n \equiv x^n + a \ (\bmod\ n)$ if and only if n divides $\binom{n}{j} x^j a^{n-j}$ for all $j = 1, \ldots, n-1$.
If $n = p$ is prime, then p appears at the numerator of $\binom{p}{j}$ but it is larger, and so does not divide any term in the denominator. Hence p divides $\binom{p}{j}$ for $j = 1, \ldots, p-1$, and so we have that the congruence holds.
Now if n is composite, let p be a prime dividing n, and α such that p^α is the largest power of p dividing n. As

$$\binom{n}{p} = \frac{n(n-1)(n-2)\ldots(n-(p-1))}{p(p-1)\ldots 1},$$

we see that $p^{\alpha-1}$ is the largest power of p dividing $\binom{n}{p}$, therefore $n \nmid \binom{n}{p}$ and the congruence doesn't hold. □

The problem is that we have to compute $(x+a)^n$, which can't be done in a polynomial time, one solution can be compute module some smaller polynomial as well as (mod n), so that neither the coefficients or the degree get larger. For example:

$$(x+a)^n \equiv x^n + a \pmod{n, x^r - 1} \ \forall a \in \mathbb{N}. \tag{2.1}$$

We have to check now if (2.1) is equivalent to the primality of n and which conditions are needed for r.

Theorem 2.2 (AKS). *For a given integer $n \geq 2$, let r be a positive integer such that $r < n$ and $d := \operatorname{ord}(n \bmod r) > \log^2 n$. Then n is prime $\Leftrightarrow$*

1. *n is not a perfect power,*
2. *n does not have any prime factor $\leq r$,*
3. *$(x+a)^n \equiv x^n + a \mod (n, x^r - 1)$ for each integer a, $1 \leq a \leq \sqrt{r}\log n$.*

Proof. ($\Rightarrow$) If n is a prime number, conditions 1. and 2. are trivial, and by theorem 2.1 the condition 3. is verified.
($\Leftarrow$) suppose 1. 2. and 3. and let show by contradiction that n is prime: suppose that n is composite, p is a prime divisor of n and $A = \sqrt{r}\log n$. By the condition 3. we have

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

for each integer a, $1 \leq a \leq \lfloor A \rfloor$. We can factor $x^r - 1$ into irreducible polynomials in $\mathbb{Z}[x]$, as $\prod_{d|r} \Phi_d(x)$, where $\Phi_d(x)$ is the $d-th$ cyclotomic polynomial, whose roots are the primitive $d-th$ roots of unity. Each $\Phi_r(x)$ is irreducible in $\mathbb{Z}[x]$, but may not be irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, so let $h(x)$ be an irreducible factor of $\Phi_r(x) (\bmod\ p)$. Then 2.2 implies that

$$(x+a)^n \equiv x^n + a \mod (p, h(x)) \tag{2.3}$$

for each integer a, $1 \leq a \leq \lfloor A \rfloor$, since $(p, h(x))$ divides $(p, x^r - 1)$. The congruence classes $\bmod\ (p, h(x))$ can be viewed as the elements of the ring $\mathbb{F} :\equiv \mathbb{Z}[x]/(p, h(x))$, which is isomorphic to the field of p^m elements (where m is the degree of h). In particular the non-zero element of $\mathbb{F}$ form a cyclic group of order $p^m - 1$, moreover, $\mathbb{F}$ contains x, an element or order r, thus r divides $p^m - 1$. Since $\mathbb{F}$ is isomorphic to a field, the congruences 2.3 are much more easier to work with than 2.2, where the congruence do not correspond to a field. Let H the elements $\mathrm{mod}(p, x^r - 1)$ generated multiplicatively by

$$\{(x + a) \ : 0 \leq a \leq \lfloor A \rfloor\}$$

and G the cyclic subgroup of $\mathbb{F}$ (i.e $\mathrm{mod}(p, h(x))$) generated multiplicatively by

$$\{(x + a) \ : 0 \leq a \leq \lfloor A \rfloor\}.$$

In other words G is the reduction of H $\mathrm{mod}(p, h(x))$. All the elements of G are non-zero, in fact if $x^n + a = 0$ in $\mathbb{F}$, then $x^n + a = (x + a)^n = 0$ in $\mathbb{F}$ by (2.3), so that $x^n = -a = x$ in $\mathbb{F}$, which would imply that $n \equiv 1(\mathrm{mod} r)$ and so $d = 1$, contradicting the hypothesis that $d > \log^2 n$. Note that an element $g \in H$ can be written as $g(x) = \prod_{0 \leq a \leq \lfloor A \rfloor}(x + a)^{e_a}$, then by (2.2)

$$g(x)^n = \prod_a ((x + a)^n)^{e_a} \equiv \prod_a (x^n + a)^{e_a} = g(x^n) \bmod (p, x^r - 1).$$

Let define

$$S = \{k \in \mathbb{N} : g(x^k) \equiv g(x)^k \bmod (p, x^r - 1) \quad \forall g \in H\}$$

note that $n \in S$ by the condition 3. and that $p \in S$ by Theorem 2.1.

Our aim now is to give upper and lower bounds on the size of G to establish a contradiction, and so n must be prime. Let's first found an upper bound of $|G|$:

Lemma 2.1. *If a, $b \in S$, then $ab \in S$.*

Proof. If $g(x) \in H$, then $g(x)^b \equiv g(x^b) \bmod (p, x^r - 1)$, and so, replacing x by x^a, we get $g((x^a)^b) \equiv g(x^a)^b \bmod (p, (x^a)^r - 1)$, and therefore $\mathrm{mod}(p, x^r - 1)$ since $x^r - 1$ divides $x^{ar} - 1$. Therefore

$$g(x)^{ab} = (g(x)^a)^b \equiv g((x^a)^b) \equiv g((x^a)^b) = g(x^{ab}) \bmod (p, x^r - 1)$$

as desired. □

Lemma 2.2. *If a, $b \in S$, and $a \equiv b(\mathrm{mod} r)$, then $a \equiv b \mod |G|$.*

Proof. For any $g(x) \in \mathbb{Z}[x]$ we have that $u - v$ divides $g(u) - g(v)$. Therefore $x^r - 1$ divides $x^{a-b} - 1$, which divides $x^a - x^b$, which divides $g(x^a) - g(x^b)$; and so we deduce that if $g(x) \in H$, then $g(x)^a \equiv g(x^a) \equiv g(x^b) \equiv g(x)^b \bmod (p, x^r - 1)$. Thus if $g(x) \in G$, then $g(x)^{a-b} \equiv 1$ in $\mathbb{F}$; but G is a cyclic group, so taking g to be a generator of G we deduce that $|G|$ divides $a - b$. □

Lemma 2.3. *$n/p \in S$.*

Proof. Suppose that $a \in S$ and $b \equiv a \bmod (n^d - 1)$ (where $d = \mathrm{ord}(n \bmod r)$). Let show that $b \in S$: as $n^d \equiv 1 \bmod r$, we have that $x^{n^d} \equiv x \bmod (x^r - 1)$. Then $x^r - 1 | (x^{n^d} - x)$, which divides $x^b - x^a$, which divides $g(x^b) - g(x^a)$ for any $g(x) \in \mathbb{Z}[x]$. If $g(x) \in H$, then $g(x)^{n^d} \equiv g(x^{n^d}) \bmod (p, x^r - 1)$ by Lemma 2.1 since $n \in S$, and $g(x^{n^d}) \equiv g(x) \bmod (p, x^r - 1)$(as $x^r - 1$ divides $x^{n^d} - x$) so that $g(x)^{n^d} \equiv g(x) \bmod (p, x^r - 1)$. But then $g(x)^b \equiv g(x)^a \bmod (p, x^r - 1)$ since $n^d - 1$ divides $b - a$. Therefore

$$g(x^b) \equiv g(x^a) \equiv g(x)^a \equiv g(x)^b \bmod (p, x^r - 1)$$

since $a \in S$, which implies that $b \in S$. Therefore we have that $a \in S$ and $b \equiv a \bmod (n^d - 1)$ implies $b \in S$.
Now let $b = n/p$ and $a = np^{\phi(n^d-1)-1}$, so that $a \in S$ by Lemma 2.1 since $p, n \in S$. And $b \equiv a \bmod (n^d - 1)$ thus $b = n/p \in S$. □

Let now R be the subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$ generated by n and p. Since n is not a power of p, the integer $n^i p^j$ with $i, j \geq 0$ are distinct, and

$$|\{n^i p^j, 0 \leq i, j \leq \sqrt{|R|}\}| > |R|$$

and so two must be congruent $\bmod r$, say $n^i p^j \equiv n^I p^J \bmod r$. By Lemma 2.1 these integers are both in S, and by Lemma 2.2 their difference is divisible by $|G|$, and therefore

$$|G| \leq |n^i p^j - n^I p^J| \leq (np)^{\sqrt{|R|}} - 1 < n^{2\sqrt{|R|}} - 1.$$

Note that $n^i p^j - n^I p^J$ is non-zero since n is neither a prime nor a perfect power. By Lemma 2.3 we have $n/p \in S$, replacing n by n/p in the argument above we get

$$|G| \leq n^{\sqrt{|R|}} - 1. \tag{2.4}$$

Let's found now the lower bound of $|G|$:

Lemma 2.4. *Suppose that $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x) \equiv g(x) \mod (p, h(x))$ and that the reduction of f and g in $\mathbb{F}$ both belong to G. If f and g both have degree $< |R|$, then $f(x) \equiv g(x) \pmod p$.*

Proof. Consider $\Delta(y) := f(y) - g(y) \in \mathbb{Z}[y]$ as reduced in $\mathbb{F}$. If $k \in S$, then

$$\Delta(x^k) = f(x^k) - g(x^k) \equiv f(x)^k - g(x)^k \equiv 0 \mod (p, h(x)).$$

As x has order r in $\mathbb{F}$, we have that $\{x^k : k \in R\}$ are all distinct roots of $\Delta(y)$ mod $(p, h(x))$. Now, $\Delta(y)$ has degree $< |R|$ (since f and g both have degree $< |R|$), but has $\geq |R|$ distinct roots $mod(p, h(x))$, and so $\Delta(y) \equiv 0(\text{mod} p)$ since its coefficients are independent of x. □

By definition R contains all the elements generated by $n \bmod r$, and so R is at least as large as d, the order of $n \bmod r$, which is $> \log^2 n$ by assumption. Therefore taking $B := \left\lfloor \sqrt{|R|} \log\ n \right\rfloor$ we have $A = \sqrt{r} \log\ n > B$ (since $|R| < r$), and $|R| > B$. We can see that for every proper subset T of $\{0, 1, 2, \dots, B\}$, the product $\prod_{a \in T}(x + a)$ give distinct elements of G. In fact if there exist two proper subset T_1, T_2 of $\{0, 1, 2, \dots, B\}$ such that $\prod_{a \in T_1}(x + a) = \prod_{b \in T_2}(x + b)$ in G, thus by the lemma 2.4 this two product will be identical also in $\mathbb{Z}_p[x]$, and so there will exist a pair $a \neq b$ such that $p | a - b$. As $a, b \leq B < \sqrt{r} \log\ n$, we have that $p < \sqrt{r} \log\ n$. But by the condition 2. we know that $p > r$, hence $r < \log^2\ n$, which contradict the fact that $d > \log^2\ n$. And so as the number un subset of a finite set U is $2^{|U|} - 1$ and $n = 2^{\log n}$, we have:

$$|G| \geq 2^{B+1} - 1 = 2^{\left\lfloor \sqrt{|R|} \log n \right\rfloor + 1} - 1 > 2^{\left\lfloor \sqrt{|R|} \log n \right\rfloor} - 1 > n^{\sqrt{|R|}} - 1, \tag{2.5}$$

which contradicts 2.4, hence the hypothesis that n is composite is false, and this completes the proof of the theorem of AKS. □

This theorem is based in the existence of this r, which exists by the following lemma:

Lemma 2.5. *Let $n \geq 4$, there is at least an integer $r < \lceil \log^5 n \rceil$ such that $d = \text{ord}(n \bmod\ r) > \log^2 n$.*

To prove Lemma 2.5 we need this result:

Lemma 2.6 (Nair)**.** *Let* $m \in \mathbb{N}$ *and* $m \geq 7$. *Then* $\operatorname{lcm}\{1, \ldots, m\} \geq 2^m$

Proof. Of Lemma 2.5. Note that as $n \geq 4$, $\lceil \log^5 n \rceil \geq 32$, thus we can apply Nair's lemma. Let $V = \lceil \log^5 n \rceil$,

$$\mathcal{V} = \{s \in \{1, \ldots, V\} : s \nmid n^{\lfloor \log V \rfloor} \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)\}$$

and $\pi_1 = n^{\lfloor \log V \rfloor} \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$

By contradiction, suppose $\mathcal{V} = \emptyset$. In this case $\forall s \in \{1, \ldots, V\}$, $s \mid \pi_1$, thus $\operatorname{lcm}\{1, \ldots, V\}$ divide π_1. But

$$\pi_1 \leq n^{\lfloor \log V \rfloor + \sum_{i=1}^{\lfloor \log^2 n \rfloor} i} = n^{\lfloor \log V \rfloor + (1/2) \lfloor \log^2 n \rfloor (\lfloor \log^2 n \rfloor + 1)} < n^{\lfloor \log^4 n \rfloor} < 2^V$$

since $n^{\lfloor \log^4 n \rfloor} = (2^{\lfloor \log n \rfloor})^{\lfloor \log^4 n \rfloor} < 2^{\lceil \log^5 n \rceil} = 2^V$.

Hence $\operatorname{lcm}\{1, \ldots, V\} < 2^V$, but, by Lemma 2.6, we get $\operatorname{lcm}\{1, \ldots, V\} \geq 2^V$, thus we have a contradiction and $\mathcal{V}$ is not empty.

Let $r = \min\ \mathcal{V}$ and q a prime divisor of r. We have that

$$\max\{\alpha \in \mathbb{N} : q^\alpha | r\} \leq \lfloor \log V \rfloor$$

then $r | \prod_{q|r} q^{\lfloor \log V \rfloor}$. Note that if every prime $p|r$ divides n, we will have $r | \prod_{q|r} q^{\lfloor \log V \rfloor} | n^{\lfloor \log V \rfloor}$ thus $r | \pi_1$ and $r \notin \mathcal{V}$. Therefore not all the prime divisor of r divide n, thus $(r, n) < r$. Let $s = \frac{r}{(r,n)}$, by the previous result $s \neq 1$. $s \in \mathcal{V}$, in fact if $s \notin \mathcal{V}$, taking $r = \prod_{p|r} p^{\alpha_r}$, for each $p|r$ and $p \nmid n$ we will have that $p^{\alpha_r} | \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$, and for each $p|r$ and $p|n$, as $\alpha_r \leq \lfloor \log V \rfloor$, we will have $p^{\alpha_r} | n^{\lfloor \log V \rfloor}$ and so $r | \pi_1$, which contradict the definition of r. Since $r = \min\ \mathcal{V}$, and as $s \leq r$ and $s \in \mathcal{V}$ we must have that $r = s$ *i.e.* $(r, n) = 1$. Therefore as $r \nmid \pi_1$ and $r \nmid n$ we have that $r \nmid \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$ and so we have that $\operatorname{ord}(n \bmod\ r) > \log^2 n$.

□

Algorithm 2.1. *AKS primality test*

1. *If* $n = \alpha^\beta$, *with* $\alpha, \beta \in \mathbb{N}$ *and* $\beta > 1$, *return "n is composite";*

2. *Find the least integer* r *with* d *(the order of* n *in* $\mathbb{Z}_r^*$*)* $\geq \lceil \log^2 n \rceil$*;*

3. *If $1 < (b,n) < n$ for some $b \leq r$, return "n is composite";*

4. *If $n \leq r$, return "n is prime";*

5. *For all integer b, $1 \leq b \leq \sqrt{r}\ \log n$ we check if*

$$(x+b)^n \not\equiv x^n + b (\text{mod } x^r - 1, n);$$

in this case return "n is composite";

6. *return "n is prime".*

Correctness:

If n is prime: is clear that the algorithm can't stop in steps 1 or 3 and by Theorem 2.1, it can't neither stop in step 5. Hence the algorithm must stop in steps 4 or 6, and in this cases the algorithm returns "n is prime" as desired.

Let's show that if the algorithm stops in steps 4 or 6, the input is really a prime number. Therefore, if the input is a composite number, it will stop in the other steps and the output will be "n is composite" as desired.

If the algorithm stops in the step 4, it means that: $n \leq r$, and that it didn't stop in the step 3, thus $\forall b < n$ we have $(b,n) = 1$ and clearly n is prime.

If the algorithm stops in the step 6: conditions 1) and 2) from the AKS theorem are verified, since in the step 1 we saw n is not a perfect power and in step 3 that it doesn't have any prime factor $\leq r$. In the step 5 we verified condition 3) and in the step 2, we verified the hypothesis of the order on n (mod r). Hence, by the AKS theorem, n is in fact a prime number.

Therefore the AKS primality test is a deterministic algorithm.

Computational complexity:

The following table presents the computational cost of the operation we will need to calculate the computational cost of the AKS algorithm, for the proof of this result see appendix A and Crandall-Pomerance [3]. We supposed $a \leq n$.

Step 1: "If $n = \alpha^\beta$, with $\alpha, \beta \in \mathbb{N}$ and $\beta > 1$". Let $L = \lceil \log\ n \rceil$. For every $k \in \mathbb{N}$ such that $1 \leq k \leq L$ we take $a = \lfloor n^{1/k} \rfloor$ and then we verify if $a^k = n$. For each k we need to compute one square root with a cost of $\mathcal{O}(\log^{2+\epsilon}\ n)$, and one exponentiation into k which has

	Method	Complexity
$n \pm a$		$\mathcal{O}(\log n)$
$n.a$		$\mathcal{O}(\log^2 n)$
(n, a)	Euclidean Algorithm	$\mathcal{O}(\log^2 n)$
n^k	Repeated squaring method	$\mathcal{O}(\log^2 n \log\ k)$
$\sqrt{n}$	Newton method	$\mathcal{O}(\log^{2+\epsilon} n)$
$n^k \pmod r$	Repeated squaring method	$\mathcal{O}(\log\ k\ \log^2\ r)$
$(x+a)^n \pmod{n, x^r - 1}$		$\mathcal{O}(r^2 \log^3 n)$

Table 2.1: Some computational cost.

a cost of $\mathcal{O}(\log^{2+\epsilon}\ n)$ (is $\mathcal{O}(\log^2\ n\ \log\ k)$ with $k < \lceil \log\ n \rceil$), we do this L times. Thus the computational complexity of this step is $\mathcal{O}\big(\log^{3+\epsilon}\ n\big)$.
Step 2: "Find the least integer r with d (the order of n in $\mathbb{Z}_r^*$) $\geq \lceil \log^2 n \rceil$": by the lemma 2.5 we know that $r \leq \lceil \log^5\ n \rceil$. For a fix r we can compute $n^k (\text{mod } r)\ \forall k \leq \log^2\ n$.
Each step takes $\mathcal{O}(\log\ k\ \log^2\ r\ \log^2 n)$. Since $k \leq \log^2\ n$, the total cost is $\mathcal{O}(\log^{2+\epsilon}\ n)$. Therefore the computational complexity of step 2 is: $\mathcal{O}(\log^{7+\epsilon}\ n)$.
Step 3: "Compute (b, n) for all $b \leq r$": we have to compute r gcd's with cost $\mathcal{O}(\log^2\ \max(r, n))$. Therefore the computational complexity of step 3 is: $\mathcal{O}(r \log^2\ \max(r, n))$. As $r \leq \lceil \log^5\ n \rceil$, for a sufficiently large [1] n the computational complexity of step 3 is: $\mathcal{O}(\log^7\ n)$.
Step 5: "For all integer b, $1 \leq b \leq \sqrt{r}\ \log\ n$ we compute $(x+b)^n - (x^n + b)(\text{mod } X^r - 1, n)$". For a fixed b each of these operations has a complexity $\mathcal{O}(r^2 \log^3 n)$ since to compute x^n mod $(x^r - 1)$ we can just remark that, if $n = qr + \ell$, where $q, \ell \in \mathbb{N}^*$, $\ell < r$, we immediately have $x^n = (x^r - 1)(x^{n-r} + x^{n-2r} + \ldots + x^{n-qr}) + x^\ell \equiv x^\ell$ mod $(x^r - 1)$. Thus the computational complexity of step 5 is: $\mathcal{O}(r^{5/2} \log^4\ n)$. As $r \leq \lceil \log^5\ n \rceil$, we have: $\mathcal{O}(\log^{33/2}\ n)$.
We have:

Step	Complexity
1	$\mathcal{O}(\log^4 n)$
2	$\mathcal{O}(\log^{7+\epsilon} n)$
3	$\mathcal{O}(\log^7 n)$
5	$\mathcal{O}(\log^{33/2} n)$

Remark 2.1. *Fact: letting* $n = qr + l$*,* $q, l \in \mathbb{N}^*$*,* $l < r$*,* $x^n = (x^r - 1)(x^{n-r} + x^{n-2r} + \cdots + n^n - qr) + x^l \equiv x^l (\text{mod} x^r - 1)$*. So to compute* $x^n (\text{mod} x^r - 1, n)$ *it is enough to compute one euclidean division.*

Therefore the computational complexity of the algorithm is: $\mathcal{O}(\log^{33/2}\ n)$, we can conclude that the AKS is solvable in a polynomial time.

