TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

The Complexity of Prime Number Tests

Diplomarbeit

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter der Anleitung von
Univ.Prof. Dipl.-Ing. Dr.techn. Michael Drmota

durch

Theres Steiner, BSc
Matrikelnummer: 01025110

Ort, Datum

Unterschrift (Student)

Unterschrift (Betreuer)

”The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.”

Carl Friedrich Gauss, Disquisitiones Arithmeticae, 1801

Ron and Hermione have 2 children: Rose and Hugo.

Vogon poetry is the 3rd worst in the universe.

Acknowledgements

First, I would like to thank my parents, Rudolf and Doris Steiner, without them I would not be where I am now.

I would also like to thank my professor Michael Drmota for supporting me and helping me with my thesis. Throughout the writing process he was always there for me and his input was always helpful.

I would also like to thank my colleagues who made this stage of my life truly amazing. Also, a special thanks to the people that gave me valuable input on my thesis, mathematically or grammatically.

5 is the 5th digit in π.

Abstract

Prime numbers have been a significant focus of mathematics throughout the years. Although the study of prime numbers may seem at first quite simple, perhaps because every schoolchild knows what a prime number is, the search for all of the secrets of prime numbers is far from over. Even one of the most famous, thus far unsolved, problems in mathematical history is directly linked to prime numbers, namely the *Riemann Hypothesis*.

Until 2002, it was simply assumed that prime numbers can be differentiated from composites in polynomial time with a great deal of certainty; however, there was no definite proof to say this problem can be solved in polynomial time. If the *General Riemann Hypothesis* is true, though, some algorithms would classify as deterministic polynomial. If a counterexample for such an algorithm can be found, the test would not longer be classified as deterministic but rather probabilistic.

In 2002, though, three Indian mathematicians developed a deterministic algorithm that runs in polynomial time; it is totally independent not only from the *Riemann Hypothesis* but also all other conjectures - the first of its kind. This result is, of course, groundbreaking for not only the specific field of number theory but also all of mathematics. The development of such an algorithm proves that the prime number problem can be deterministically solved in polynomial time. Additionally, following this initial discovery, further optimizations have been made by other researchers.

007 is James Bond's secret agent number.

Contents

Introduction

While mathematicians have spent years attempting to understand prime numbers, their efforts have not remained purely of theoretical relevance. Many people may not realize it but prime numbers are found in some of the most important aspects of their everyday lives. For instance, all encryption methods used to guard personal data, Internet banking transactions and even the simple withdrawal of money, are all based on prime numbers.

This paper will initially provide an overview of the history of the study of prime numbers and explain the difference between probabilistic and deterministic prime number tests. Additionally, attention will be paid to the *Riemann Hypothesis* and its relevance to prime numbers and it will be shown how previously probabilistic tests can be made deterministic. The paper will then focus on the primary topic, namely the first deterministic polynomial algorithm for determining the primality of a given number.

The secret formula for Kentucky Fried Chicken includes 11 herbs and spices.

1. History

1.1. Pythagoras and Euclid

Definition 1.1.1 (Prime numbers):

An integer $p > 1$ is called a *prime number* iff its only divisors are trivial (1 and p).
An integer $m > 1$, which is not prime, is called *composite*.

Research on prime numbers and its properties began with the ancient Greeks and Pythagoras (circa 500 BC). In 300 BC, Euclid wrote a series of 13 books, called *Elements*, on geometry and number theory. [29][30] In Book IX of *Elements*, Euclid stated and proved that prime numbers are more than any assigned multitude of prime numbers [17][book IX, proposition 20]:

Proposition 1.1.2:

There are infinitely many prime numbers.