Remark 2.2. *There exists a method to multiply two polynomial in a faster way called FFT (Fast Fourier transformation), see ch.9.5 of Crandall-Pomerance [3]. Using it, the step 5 is computed in* $\mathcal{O}(r^{3/2} \log^{3+\epsilon}\ n)$ *elementary operations. Therefore the total cost of the algorithm will be* $\mathcal{O}(\log^{21/2+\epsilon} n)$*.*

[1] $n \geq \lceil \log^5\ n \rceil$ i.e $n \geq 5690034$

We have prove that the AKS is a deterministic and polynomial primality test. It's computational cost is greater than the Miller-Rabin's one, thus in practice it is not used. Nevertheless it is a big step from a theoretical point of view, since the second one is conditioned to the GRH, and the AKS one is not. In the next chapter we will see a variation of this algorithm, which will give a better computational cost, and it is still not conditioned.

Chapter 3

Lenstra-Pomerance Algorithm

Let's now introduce another primality test, based on the AKS one. This version done by Lenstra and Pomerance is a deterministic and polynomial test with a computational cost $\widetilde{\mathcal{O}}((\log n)^6)$ (the notation $\widetilde{\mathcal{O}}(X)$ means a bound $c_1 X(\log X)^{c_2}$ for suitable positive constants c_1, c_2). The main difference here is that the auxiliary polynomial that we use is allowed to be any monic polynomial in $\mathbb{Z}[x]$ that "behaves" as if it is irreducible over the "finite field" $\mathbb{Z}/n\mathbb{Z}$. This chapter is divided in two parts, the first one introduces the primality test, and the second is the proof of a theorem assumed in the first one. The reason of this is that the proof needs some preliminary results.

3.1 Lenstra-Pomerance Algorithm

We say that a positive integer is B-smooth if it is not divisible by any prime exceeding B. The following is the main theorem behind the primality test:

Theorem 3.1. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree d, let $n > 1$ be an integer, let $A = \mathbb{Z}[x]/(n, f)$, and let $\alpha = x + (n, f) \in A$. Assume that*

$$f(\alpha^n) = 0, \tag{3.1}$$

$$\alpha^{n^d} = \alpha, \tag{3.2}$$

$$\alpha^{n^{d/l}} - \alpha \in A^* \text{ for all primes } l | d, \tag{3.3}$$

$$d > (\log_2 n)^2, \tag{3.4}$$

$$(\alpha + a)^n = \alpha^n + a \text{ for each integer } a,\ 1 \leq a \leq B := \left\lfloor \sqrt{d} \log_2 n \right\rfloor. \tag{3.5}$$

Then n is a B-smooth number or a prime power.

First we are going to prove this theorem and then we will see an algorithm to build such polynomials.

3.1.1 Proof of theorem 3.1

Suppose $f \in \mathbb{Z}[x]$ is monic of degree $d > 0$, n is an integer with $n > 1$, and $A = \mathbb{Z}[x]/(n, f)$. Let $\alpha = x + (n, f) \in A$. Note that if n is prime, then (3.1) holds. And that if n is prime, then (3.2) and (3.3) hold if and only if f is irreducible modulo n.

Note that A is a free $\mathbb{Z}/n\mathbb{Z}-$module with basis $1, \alpha, \ldots, \alpha^{d-1}$. Let σ the ring homomorphism from A to A which take α to α^n, induced by the ring homomorphism from $\mathbb{Z}[x]$ to $Z[x]$ which takes x to x^n. By (3.2) σ^d is the identity map on A, so that σ is an automorphism of A and by (3.2) and (3.3) it has order d. Let's consider some preliminary results that we need to prove Theorem 3.1.

Lemma 3.1. *Suppose that $\mathcal{R}$ is a commutative ring with unit, $f \in \mathcal{R}[x]$, $\beta_1, \ldots, \beta_k \in \mathcal{R}$ with $f(\beta_i) = 0$ for $1 \leq i \leq k$ and $\beta_j - \beta_i \in \mathcal{R}^*$ for $1 \leq i < j \leq k$. Then $\prod(x - \beta_i)|f(x)$.*

Proof. We are going to prove it by induction:
For $k = 1$: there exist $q \in R[x]$ and $\rho \in R$ such that $f(x) = (x - \beta_1)q(x) + \rho$. If $x = \beta_1$ we have $0 = f(\beta_1) = \rho$, thus $(x - \beta_1)|f(x)$.
The induction step: we assume the thesis for $k = j - 1$; let's prove it for $k = j$. By hypothesis we have that $f(x) = h(x)(x - \beta_1) \cdots (x - \beta_{j-1})$; putting $x = \beta_j$ we have $(\beta_i - \beta_j) \neq 0$ for all $i < j$. Hence we have that $(\beta_j - \beta_1) \cdots (\beta_j - \beta_{j-1})$ is invertible and, using $0 = f(\beta_j) = h(\beta_j)(\beta_j - \beta_1) \cdots (\beta_j - \beta_{j-1})$, it follows that $h(\beta_j) = 0$. By the first case $(x - \beta_j)|h(x)$, and the lemma is proved. □

Lemma 3.2. *In $A[y]$ we have $f(y) = \prod_{i=0}^{d-1}(y - \sigma^i\alpha)$.*

Proof. If we show the two following assertions

1. $f(\sigma^i\alpha) = 0$ and that

2. $\sigma^i\alpha - \sigma^j\alpha \in A^*$, for $0 \leq j < i < d$,

by Lemma 3.1, we obtain $\prod_{i=0}^{d-1}(y - \sigma^i\alpha)|f(y)$ and, since they are both monic of degree d, the equality holds.
Let's prove the assertions 1 and 2:
Since σ is an automorphism of A, $f(\sigma^i\alpha) = 0$.
To prove 2. as σ is an automorphism, it suffices to consider the case $j = 0$, *i.e.* $\sigma^i\alpha - \alpha \in A^*$, for $0 < i < d$. As $d \nmid i$, there is some prime $l|d$ with $(i, d)|(d/l)$. Since there are integers u, v with $ui + vd = d/l$, and σ has order d, we have $\sigma^{ui}\alpha = \sigma^{d/l}\alpha$. Hence by (3.3), $\sigma^{ui}\alpha - \alpha \in A^*$. But $n^i - 1|n^{ui} - 1$ so that $\alpha^{n^i-1} - 1|\alpha^{n^{ui}-1} - 1$, and we finally get

$$\sigma^i\alpha - \alpha = \alpha^{n^i} - \alpha|\alpha^{n^{ui}} - \alpha = \sigma^{ui}\alpha - \alpha.$$

Hence $(\sigma^i\alpha - \alpha)$ is a divisor of a unit, thus it is a unit. □

Let p be a prime factor of n, and $R = A/pA \cong \mathbb{Z}[x]/(p, f)$. We identify members of A with their image in R, so in particular the coset $x + (p, f)$ is denoted by α. The ring R is a vector space over $\mathbb{Z}/p\mathbb{Z}$ with basis $1, \alpha, \ldots, \alpha^{d-1}$. The automorphism σ of A induces an automorphism of R, which we will continue to denote σ. By (3.3) σ has order d as well when considered as an R-automorphism.
Let ϕ be the Frobenius automorphism in R, that sends every element to its p-th power.

Lemma 3.3. *Viewing σ as an automorphism of R, there is some integer i with $\sigma^i = \phi$.*

Proof. It is sufficient to show that for some integer i we have $\sigma^i\alpha = \alpha^p$, since if two automorphisms agree on a generator of the ring, they are the same automorphism. As ϕ is an automorphism of R it follows that $f(\phi\alpha) = 0$, thus by Lemma 3.2 taken over R we have

$$f(\alpha^p) = \prod_{i=0}^{d-1}(\alpha^p - \sigma^i\alpha) = 0.$$

To see that a factor in this product must be 0, let's assume the following claim, that we will prove at the end of the proof.
Claim: for $\beta \in R$,

$$\text{if } \sigma\beta \in \beta R \Rightarrow \beta = 0 \text{ or } \beta \in R^*. \tag{3.6}$$

For any integer i, j we have

$$\sigma(\alpha^j - \alpha^i) = \alpha^{jn} - \alpha^{in} = (\alpha^j - \alpha^i)(\alpha^{j(n-1)} + \alpha^{j(n-2)+i} + \cdots + \alpha^{i(n-1)}) \in (\alpha^j - \alpha^i)R.$$

By (3.6) we have $(\alpha^i - \alpha^j) = 0$ or $\sigma(\alpha^i - \alpha^j) \in R^*$. This is true for all i, j thus in particular for $j = p$ and all i. But, as $\prod_{i=0}^{d-1}(\alpha^p - \sigma^i\alpha) = 0$ not all can be units, it exists at least one i such that $\sigma(\alpha^p - \alpha^{n^i}) = 0$. Thus we have an i such that $\sigma^i = \phi$.

Proof of the claim: assume $\sigma\beta \in \beta R$ and that β is not 0 and not an unit. Write $\beta = g(\alpha)$ where $g \in (\mathbb{Z}/p\mathbb{Z})[y]$, $\deg g < d$. Since β is not an unit, we get $\beta R \neq R$ and whence the projection $R \to R/\beta R$ takes units to units. The ring $R/\beta R$ also contains $\mathbb{Z}/p\mathbb{Z}$ so that, if we use an overbar to denote the image of an R-element in $R/\beta R$, then $\overline{g(\gamma)} = g(\overline{\gamma})$ for all $\gamma \in R$. By assumption we know that $\sigma\beta \in \beta R$ and so $\sigma^i\beta \in \beta R$. So we obtain

$$0 = \overline{\sigma^i\beta} = \overline{g(\sigma^i\alpha)} = g(\overline{\sigma^i\alpha}).$$

In the proof of Lemma 3.2 we shown that $\sigma^i\alpha - \sigma^j\alpha \in A^*$, for $0 \le j < i < d$, thus we have that $\overline{\sigma^i\alpha} - \overline{\sigma^j\alpha} \in (R/\beta R)^*$, for $0 \le j < i < d$. And we just have to prove that $g(\overline{\sigma^i\alpha}) = 0$, therefore by Lemma 3.1 we know that the degree of g is at least d, a contradiction. □

Let $G = \{\beta \in R : \beta \neq 0, \sigma\beta = \beta^n\}$. Note that $1,\ \alpha \in G$ and $\sigma G \subset G$.

Lemma 3.4. *G is a cyclic subgroup of R^*.*

Proof. It is clear from the definition of G and (3.6) that G is a subgroup of R^*; so it remains to show that it is cyclic. Let f_1 be an irreducible factor of f considered over $\mathbb{Z}/p\mathbb{Z}$, and $K = \mathbb{Z}[x]/(p, f_1)$. Let ψ be the natural projection form R to K. Let's prove that the restriction of ψ to G is injective, in that case, G will be isomorphic to a subgroup of K^*; since K^* is itself cyclic, the lemma will be proved.
Let $\beta \in G$ and $\psi\beta = 1$, write $\beta = g(\alpha)$ where $g \in (\mathbb{Z}/p\mathbb{Z})[y]$ has degree $< d$. Since $\beta \in G$ we have $\sigma^i\beta = \beta^{n^i}$ for each i, so that

$$g(\psi\sigma^i\alpha) = \psi\sigma^i g(\alpha) = \psi\sigma^i\beta = \psi(\beta^{n^i}) = (\psi\beta)^{n^i} = 1.$$

In the proof of Lemma 3.2 we shown that $\sigma^i\alpha - \sigma^j\alpha \in A^*$, for $0 \leq j < i < d$, thus we have it in K^*. Hence we have $\psi\sigma^i\alpha - \psi\sigma^j\alpha \in K^*$, for $0 \leq j < i < d$. And we just have to prove that $g(\psi\sigma^i\alpha) - 1 = 0$, therefore by Lemma 3.1 we know that the degree of $g(y) - 1$ is at least d, or it is the 0-polynomial. Hence it is 0, and so $1 = g(\alpha) = \beta$. Therefore we have that $\psi\beta = 1$ implies $\beta = 1$, thus $\psi|_G$ is injective, and this completes the proof of the lemma.

□

Lemma 3.5. *Among the ordered pairs of integers (i, j) with $0 \leq i,\ j \leq \sqrt{d}$ there are two different pairs $(i_0, j_0), (i_1, j_1)$ such that*

$$p^{i_0}(n/p)^{j_0} \equiv p^{i_1}(n/p)^{j_1} (\text{mod } \#G).$$

Proof. We consider the automorphism group of G. For any finite cyclic group G under multiplication, the automorphism group is naturally isomorphic to $(\mathbb{Z}/(\#G)\mathbb{Z})^*$ where a residue m correspond to $\pi_m : x \to x^m$, for all elements $x \in G$. By the definition of G, the ring automorphism σ acts as well as a group automorphism of G and is identified with π_n. We consider the subgroup $\langle\sigma\rangle = \langle\pi_n\rangle$ of Aut G, of order d. By Lemma 3.3, the Frobenius map ϕ is in this subgroup and it is identified by π_p. Therefore $\sigma\phi^{-1}$, identified by $\pi_{n/p}$, is in the subgroup as well.

Now, we consider the automorphism $\pi_p^i\pi_{n/p}^j$ for integers i, j with $0 \leq i, j \leq \sqrt{d}$. There are more than d of these expressions, and they lie in a subgroup of order d, so at least two of them must be equal: say

$$\pi_p^{i_0}\pi_{n/p}^{j_0} = \pi_p^{i_1}\pi_{n/p}^{j_1}$$

where $(i_0, j_0), (i_1, j_1)$ are different pairs. Then

$$p^{i_0}(n/p)^{j_0} \equiv p^{i_1}(n/p)^{j_1} (\text{mod } \#G).$$

This completes the proof. □

Note that for (i, j) with $0 \leq i, j \leq \sqrt{d}$, we have $p^i(n/p)^j \leq p^{\sqrt{d}}(n/p)^{\sqrt{d}} = n^{\sqrt{d}}$. So, if under some hypotheses, we have $\#G > n^{\sqrt{d}} - 1$, then the congruence in Lemma 3.5 will be an equality.

We can now start the proof of Theorem 3.1 whose statement we rewrite here:
Theorem 3.1 *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree d, let $n > 1$ be an integer, let $A = \mathbb{Z}[x]/(n, f)$, and let $\alpha = x + (n, f) \in A$. Assume that*

$$f(\alpha^n) = 0, \tag{3.7}$$

$$\alpha^{n^d} = \alpha, \tag{3.8}$$

$$\alpha^{n^{d/l}} - \alpha \in A^* \textit{ for all primes } l|d, \tag{3.9}$$

$$d > (\log_2 n)^2, \tag{3.10}$$

$$(\alpha + a)^n = \alpha^n + a \textit{ for each integer } a,\ 1 \leq a \leq B := \left\lfloor \sqrt{d}\log_2 n \right\rfloor. \tag{3.11}$$

Then n is a B-smooth number or a prime power.

Proof. Suppose that n is not B-smooth, so that n has prime factor $p > B$. Recall that $R \cong \mathbb{Z}[x]/(p, f)$, $\sigma : \alpha \to \alpha^n$ is an automorphism of R and $G = \{\beta \in R : \beta \neq 0, \sigma\beta = \beta^n\}$. Claim: for each proper subset S of $\{0, 1, \dots, B\}$,

1. $\left(\prod_{a \in S}(\alpha + a)\right) \in G$.

2. Different choices for S give rise to different members of G.

Proof of the claim:

1. by (3.5), $\sigma(\alpha + a) = \alpha^n + a = (\alpha + a)^n$ for $1 \leq a \leq B$, the same is true for $a = 0$. Thus each product is in fact in $G \cup \{0\}$.

2. Consider $g_S = \prod_{a \in S}(x + a)$, since $d > B$, and $p > B$ it follows that these polynomials over $\mathbb{Z}/p\mathbb{Z}$ are distinct, nonzero and have degree $< d$. Evaluating this g_S in α we obtain distinct, nonzero members of R.

By the previous claim we have that $\#G$ is greater than the number of such sets S, that is

$$\#G \geq 2^{B+1} - 1 > 2^{\sqrt{d}\log_2 n} - 1 = n^{\sqrt{d}} - 1. \tag{3.12}$$

As we noted before, for $0 \leq i, j \leq \sqrt{d}$, we have $p^i(n/p)^j \leq p^{\sqrt{d}}(n/p)^{\sqrt{d}} = n^{\sqrt{d}}$. Thus if we have two different pairs (i, j) in this range, the gap between the two expressions $p^i(n/p)^j$ is at most $n^{\sqrt{d}} - 1$. Considering the two different pairs (i_0, j_0) and (i_1, j_1) we obtained in Lemma 3.5 and using (3.12), we have

$$p^{i_0}(n/p)^{j_0} = p^{i_1}(n/p)^{j_1}. \tag{3.13}$$

If $j_0 = j_1$, equation (3.13) will imply that $p^{i_0} = p^{j_0}$, thus that $i_0 = i_1$ which is a contradiction, since (i_0, j_0) and (i_1, j_1) are different. Thus we have $j_0 \neq j_1$ and by unique factorization we will have that n is a power of p. This completes the proof of the theorem. □

3.1.2 Gaussian periods and period systems

Definition 3.1.

- *Let G be a group. A character of G is an homomorphism $\chi : G \to \mathbb{C}$, $\chi \neq 0$.*

- *The trivial character $\chi_0(g) = 1 \forall g \in G$ is called the principal character.*

- *A Dirichlet character* $(\bmod\ r)$ *is the extension of a $(\mathbb{Z}/r\mathbb{Z})^*$ character.*

- *If $r'|r$ and $\chi \neq \chi_0 \bmod r$, it is possible that*

$$\chi(n) = \begin{cases} \chi'(n) & \textit{if } (n, q) = 1 \\ 0 & \textit{if } (n, q) > 1 \end{cases}$$

where χ' is a suitable character $\bmod\ r'$. *In this case we say that $\chi \bmod r$ is induced by $\chi' \bmod r'$.*

- *A Dirichlet character* $\chi(\text{mod } r)$*,* $\chi \neq \chi_0$*, is primitive if it is not induced by any Dirichlet character* $(\text{mod } r')$ *for every proper divisor* r' *of* r*.*

Letting m be a positive integer and a be an integer coprime to m, we denote by $ord(a \bmod m)$ the multiplicative order of a modulo m.

Definition 3.2 (Gaussian period $\eta_{r,q}$)**.** *Let* r *be a prime,* $\zeta_r = e^{2\pi i/r}$*,* q *a positive integer such that* $q|r-1$ *and* $S = \{s \bmod r : s^{(r-1)/q} \equiv 1(\text{mod } r)\}$ *the subgroup of* q*-th powers in* $(\mathbb{Z}/r\mathbb{Z})^*$*. We define the Gaussian period by*

$$\eta_{r,q} = \sum_{s \in S} \zeta_r^s.$$

Let w be a residue modulo r such that $ord(w^{(r-1)/q} \bmod r) = q$ (note that any primitive root modulo r has this property). Then the q cosets of S in $(\mathbb{Z}/r\mathbb{Z})^*$ are $w^j S$ for $j = 0, 1, \ldots, q-1$. Let $g_{r,q}$ be the minimum polynomial for $\eta_{r,q}$ over $\mathbb{Q}$, so that

$$g_{r,q} = \prod_{j=0}^{q-1} \left(x - \sum_{s \in S} \zeta_r^{w^j s}\right).$$

This polynomial is monic and irreducible in $\mathbb{Q}[x]$. For a prime p we may ask if it is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$.

Lemma 3.6 (Kummer)**.** *Let* p *and* r *be two primes, and* q *a positive divisor of* $r-1$*. The polynomial* $g_{r,q}(x)$ *is irreducible when considered in* $\mathbb{Z}/p\mathbb{Z}[x]$ *provided that* $ord(p^{(r-1)/q} \bmod r) = q$*.*

Proof. Suppose that $q > 1$ and that $ord(p^{(r-1)/q} \bmod r) = q$. Let's prove that $g_{r,q}(x)$ is irreducible when considered in $\mathbb{Z}/p\mathbb{Z}[x]$. Let K be the field of $rq-th$ roots of unity over $\mathbb{Z}/p\mathbb{Z}$ and ψ the natural projection of $\mathbb{Z}[\zeta_r, \zeta_q]$ to K, such that $\eta = \psi(\eta_{r,q})$. Since $g_{r,q}(\eta) = 0$, and the degree of $g_{r,q}(x)$ is q, if the degree d of η over $\mathbb{Z}/p\mathbb{Z}$ is q, we have that $g_{r,q}(x)$ is irreducible when considered in $\mathbb{Z}/p\mathbb{Z}[x]$.
Let ϕ be the Frobenius p-th power automorphism of K, so that the degree d of an element α of K over $\mathbb{Z}/p\mathbb{Z}$ is the least positive integer d such that $\phi^d(\alpha) = \alpha$. Let $\zeta = \psi(\zeta_r)$, we have

$$\phi^j(\eta) = \eta^{p^j} = \sum_{s \in S} \zeta^{p^j s},$$

where $S = \{s \bmod r : s^{(r-1)/q} \equiv 1(\text{mod } r)\}$ as previously. By Fermat's little theorem $p^{r-1} \equiv 1 \bmod r$, $p^q \bmod r$ is a member of S. It follows that $\phi^q(\eta) = \eta^{p^q} = \sum_{s \in S} \zeta^{p^q s}$; as $p^q \in S$ we have that $\phi^q(\eta) = \eta$ and so we obtain that $d|q$.
Let χ be the Dirichlet character modulo r which sends S to 1 and p to ζ_q. Since $S, pS, \ldots, p^{q-1}S$ are the cosets of S in $(\mathbb{Z}/r\mathbb{Z})^*$, the two conditions are sufficient to define χ. Since $q > 1$ and q is the order of χ, we have that χ is non principal, and since r is prime, it follows that χ is primitive. Thus if $\tau(\chi)$ is the Gauss sum, by Lemma 1.1 we have $\tau(\chi)\overline{\tau(\chi)} = r$, in particular $\psi(\tau(\chi)) \neq 0$ (if it is 0, we will have $\psi(\tau(\chi)\overline{\tau(\chi)}) = 0$ therefore $\psi(r) = 0$, and we will have a contradiction). Let $w = \psi(\zeta_q)$; we have

$$\psi(\tau(\chi)) = \sum_{j=1}^{r-1} \psi(\chi(j))\zeta^j = \sum_{i=0}^{q-1} w^i \sum_{j \in p^i S} \zeta^j = \sum_{i=0}^{q-1} w^i \eta^{p^i} \tag{3.14}$$

the last equality holds, since we are doing the sum in each coset. In the the i-th one we have:

$$\sum_{j\in p^iS}\psi(\chi(j))\zeta^j=\sum_{j\in p^iS}\psi(\zeta^i)\zeta^j=\sum_{j\in p^iS}w^i\zeta^j=w^i\sum_{j\in p^iS}\zeta^j.$$

We reorganize the sum (3.14) by writing $i=m+ld$, with $0\leq m\leq d-1$, $0\leq l\leq(q/d)-1$, getting

$$\psi(\tau(\chi))=\sum_{m=0}^{d-1}\eta^{p^m}\sum_{l=0}^{q/d-1}w^{m+ld}=\sum_{m=0}^{d-1}\eta^{p^m}w^m\sum_{l=0}^{q/d-1}w^{ld}. \tag{3.15}$$

Since

$$\sum_{i=0}^{q-1}w^i\eta^{p^i}=\sum_{m=0}^{d-1}\sum_{l=0}^{q/d-1}w^{m+ld}\eta^{p^{m+ld}}\text{ and }\eta^{p^{m+ld}}=\eta^{p^m}\eta^{p^{ld}}=\eta^{p^m},$$

we have

$$\psi(\tau(\chi))=\sum_{m=0}^{d-1}\eta^{p^m}\sum_{l=0}^{q/d-1}w^{m+ld}.$$

But if d is a proper divisor of q, letting $t=q/d$ we have:

$$\sum_{l=0}^{t-1}w^{ld}=\sum_{l=0}^{t-1}(\psi(\zeta_q))^{ld}=\psi\Big(\sum_{l=0}^{t-1}\zeta_q^{ld}\Big)=\psi\Big(\sum_{l=0}^{t-1}\zeta_t^{l}\Big)=0.$$

Therefore by (3.15) we get $\psi(\tau(\chi))=0$ and so we have a contradiction. Hence $d=q$, which proves the lemma. □

Corollary 3.1. *Suppose $r_1,\dots,r_k$ are primes, $q_1,\dots,q_k$ are pairwise coprime positive integers, with each $q_i|r_i-1$, and p is a prime with each ord$(p^{(r_i-1)/q_i}\bmod r_i)=q_i$. If η is the product of the Gaussian periods η_{r_i,q_i} and f is the minimum polynomial for η over $\mathbb{Q}$, then f is irreducible when considered in $\mathbb{Z}/p\mathbb{Z}[x]$.*

Proof. By Lemma 3.6, each η_{r_i,q_i}, when considered in an appropriate extension of $\mathbb{Z}/p\mathbb{Z}$, has degree q_i over $\mathbb{Z}/p\mathbb{Z}$. But in general, if $\alpha_1,\alpha_2,\dots,\alpha_k$ all lie in an extension of $\mathbb{Z}/p\mathbb{Z}$ and have pairwise coprime degrees, their product α has degree $q=q_1q_2\cdots q_k$ over $\mathbb{Z}/p\mathbb{Z}$. Indeed, if ϕ is the Frobenius p-th power automorphism, and l is a prime factor of q, say $l|q_i$, then $\phi^{q/l}(\alpha_j)=\alpha_j$ for $j\neq i$ and $\phi^{q/l}(\alpha_i)\neq\alpha_i$, so that $\phi^{q/l}(\alpha)\neq\alpha$. Thus f has at least order q, hence it is irreducible.

□

Now we are ready to define a period system.

Definition 3.3 (Period system for n)**.** *Let n a positive integer, we say that a sequence $(r_1,q_1),\dots,(r_k,q_k)$ of ordered pairs of positive integers is a period system for n if*

- *$r_1,\dots,r_k$ are primes,*
- *for $i=1,2,\dots,k$, we have $q_i|r_i-1$, $q_i>1$, and ord$(n^{(r_i-1)/q_i}\bmod r_i)=q_i$,*

- $q_1, \ldots, q_k$ *are pairwise coprime.*

Now we see that we can build "easily" such a period system.

Theorem 3.2. *There is a deterministic algorithm such that for each integer $m > 0$ the algorithm produce an integer D_m and further, for each integer $n > 1$, and each integer D with $D > D_m$ and $D > (\log n)^{11/6+1/m}$, the algorithm finds a period system $(r_1, q_1), \ldots, (r_k, q_k)$ for n with each $r_i < D^{6/11}$ and each $q_i < D^{3/11}$, with $D \leq q_1 q_2 \cdots q_k < 4D$, and with $k = \mathcal{O}((\log\log D)^2)$. The running time of this algorithm is $\widetilde{\mathcal{O}}(D^{12/11})$. The implied constant may depend on the choice of m.*

Remark 3.1. *We will apply this theorem in the case $D = (\log_2 n)^2$ so that m must be taken as 6. There is nothing special about the number 4 in the theorem, it is only a convenient choice that can be replaced with any other number greater than 1.*

By now we are going to assume Theorem 3.2 that we will prove in the next section, in fact we are going to prove it with $q_1, q_2, \ldots, q_k$ being distinct primes. In the following we will denote $1/m$ by ϵ.

Let's consider the following algorithm for the construction of a period system:

Algorithm 3.1. *Input: an integer $n > 1$, $D > (\log n)^{11/6}$.*
Output: the algorithm produces a period system $(r_1, q_1), \ldots, (r_k, q_k)$ for n.

1. *Using a modified sieve of Eratosthenes, compute the prime factorizations of every integer in $[1, 4D]$.*
2. *For each prime $r < D^{6/11}$ and prime $q | r-1$ with $exp\left(\frac{\log D}{(\log\log(2D))^2}\right) < q < D^{3/11}$, compute $n^{(r-1)/q} \bmod r$.*
3. *Compute the set $\mathcal{S}$ of ordered pairs (r, q) where r, q are as in step 2 and $n^{(r-1)/q} \not\equiv 1 \bmod r$.*
4. *Compute the set $\mathcal{Q}$ of primes q such that $(r, q) \in \mathcal{S}$ for some r.*
5. *If there is some integer in $[D, 4D]$ which is squarefree and composed solely of primes from $\mathcal{Q}$, let d be the last one. If not, replace D with $4D$ and go to step 1.*
6. *Using the prime factorization $q_1 q_2 \ldots q_k$ of d, find for each q_i some r_i with $(r_i, q_i) \in \mathcal{S}$.*
7. *Return the pairs $(r_1, q_1), \ldots, (r_k, q_k)$.*

Computational cost of Algorithm 3.1:

Step 1: The computational cost of this step is $\widetilde{\mathcal{O}}(D)$.
Step 2: In each iteration we have to compute $n^{(r-1)/q} \bmod r$, for this we first need to compute $\overline{n} = n \bmod r$ that has a computational cost of $\widetilde{\mathcal{O}}(\log n)$, then $\overline{n}^{(r-1)/q} \bmod r$ which has a computational cost of $\widetilde{\mathcal{O}}((\log r)^2)$(using FFT the cost of computing $n^k \bmod r$ is $\widetilde{\mathcal{O}}(\log k \log r)$). As we have to do it q times and q is less than the number of divisor of $r-1$ which is less than $\log r$

we have that the computational cost is $\widetilde{\mathcal{O}}(\log n)$. Now we have to compute this $r < D^{6/11}$ times, the total computational cost is $\widetilde{\mathcal{O}}(D^{6/11}\log n)$. As $D > (\log n)^{11/6}$ we have $\log n = \mathcal{O}(D^{6/11})$. Thus the total cost of this step is $\widetilde{\mathcal{O}}(D^{12/11})$.

We can see that the computational costs of steps 3 and 4 are embedded in the cost in step 2, and the computational cost of step 6 is negligible by the cost of step 2. Now we have to compute how many times the step 2 has to be repeated.

If step 5 sends us back to step 1 at least $\lceil \frac{1}{100} \log\log(2n) \rceil$ times, our D will be greater than $(\log n)^{11/6+1/100}$. In fact each time that we come back to the step 2, D is multiplied by 4, thus if we repeat this step $T = \lceil \frac{1}{100} \log\log(2n) \rceil$ times, calling D' this new D, we will obtain: $D' = 4^T D > 4^{\log(\log(2n)^{\frac{1}{100}})} D > e^{\log(\log(2n)^{\frac{1}{100}})} D = \log(2n)^{\frac{1}{100}} D > \log(n)^{\frac{1}{100}} \log(n)^{11/6} = \log(n)^{1/100+11/6}$. Therefore as $T = \lceil \frac{1}{100} \log\log(2n) \rceil = \mathcal{O}_D(1)$, with at most $\mathcal{O}_D(1)$ iteration, will ensure that $D > D_{100}$ (using the notation in Theorem 3.2). Putting $\mathcal{O}_D(1)$ in the constant, we have that the running time is $\widetilde{\mathcal{O}}(D^{12/11})$. The $\mathcal{O}$-constant being computable in principle.

The correctness of this algorithm follows immediately of the computational cost of step 5. Since we are sure that the algorithm will stop at most in the $\mathcal{O}_D(1)$ iteration.

3.1.3 Period polynomial

In this section we are going to look for a given natural number $n > 1$, a deterministic procedure that either proves that n is composite or construct a monic polynomial $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ of degree $d = q_1 q_2 \cdots q_k$ for which (3.1), (3.2) and (3.3) holds.

If $\eta_i = \eta_{r_i,q_i}$ is the Gaussian period discussed before, and if $\eta = \eta_1\eta_2\cdots\eta_k$, then the polynomial f that we hope to produce is the reduction modulo n of the minimal polynomial for η over $\mathbb{Q}$.

We are going to build it in 3 stages: in the first one, we are going to compute monic polynomials $g_i \in (\mathbb{Z}/n\mathbb{Z})[x]$ for $i = 1, 2, \ldots, k$ with $\deg g_i = q_i$. If n is prime, g_i is irreducible modulo n. In the second stage we verify (3.1), (3.2) and (3.3) for $g_1, g_2, \ldots, g_k$, and where q_i plays the role of d in these equations. If one of these properties fails, we can declare n composite. Finally in the third stage we assemble the polynomial f of degree d.

The first stage:

We suppose that we have a pair (r, q) with r prime, $q|(r-1)$, $ord(n^{(r-1)/q} \bmod r) = q$ and $q > 1$.

1. Let z be a primitive root for r, for $j = 0, 1, \ldots, q-1$, and
$$S_j = \{z^{j+lq} \bmod r : l = 0, 1, \ldots, \frac{r-1}{q} - 1\}.$$
2. Compute the period polynomial $g(x)$ for the degree q subfield of the r-th cyclotomic field. Note that we will reduce modulo n in each intermediate calculation. Let $\zeta_r = e^{2\pi i/r}$,
$$g(x) := \prod_{j=0}^{q-1} \Big(x - \sum_{m \in S_j} \zeta_r^m \Big) \in \big(\mathbb{Z}[\zeta_r]/(n)]\big)[x].$$

Computational cost:

Step 1 can be done by running through $z^0 \bmod r, z^1 \bmod r, \dots$ placing each residue in its proper set. Or can build each S_j, computing $z^j \bmod r$ and $z^q \bmod r$, and build $z^{j+lq} \bmod r$ from $z^{j+(l-1)q} \bmod r$. The time to build this S_j is $\widetilde{\mathcal{O}}(r)$. The time to obtain a prime factorization of r via trial division is $\widetilde{\mathcal{O}}(r^{1/2})$. And the time to check each z to see if it is a primitive root is $(\log r)^{\mathcal{O}(1)}$. Thus the cost of step 1 is $\widetilde{\mathcal{O}}(r)$.

A multiplication in $\mathbb{Z}[\zeta_r]/(n)$ can be done in $\widetilde{\mathcal{O}}(r(\log n)^2)$ (since it is a multiplication of two polynomials of degree r in $\mathbb{Z}/nZ$ with r is much smaller than n, hence the computational cost follows from A.3). We take the q polynomials by pairs, (if q is odd it remains one alone), the product of the pairs can be computed in time $\widetilde{\mathcal{O}}(qr(\log n)^2)$. We do again the same procedure, *i.e.* we form again pairs with the polynomials we have, such that at most we have one polynomial alone. As they are $\mathcal{O}(\log q)$ pair-assembly, the total cost of this multiplication is $\widetilde{\mathcal{O}}(qr(\log n)^2)$.

Now we have to repeat this for each pair (r_i, q_i) with $i = 1, \dots, k$. Therefore the total cost of this stage is

$$\widetilde{\mathcal{O}}((\sum_{i=1}^{k} q_i r_i)(\log n)^2).$$

The second stage:

For (r, q) one of the pairs in the first stage, and with g the polynomial in $(\mathbb{Z}/n\mathbb{Z})[x]$ we have construct, let $A = \mathbb{Z}[x]/(n, g)$, and let $\alpha = x + (n, g)$.
The time for a multiplication in A is $\widetilde{\mathcal{O}}(q(\log n)^2)$ (since it is a multiplication of two polynomials of degree q in $\mathbb{Z}/nZ$ with q is much smaller than n, hence the computational cost follows from A.3). Then the time to compute α^n is $\widetilde{\mathcal{O}}(q(\log n)^3)$.

- We want to verify if the equation (3.1) hold, (*i.e.* if $g(\alpha^n) = 0$), since the time to compute $g(\alpha^n)$ is $\widetilde{\mathcal{O}}(q^2(\log n)^2)$ (q operation of cost $\widetilde{\mathcal{O}}(q(\log n)^2)$), this is the time to check (3.1).
- Now to verify (3.2), *i.e.* $\alpha^{n^q} = \alpha$, we have to compute $\alpha^{n^q} = \alpha^{\overbrace{nn\cdots n}^{q \text{ times}}} = (\alpha^n)^{\overbrace{nn\cdots n}^{q-1 \text{ times}}}$. Thus we have to compute q times α^n which has a computational cost of $\widetilde{\mathcal{O}}(q(\log n)^3)$, thus the total cost to verify (3.2) is $\widetilde{\mathcal{O}}(q^2(\log n)^3)$. Not that in this step we also computed $(\alpha^n)^{q/s}$ for each prime $s|q$.
- To verify (3.3) (*i.e.* $\alpha^{n^{q/s}} - \alpha \in A^*$ for all primes $s|q$), let $\beta = \alpha^{n^{q/s}} - \alpha$ for one of the primes $s|q$. As A is a free $\mathbb{Z}/n\mathbb{Z}$-module with basis $1, \alpha, \dots, \alpha^{q-1}$, we have $\beta = h(\alpha)$ for some $h \in (\mathbb{Z}/n\mathbb{Z})[x]$ with either $h = 0$ or $\deg h < q$. If $h = 0$, then $\beta = 0$ and condition (3.3) fails, thus n is composite and stop. So, assume $h \neq 0$. We perform Euclid's algorithm on $h(x), g(x)$ in $(\mathbb{Z}/n\mathbb{Z})[x]$. After each division with a nonzero remainder we multiply by the inverse in $\mathbb{Z}/n\mathbb{Z}$ of its leading coefficient so as to make it monic. If one of this leading coefficient is not a unit in $\mathbb{Z}/n\mathbb{Z}$, we declare n is composite, and stop. Assuming we have not stopped, Euclid's algorithm will stop at a non zero monic polynomial $h_0 \in (\mathbb{Z}/n\mathbb{Z})[x]$. If $\deg h_0 > 0$, then β is not a unit in A, declare n composite and

stop. Otherwise $\beta \in A^*$, that is, property (3.3) holds. The total cost to verify (3.3) is $\widetilde{\mathcal{O}}(q^2(\log n)^3)$.

Therefore the total time to verify (3.1), (3.2) and (3.3) for $g_1, g_2, \dots, g_k$ is:

$$\widetilde{\mathcal{O}}((\sum_{i=1}^{k} q_i^2)(\log n)^3).$$

The third stage:

First we are going to see the case $k = 2$: suppose f_1, f_2 are two monic polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ of degree d_1, d_2 respectively, where $d_1, d_2 > 1$ and $(d_1, d_2) = 1$. For $i = 1, 2$ let $A_i = \mathbb{Z}[x]/(n, f_i)$ and let $\alpha_i = x + (n, f_i)$. Assume that (3.1), (3.2) and (3.3) hold for f_i, α_i for $i = 1, 2$. By (3.3) $\alpha_1 \in A_1^*$, thus we can write α_1^{-1}. Let

$$M(f_1, f_2)(t) = \prod_{j=0}^{d_1-1} \alpha_1^{d_2 n^j} f_2(t\alpha_1^{-n^j}),$$

so that $M(f_1, f_2)$ is a polynomial in $A_1[t]$.

Proposition 3.1. *With the above assumptions, $M(f_1, f_2)$ is a polynomial in $(\mathbb{Z}/n\mathbb{Z})[t]$, monic of degree $d_1 d_2$, and satisfying properties* (3.1)*,* (3.2) *and* (3.3)*.*

Proof. Let $f = M(f_1, f_2)$, $d = d_1 d_2$. It is clear that f is monic and has degree d. Let's see if f is in fact a polynomial in $(\mathbb{Z}/n\mathbb{Z})[t]$.
Let σ_1 the automorphism of A_1 that takes α_1 to α_1^n discussed before, to simplify the notation let $\sigma = \sigma_1$. Note that σ let the coefficients of f invariant. Let $\beta \neq 0$ one of these coefficients, $\beta = h(\alpha_1)$, where $h \in (\mathbb{Z}/nZ)[x]$ is 0 or has degree less than d_1. Now consider the polynomial $H(x) = h(x) - \beta \in A_1[x]$; it has the d_1 roots $\sigma^j \alpha_1$ for $j = 0, 1, \dots, d_1 - 1$. In the proof of Lemma 3.2 we shown that $\sigma^i \alpha - \sigma^j \alpha \in A^*$, for $0 \leq j < i < d$, thus, by Lemma 3.1, $h(x) - \beta$ is either 0, or has degree at least d_1, but this cannot occurs, thus $\beta = h(0) \in \mathbb{Z}/n\mathbb{Z}$. Therefore $f \in (\mathbb{Z}/n\mathbb{Z})[t]$ as wished.

Let $A' = \mathbb{Z}[t]/(n, f)$ and $\alpha = t + (n, f)$. In order to show that (3.1), (3.2) and (3.3) hold for the pair f, α, let's prove it first in a similar situation.
Let $A = \mathbb{Z}[x_1, x_2]/(n, f_1(x), f_2(x))$, note that there is a natural embedding of A_1, A_2 into A such that α_i is sent to $x_i + (n, f_1(x_1), f_2(x_2))$ for $i = 1, 2$. Let σ the endomorphism on A such that α_i is sent to α_i^n for $i = 1, 2$, note that σ restricted to each A_i is the automorphism considered before. Let's prove that the three equations hold for f, α_1, α_2.

- By Lemma 3.2 we have

$$f(t) = \prod_{j=0}^{d_1-1} \prod_{l=0}^{d_2-1} (t - \sigma^j(\alpha_1)\sigma^l(\alpha_2)),$$

hence $f(\alpha_1\alpha_2) = 0$, and $f(\sigma(\alpha_1\alpha_2)) = f((\alpha_1\alpha_2)^n) = 0$, thus (3.1) holds.