Proof. Let all the prime numbers be a finite set $P = \{p_1, p_2, \ldots, p_r\}$.
Let m be $p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$.
m is either prime or composite.
If m is prime we found a prime number that is not in the set P.
If m is composite, it is divisible by a prime number p. If p would be one of the prime numbers of the set, it would also divide the difference $m - p_1 \cdot p_2 \cdot \ldots \cdot p_r = 1$.
Because p cannot divide 1, we found a prime number not in the set P. $\square$

This proof uses another crucial proposition from another one of Euclid's 13 books of *Elements* [17][book XII, proposition 31]: *Any composite number is measured by some prime number.*

1.2. Eratosthenes

In 200 BC, Eratosthenes invented an algorithm to distinguish between prime and composite numbers. This algorithm is called the *Sieve of Eratosthenes*. The first step is to write down all natural numbers beginning with 2 up to a limit N (for example 100). The next step is to cross out all the numbers that are divisible by 2, which excludes every second number. The next number that is not crossed out is 3, so all other numbers that are divisible by 3 are crossed out. This goes on with the next number that is not crossed out, namely 5. If this is continued until the last number, all remaining numbers are prime and all crossed out numbers are composite [30]

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

The method behind this algorithm is very simple. 2 is a prime number, all of its multiples are crossed out. The next number that is not crossed out has to be a prime number and the search continues for numbers that are not divisible by a prime. Furthermore, the algorithm can be modified to have a better running time using the following proposition:

Proposition 1.2.1:

Every composite number n has a prime factor which is at most $\sqrt{n}$.

Proof. n is a composite number with prime factors $p_1, p_2, \dots, p_r$. So $n = p_1 \cdot p_2, \dots p_r$.
Without loss of generality, take two arbitrary prime factors, p_i and p_j. If $p_i > \sqrt{n}$ and $p_j > \sqrt{n}$, then $p_i \cdot p_j > \sqrt{n} \cdot \sqrt{n} = n$. Thus, one of the prime factors must be less than or equal to $\sqrt{n}$. □

Sirus Black was wrongfully convicted of the murder of 13 people.

First, in step i of the algorithm, all composite numbers between 0 and p_i^2 have already been crossed out. Additionally, the algorithm can be terminated when jumping to a prime number p_j, whose square is bigger than the limit N. In the example above, mulitples of 11 do not have to be looked at, because $\sqrt{100} < 11$. This concludes that in just four steps (with using the prime numbers $2, 3, 5$ and 7) all numbers between 2 and 100 can be identified to be prime or composite. Although this adjustment makes the algorithm much more efficient, it is very inefficient for larger numbers. To check the primality of a number n, every single number up to $\sqrt{n}$ has to be dealt with first. [29][33][35]

1.3. Fermat

After Eratosthenes, a significant amount of time passed without any great effort towards better understanding prime numbers, which coincided with the Dark Ages. In the 17th century, Pierre de Fermat had a huge impact on number theory. His most important works (all named after him, of course) include *Fermat's Little Theorem*, *Fermat's Factorization Method* and *Fermat's Last Theorem*. The latter was first proven by Andrew Wiles in 1995. With his Factorization Method, he invented a new method in factorizing large numbers. [29][41]

Moreover, to this day, his Little Theorem is extremely important, serving as the foundation for many other number-theoretical findings.

Theorem 1.3.1 (Fermat's Little Theorem):

If p is prime and a is an integer > 1 with (a,p)=1, then

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

Another commonly seen version of this theorem states (with the same properties):

$$a^p \equiv a \pmod{p}$$

Those two versions are congruent to each other.

Before proving *Fermat's Little Theorem* other theorems have to be stated first:

Lemma 1.3.2:

If p is a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo p iff $a \equiv \pm 1 \pmod{p}$.

Proof. "⇒": Assume a is its own inverse modulo p. Then $a^2 \equiv 1 \pmod{p}$. This is equivalent to $(a^2-1) \equiv 0 \pmod{p}$. So $p|(a^2-1)$ and $(a^2-1) = (a+1)(a-1)$. So p has to divide either $a+1$ or $a-1$. It follows that $a \equiv +1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.
"⇐": Assume $a \equiv \pm 1 \pmod{p}$. Then $a^2 \equiv 1 \pmod{p}$. So it follows that a is its own inverse modulo p. [41] □