- $$(\alpha_1\alpha_2)^{n^d} = \sigma^d(\alpha_1\alpha_2) = \sigma^{d_1d_2}(\alpha_1)\sigma^{d_2d_1}(\alpha_2) = \alpha_1\alpha_2$$
  thus (3.2) holds.

- Letting q be a positive integer such that $q \mid d_1$, we have
  $$(\alpha_1\alpha_2)^{n^{d/q}} - \alpha_1\alpha_2 = (\alpha_1^{n^{d/q}} - \alpha_1)\alpha_2. \tag{3.16}$$
  For any positive integer u we have $\alpha_1^{n^{d/q}} - \alpha_1 | \alpha_1^{n^{ud/q}} - \alpha_1$ in A_1; choosing $u \equiv d_2^{-1}$, we have $\alpha_1^{n^{d/q}} - \alpha_1 | \alpha_1^{n^{d_1/q}} - \alpha_1$, or $\alpha_1^{n^{d_1/q}} - \alpha_1 \in A_1^*$ (by (3.3) applied to α_1) hence $\alpha_1^{n^{d/q}} - \alpha_1 \in A_1^* \subset A^*$. Or using (3.3) for α_2 we see that $\alpha_2 \in A_2^* \subset A^*$. Therefore by (3.16) we have $(\alpha_1\alpha_2)^{n^{d/q}} - \alpha_1\alpha_2 \in A^*$ thus (3.3) holds for $\alpha_1\alpha_2$. We have also that σ is then an automorphism for A with order d.

To complete the proof it will suffice to show that $A' \cong A$ with $\alpha \in A$ corresponding to $\alpha_1\alpha_2 \in A$. Consider the map $\phi : A' \to A$ where $\phi(\alpha) = \alpha_1\alpha_2$, let's show that ϕ is an isomorphism. It is well defined since for $g, h \in (\mathbb{Z}/n\mathbb{Z})[t]$ with $g(\alpha) = h(\alpha)$, we know that $g(t) = h(t) + u(t)f(t)$ for some $u \in (\mathbb{Z}/n\mathbb{Z})[t]$. Thus $\phi g(\alpha) = g(\alpha_1\alpha_2) = h(\alpha_1\alpha_2) = \phi h(\alpha)$.
Let's show that it is an isomorphism: it is clearly an homomorphism, let's see that it is injective. Suppose $\phi g(\alpha) = 0$ where g is 0 or has degree less than d, then $g(\alpha_1\alpha_2) = 0$. As σ is an automorphism for A, we have $g(\sigma^j(\alpha_1\alpha_2)) = 0$ for $j = 0, 1, \ldots, d-1$. As (3.3) holds for $\alpha_1\alpha_2$, we have that $\sigma^i\alpha_1\alpha_2 - \sigma^j\alpha_1\alpha_2 \in A^*$, for $0 \le j < i < d$, thus by Lemma 3.1 that $f(t)|g(t)$ in $A[t]$. Therefore g can not have a degree less than d, so that $g = 0$ and ϕ is injective. As A, A' have n^d elements it follows that ϕ is also surjective. Thus $A' \cong A$ as claimed. □

Let's generate now the polynomial of degree $q_1q_2\cdots q_k$ for an arbitrary $k > 1$, using the M-operator for $g_1, g_2, \ldots g_k$. As the M-operator has only two entrances, we have several choices; we will choose the one with minimal computational cost. For this we compute the computational cost of $M(f_1, f_2)$ with the above assumption. We have

$$M(f_1, f_2)(t) = \prod_{j=0}^{d_1-1} \alpha_1^{d_2n^j} f_2(t\alpha_1^{-n^j}).$$

We saw in Appendix A that, α_1^{-1} is computed in $\widetilde{\mathcal{O}}(d_1(\log n)^2)$. Compute $(\alpha_1^{-1})^{n^j}$ from $(\alpha_1^{-1})^{n(j-1)}$ is $\widetilde{\mathcal{O}}(d_1(\log n)^3)$, thus the total cost for computing $(\alpha_1^{-1})^{n^j}$ from (α_1^{-1}) is $\widetilde{\mathcal{O}}(d_1^2(\log n)^3)$. We use Corollary 10.8 of [13] to evaluate f_2 at the set of points $t\alpha_1^{-n^j}$. If $d_1 > d_2$ this takes $\widetilde{\mathcal{O}}(d_1)$ operation in $A_1[t]$ with polynomials of degree at most d_2, thus the total cost is $\widetilde{\mathcal{O}}(d_1^2d_2(\log n)^2)$. If $d_1 < d_2$, the cost is $\widetilde{\mathcal{O}}(d_1d_2^2(\log n)^2)$. Using the previous results, the time to compute $\alpha_1^{d_2n^j}$ for each j and multiply it into $f_2(t\alpha_1^{-n^j})$ is $\widetilde{\mathcal{O}}(d_1d_2(\log n)^2)$.
Thus, the total time to assemble $M(f_1, f_2)$ is

$$\widetilde{\mathcal{O}}(d_1^2(\log n)^3 + d_1d_2(d_1 + d_2)(\log n)^2). \tag{3.17}$$

As the cost increases significantly with the degree of the polynomials, the strategy to have the lowest possible cost is:

Among all sets $S \subset \{1, 2 \dots, k\}$ with $\prod_{s \in S} q_s < d^{1/2}$ choose the one, call it S_1, with this product maximal, and let this product be denoted by d_1. Let $d_2 = d/d_1$. Say $S_1 = \{s_1, \dots, s_l\}$ and let $f_1 = M(g_{s_1}, \dots, g_{s_l})$ built up two at time. By (3.17) the computational cost of this is $\widetilde{\mathcal{O}}(d_1^2(\log n)^3 + d_1^3(\log n)^2)$ (since in this case $d_2 < d_1$). Let

$$S_2 = \{1, 2, \dots, k\} \setminus S_1 = \{t_1, t_2, \dots, t_{k-l}\}.$$

We build $f_2 = M(g_{t_1}, g_{t_2}, \dots, g_{t_{k-l}})$ in the same way as f_1. As $d_2/q_{t_i} < d_1$, the computational cost of the construction of f_2 will be dominated by (3.17). Finally we compute $M(f_1, f_2)$ and the total time is (3.17).

It remains now to estimate d_1 and d_2: for this we shall assume that the period system $(r_1, q_1), (r_2, q_2), \dots, (r_k, q_k)$ was produced by the Algorithm 3.1. Thus we are assuming that $d > (\log n)^{11/6}$, each $q_i \leq d^{3/11}$ and each $r_i \leq d^{6/11}$. Let's show that $d_1 \geq d^{2/5}, d_2 \leq d^{3/5}$.
If the product of the largest two q_i's is at least $d^{2/5}$ then we choose d_1 as this product, or the complementary product of the remaining q_i's, whichever is smaller. Since $q_i \leq d^{3/11}$, the maximum value of $q_i q_j$ for $i \neq j$ is $d^{6/11}$, thus the complementary product must be at least $d^{5/11}$. Now, assuming that the product of the largest two q_i's is smaller than $d^{2/5}$, then every remaining q_i is smaller than $d^{1/5}$. If we multiply, one at a time, to our product we will have a result between $d^{2/5}$ and $d^{3/5}$. And we will take d_1 as the minimum between this product and the complementary one.
Using $d^{2/5} \leq d_1 < d^{1/2} < d_2 \leq d^{3/5}$ and that $d > (\log n)^{11/6}$, the complexity time for the third stage is: $\widetilde{\mathcal{O}}(d^{8/5}(\log n)^2)$. Since

$$\widetilde{\mathcal{O}}(d_1^2(\log n)^3 + d_1 d_2(d_1 + d_2)(\log n)^2) = \widetilde{\mathcal{O}}(d(\log n)^3 + d(d^{1/2} + d^{3/5})(\log n)^2)$$

or $d > (\log n)^{11/6}$ implies that $d^{6/11} > \log n$ thus we have

$$\widetilde{\mathcal{O}}(d_1^2(\log n)^3 + d_1 d_2(d_1 + d_2)(\log n)^2) = \widetilde{\mathcal{O}}(dd^{6/11}(\log n)^2 + dd^{1/2}(\log n)^2 + dd^{3/5}(\log n)^2)$$

$$\widetilde{\mathcal{O}}(d_1^2(\log n)^3 + d_1 d_2(d_1 + d_2)(\log n)^2) = \widetilde{\mathcal{O}}(d^{17/11}(\log n)^2 + d^{3/2}(\log n)^2 + d^{8/5}(\log n)^2)$$

Hence

$$\widetilde{\mathcal{O}}(d_1^2(\log n)^2 + d_1 d_2(d_1 + d_2)(\log n)^2) = \widetilde{\mathcal{O}}(d^{8/5}(\log n)^2).$$

Computational complexity:

As $r_i \leq d^{6/11}$ and $q_i \leq d^{3/11}$ the time of the first stage is:

$$\widetilde{\mathcal{O}}((\sum_{i=1}^{k} q_i r_i)(\log n)^2) = \widetilde{\mathcal{O}}(d^{9/11}(\log n)^2).$$

For the second stage it is:

$$\widetilde{\mathcal{O}}((\sum_{i=1}^{k} q_i^2)(\log n)^2) = \widetilde{\mathcal{O}}(d^{6/11}(\log n)^3).$$

Thus the computational cost is dominated by the third stage, hence it is: $\widetilde{\mathcal{O}}(d^{8/5}(\log n)^2)$.
In the particular case, when we choose d of order of magnitude $(\log n)^2$, the time complexity for this procedure is $\widetilde{\mathcal{O}}(\log n)^{26/5}$.
In the particular case, when we have n prime, we have the following algorithm:

Algorithm 3.2. *Input: a prime p, and D an integer with $D > (\log p)^{1.84}$.*
Output: An irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d, where $D \leq d = \mathcal{O}(D)$. Moreover, if p is larger than an effectively computable bound, we have $d \leq 4D$.

1. *Using Algorithm 3.1, find a period system $(r_1, q_1), \ldots, (r_k, q_k)$ for $n = p$ with $d := q_1 q_2 \cdots q_k \geq D$ and $d = \mathcal{O}(D)$. (For p beyond an effectively computable bound, this algorithm finds such a number d with $d \leq 4D$.)*

2. *With the the stage 1 and 3 of this section, construct a monic polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d.*

3. *Return $f(x)$.*

And so we proved the following theorem.

Theorem 3.3. *There is a deterministic algorithm and an effectively computable number B, such that, given a prime $p > B$ and an integer $d > (\log p)^{1.84}$, it produces an irreducible polynomial over $\mathbb{F}_p$ of degree d', where $d \leq d' \leq 4d$. Moreover the running time is $\widetilde{\mathcal{O}}(d^{1.6}(\log p)^2)$, with effective constants.*

3.1.4 The primality test

Algorithm 3.3. *Input: an integer $n > 1$.*
Output: The algorithm determines whether n is prime or composite.

1. *Check if n is a power other than a first power. If it is, declare n composite and stop.*

2. *Let $D = \lceil (\log_2 n)^2 \rceil$, using Algorithm 3.1, find a period system $(r_1, q_1), \ldots, (r_k, q_k)$, for n with $d := q_1 q_2 \cdots q_k \geq D$ and $d = \mathcal{O}(D)$. (For n beyond an effectively computable bound, we will have $d \leq 4D$ as discussed before.)*

3. *Let $B = \lfloor d^{1/2} \log_2 n \rfloor$. Check to see if n has a prime factor in $[1, B]$. If n has such a factor that is not equal to n, declare n composite and stop. If n itself is this prime factor then declare n is prime and stop.*

4. *Using the Algorithm 3.2, we try to find a monic polynomial f in $(\mathbb{Z}/n\mathbb{Z})[x]$ of degree d and for which (3.1), (3.2) and (3.3) hold. This algorithm gives us a polynomial satisfying properties (3.1), (3.2) and (3.3), or conclude that n is composite, in which case we can conclude the same and stop.*

5. *For each integer a, $1 \leq a \leq B$, check if $(x + a)^n \equiv x^n + a \bmod (n, f(x))$. If one of these congruences fail, we conclude n is composite and the algorithm stops. Otherwise we declare n is prime and stop.*

Computational complexity:

Step 1: as in the first step of the original AKS method this computational cost is $\widetilde{\mathcal{O}}(\log n)^3$.
Step 2: as we saw previously, the algorithm 3.1 has a computational cost of $\widetilde{\mathcal{O}}(D^{12/11})$, as $D = \mathcal{O}((\log_2 n)^2)$, we have that the cost of step 2 is $\widetilde{\mathcal{O}}((\log n)^{24/11})$.
Step 3: as in step 3 of the AKS algorithm, we have to do $B = \mathcal{O}(d^{1/2} \log_2 n)$ operation, each one of cost $\mathcal{O}(\log n)$. With $d = \mathcal{O}(D) = \mathcal{O}((\log n)^2)$ thus the computational cost is $\mathcal{O}((\log n)^3)$.
Step 4: we saw in the previous subsection that this step has a computational cost of $\widetilde{\mathcal{O}}((\log n)^{26/5})$.
Step 5: each congruence can be verified in $\widetilde{\mathcal{O}}(d(\log n)^2)$, as we have to verify $B = \mathcal{O}(d^{1/2} \log_2 n)$ of this, the total cost is $\widetilde{\mathcal{O}}(d^{3/2}(\log n)^3)$. And since $d = \mathcal{O}(D) = \mathcal{O}((\log n)^2)$, the total computational cost is $\widetilde{\mathcal{O}}((\log n)^6)$.
Therefore the computational cost of this algorithm is $\widetilde{\mathcal{O}}((\log n)^6)$.
By Theorem 3.1 and Lemma 3.6 this algorithm is correct, hence we have a deterministic primality algorithm, which runs in polynomial time $\widetilde{\mathcal{O}}((\log n)^6)$.

We can see that the main difference between the original AKS primality test and the Lenstra-Pomerance algorithm, is the fact that we are not constrained to use the cyclotomic polynomial. In this case we have more freedom to choose the polynomials which give us a lower computational cost. The first of two main sources of this diminishment of the computational cost is that $r \leq \log_2^5 n$ for the original AKS while in this version, the degree of the polynomial is $d = \mathcal{O}((\log_2 n)^2)$. The second reason, is that in the AKS we have to repeat the most expensive step $\sqrt{r} \log n$ times, while in this new version, the equivalent step is repeated $\lfloor d^{1/2} \log_2 n \rfloor$ times.

It remains to prove Theorem 3.2, that is the purpose of the following section.

3.2 Proof of Theorem 3.2

The goal of this section is to prove the following theorem:

Theorem 3.4. *There is a deterministic algorithm $\mathcal{A}$ such that, for each integer $m > 0$, $\mathcal{A}$ produces an integer D_m and further, for each integer $n > 1$, and each integer D with $D > D_m$ and $D > (\log n)^{11/6+1/m}$, the algorithm finds a period system $(r_1, q_1), \dots, (r_k, q_k)$ for n with each $r_i < D^{6/11}$ and each $q_i < D^3/11$, with $D \leq q_1 q_2 \cdots q_k < 4D$, and with $k = \mathcal{O}((\log \log D)^2)$. The running time of this algorithm is $\widetilde{\mathcal{O}}(D^{12/11})$. The implied constant may depend on the choice of m.*

For this we need some lemmas that we are going to introduce in the first three subsections. In the last one we will prove Theorem 3.4.

3.2.1 Some preliminar results

Definition 3.4 (Dickman-de Brujin function). *Let $\rho(u)$ be a continuous function on $[0, \infty)$ that satisfies*

- $\rho(u) = 1$ *for* $0 \leq u \leq 1$,

- $u\rho'(u) = -\rho(u-1)$ *for* $u > 1$ *and*
- $\log \rho(u) = -u\log(u \log u) + \mathcal{O}(u)$ *for* $u \geq 2$.

Let $\pi(x)$ denote the number of primes in the interval $[1, x]$.

Lemma 3.7. *There is an absolute and effectively computable positive number* c_0 *with the following property. Let* α *be a number with* $0 < \alpha < 1$*, and let* x *be so large that* $\frac{\log x}{\log\log x} > \frac{1}{\alpha^4}$*. The number of primes* $r \leq x$ *such that* $r-1$ *has a divisor* m *with* $m > x^\alpha$ *and with* m *being* x^{α^2}*- smooth is at most* $D(\alpha)\pi(x)$*, where*

$$D(\alpha) = \frac{c_0}{\alpha^2}\Big(\frac{\rho(1/\alpha)}{\log(2/\alpha)} + \rho(1/\alpha^2)\Big).$$

For the proof, see [12].

Proposition 3.2. *Let* $n > 20$ *be a natural number, let* x *be a number such that* $x \geq (\log n)^{1+3/\log\log\log n}$*, and let* $\alpha = \alpha(x) = 1/\log\log x$*. Let* $R(x, n)$ *denote the number of primes* $r \leq x$ *such that* $r-1$ *has a prime divisor* $q > x^{\alpha^2}$ *with* $ord(n^{(r-1)/q}) \bmod r) = q$*. For* n *larger than an effectively computable bound, we have*

$$R(x, n) \geq (1 - D(\alpha))\pi(x) - x^{1-\alpha^2} - x^{1-\alpha/4}.$$

Proof. Let A be the number of primes r which divides n or some $n^j - 1$ for $j \leq x^\alpha$. We have

$$A < \log_2 n + \sum_{j \leq x^\alpha} j \log_2 n = \log_2 n(1 + \sum_{j\leq x^\alpha} j) < x^{2\alpha}\log_2 n < x^{1-\alpha/4}$$

if n is so large that $\log_2 n < x^{1-9\alpha/4}$. Thus, there are at least $\pi(x) - x^{1-\alpha/4}$ primes $r \leq x$ not dividing n, and not dividing any $n^j - 1$ for all $j \leq x^\alpha$. Such a prime r has $\text{ord}(n \bmod r) > x^\alpha$. Let q_r denote the greatest prime factor of $\text{ord}(n \bmod r)$. If x is so large that $\log/\log\log x > 1/\alpha^4$, we can apply Lemma 3.7, and we thus get that $q_r > x^{\alpha^2}$, but for at most $D(\alpha)\pi(x)$ exceptional primes $r \leq x$. Note that the number of integers $r \leq x$ with $r - 1$ divisible by some l^2 with l prime and $l > x^{\alpha^2}$ is at most

$$\sum_{\substack{l \text{ prime} \\ l > x^{\alpha^2}}} \frac{x}{l^2} = x \sum_{\substack{l \text{ prime} \\ l > x^{\alpha^2}}} \frac{1}{l^2} \leq x \int_{x^{\alpha^2}}^{x} \frac{dt}{t^2} = x(\frac{-1}{x} + \frac{1}{x^{\alpha^2}}) < x^{1-\alpha^2}.$$

Hence, there are at least

$$\pi(x) - (x^{1-\alpha/4}) + D(\alpha)\pi(\alpha) - x^{1-\alpha^2} = (1 - D(\alpha))\pi(\alpha) - x^{1-\alpha^2} - x^{1-\alpha/4}$$

primes $r \leq x$ with $q_r > x^{\alpha^2}$ and q_r^2 does not divide $r - 1$. For such a prime we have $ord(n^{(r-1)/q_r} \bmod r) = q_r$. This complete the proof of the proposition. □

Remark: Proposition 3.2 implies that for n, x as given, we have

$$\pi(x) - R(x, n) = \mathcal{O}(x/(\log x)^{\log\log\log x}).$$

In fact, it is clear that $R(x,n) \leq \pi(x)$ and by the previous proposition we have that

$$\pi(x) - R(x,n) = D(\alpha)\pi(\alpha) + x^{1-\alpha^2} + (x^{1-\alpha/4}).$$

Now note that

$$x/(\log x)^{\log\log\log x} = exp(\log x - \log\log\log x \log\log x).$$

Since

$$x^{1-\alpha/4} = \frac{x}{x^{1/4\log\log x}} = exp(\log x - \frac{1}{4\log\log x}\log x)$$

and for a sufficient large x

$$\frac{\log x}{\log\log x} > \log\log\log x \log\log x$$

we have that

$$(x^{1-\alpha/4}) = \mathcal{O}(x/(\log x)^{\log\log\log x}).$$

We also have that

$$x^{1-\alpha^2} = \frac{x}{x^{(1/\log\log x)^2}} = exp(\log x - \frac{1}{(\log\log x)^2}\log x),$$

since for a sufficient large x

$$\frac{\log x}{(\log\log x)^2} > \log\log\log x \log\log x$$

we have that

$$(x^{1-\alpha^2}) = \mathcal{O}(x/(\log x)^{\log\log\log x}).$$

Now lets see if

$$D(\alpha)\pi(\alpha) = \mathcal{O}(x/(\log x)^{\log\log\log x}).$$

and we will prove the remark.

$$D(\alpha) = \frac{c_0}{\alpha^2}\Big(\frac{\rho(1/\alpha)}{\log(2/\alpha)} + \rho(1/\alpha^2)\Big).$$

And

$$\log\rho(u) = -u\log(u\log u) + \mathcal{O}(u),$$

thus

$$\rho(u) = exp(-u\log(u\log u) + \mathcal{O}(u)) = \mathcal{O}(exp(-u\log u - u\log\log u)).$$

Then

$$\rho(1/\alpha) = \mathcal{O}(exp(-\log\log x\log\log\log x - \log\log x\log\log\log\log x))$$

and

$$\frac{\rho(1/\alpha)}{\log(2/\alpha)} = \mathcal{O}(exp(-\log\log x\log\log\log x - \log\log x\log\log\log\log x - \log\log\log\log x)).$$

We also have

$$\rho(1/\alpha^2) = \mathcal{O}(exp(-2(\log\log x)^2 \log\log\log x - (\log\log x)^2 \log\log\log\log x)).$$

Then

$$D(\alpha) = \frac{c_0}{\alpha^2}\mathcal{O}(exp(-\log\log x \log\log\log x - \log\log x \log\log\log\log x - \log 2 \log\log x))$$

$$D(\alpha) = \mathcal{O}(exp(-\log\log x \log\log\log x - \log\log x \log\log\log\log x - \log\log\log x + \log\log x)).$$

Then

$$D(\alpha)\pi(x) = \mathcal{O}(exp(\log x - \log\log x - \log\log x \log\log\log x - \log\log x \log\log\log\log x - \log\log\log\log x))$$

hence we have

$$D(\alpha)\pi(\alpha) = \mathcal{O}(x/(\log x)^{\log\log\log x}).$$

3.2.2 Sieved primes

The goal of this subsection is to prove the following result about the distribution of primes r with $r-1$ free of prime factors in some given set.

Proposition 3.3. *There are effectively computable positive functions $X_\epsilon, \delta_\epsilon$ of the positive variable ϵ satisfying the following property. If $x \geq X_\epsilon$ and $\mathcal{Q}$ is a set of primes in the interval $(1, x^{1/2}]$ with*

$$\sum_{q\in\mathcal{Q}} \frac{1}{q-1} \leq \frac{3}{11} - \epsilon.$$

Let B the number of primes $r \leq x$ such that every factor q of $r-1$ satisfies $q \leq x^{1/2}$ and $q \notin \mathcal{Q}$. Then $B \geq \delta_\epsilon x/(\log x)^2$.

Before proving this, we give some preliminary facts we will need.

Definition 3.5. *Let $q \in \mathbb{N}$, and $a \in \mathbb{N}$ such that $(a,q) = 1$, $x \in \mathbb{R}$, let*

- *$\pi(x,q,a)$ denote the number of primes $p \leq x$ with $p \equiv a \bmod p$;*
- $$\psi(x,q,a) = \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} \Lambda(n);$$
- $$\theta(x,q,a) = \sum_{\substack{p\leq x, p\ prime \\ p\equiv a \bmod q}} \log p;$$
- $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$,

where $\Lambda(n)$ is the von Mangoldt's function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^j \text{ for some prime } p \text{ and some positive integer } j \\ 0 & \text{if } n \text{ is not the power of a prime,} \end{cases}$$

and $\varphi(n)$ will represent the Euler totient function.

Lemma 3.8. *[Brun-Titchmarsh inequality] If $x > q$ we have*

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

For the proof, see [10].

Lemma 3.9. *[effective Bombieri-Vinogradov inequality] There are absolute, effectively computable numbers c_1, c_2 such that for all numbers $x \geq 3$, there is an integer set $\mathcal{S}(x)$ of cardinality 0 or 1 with $\mathcal{S}(x) \subset (\log x)^{1/2}, \exp((\log x)^{1/2})]$, such that for each number $Q \in [x^{1/3}\log x, x^{1/2}]$,*

$$\sum_{q \in Q}{}' \max_{2 \leq y \leq x} \max_{gcd(a,q)=1} |\psi(y, q, a) - \frac{y}{\varphi(q)}| \leq c_1 x^{1/2} Q (\log x)^5 + c_1 x \exp(-c_2 (\log x)^{1/2}),$$

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

For the proof, see [4].

Lemma 3.10. *With the same notation and hypotheses as Lemma 3.9, we have*

$$\sum_{q \in Q}{}' \max_{gcd(a,q)=1} |\pi(x, q, a) - \frac{\mathrm{li}(x)}{\varphi(q)}| \leq c_4 x^{1/2} Q (\log x)^5 + c_4 x \exp(-c_2 (\log x)^{1/2}),$$

where c_2 is as in Lemma 3.9, and c_4 is an absolute, effectively number.

Proof. First note than we can replace the expressions $\psi(y, q, a)$ in Lemma 3.9 with $\theta(y, q, a)$, since

$$|\psi(y, q, a) - \theta(y, q, a)| \leq \sum_{\substack{n \leq y \\ n \text{ is a prime power}}} \log y = \mathcal{O}(y^{1/2}\log y).$$

We have by the partial summation formula that

$$\pi(x, q, a) = \frac{\theta(x, q, a)}{\log x} + \int_2^x \frac{\theta(y, q, a)}{y(\log y)^2} dy. \tag{3.18}$$

This identity let's show that

$$|\pi(x, q, a) - \frac{\mathrm{li}(x)}{\varphi(q)}| \leq |\theta(x, q, a) - \frac{x}{\varphi(q)}|.$$

In fact

$$|\pi(x, q, a) - \frac{\mathrm{li}(x)}{\varphi(q)}| \leq |\frac{\theta(x, q, a)}{\log x} + \int_2^x \frac{\theta(y, q, a)}{y(\log y)^2} dy - \frac{1}{\varphi(q)} \int_2^x \frac{1}{\log y} dy|$$

$$\leq |\theta(x,q,a)\Big(\frac{1}{\log x}+\frac{x-2}{x(\log x)^2}\Big)-\frac{1}{\varphi(q)}\frac{x}{\log x}|$$
$$\leq \frac{1}{\log x}|\theta(x,q,a)-\frac{x}{\varphi(q)}| \leq |\theta(x,q,a)-\frac{x}{\varphi(q)}|.$$

Thus, the result follows directly from Lemma 3.9 and the identity (3.18). □

Lemma 3.11. *[Deshouillers-Iwaniec] There is an effectively computable function x_ϵ, defined for positive numbers ϵ, and absolute and effectively computable positive numbers c_5, c_6 with the following property. For arbitrary numbers ϵ, x, Q with $\epsilon > 0, x \geq x_\epsilon$, and $x^{1/2} \leq Q \leq x^{1-\epsilon}$, and for an arbitrary integer a with $0 \leq |a| < x^\epsilon$, we have for almost all integers $q \in [Q, 2Q]$ with $gcd(q,a) = 1$, the number of exceptions being less thaN $Qx^{-\epsilon c_6}$,*

$$\pi(x,q,a) \leq \frac{(4/3+\epsilon c_5)x}{\varphi(q)\log(x/q)}.$$

For the proof, see [5].

Definition 3.6 (The Möbius function). *For $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, we define $\mu(n)$ by*

$$\mu(n) = \begin{cases} 1 & \textit{if n=1} \\ (-1)^k & \textit{if } \alpha_i = 1 \textit{ for } i = 1,\dots,k, \\ 0 & \textit{otherwise} \end{cases}$$

Proposition 3.4. *Let f be a multiplicative function (i.e. $f(a\cdot b) = f(a)\cdot f(b)$) we have*

$$\sum_{d|n}\mu(d)f(d) = \prod_{p|n}(1-f(p)).$$

Proof. (From [2] chapter 2.) Let

$$g(n) = \sum_{d|n}\mu(d)f(d).$$

Then g is multiplicative, so to determine $g(n)$ it suffices to compute $g(p^\alpha)$. But

$$g(p^\alpha) = \sum_{d|p^\alpha}\mu(d)f(d) = \mu(1)f(1)+\mu(p)f(p) = 1-f(p).$$

Hence

$$g(n) = \prod_{p|n}g(p^\alpha) = \prod_{p|n}(1-f(p)).$$

□

Definition 3.7 (The Riemann zeta function). *Let $s \in \mathbb{C}$ such that $\Re s > 1$. We will call Riemann zeta function the following*

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}.$$

Theorem 3.5 (Euler identity)**.** *For $Re(s) > 1$ and $\mathcal{P}$ the set of primes,*

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{(1 - p^{-s})}.$$

For the proof, see [3]

Definition 3.8 (Euler-Mascheroni constant)**.** *We define*

$$\gamma = \lim_{t \to \infty} \sum_{n=1}^{t} (\frac{1}{n} - \log t).$$

We have the following result about this constant:

$$\gamma = \sum_{k=1}^{n} \frac{1}{k} - \log(n) - \mathcal{O}(1/n). \tag{3.19}$$

Definition 3.9 (Divisor function)**.** *For a real or complex α and any integer $n \geq 1$ we define*

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

the sum of the α-th powers of the divisors of n.
When $\alpha = 0$, $\sigma_0(n)$ is the number of divisors of n; this is often denoted by $d(n)$.
When $\alpha = 1$, $\sigma_1(n)$ is the sum of divisors of n; this is often denoted by $\sigma(n)$.

Proposition 3.5. *For $n \geq 2$*

$$\frac{n}{\varphi(n)} < \zeta(2) \frac{\sigma(n)}{n}.$$

Proof.

$$\frac{n}{\varphi(n)} = \frac{1}{\prod_{p|n}(1 - \frac{1}{p})} = \prod_{p|n} \frac{p}{p-1} = \prod_{p|n} \frac{p+1}{p} \frac{p^2}{p^2-1} = \prod_{p|n} \frac{(p+1)/p}{(p^2-1)/p^2}$$
$$= \frac{\prod_{p|n}(p+1)/p}{\prod_{p|n}(p^2-1)/p^2} < \frac{\prod_{p|n}(p+1)/p}{\prod_{p}(p^2-1)/p^2},$$

by Euler identity we have

$$\frac{n}{\varphi(n)} < \prod_{p|n}(1 + \frac{1}{p})\zeta(2).$$

Now

$$\sigma(n) = \prod_{p^\alpha | n} \frac{p^{\alpha+1} - 1}{p - 1},$$

then

$$\frac{\sigma(n)}{n} = \prod_{p^\alpha | n} \frac{p^{\alpha+1} - 1}{p^\alpha (p-1)}.$$

But $\forall p|n$ and $\alpha \geq 1$ as $p(p^{\alpha+1} - p) \geq p^{\alpha}(p^2 - 1)$ we have

$$\frac{p^{\alpha+1} - 1}{p^{\alpha}(p-1)} \geq \frac{p+1}{p}.$$

Then we have that

$$\frac{\sigma(n)}{n} \geq \prod_{p^{\alpha}|n} \frac{p+1}{p} > \prod_{p|n} \frac{p+1}{p}.$$

And we conclude as desired that

$$\frac{n}{\varphi(n)} < \zeta(2)\frac{\sigma(n)}{n}.$$

□

Proposition 3.6. *For $n \geq 2$*

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = \mathcal{O}(\log x).$$

Proof. By Proposition 3.5 we have that

$$\frac{1}{\varphi(n)} < \zeta(2)\frac{\sigma(n)}{n^2}.$$

Then

$$\sum_{n \leq x} \frac{1}{\varphi(n)} << \sum_{n \leq x} \frac{\sigma(n)}{n^2} = \sum_{n \leq x} \sum_{d|n} \frac{d}{n^2} = \sum_{qd \leq x} \frac{d}{q^2 d^2} = \sum_{d \leq x} \frac{1}{d} \sum_{d \leq x/d} \frac{1}{q^2}$$

$$= \sum_{d \leq x} \frac{1}{d}\Big(\zeta(2) - \sum_{q > x/d} \frac{1}{q^2}\Big) = \sum_{d \leq x} \frac{\zeta(2)}{d} + \mathcal{O}(\sum_{d \leq x} \frac{1}{d} \int_{x/d}^{+\infty} \frac{dt}{t^2})$$

$$= \sum_{d \leq x} \frac{1}{d} + \mathcal{O}(\sum_{d \leq x} \frac{1}{d}\frac{d}{x}) = \log x + \mathcal{O}(1).$$

Therefore

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = \mathcal{O}(\log x).$$

□

Lemma 3.12. *For any number $t > 1$, we have that*

$$\sum_{d < t} \frac{1}{\varphi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log t + \nu + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big),$$

where ζ is the Riemann zeta-function and where ν is a constant we will describe below.

Proof. Let's assume the following claim (we are going to prove it at the end of the proof).

Claim 1:

$$\frac{1}{\varphi(d)} = \frac{1}{d}\sum_{u|d}\frac{\mu^2(u)}{\varphi(u)}.$$

Hence putting $k \in \mathbb{N}$ such that $d = ku < t$, we have

$$\sum_{d<t}\frac{1}{\varphi(d)} = \sum_{d<t}\sum_{u|d}\frac{1}{d}\frac{\mu^2(u)}{\varphi(u)} = \sum_{u<t}\sum_{\substack{d<t\\u|d}}\frac{\mu^2(u)}{\varphi(u)}\frac{1}{d} = \sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}\sum_{\substack{d<t\\u|d}}\frac{1}{d}.$$

Since

$$\sum_{\substack{d<t\\u|d}}\frac{1}{d} = \sum_{\substack{d<t\\u|d}}\frac{1}{ku} = \sum_{k\leq t/u}\frac{1}{ku} = \frac{1}{u}\sum_{k\leq t/u}\frac{1}{k},$$

by (3.19) we have

$$\sum_{\substack{d<t\\u|d}}\frac{1}{d} = \frac{1}{u}(\gamma + \log\Big(\frac{t}{u}\Big) + \mathcal{O}(u/t)).$$

Therefore

$$\sum_{d<t}\frac{1}{\varphi(d)} = \sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}\frac{1}{u}(\gamma + \log\Big(\frac{t}{u}\Big) + \mathcal{O}(u/t))$$

$$\sum_{d<t}\frac{1}{\varphi(d)} = \log t\sum_{u<t}\frac{\mu^2(u)}{u\varphi(u)} + \sum_{u<t}\frac{\mu^2(u)(\gamma - \log u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}). \tag{3.20}$$

We define $\nu = \sum_{u<t}\frac{\mu^2(u)(\gamma-\log u)}{u\varphi(u)}$ and assume the following claim that we will prove at the end:

Claim 2:

$$\log t\sum_{u<t}\frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}) = \log t\prod_{p\text{ prime}}\Big(1 + \frac{1}{p(p+1)}\Big) + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big).$$

Hence (3.20) becomes

$$\sum_{d<t}\frac{1}{\varphi(d)} = \log t\prod_{p\text{ prime}}\Big(1 + \frac{1}{p(p+1)}\Big) + \nu + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big). \tag{3.21}$$

Using Theorem 3.5 we get

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} = \prod_{p\text{ prime}}\Big(\frac{1}{1-\frac{1}{p^2}}\Big)\Big(\frac{1}{1-\frac{1}{p^3}}\Big)\Big(1 - \frac{1}{p^6}\Big),$$

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} = \prod_{p\text{ prime}}\Big(\frac{p^2}{p^2-1}\Big)\Big(\frac{p^3}{p^3-1}\Big)\Big(\frac{p^6-1}{p^6}\Big) = \frac{p^2p^3(p^6-1)}{(p^2-1)(p^3-1)p^6},$$

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} = \prod_{p \text{ prime}} \frac{p^2p^3(p^3-1)(p+1)(p^2-p+1)}{(p-1)(p+1)(p^3-1)p^2p^3p} = \prod_{p \text{ prime}} \frac{p^2-p+1}{p(p-1)} = \prod_{p \text{ prime}} \Big(1+\frac{1}{p(p+1)}\Big).$$

Thus from (3.21) we have

$$\sum_{d<t} \frac{1}{\varphi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log t + \nu + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big)$$

and the lemma is proved. It remains to prove the two claims:

Proof of claim 1:

$$\frac{1}{\varphi(d)} = \frac{1}{d}\sum_{u|d} \frac{\mu^2(u)}{\varphi(u)}.$$

Let $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$, let's do the proof by induction:
Case $s=1$: ($i.e$ $n=p^\alpha$). We have $\varphi(n)^{-1} = \varphi(p^\alpha)^{-1} = (p^\alpha - p^{\alpha-1})^{-1} = ((p-1)p^{\alpha-1})^{-1}$ and

$$\frac{1}{d}\sum_{u|d}\frac{\mu^2(u)}{\varphi(u)} = \frac{1}{p^\alpha}(1+\frac{1}{\varphi(p)}) = \frac{1}{(p-1)p^{\alpha-1}}.$$

Inductive step: suppose the claim is true for $d = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{s-1}^{\alpha_{s-1}}$, to simplify the equations let $B_d = \sum_{u|d}\frac{\mu^2(u)}{\varphi(u)}$ and $D = p^\alpha p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ where $p = p_s$ and $\alpha = \alpha_s$. Let's show that $B_D = \frac{D}{\varphi(D)}$:

$$\frac{D}{\varphi(D)} = \frac{dp^\alpha}{\varphi(dp^\alpha)} = \frac{d}{\varphi(d)}\frac{p^\alpha}{\varphi(p^\alpha)} = \frac{p^\alpha}{p^\alpha - p^{\alpha-1}}B_d = \frac{1}{1-(1/p)}B_d = \frac{p}{(p-1)}B_d.$$

Now $B_D = \sum_{u|D}\frac{\mu^2(u)}{\varphi(u)} = B_d + \sum_{u|d}\frac{1}{\varphi(up)} = B_d + \frac{1}{\varphi(p)}B_d = B_d(\frac{p}{p-1})$. And the claim is proved.

Proof of claim 2:

$$\log t\sum_{u<t}\frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}) = \log t \prod_{p \text{ prime}}\Big(1+\frac{1}{p(p+1)}\Big) + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big)$$

Let

$$A = \log t\sum_{u<t}\frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}),$$

$$A = \log t\sum_{u}\frac{\mu^2(u)}{u\varphi(u)} - \log t\sum_{u\geq t}\frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}),$$

since $\frac{\mu(n)}{n\varphi(n)}$ is a multiplicative function we can use Proposition 3.4:

$$A = \log t \prod_{p \text{ prime}}(1-\frac{\mu(p)}{p\varphi(p)}) - \log t\sum_{u\geq t}\frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t}\sum_{u<t}\frac{\mu^2(u)}{\varphi(u)}),$$

$$A = \log t \prod_{p \text{ prime}} (1 + \frac{1}{p(p-1)}) - \log t \sum_{u \geq t} \frac{\mu^2(u)}{u\varphi(u)} + \mathcal{O}(\frac{1}{t} \sum_{u<t} \frac{\mu^2(u)}{\varphi(u)}).$$

By Proposition 3.6 we have that

$$\sum_{u<t} \frac{\mu^2(u)}{\varphi(u)} \leq \sum_{u<2t} \frac{1}{\varphi(u)} = \mathcal{O}(\log(2t)).$$

Hence

$$A = \log t \prod_{p \text{ prime}} (1 + \frac{1}{p(p-1)}) + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big).$$

□

We can now prove Proposition 3.3 (that we rewrite here the statement):

Proposition 3.3

There are effectively computable positive functions $X_\epsilon, \delta_\epsilon$ of the positive variable ϵ satisfying the following property. If $x \geq X_\epsilon$ and $\mathcal{Q}$ is a set of primes in the interval $(1, x^{1/2}]$ with

$$\sum_{q \in \mathcal{Q}} \frac{1}{q-1} \leq \frac{3}{11} - \epsilon. \tag{3.22}$$

Let B the number of primes $r \leq x$ such that every factor q of $r-1$ satisfies $q \leq x^{1/2}$ and $q \notin \mathcal{Q}$. Then $B \geq \delta_\epsilon x/(\log x)^2$.

Proof. Let $0 < \epsilon < 3/11$, x a large number, $\mathcal{Q}$ a set of primes satisfying (3.3). For a prime $r \leq x$, let $g(r)$ denote the number of factorizations of $r-1$ as lh, where

1. $x^{1/2-2\beta} < l < x^{1/2-\beta}$, and $x^{1/2+\beta} < l < x^{1/2+2\beta}$,

2. lh is not divisible by any member of $\mathcal{Q}$,

3. l is not divisible by any member of $\mathcal{S}(x)$,

4. h is not divisible by any prime larger than $x^{1/2}$,

where $\mathcal{S}(x)$ is defined in Lemma 3.9. Note that $g(r)$ can be 0, let N denote the number of primes $r \leq x$ with $g(r) > 0$. Our goal is to get a good lower bound A for N, in fact if $A = \delta_\epsilon x/(\log x)^2$ we have $B \geq N \geq A = \delta_\epsilon x/(\log x)^2$ and the proposition is proved.

From Cauchy's inequality, we obtain

$$\Big(\sum_{r \leq x} g(r)\Big)^2 \leq \Big(\sum_{r \leq x} g(r)^2\Big)\Big(\sum_{r \leq x} 1\Big),$$

hence we have that

$$N \geq \Big(\sum_{r \leq x} g(r)\Big)^2 \Big(\sum_{r \leq x} g(r)^2\Big)^{-1}.$$

Now we are going to found an upper bound for $\sum_{r\leq x} g(r)^2$ and a lower bound for $\Big(\sum_{r\leq x} g(r)\Big)^2$ in order to found A.

In order to found the upper bound for $\sum_{r\leq x} g(r)^2$ we ignore the non-divisibility requirements in the definition of $g(r)$. We denote $[a,b]$ for the least common multiple of a,b,

$$\sum_{r\leq x} g(r)^2 \leq \sum_{r\leq x} \sum_{\substack{l_1,l_2|r-1\\ x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}}} 1 = \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \sum_{\substack{l_1,l_2|r-1\\ r\leq x}} 1 = \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \pi(x,[l_1,l_2],1).$$

By Lemma 3.8 we have that

$$\sum_{r\leq x} g(r)^2 \leq \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{2x}{\varphi([l_1,l_2])\log(x/[l_1,l_2])}.$$

We know that $[l_1,l_2] < x^{1/2-\beta}x^{1/2-\beta} = x^{1-2\beta}$, hence $\frac{1}{\log(x/[l_1,l_2])} < \frac{1}{\log(x/x^{1-2\beta})}$ and we have

$$\sum_{r\leq x} g(r)^2 \leq \frac{2x}{\log(x^{2\beta})} \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1,l_2])} = \frac{x}{\beta\log x} \sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1,l_2])}.$$

Since

$$\sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1,l_2])} = \sum_{d<x^{1/2-\beta}} \sum_{\substack{gcd(l_1,l_2)=d\\ x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}}} \frac{1}{\varphi(l_1l_2/d)}$$

we get

$$\sum_{x^{1/2-2\beta}<l_1,l_2<x^{1/2-\beta}} \frac{1}{\varphi([l_1,l_2])} \leq \sum_{d<x^{1/2-\beta}} \sum_{a,b<(x^{1/2-\beta})/d} \frac{1}{\varphi(abd)} \leq \Big(\sum_{d<x} \frac{1}{\varphi(d)}\Big)^3.$$

The last inequality holds since $\sum_{d<x^{1/2-\beta}} \sum_{a,b<(x^{1/2-\beta})/d} \frac{1}{\varphi(abd)} \leq \sum_{d\leq x} \sum_{a,b<x/d} \frac{1}{\varphi(abd)} \leq \sum_{d\leq x} \frac{1}{\varphi(d)} \sum_{a<x/d} \frac{1}{\varphi(a)} \sum_{b<x/d} \frac{1}{\varphi(b)} \leq \Big(\sum_{d<x} \frac{1}{\varphi(d)}\Big)^3$.

Therefore we have that

$$\sum_{r\leq x} g(r)^2 \leq \frac{x}{\beta\log x}\Big(\sum_{d<x} \frac{1}{\varphi(d)}\Big)^3.$$

Using Lemma 3.12 we have

$$\sum_{r\leq x} g(r)^2 \leq \frac{x}{\beta\log x}\Big(\frac{\zeta(2)\zeta(3)}{\zeta(6)}\log x + \nu + \mathcal{O}\Big(\frac{\log(2x)}{x}\Big)\Big)^3.$$

Recalling that $\nu = \sum_{u<t} \frac{\mu^2(u)(\gamma-\log u)}{u\varphi(u)}$, we have

$$\sum_{r\leq x} g(r)^2 \leq \frac{x}{\beta\log x}\Big(\frac{\zeta(2)\zeta(3)}{\zeta(6)}\log x\Big)^3 + \nu^3 + \mathcal{O}\Big(\frac{\log(2x)}{x}\Big)^3,$$

$$\sum_{r\le x} g(r)^2 = \mathcal{O}\Big(\frac{x(\log x)^2}{\beta}\Big). \tag{3.23}$$

This is the desired upper bound. Now let's found a lower bound for $\sum_{r\le x} g(r)$:
Let $\mathcal{L}$ denote the set of integers l with $x^{1/2-2\beta} < l < x^{1/2-\beta}$, and l is not divisible by any member of $\mathcal{S}(x)$. And $\mathcal{H}$ denote the set of integers h with $x^{1/2+\beta} < h < x^{1/2+2\beta}$. By the definition of $g(r)$ we have that

$$\sum_{r\le x} g(r) \ge \sum_{l\in\mathcal{L}} \pi(x,l,1) - \sum_{\substack{l\in\mathcal{L}\\ q\mid l \text{ for some } q\in\mathcal{Q}}} \pi(x,l,1) -$$
$$\sum_{\substack{h\in\mathcal{H}\\ q\mid h \text{ for some } q\in\mathcal{Q}}} \pi(x,h,1) - \sum_{\substack{h\in\mathcal{H}\\ q\mid h \text{ for some prime } q>x^{1/2}}} \pi(x,h,1).$$

$$= S_1 - S_2 - S_3 - S_4.$$

Let's give an estimation for S_1, S_2, S_3 and S_4:

- For S_1 we use Lemma 3.10 we have

$$\sum_{l\in\mathcal{L}} |\pi(x,l,1) - \frac{\mathrm{li}(x)}{\varphi(l)}| = \mathcal{O}(x^{1/2}x^{1/2-\beta}(\log x)^5) = \mathcal{O}(x^{1-\beta/2}).$$

Hence,

$$\sum_{l\in\mathcal{L}} (\pi(x,l,1) - \frac{\mathrm{li}(x)}{\varphi(l)}) \le \sum_{l\in\mathcal{L}} |\pi(x,l,1) - \frac{\mathrm{li}(x)}{\varphi(l)}| = \mathcal{O}(x^{1-\beta/2}).$$

Then

$$S_1 = \mathrm{li}(x)\sum_{l\in\mathcal{L}} \frac{1}{\varphi(l)} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big). \tag{3.24}$$

Using Lemma 3.12 to estimate the sum of $\frac{1}{\varphi(l)}$ and letting $\tau = \frac{\zeta(2)\zeta(3)}{\zeta(6)}$ and $\xi = \tau\beta$, we have that

$$\sum_{d<t} \frac{1}{\varphi(d)} = \tau\log t + \nu + \mathcal{O}\Big(\frac{\log(2t)}{t}\Big),$$

thus

$$\sum_{l\in\mathcal{L}} \frac{1}{\varphi(l)} = \sum_{l\le x^{1/2-\beta}} \frac{1}{\varphi(l)} - \sum_{l\le x^{1/2-2\beta}} \frac{1}{\varphi(l)} - \sum_{\substack{\bar{l} \text{ such that } \bar{q}\mid\bar{l}\\ \text{where } \mathcal{S}(x)=\{\bar{q}\}}} \frac{1}{\varphi(\bar{l})},$$

$$\sum_{l\in\mathcal{L}} \frac{1}{\varphi(l)} = \tau\log\Big(\frac{x^{1/2-\beta}}{x^{1/2-2\beta}}\Big) + \mathcal{O}\Big(\frac{\log(2x^{1/2-\beta})}{x^{1/2-\beta}}\Big) + \sum_{\substack{\bar{l} \text{ such that } \bar{q}\mid\bar{l}\\ \text{where } \mathcal{S}(x)=\{\bar{q}\}}} \frac{1}{\varphi(\bar{l})}.$$

Now $\varphi(\bar{l}) > \frac{\bar{l}}{(\log\log\bar{l})^A}$ for a positive constant A, and $\bar{l} > \sqrt{\log x}$ by the definition of $\mathcal{S}(x)$. So $\varphi(\bar{l}) > \frac{\sqrt{\log x}}{(\log\log x)^A} > (\log x)^{1/4}$. Hence

$$\sum_{\substack{\bar{l} \text{ such that } \bar{q}|\bar{l} \\ \text{where } \mathcal{S}(x)=\{\bar{q}\}}} \frac{1}{\varphi(\bar{l})} = \mathcal{O}\Big(\frac{x^{1/2-\beta}}{(\log x)^{1/4}}\Big)$$

and we have

$$\sum_{l\in\mathcal{L}} \frac{1}{\varphi(l)} = \xi\log x + \mathcal{O}\Big(\frac{x}{(\log x)^{1/4}}\Big).$$

Thus

$$S_1 = \xi x + \mathcal{O}\Big(\frac{x}{(\log x)^{1/4}}\Big).$$

- For

$$S_2 = \sum_{\substack{l\in\mathcal{L} \\ q|l \text{ for some } q\in\mathcal{Q}}} \pi(x,l,1) = \sum_{q\in\mathcal{Q}}\sum_{l\in L, q|l} \pi(x,l,1)$$

using (3.24) we get

$$S_2 = \sum_{q\in\mathcal{Q}}\sum_{l\in L,q|l} \mathrm{li}(x)\sum_{l\in\mathcal{L}}\frac{1}{\varphi(l)} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big),$$

$$S_2 \leq \mathrm{li}(x)\sum_{q\in\mathcal{Q}}\sum_{qd\in L}\frac{1}{\varphi(qd)} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big)$$

$$S_2 \leq \mathrm{li}(x)\sum_{q\in\mathcal{Q}}\frac{1}{q-1}\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big).$$

Using now Lemma 3.12 we have

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)}\begin{cases} = \xi\log x + \mathcal{O}(q\log(2x)x^{2\beta-1/2}), & \text{for } q < x^{1/2-2\beta} \\ \leq \xi\log x + \mathcal{O}(q\log(2x)x^{\beta-1/2}), & \text{for } x^{1/2-2\beta} \leq q \leq x^{1/2-\beta} \\ = 0, & \text{for } q > x^{1/2-\beta}. \end{cases}$$

This is clear for $q > x^{1/2-\beta}$. Now for $x^{1/2-2\beta} \leq q \leq x^{1/2-\beta}$, since $x^{1/2-2\beta}/q \leq 1$ we have that

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)} = \sum_{1<l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)} \leq \sum_{l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)}.$$

By Lemma 3.12 we have that

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q}\frac{1}{\varphi(l)} \leq \tau\log(\frac{x^{1/2-\beta}}{q}) + \mathcal{O}\Big(\frac{\log(2x^{1/2-\beta})/q}{x^{1/2-\beta}/q}\Big)$$

since $\frac{1}{x^{1/2-\beta}} \leq \frac{1}{q} \leq \frac{1}{x^{1/2-2\beta}}$ we have that

$$\log(\frac{x^{1/2-\beta}}{q}) \leq \log(\frac{x^{1/2-\beta}}{x^{1/2-2\beta}}) = \beta \log x.$$

Then in this case we have

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} \leq \xi \log x + \mathcal{O}(q \log(2x) x^{\beta-1/2})$$

as desired.

Now in the first case when $q < x^{1/2-2\beta}$ we have that

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} = \sum_{l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} - \sum_{l\leq x^{1/2-2\beta}/q} \frac{1}{\varphi(l)}.$$

By Lemma 3.12 we have

$$\sum_{l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} = \tau \log(\frac{x^{1/2-\beta}}{q}) + \nu + \mathcal{O}\Big(\frac{\log(2x^{1/2-\beta})/q}{x^{1/2-\beta}/q}\Big)$$

and

$$\sum_{l\leq x^{1/2-2\beta}/q} \frac{1}{\varphi(l)} = \tau \log(\frac{x^{1/2-2\beta}}{q}) + \nu + \mathcal{O}\Big(\frac{\log(2x^{1/2-2\beta})/q}{x^{1/2-2\beta}/q}\Big).$$

But in this case

$$\frac{\log(2x^{1/2-\beta})/q}{x^{1/2-\beta}/q} \ll \frac{\log(2x^{1/2-2\beta})/q}{x^{1/2-2\beta}/q},$$

then we have that

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} = \tau \log(x^{\beta}) + \mathcal{O}\Big(\frac{\log(2x^{1/2-2\beta})/q}{x^{1/2-2\beta}/q}\Big).$$

Hence

$$\sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} = \xi \log x + \mathcal{O}(q \log(2x) x^{2\beta-1/2}).$$

We have from before that

$$S_2 \leq \mathrm{li}(x) \sum_{q\in\mathcal{Q}} \frac{1}{q-1} \sum_{x^{1/2-2\beta}/q<l<x^{1/2-\beta}/q} \frac{1}{\varphi(l)} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big).$$

Then, we have

$$S_2 \leq \xi x \sum_{q\in\mathcal{Q}} \frac{1}{q-1} + \mathcal{O}\Big(\frac{x}{\log x}\Big).$$

- For S_3 we use Lemma 3.11 with "ϵ" chosen as β and with "Q" being various power of 2 so that the intervals $[Q, 2Q]$ cover the interval $(x^{1/2+\beta}, x^{1/2+2\beta})$. If h is an exceptional modulus in Lemma 3.11, we use the trivial estimate $\pi(x,h,1) \leq x/h$. We thus get

$$S_3 = \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some } q\in\mathcal{Q}}} \pi(x,h,1) \leq (4/3+\mathcal{O}(\beta))x \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some } q\in\mathcal{Q}}} \frac{1}{\varphi(h)\log(x/h)} + \sum_{h \text{ exeption}} \frac{x}{h}.$$

Since

$$\sum_{h \text{ exeption}} \frac{x}{h} = x \sum_{i=1}^{\mathcal{O}(\log x)} \sum_{\substack{h\in(Q_i,2Q_i) \\ \text{exeption}}} \frac{1}{h} \leq x \sum_{i=1}^{\mathcal{O}(\log x)} \frac{Q_i x^{\mathcal{O}(\beta)}}{Q_i} = x^{1-\mathcal{O}(\beta)}\mathcal{O}(\log x) = \mathcal{O}(\frac{x}{\log x})$$

we have

$$S_3 \leq (4/3+\mathcal{O}(\beta))x \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some } q\in\mathcal{Q}}} \frac{1}{\varphi(h)\log(x/h)} + \mathcal{O}(\frac{x}{\log x}),$$

$$S_3 \leq (8/3+\mathcal{O}(\beta))\frac{x}{\log x} \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some } q\in\mathcal{Q}}} \frac{1}{\varphi(h)} + \mathcal{O}(\frac{x}{\log x}),$$

$$S_3 \leq (8/3+\mathcal{O}(\beta))\frac{x}{\log x}\sum_{q\in\mathcal{Q}} \frac{1}{q-1} \sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} + \mathcal{O}(\frac{x}{\log x}).$$

Thus

$$S_3 = (8/3+\mathcal{O}(\beta))\xi x \sum_{q\in\mathcal{Q}} \frac{1}{q-1} + \mathcal{O}(\frac{x}{\log x}).$$

Since using Lemma 3.12 we have

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} \begin{cases} = \xi\log x + \mathcal{O}(q\log(2x)x^{-\beta-1/2}), & \text{for } q < x^{1/2+\beta} \\ \leq \xi\log x + \mathcal{O}(q\log(2x)x^{-2\beta-1/2}), & \text{for } x^{1/2+\beta} \leq q \leq x^{1/2+2\beta} \\ = 0, & \text{for } q > x^{1/2+2\beta}. \end{cases}$$

This is clear for $q > x^{1/2+2\beta}$. Now for $x^{1/2+\beta} \leq q \leq x^{1/2+2\beta}$, since $x^{1/2+\beta}/q \leq 1$ we have that

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} = \sum_{1<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} \leq \sum_{h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)}.$$

By Lemma 3.12 we have that

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} \leq \tau\log(\frac{x^{1/2+2\beta}}{q}) + \mathcal{O}\Big(\frac{\log(2x^{1/2+2\beta})/q}{x^{1/2+2\beta}/q}\Big)$$

since $\frac{1}{x^{1/2+2\beta}} \leq \frac{1}{q} \leq \frac{1}{x^{1/2+\beta}}$ we have that

$$\log(\frac{x^{1/2+2\beta}}{q}) \leq \log(\frac{x^{1/2+2\beta}}{x^{1/2+\beta}}) = \beta \log x.$$

Then in this case we have

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} \leq \xi \log x + \mathcal{O}(q \log(2x) x^{-2\beta-1/2})$$

as desired.

Now in the first case when $q < x^{1/2+\beta}$ we have that

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} = \sum_{h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} - \sum_{h\leq x^{1/2+\beta}/q} \frac{1}{\varphi(h)}.$$

By Lemma 3.12 we have

$$\sum_{h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} = \tau \log(\frac{x^{1/2+2\beta}}{q}) + \nu + \mathcal{O}\Big(\frac{\log(2x^{1/2+2\beta})/q}{x^{1/2+2\beta}/q}\Big)$$

and

$$\sum_{h\leq x^{1/2+\beta}/q} \frac{1}{\varphi(h)} = \tau \log(\frac{x^{1/2+\beta}}{q}) + \nu + \mathcal{O}\Big(\frac{\log(2x^{1/2+\beta})/q}{x^{1/2+\beta}/q}\Big).$$

But in this case

$$\frac{\log(2x^{1/2+2\beta})/q}{x^{1/2+2\beta}/q} \ll \frac{\log(2x^{1/2+\beta})/q}{x^{1/2+\beta}/q},$$

then we have that

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} = \tau \log(x^{\beta}) + \mathcal{O}\Big(\frac{\log(2x^{1/2+\beta})/q}{x^{1/2+2\beta}/q}\Big).$$

Hence

$$\sum_{x^{1/2+\beta}/q<h<x^{1/2+2\beta}/q} \frac{1}{\varphi(h)} = \xi \log x + \mathcal{O}(q \log(2x) x^{-\beta-1/2}).$$

- For

$$S_4 = \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \pi(x, h, 1)$$

we use the Lemma 3.8 and we thus get

$$S_4 \leq 2x \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)\log(x/h)},$$

$$S_4 \leq \frac{2x}{\log(x^{1/2-\beta})} \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)},$$

$$S_4 = \mathcal{O}\Big(\frac{x}{\log x} \sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)}\Big).$$

Now

$$\sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)} \leq \sum_{\substack{x^{1/2}<q<x^{1/2+2\beta} \\ q \text{ prime}}} \frac{1}{q-1} \sum_{h\leq x^{2\beta}} \frac{1}{\varphi(h)}.$$

By Lemma 3.12 we have

$$\sum_{t\leq x^{2\beta}} \frac{1}{\varphi(h)} = \tau \log(x^{2\beta}) + \mathcal{O}(\frac{\log(2x^{2\beta})}{\log(x^{2\beta})}) = \mathcal{O}(\beta \log x).$$

And by Mertens's theorem we have that

$$\sum_{p\leq U} \frac{1}{p} \sim \log\log U,\ U \to \infty.$$

For $q \geq 2$ we have $\frac{1}{q-1} \leq \frac{c}{q}$ then we have that

$$\sum_{\substack{x^{1/2}<q<x^{1/2+2\beta} \\ q \text{ prime}}} \frac{1}{q-1} \sim \log\log(x^{1/2+2\beta}) - \log\log(x^{1/2}) = \mathcal{O}(\beta).$$

Thus

$$\sum_{\substack{h\in\mathcal{H} \\ q|h \text{ for some prime } q>x^{1/2}}} \frac{1}{\varphi(h)} = \mathcal{O}(\beta^2 \log x).$$

And so we get

$$S_4 = \mathcal{O}(\beta^2 x).$$

Now putting together the estimates for S_1, S_2, S_3 and S_4, we have that

$$\sum_{r\leq x} g(r) \geq \xi x\Big(1 - (11/3 + \mathcal{O}(\beta)) \sum_{q\in\mathcal{Q}} \frac{1}{q-1}\Big) + \mathcal{O}(\beta^2 x) + \mathcal{O}\Big(\frac{x}{(\log x)^{1/4}}\Big).$$

Using $\sum_{q\in\mathcal{Q}} \frac{1}{q-1} \leq 3/11 - \epsilon$ we obtain

$$\sum_{r\leq x} g(r) \geq \xi x\Big(1 - (11/3 + \mathcal{O}(\beta))(\frac{3}{11} - \epsilon)\Big) + \mathcal{O}\Big(\frac{x}{(\log x)^{1/4}}\Big),$$

and hence

$$\sum_{r\leq x} g(r) \geq \xi x\Big(\frac{11}{3}\epsilon + \mathcal{O}(\beta)\Big) + \mathcal{O}\Big(\frac{x}{(\log x)^{1/4}}\Big).$$

Thus if β is chosen as a small absolute constant times ϵ, we have

$$\sum_{r\leq x} g(r) \geq \epsilon\xi x.$$

Now we have

$$\sum_{r\leq x} g(r) \geq \epsilon\xi x \text{ and } \sum_{r\leq x}(g(r))^2 = \mathcal{O}\Big(\frac{1}{\epsilon}x(\log x)^2\Big),$$

and

$$N \geq \Big(\sum_{r\leq x} g(r)\Big)^2\Big(\sum_{r\leq x}(g(r))^2\Big)^{-1}.$$

Hence

$$N \geq (\epsilon\xi x)^2\Big(\mathcal{O}\Big(\frac{1}{\epsilon}x(\log x)^2\Big)\Big)^{-1} = (\epsilon\xi x)^2\mathcal{O}\Big(\frac{\epsilon}{x(\log x)^2}\Big) = \mathcal{O}\Big(\frac{\epsilon^5\tau x}{(\log x)^2}\Big) = \mathcal{O}\Big(\frac{\epsilon^5 x}{(\log x)^2}\Big)$$

so, we may choose δ_ϵ as a small constant time ϵ^5, and the theorem is proved.

□

3.2.3 The continuous Frobenius problem

Given a finite set of positive coprime integers, every sufficiently large integer may be written as a nonnegative integral linear combination of the given set. The problem known as the Frobenius postage problem is to find the largest integer which cannot be so represented.
The goal of this subsection is to prove the following result that might be viewed as a continuous analogue of the Frobenius postage problem.

Proposition 3.7. *[Daniel Bleichenbacher] 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 $t \in (0,1]$, the dx/x measure of $S \cap (0,t)$ is less than t.*

Proof. Let M be a positive differentiable measure on the positive reals, with derivative m. Thus if $\mathcal{S}$ is any measurable subset of the positive reals with characteristic function $\chi_{\mathcal{S}}$, we have

$$M(\mathcal{S}) = \int_0^\infty \chi_{\mathcal{S}}(x)m(x)dx.$$

Let S be as in the hypothesis of the theorem, and $S_t = S \cap (0,t)$. Let suppose that S_t is a finite union of open intervals; that is

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

where

$$t \geq b_1 \geq a_1 \geq \cdots \geq b_n \geq a_n \geq 0. \tag{3.25}$$

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

$$\text{either } \mathbf{h} \cdot \mathbf{a} \geq 1 \text{ or } \mathbf{h} \cdot \mathbf{b} \leq 1. \tag{3.26}$$

That is, it is not 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

$$t \geq b_1 > b_2 > \cdots > b_n > 0. \tag{3.27}$$

If $j > 1/b_n$ is an integer, taking $\mathbf{h} = (0, \ldots, 0, j)$ we have $\mathbf{h} \cdot \mathbf{b} = jb_n > 1$, then (3.26) implies that $ja_n = \mathbf{h} \cdot \mathbf{a} \geq 1$ thus that $a_n \geq 1/j$. In particular, we must have $a_n \geq b_n/2$ (taking for example $j = \lceil 1/b_n \rceil + 1$). Hence, the set of vectors $\mathbf{a}$ which, with the fixed vector $\mathbf{b}$, satisfy (3.25) and (3.26) form a compact subset of $(\mathbb{R}_{>0})^n$. Thus there is a choice of the vector $\mathbf{a}$ which maximizes $M(S_t)$ for the given vector $\mathbf{b}$. We will call this maximum $M_{\mathbf{b}}$ and assume that $\mathbf{a}$ is fixed at a choice which produces this maximum.

Note that as we allow empty intervals, it's possible that we have the case $a_i = b_i$. It is clear that if we delete some coordinates from $\mathbf{b}$ to form a shorter vector **b'** we will have $M_{\mathbf{b'}} \leq M_{\mathbf{b}}$. Then by possibly replacing $\mathbf{b}$ with a shorter vector, we may assume that each $a_i < b_i$.
If we can assume that $a_{i-1} > b_i$ for $2 \leq i \leq n$ we may assume that the vector $\mathbf{a}$ satisfies

$$1 \geq b_1 > a_1 > \cdots > b_n > a_n > 0. \tag{3.28}$$

Let's show that we can assume that $a_{i-1} > b_i$ for $2 \leq i \leq n$. Suppose that $a_{i-1} = b_i$, we may consolidate the two intervals $(a_i, b_i), (a_{i-1}, b_{i-1})$ into an interval (a_i, b_{i-1}). In fact, if 1 is not in the additive semigroup generated by $S_t \cup b_i$, we can consolidate it; if not 1 is representable by a sum of members of $S_t \cup b_i$, so that b_i must be involved in the sum, say with a positive integral coefficient c. If $c = 1$, for a suitable small ϵ we can replace in the sum b_i by $b_i + \epsilon$ and then replace another member $x \in S_t$ of the sum with $x - \epsilon$ (there must be another number in the sum since $b_i < 1$). If ϵ is small enough, $b_i + \epsilon$ and $x - \epsilon$ are in S_t, and we have represented 1 as a sum of members of S_t, a contradiction. Now if $c \geq 2$, then since $b_i + \frac{\epsilon}{c-1}$ and $b_i - \epsilon$ are both in S_t for ϵ a small enough, we can replace cb_i in the sum by $(c-1)(b_i + \frac{\epsilon}{c-1}) + (b_i - \epsilon)$, and so 1 is represented as a sum of members of S_t, a contradiction. Hence we may assume that $a_{i-1} > b_i$ for $2 \leq i \leq n$ and then that $\mathbf{a}$ satisfies (3.28).
Now let

$$H_o = \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} < 1\},$$

$$H_1 = \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} = 1\},$$

$$H_2 = \{\mathbf{h} \in (\mathbb{N}_{\geq 0})^n : \mathbf{h} \cdot \mathbf{a} > 1\}.$$

Since the a_i are fixed positive natural numbers, it follows that H_0, H_1 are finite sets. We now show that by contradiction that H_1 is not empty. Suppose that H_1 is empty and let $\mathbf{u} = (1, 1, \ldots, 1)$.

Claim: if $\epsilon > 0$ is small enough, then the pair $\mathbf{a} - \epsilon\mathbf{u}, \mathbf{b}$ still satisfies (3.26) and (3.28). Assuming this claim, we will have a choice for S_t with strictly larger $M(S_t)$, a contradiction, thus H_1 is non empty.

Let's now prove the claim: it is clear that we may choose $\epsilon > 0$ small enough so as to preserve the condition (3.28). For $\mathbf{h} \in H_0$ we have $\mathbf{h} \cdot \mathbf{b} \leq 1$, so the vectors in H_0 do not pose a problem for condition (3.26). Since H_1 is assumed empty, H_1 also does not pose a problem. Now there are only finitely many $\mathbf{h} \in H_2$ with $\mathbf{h} \cdot \mathbf{a} \leq 2$. In this case, we can found an $\epsilon > 0$ small enough so that $\mathbf{h} \cdot (\mathbf{a} - \epsilon\mathbf{u}) \geq 1$ for all such $\mathbf{h}$. Now if $\mathbf{h} \cdot \mathbf{a} > 2$ and if we choose $\epsilon < a_n/2$, then $\mathbf{h} \cdot (\mathbf{a} - \epsilon\mathbf{u}) > \frac{1}{2}\mathbf{h} \cdot \mathbf{a} > 1$. Hence $\mathbf{a} - \epsilon\mathbf{u}, \mathbf{b}$ still satisfy (3.26) and (3.28). Hence the claim is proved and H_1 is non empty.

Let $\mathbf{h} \in H_1$, and for notational convenience, let $a_{n+1} = b_{n+1} = 0$, and $\mathbf{e}_k$ be the k-th standard basis vector in $\mathbb{R}^n$. For any k, 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 $k = n$. Then $\mathbf{h}' \in H_0$. Hence, from (3.26), we have that $\mathbf{h}' \cdot \mathbf{b} \leq 1$. That is,

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

Since $\mathbf{h} \in H_1$ we get that

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

Thus we have

$$h_k \mathbf{h} \cdot (\mathbf{b} - \mathbf{a}) \leq h_k(b_k - b_{k+1}). \tag{3.29}$$

Let $\mathbf{v} \in \mathbb{R}^n$ and let

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

For $m(\mathbf{a}) = (m(a_1), \ldots, m(a_n))$, we have that

$$f'_{\mathbf{v}}(0) = -\mathbf{v}m(\mathbf{a}).$$

In fact let $U = \bigcup_{i=1}^{n}(a_i + xv_i, b_i)$ with characteristic function χ_U, we have

$$f_{\mathbf{v}}(x) = \int_0^\infty \chi_U(u)m(u)du,$$

then

$$f'_{\mathbf{v}}(x) = \frac{d}{dx}\sum_{i=1}^{n}\int_0^\infty \chi_{(a_i+xv_i,b_i)}(u)m(u)du,$$

$$f'_{\mathbf{v}}(x) = \sum_{i=1}^{n}\frac{d}{dx}\int_{a_i+xv_i}^{b_i} m(u)du = -\sum_{i=1}^{n}\frac{d}{dx}\int_{b_i}^{a_i+xv_i} m(u)du,$$

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

thus

$$f'_{\mathbf{v}}(0) = -\sum_{i=1}^{n} m(a_i) \cdot v_i = -\mathbf{v} \cdot m(\mathbf{a}).$$

Note that by the maximality of $\mathbf{a}$, if $\mathbf{a} + x\mathbf{v}$ satisfies (3.26) and (3.28) for all x in some interval $[0, \epsilon)$ with $\epsilon > 0$, then $f'_{\mathbf{v}}(0) \leq 0$, that is $\mathbf{v} \cdot m(\mathbf{a}) \geq 0$. Let's see that this occurs when $\mathbf{h} \cdot \mathbf{v} \geq 0 \ \forall \mathbf{h} \in H_1$. Indeed suppose that

$$\mathbf{h} \cdot \mathbf{v} \geq 0 \ \forall \mathbf{h} \in H_1 \text{ and} \tag{3.30}$$

$$\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) < 1 < \mathbf{h}' \cdot b \text{ for some } \mathbf{h}' \in (N_{\geq 0})^n. \tag{3.31}$$

Since $\mathbf{h} \cdot \mathbf{b} \leq 1$ for all $\mathbf{h} \in H_0$ we have $\mathbf{h}' \notin H_0$. If $\mathbf{h}' \in H_1$ $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) = 1 + x\mathbf{h}' \cdot \mathbf{v}$, then by (3.30), $\mathbf{h}' \cdot (\mathbf{a} + x\mathbf{v}) \geq 1$ for all $x \geq 0$ so that $\mathbf{h}' \notin H_1$. For any given $\epsilon > 0$, there are only finitely many $\mathbf{h}' \in H_2$ with $\mathbf{h}' \cdot (\mathbf{a} + \epsilon\mathbf{v}) < 1 < \mathbf{h}' \cdot \mathbf{a}$. Reducing the size of ϵ to a small enough positive quantity makes this set of $\mathbf{h}'$ empty, and so $\mathbf{h}' \notin H_2$.
It follows that for $\epsilon > 0$ small enough, if (3.30) hold, then $\mathbf{a}x + \mathbf{v}$ satisfy (3.26) and (3.28) for $0 \leq x < \epsilon$, and so $\mathbf{v}.m(\mathbf{a}) \geq 0$.

We now apply a theorem of Farkas [6]:

Lemma 3.13 (J. Farkas). *Suppose A is an $n \times k$ real matrix and $\boldsymbol{m} \in \mathbb{R}^n$. Then the inequalities $A\boldsymbol{v} \geq 0$, $\boldsymbol{m} \cdot \boldsymbol{v} < 0$ are unsolvable for a vector $\boldsymbol{v} \in \mathbb{R}^n$ if and only if there is a vector $\boldsymbol{p} \in \mathbb{R}^k$ with $\boldsymbol{p} \geq 0$ and $\boldsymbol{p}^T A = \boldsymbol{m}$.*

(We say that a vector is $\geq \mathbf{0}$ when each entry of the vector is ≥ 0). Say $H_1 = \{\mathbf{h}_1, \ldots, \mathbf{h}_u\}$, and let each $\mathbf{h}_j = (h_{j1}, \ldots, h_{jn})$. We apply this lemma to the matrix A whose rows are the u vectors in H_1 and to the vector $\mathbf{m} = m(\mathbf{a})$. Since we have already shown that $A\mathbf{v} \geq \mathbf{0}$ implies $\mathbf{m} \cdot \mathbf{v} \geq 0$, the lemma implies that there is a vector $\mathbf{p} \in \mathbb{R}^u$ with $\mathbf{p} \geq \mathbf{0}$ and $\mathbf{p}^T A = \mathbf{m}$. We have

$$\sum_{j=1}^{u} p_j h_{ji} = m(a_i) \text{ for } 1 \leq i \leq n.$$

Multiplying (3.29) applied to $\mathbf{h}_j$ by p_j and summing over j we have for $1 \leq k \leq n$

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

Multiplying by a_k and summing over k, we get

$$\sum_{k=1}^{n} a_k \sum_{j=1}^{u} p_j h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) \leq \sum_{k=1}^{n} a_k m(a_k)(b_k - b_{k+1}). \tag{3.32}$$

The left side of (3.32) is

$$\sum_{j=1}^{u} p_j \sum_{k=1}^{n} a_k h_{jk} \sum_{i=1}^{n} h_{ji}(b_i - a_i) = \sum_{j=1}^{u} p_j \sum_{i=1}^{n} h_{ji}(b_i - a_i)$$

$$= \sum_{i=1}^{n}(b_i - a_i) \sum_{j=1}^{u} p_j h_{ji}$$

$$= \sum_{i=1}^{n}(b_i - a_i) m(a_i).$$

Thus,

$$\sum_{i=1}^{n}(b_i - a_i)m(a_i) \leq \sum_{k=1}^{n} a_k m(a_k)(b_k - b_{k+1}). \tag{3.33}$$

Now, taking the measure M being dx/x, each $m(a_i) = 1/a_i$, thus we have

$$\sum_{i=1}^{n}(b_i/a_i - 1) \leq \sum_{k=1}^{n}(b_k - b_{k+1}) \leq t. \tag{3.34}$$

However, $M((a_i, b_i)) = \log(b_i/a_i) < b_i/a_i - 1$. hence, by (3.34)

$$M_{\mathbf{b}} = \sum_{i=1}^{n} \log(b_i/a_i) < t.$$

Thus the proposition holds for S_t being a finite union of disjoint intervals; it remains to handle the case of S_t being the union of infinitely many disjoint open intervals. Suppose $S_t = \bigcup_{i=1}^{\infty}(a_i, b_i)$, where the intervals are non-empty and disjoint. For each n, (3.34) implies that $\sum_{i=1}^{n}(b_i/a_i - 1) \leq t$. Thus,

$$\sum_{i=1}^{\infty}(b_i/a_i - 1) \leq t.$$

But

$$M(S_t) = \sum_{i=1}^{\infty} \log(b_i/a_i) < \sum_{i=1}^{\infty}(b_i/a_i - 1) \leq t,$$

so $M(S_t) < t$. This concludes the proof of the theorem. □

Remark: The inequality of the theorem is the best possible. Indeed, suppose S_n is the additive semigroup generated by $(1/(n+1), 1/n)$, where n is a positive integer. Then 1 is not in S^n and we have

$$M(S_t^n) \geq \sum_{j=1}^{\lfloor tn \rfloor} \log(1 + 1/n) = \lfloor tn \rfloor \left(1/n + \mathcal{O}(1/n^2)\right) \sim t \text{ as } n \to \infty.$$

3.2.4 Proof of Theorem 3.2

We are now ready to prove Theorem 3.2 whose statement is

Theorem 3.2 *There is a deterministic algorithm such that for each integer $m > 0$ the algorithm produce an integer D_m and further, for each integer $n > 1$, and each integer D with $D > D_m$ and $D > (\log n)^{11/6+1/m}$, the algorithm finds a period system $(r_1, q_1), \dots, (r_k, q_k)$ for n with each $r_i < D^{6/11}$ and each $q_i < D^3/11$, with $D \leq q_1 q_2 \cdots q_k < 4D$, and with $k = \mathcal{O}((\log\log D)^2)$. The running time of this algorithm is $\widetilde{\mathcal{O}}(D^{12/11})$. The implied constant may depend on the choice of m.*

Proof. We have that $D > (\log n)^{(11/6)+\epsilon}$. Let $x = D^{(6/11)-\epsilon/4}$, so that if n is sufficiently large, we have that $x \geq (\log n)^{1+3/\log\log\log n}$. Let $\alpha = \alpha(x) = 1/\log\log x$. For a prime $r \leq x$, let

$$Q(r) = \{q \text{ prime } : q|(r-1) \text{ with } x^{\alpha^2} < q \leq x^{1/2} \text{ and } ord(n^{(r-1)/q} \bmod\ r) = q\}.$$

We suppose that $Q(r)$ have been computed for each prime $r \leq x$, and we denote

$$\mathcal{Q} = \bigcup_{r \leq x} Q(r).$$

For each $q \in \mathcal{Q}$, find the least prime r_q with $q \in Q(r_q)$.
We use a modified sieve of Eratosthenes to find the prime factorization of every integer up to x; the cost of this is $\widetilde{\mathcal{O}}(x \log n) = \widetilde{\mathcal{O}}(D^{12/11})$.

For a bounded interval I, let $|I|$ denote the length of I. Let $N = \lceil 3\alpha^{-2} \log x \rceil$.

Definition 3.10. *For each $i = 1, 2, \dots, N$, let*

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

Note that the intervals I_i are a partition of $[1, x)$, and that the "expected" number of primes in I_i is about $|I_i|/\log(x^{i/N})$.

- $k_i^0 = \min\{\#(I_i \cap \mathcal{Q}), \lfloor |I_i|/\log(x^{i/N}) \rfloor\}$;
- $k_i = \begin{cases} 0, & \textit{if } k_i^0 \leq 2\alpha^{-2} \\ k_i^0, & \textit{otherwise}; \end{cases}$
- $\mathcal{Q}_i$ *the set of the least k_i primes in $\mathcal{Q} \cap I_i$;*
- $J_i = (x^{(i-1)/N}, x^{(i-1)/N} + k_i \log(x^{i/N}))$;
- $S_i = \Big(\log\left(x^{(i-1)/N}\right), \log\left(x^{(i-1)/N} + k_i \log(x^{i/N})\right)\Big)$;
- *S is the additive subgroup generated by $\bigcup_i \frac{1}{\log(2D)} S_i$.*

Note that each $J_i \subset I_i$, the sets $\mathcal{Q}_i$ are disjoint with their union contained in $\mathcal{Q}$, and that $J_i = \emptyset$ for $i < \alpha^2 N$. Since for $i < \alpha^2 N$, $I_i = [x^{(\alpha^2 N-1)/N}, x^{\alpha^2})$, or all the $q \in \mathcal{Q}$ are such that $x^{\alpha^2} < q \leq x^{1/2}$, hence $I_i \cap \mathcal{Q} = \emptyset$ and we have $J_i = \emptyset$ as desired.

To prove the theorem we need the following three claims we will prove at the end of this section.

Claim 1: For n sufficiently large, we have

$$\sum_{q \in \mathcal{Q}} \frac{1}{q} > \frac{3-\epsilon}{11}. \tag{3.35}$$

Claim 2: For n sufficiently large, we have

$$\sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q} > \frac{3}{11} - \frac{\epsilon}{10}. \tag{3.36}$$

Claim 3: For n sufficiently large, we have

$$\sum_i \int_{S_i} \frac{du}{u} > \frac{3}{11} - \frac{\epsilon}{10}. \tag{3.37}$$

Note that if $S_i \neq \emptyset$ we have $x^{(i-1)/N} \leq x^{1/2}$, thus $x^{i/N} \leq x^{1/2+1/N}$; hence we have

$$\frac{\log x^{i/N}}{\log(2D)} \leq \frac{\log(x^{1/2+1/N})}{\log 2D} \leq \Big(\frac{1}{2} + \frac{1}{N}\Big)\Big(\frac{\log x}{\log 2D}\Big).$$

As $x = D^{(6/11)-\epsilon/4}$ we have $\frac{\log x}{\log D} = \frac{6}{11} - \frac{\epsilon}{4}$ hence

$$\frac{\log x^{i/N}}{\log(2D)} \leq \Big(\frac{1}{2} + \frac{1}{N}\Big)\Big(\frac{6}{11} - \frac{\epsilon}{4}\Big) \leq \Big(\frac{1}{2}\Big)\Big(\frac{6}{11} - \frac{\epsilon}{4}\Big) < \Big(\frac{3}{11} - \frac{\epsilon}{9}\Big).$$

Thus from Claim 3 we have, for n sufficiently large, that

$$\int_0^{3/11-\epsilon/9} \frac{\chi_S(u)}{u} du = \sum_i \int_{S_i} \frac{du}{u} > \frac{3}{11} - \frac{\epsilon}{9}.$$

Thus, from Proposition 3.7, we know that $1 \in S$. Hence there is a finite subset F of $\cup_i S_i$ and a positive integer κ_f for each $f \in F$, such that

$$\sum_{f \in F} \kappa_f f = \log(2D).$$

Let $F_i = F \cap S_i$ and $\kappa_i = \sum_{f \in F_i} \kappa_f$. Then, for sufficiently large n, we obtain

$$\sum_i \kappa_i = \sum_i \sum_{f \in F_i} \kappa_f \leq \sum_i \frac{1}{\log(x^{(i-1)/N})} \sum_{f \in F_i} \kappa_f f.$$

As $\alpha = \alpha(x) = 1/\log\log x$, $N = \lceil 3\alpha^{-2}\log x\rceil$, for sufficiently large n, we have

$$\sum_i \kappa_i < \frac{1}{\log(x^{\alpha^2 - N^{-1}})} \sum_i \sum_{f \in F_i} \kappa_f f = \frac{\log(2D)}{\log(x^{\alpha^2 - N^{-1}})} < 2\alpha^{-2}. \tag{3.38}$$

The last inequality holds since we have $x = D^{6/11-\epsilon/4}$, let's call $A = 6/11 - \epsilon/4$, we have that $2^A x = (2D)^A$, hence we have that $A\log(2D) = A\log 2 + \log x$ thus

$$\frac{\log(2D)}{(\alpha^2 - 1/N)\log x} = \frac{\log 2}{(\alpha^2 - 1/N)\log x} + \frac{1}{(\alpha^2 - 1/N)A}$$

Recalling $1/N \leq \frac{\alpha^2}{3\log x}$, for a sufficiently large x and $\epsilon < 2/11$, we have $\alpha^2 - 1/N \geq \alpha^2(1 - \frac{1}{3\log x}) > 0$ and $(1 - \frac{1}{3\log x})A > 2$. Hence

$$\frac{\log(2D)}{(\alpha^2 - 1/N)\log x} < \frac{1}{(\alpha^2 - 1/N)A} \leq \frac{1}{\alpha^2(1 - \frac{1}{3\log x})A} < \frac{2}{\alpha^2}.$$

Since, for each i with $S_i \neq \emptyset$, we have $k_i > 2\alpha^{-2}$, it follows that for each i with $\kappa_i > 0$ there are more than κ_i distinct primes in $\mathcal{Q}_i$, because there are k_i primes and we have $k_i > 2\alpha^{-2} > \sum_i \kappa_i$. We will call such primes $q_{1,i}, q_{2,i}, \ldots, q_{\kappa_i,i}$.
Since $\log(x^{(i-1)/N}) \leq f \leq \log(x^{i/N})$ and $\kappa_i = \sum_{f\in F_i} \kappa_f$, we have

$$\sum_{f\in F} \kappa_f f = \sum_i \sum_{f\in F_i} \kappa_f f < \sum_i \log(x^{i/N}) \sum_{f\in F_i} \kappa_f = \sum_i \kappa_i \log(x^{i/N}).$$

On the other hand, since $q_{l,i} > \log(x^{(i-N)/N})$, we have

$$\sum_i \sum_j^{\kappa_i} \log(q_{i,j}) > \sum_i \kappa_i \log(x^{(i-1)/N}).$$

Hence we have

$$|\sum_{f\in F} \kappa_f f - \sum_i \sum_j^{\kappa_i} \log(q_{i,j})| < \sum_i \kappa_i \Big(\log(x^{i/N}) - \log(x^{(i-1)/N})\Big) = \log(x^{1/N}) \sum_i \kappa_i.$$

Therefore by (3.38), and $N = \lceil 3\alpha^{-2}\log x\rceil$, we have

$$|\sum_{f\in F} \kappa_f f - \sum_i \sum_j^{\kappa_i} \log(q_{i,j})| < \frac{\log(x)}{N} 2\alpha^{-2} \leq \frac{2}{3}.$$

Hence, recalling that $\sum_{f\in F} \kappa_f f = \log(2D)$, we have that

$$0 \leq |\log(2D) - \sum_i \sum_j^{\kappa_i} \log(q_{i,j})| = | - \log(2D) + \log\Big(\prod_i \prod_j^{\kappa_i} (q_{i,j})\Big)| < \frac{2}{3},$$

$$-\frac{2}{3} \leq \log\Big(\prod_i \prod_j^{\kappa_i} \frac{(q_{i,j})}{2D}\Big) < \frac{2}{3}.$$

Since $1 < e^{\frac{2}{3}} < 2$, it follows that

$$\frac{1}{2} < e^{-\frac{2}{3}} \leq \prod_i \prod_j^{\kappa_i} \frac{(q_{i,j})}{2D} < e^{\frac{2}{3}} < 2.$$

Thus

$$D < \prod_i \prod_j^{\kappa_i} (q_{i,j}) < 4D.$$

We conclude that there is a squarefree integer Q in the interval $(D, 4D)$ supported solely on primes from $\mathcal{Q}$. By sieving this interval with a modified version of the sieve of Eratosthenes that produces a complete prime factorisation for each integer in this interval, we may find such an integer Q, and with a running time of at most $\widetilde{\mathcal{O}}(D)$. Once we had found Q, the pairs (r_q, q) with q running over the prime factors of Q, form a period system for n. This completes the proof of the theorem. It remains to prove the three claims:

Proof of Claim 1: for n sufficiently large, we have

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

By contradiction, suppose not. We apply proposition 3.3 to $\mathcal{Q}$, with the "ϵ" of the proposition equal to $\epsilon/11$. Thus, there is some $\delta > 0$ such that for n sufficiently large we have at least $\delta x/(\log x)^2$ primes $r \leq x$ such that every prime factor of $r - 1$ is below $x^{1/2}$ and not in $\mathcal{Q}$.
As in proposition 3.2 let

$$R(x, n) = \{r \text{ primes} : (r-1) \text{ has a prime divisor } q > x^{\alpha^2} \text{ and } ord((n^{(r-1)/q}) \bmod r) = q\}.$$

By the Remark of proposition 3.2 we get $|\{r \text{ primes} : r \leq x, r \notin R(x,n)\}| = \mathcal{O}\Big(\frac{x}{(\log x)^{\log\log\log x}}\Big)$.
Thus, for n sufficiently large, there is a prime $r \leq x$ counted by $R(x, n)$ such that $(r - 1)$ has every prime factor below $x^{1/2}$ and not in $\mathcal{Q}$.
But if r is in $R(x, n)$ for all $q|(r - 1)$, $x^{\alpha^2} < q < x^{1/2}$ and $ord((n^{(r-1)/q}) \bmod r) = q$, we obtain $q \in \mathcal{Q}$ and hence we have a contradiction. This complete the proof of Claim 1.

Proof of Claim 2: if n is sufficiently large we have

$$\sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q} > \frac{3}{11} - \frac{\epsilon}{10}.$$

The difference between $\sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q}$ and $\sum_{q \in \mathcal{Q}} \frac{1}{q}$ comes from two sources:

1. intervals I_i with $k_i^0 \leq 2\alpha^{-2}$ and
2. intervals I_i with $\#(I_i \cap \mathcal{Q}) > \lfloor |I_i| / \log(x^{i/N}) \rfloor$.

Let's see what is the contribution by each one of this sources to the final sum. For the first one, note that

$$\sum_{q \in I_i : k_i \leq 2\alpha^{-2}} \frac{1}{q} < 2\alpha^{-2} \sum_{i \geq \alpha^2 N} \frac{1}{x^{(i-1)/N}}$$

since $k_i^0 \leq 2\alpha^{-2}$, thus we know that there is no more than $2\alpha^{-2}$ primes in this sum, and that each one of this primes is in I_i thus $q > x^{(i-1)/N}$. The sum is over the nonempty intervals, *i.e.*, over $i \geq \alpha^2 N$. For n sufficiently large

$$2\alpha^{-2} \sum_{i \geq \alpha^2 N} \frac{1}{x^{(i-1)/N}} < \frac{2x^{2/N}}{\alpha^2 x^{\alpha^2}(x^{1/N} - 1)} \ll \frac{1}{\alpha^4 x^{\alpha^2}}. \tag{3.39}$$

The first inequality holds since

$$\sum_{i \geq \alpha^2 N} \frac{1}{x^{(i-1)/N}} = \sum_{i=0}^{\infty} \frac{1}{x^{(i-1)/N}} - \sum_{i < \alpha^2 N} \frac{1}{x^{(i-1)/N}} = x^{1/N} \Big(\sum_{i=0}^{\infty} \frac{1}{x^{(1/N)^i}} - \sum_{i < \alpha^2 N} \frac{1}{x^{(1/N)^i}} \Big).$$

We have a geometric series, thus

$$\sum_{i \geq \alpha^2 N} \frac{1}{x^{(i-1)/N}} < \Big(\frac{1}{x^{1/N} - 1} \Big) - x^{1/N}(\alpha^2 N - 1) \frac{1}{x^{\alpha^2 - 1/N}} = \frac{1}{x^{1/N} - 1} - \frac{(\alpha^2 N - 1)x^{2N}}{x^{\alpha^2}}$$

and finally we have

$$\sum_{i \geq \alpha^2 N} \frac{1}{x^{(i-1)/N}} < \frac{x^{2N}}{x^{\alpha^2}(x^{1/N} - 1)}.$$

In the second inequality (3.39), we use the notation "$a \ll b$" for "there exist a positive constant c such that $a < cb$". In order to prove this inequality we see that

$$\frac{2x^{2/N}}{(x^{1/N} - 1)} < \tau \frac{1}{\alpha^2} \tag{3.40}$$

where τ is a suitable positive constant, that we will determinate. As we are interested in large values of x, to prove this inequality is equivalent to prove

$$\frac{2x^{2/M}}{(x^{1/M} - 1)} < \tau \frac{1}{\alpha^2}$$

where $M = 3(\log x)\alpha^{-2}$. The following inequalities are equivalent to the previous one:

$$2x^{2/M} < \tau \alpha^{-2}(x^{1/M} - 1),$$

$$2(\exp(\frac{2}{M}\log x)) < \tau\alpha^{-2}\Big(\big(\exp(\frac{1}{M}\log x)\big) - 1\Big),$$

$$2\exp\left(\frac{\alpha^2}{3}\right) < \tau\alpha^{-2}\Big(\big(\exp\left(\frac{\alpha^2}{3}\right)\big) - 1\Big).$$

Letting $u = \frac{\alpha^2}{3}$, we have to see for which τ we get

$$2e^u < \frac{\tau}{3}\Big(\frac{e^u - 1}{u}\Big).$$

But since $\lim_{x\to\infty} u = 0$, $\lim_{u\to 0} e^u = 1$ and $\lim_{u\to 0}\frac{e^u-1}{u} = \lim_{u\to 0} e^u = 1$, we have that for $\tau > 6$, the inequality (3.40) holds.

Thus, if n is sufficiently large, the contribution coming from the first source is negligible.

Now, let's calculate the contribution of the second source, *i.e.* we are in the case where the intervals I_i are such that $\#(I_i \cap \mathcal{Q}) > \big\lfloor |I_i|/\log(x^{i/N})\big\rfloor$. Let

$$A = \{\text{ the largest } \#(I_i \cap \mathcal{Q}) - \big\lfloor |I_i|/\log(x^{i/N})\big\rfloor \text{ primes } q \in I_i\}.$$

By the prime number theorem, the total number of primes in I_i is at most

$$\big\lfloor |I_i|/\log(x^{i/N})\big\rfloor + \mathcal{O}\Big(\frac{x^{i/N}}{(\log(x^{i/N}))^2}\Big).$$

Then, we have that

$$\sum_{q\in A}\frac{1}{q} \ll \frac{1}{x^{i/N}}\sum_{q\in A} 1 \ll \frac{1}{(\log(x^{i/N}))^2}.$$

Hence the contribution for each i is

$$\mathcal{O}\Big(\frac{1}{(\log(x^{i/N}))^2}\Big) = \mathcal{O}\Big(\frac{N^2}{i^2(\log(x))^2}\Big).$$

As in the previous case, we sum over $1 \geq \alpha^2 N$, and the total contribution is

$$\mathcal{O}\Big(\frac{N}{\alpha^2(\log x)^2}\Big) = \mathcal{O}\Big(\frac{1}{\alpha^4\log x}\Big).$$

Since

$$\sum_{i=\alpha^2 N}^{N} i^{-2} < \int_{\alpha^2 N}^{N} v^{-2}dv = \frac{1-\alpha^2}{\alpha^2 N} \ll \frac{1}{\alpha^2 N},$$

even this contribution is negligible as well. This proves Claim 2.

Proof of Claim 3: if n is sufficiently large we have

$$\sum_i \int_{S_i}\frac{du}{u} > \frac{3}{11} - \frac{\epsilon}{10}.$$

We have by Claim 2 that

$$\sum_i \frac{1}{x^{(i-1)/N}} k_i > \sum_i \sum_{q \in \mathcal{Q}_i} \frac{1}{q} > \frac{3}{11} - \frac{\epsilon}{10}. \tag{3.41}$$

We know that, if $S_i \neq \emptyset$, that is, if $k_i > 0$, then

$$\int_{S_i} \frac{du}{u} = \log\Big(\frac{\log\big(x^{(i-1)/N} + k_i \log(x^{i/N})\big)}{\log(x^{(i-1)/N})}\Big).$$

To simplify the equation we are going to define a_i and b_i as follows:

$$a_i = x^{(i-1)/N}, \qquad b_i = k_i \log(x^{i/N}).$$

Hence, we have

$$\int_{S_i} \frac{du}{u} = \log\Big(\frac{\log\big(a_i + b_i\big)}{\log a_i}\Big).$$

Now,

$$\log(a_i + b_i) > \log a_i + \frac{b_i}{a_i} - \Big(\frac{b_i}{a_i}\Big)^2$$

and so we can write

$$\int_{S_i} \frac{du}{u} > \frac{b_i}{a_i \log a_i} - \frac{2}{\log a_i}\Big(\frac{b_i}{a_i}\Big)^2 = \frac{b_i}{a_i \log a_i}\Big(1 - \frac{2b_i}{a_i}\Big) > \frac{k_i}{a_i}\Big(1 - \frac{2b_i}{a_i}\Big).$$

Then, putting the values of a_i and b_i we have:

$$\int_{S_i} \frac{du}{u} > \frac{k_i}{x^{(i-1)/N}}\Big(1 - \frac{2k_i \log(x^{i/N})}{x^{(i-1)/N}}\Big).$$

Since $k_i > 0$ and it is defined to be less or equal than $|I_i|/\log(x^{i/N})$, we have that

$$k_i \log(x^{i/N}) \leq x^{(i-1)/N} - x^{i/N} = x^{(i-1)/N}(x^{1/N} - 1) < \frac{\alpha^2}{2} x^{(i-1)/N}$$

The last inequality holds since $N > 3\alpha^{-2} \log x$, thus $\frac{1}{N} < \frac{\alpha^2}{3 \log x}$. Hence

$$x^{1/N} < x^{\frac{\alpha^2}{3 \log x}} = e^{\log(x^{\frac{\alpha^2}{3 \log x}})} = e^{\frac{\alpha^2}{3 \log x} \log x} = e^{\frac{\alpha^2}{3}},$$

therefore we have

$$x^{1/N} - 1 < e^{\frac{\alpha^2}{3}} - 1 \approx \frac{\alpha^2}{3} < \frac{\alpha^2}{2}.$$

Thus,

$$\int_{S_i} \frac{du}{u} > \frac{k_i}{x^{(i-1)/N}}(1 - \alpha^2).$$

Then by (3.41) we have

$$\sum_i \int_{S_i} \frac{du}{u} > \sum_i \frac{k_i}{x^{(i-1)/N}}(1 - \alpha^2) > (1 - \alpha^2)\Big(\frac{3}{11} - \frac{\epsilon}{10}\Big) > \frac{3}{11} - \frac{\epsilon}{9},$$

since $\lim_{x \to \infty} \alpha = \lim_{x \to \infty} 1/\log\log x = 0$. This concludes the proof of Claim 3, and hence Theorem 3.2 holds. □

Appendix A

Computational cost

We said that a polynomial f has order g or $f(x) = \mathcal{O}(g(x))$ if $\exists C > 0$ and $x_0 > 0$ such that for every $x \geq x_0$, $|f(x)| \leq C|g(x)|$.

Repeated Squaring method:

The goal is to compute n^k $(mod\ r)$, where $k \in \mathbb{N}^*$. For this let's write n^k as a product of powers, which base is n, and the exponent is a power of 2.
For example if $k = 23 = 1 + 2 + 4 + 16$, thus $n^k = nn^2n^4n^{16}$, and we just have to compute in this case 4 element to the power 2, for a total of 7 operations and not 22.
In general we can see that we have to do $\mathcal{O}(\log_2 k)$ squares modulo r, each one has $\mathcal{O}(\log_2^2 r)$.
Hence, the total cost of n^k $(mod\ r)$ is $\mathcal{O}(\log_2 k \log_2^2 r)$

Let f be a polynomial in $\mathbb{Z}/n\mathbb{Z}[x]$ of degree $r-1$. Let's prove that the cost of $f(x)^n \pmod{x^r - 1, n}$ is $\mathcal{O}(r^2 \log_2^3 n)$: using the same idea of the repeated squaring method, we have to know the binary representation of n, and the problem is reduced to multiply at most $(\log_2 n)$ times $f(x)^2 \pmod{x^r - 1, n}$.
Now let's show that the cost of computing this square is $\mathcal{O}(r^2 log_2^2 n)$. In this case the cost of $f(x)^n(\text{mod } x^r - 1, n)$ will be $\mathcal{O}(r^2 \log_2^3 n)$. For this we have to:

- compute the square of $f(x)(\text{mod } n)$: this means to do $\mathcal{O}(r^2)$ products $\pmod{n}$ therefore the cost is $\mathcal{O}(r^2 log_2^2 n)$
- reduce it $\pmod{x^r - 1}$: Let $h(x) = f^2(x)(\text{mod } n) = \sum_{i=0}^{2r-2} h_i x^i$ with $h_i \pmod{n}$.

$$h(x) = h_0 x^0 + h_1 x^1 + \cdots + h_{r-1} x^{r-1} + h_r x^r + h_{r+1} x^{r+1} + \cdots + h_{2r-2} x^{2r-2}$$

To reduce $\pmod{x^r - 1}$ we need $\mathcal{O}(r)$ sums, each one of cost $\mathcal{O}(\log_2 n)$, in fact:

$$h(x) = (\sum_{i=0}^{r-2} (h_i + h_{i+r} x^i)) + h_{r-1} x^{r-1} \bmod (x^{r-1}, n).$$

Therefore this second step costs $\mathcal{O}(r \log_2 n)$. Hence the total cost of $f(x)^2 \pmod{x^r - 1, n}$ is in fact $\mathcal{O}(r^2 \log^2 n)$.

We have now prove the cost assumed in table 2.1 at the end of Chapter 2. Now let's see the cost we used in Chapter 3.

Using fast Fourier transform (FFT):

The notation $\widetilde{\mathcal{O}}(X)$ means a bound $c_1 X(\log X)^{c_2}$ for suitable positive constants c_1, c_2. In chapter 9.5 of [3] we can see that the bit complexity of multiply two size-N numbers using FFT is

$$\mathcal{O}(\log N(\log\log N)(\log\log\log N))$$

By chapter 9.6 of [3] we know that multiplying two degree-D polynomials in $\mathbb{Z}/_m\mathbb{Z}[x]$, that is, all coefficients are reduced mod m is

$$\mathcal{O}(M(D\log(Dm^2))), \tag{A.1}$$

where $M(n)$ is the bit complexity for multiplying two integers of n bits each. With the FFT we have:

$$\mathcal{O}(\log m(\log\log m)(\log\log\log m)(D\log(Dm^2))),$$

using the $\widetilde{\mathcal{O}}$ notation, we have that the total cost is

$$\widetilde{\mathcal{O}}(D\log(m)(\log D + \log m)). \tag{A.2}$$

Where D is much smaller than m we have that the bit complexity for multiplying two polynomials of degree D in $\mathbb{Z}/m\mathbb{Z}$ is

$$\widetilde{\mathcal{O}}(D(\log m)^2). \tag{A.3}$$

We know that the inverse of a polynomial of degree D in $\mathbb{Z}/m\mathbb{Z}$ is $\widetilde{\mathcal{O}}(D(\log m)^2)$, and that the computational cost to perform Euclid's algorithm on $h(x)$ and $g(x)$, two polynomial of degree D on $\mathbb{Z}/m\mathbb{Z}$ is $\widetilde{\mathcal{O}}(D(\log m)^3)$.

References

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.

[2] T. Apostol. *Introduction to Analytic Number Theory*. UTM. Springer Verlag, 1975.

[3] R. Crandall and C. Pomerance. *Prime numbers. A computational perspective*. Springer-Verlag, Berlin, Heidelberg, New York, second edition, 2005.

[4] H. Davenport. *Multiplicative number theory*. Spring-Verlag, New-York-Berlin, second edition, 1980.

[5] J. M. Deshouillers and H. Iwaniec. Kloosterman sums and Fourier coefficients of cusp forms. *Invent. Math.*, 70:219–288, 1982/83.

[6] J. B. Friedlander. Shifted primes without large prime factors. *Number theory and applications (R.A. Mollin, ed.), Kluwer Academic Publisher, Dodrecht*, pages 393–401, 1989.

[7] A. Granville. It is easy to determine whether a given integer is prime. *Bulletin of the American Mathematical Society*, 42:3–38, 2004.

[8] A. Granville and C. Pomerance. Two contradictory conjectures concerning Carmichael numbers. *Mathematics of Computation*, 71:873–881, 2002.

[9] Jr. H.W. Lenstra and C. Pomerance. Primality testing with gaussian periods. 2005.

[10] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.

[11] C. Pomerance, J.L. Selfridge, and S.S. Wagstaff. "The pseudoprimes to $25 \cdot 10^9$". *Math. Comp.*, 35:1003–1026, 1980.

[12] C. Pomerance and I.E. Shparlinski. Smooth orders and cryptographic applications. *Algorithmic Number Theory, Proceeding of ANTS-V, Sydney,Australia*, 2002.

[13] J. von zur Gathen and J. Gerhard. Modern computer algebra. 1999.