Theorem 1.3.3 (Wilson's Theorem):

p is a prime number iff

$$(p-1)! \equiv -1 \pmod{p} \tag{1.3.1}$$

Proof. "⇒": For $p=2$ and $p=3$ it is true. So assume $p>3$. Each integer a with $1 \le a \le p-1$ has a unique inverse (a proof can be found in [41][pages 49-51]) modulo p. W.l.o.g. a' with $1 \le a' \le p-1$ is the inverse of a. Because of Lemma 1.3.2 $a \ne a'$ for $2 \le a \le p-2$.
So when looking at $2 \cdot 3 \cdots (p-2) = (p-2)!$, every a with $2 \le a \le p-2$ also has its (unique) inverse in the product too. So $(p-2)! \equiv 1 \pmod{p}$. Multiplying both sides with $p-1$ leaves $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.
"⇐": Let $n = ab$ with $a, b \in \mathbb{Z}$ with $1 \le a < n$. Obviously, $a|(n-1)!$. Because $n|((n-1)!+1)$ ($(n-1)! \equiv -1 \pmod{n}$) and $a|n$, $a|((n-1)!+1)$. So, $a|((n-1)!+1-(n-1)!$. If follows that $a|1$, so $a=1$. [41] □

Proof of Fermat's Little Theorem. All the integers a, $2a$, $3a$,.. $(p-1)a$ are not divisible by p, because $(a,p)=1$ and $(i,p)=1$ for $1 \le i \le p-1$.
Also none of those integers are congruent. If $ia \equiv ja \pmod{p}$ then $iaa' \equiv jaa' \pmod{p}$, with a' being the inverse of a. So this is only true for $i \equiv j \pmod{p}$.
So the set $\{a, 2a, 3a, ..(p-1)a\}$ has to be congruent to the set $\{1, 2, 3, ...p-1\}$.
If follows that

$$a \cdot 2a \cdot 3a \cdot ...(p-1)a = a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Applying Theorem 1.3.1 (Wilson's Theorem) the congruence becomes $-a^{p-1} \equiv -1 \pmod{p}$. This is equivalent to $a^{p-1} \equiv 1 \pmod{p}$. [41] □

With this Theorem, he also proved one half of the *Chinese Hypothesis*, dating back 2000 years:
An integer n is prime iff $2^n - 2$ is divisible by n.
"$\Rightarrow$" is *Fermat's Little Theorem*, because $2^n - 2$ is divisible by n is equivalent to $2^n \equiv n \pmod{n}$.
For "$\Leftarrow$" counterexamples were found, for example $2^{341} - 2$ is divisible by 341. But 341 is composite: $341 = 11 \cdot 31$. [29]

Fermat's Little Theorem can rather easily tell if a number is composite, because if $a^n \not\equiv a \pmod{n}$ for an integer number n, n cannot be prime. But on the other hand, if n passes the test, it may be prime.

Definition 1.3.4 (Fermat Pseudoprime):

Composite numbers that pass the test with a certain a are called *Fermat pseudoprimes to base a.*

Example 1.3.5:
231 is a pseudoprime to base 2.

[31]

Definition 1.3.6 (Carmichael Number):

Composite numbers that pass the test for all $a > 1$ with $(a, n) = 1$ are called *Carmichael Numbers.*

The smallest Carmichael Number is $561 = 3 \cdot 11 \cdot 17$. Although Carmichael Numbers occur rarely, it was proven in 1994 by *Alford, Granville and Pomerance* in [3] that there are infinitely many Carmichael Numbers. [29][41]

Fermat and *Mersenne* studied certain kinds of numbers that they thought associated with prime numbers. *Fermat* conjectured that numbers of the form $2^{2^n} + 1$ are always prime for $n \in \mathbb{N}$. Those numbers are named after him, namely *Fermat* *numbers.* Although it is true for $n = 0, ..., 4$, *Euler* found out that $2^{2^5} + 1$ is divisible by 641. To this day, no other primes of this type have been found. It remains a conjecture if there are any more, maybe even infinitely many. [29]

Theorem 1.3.7:

Numbers of the form $2^n + 1$ for $n \neq 2^k$, with $k \in \mathbb{N}$, are composite.

Proof. If n is not a power of 2, then n has an odd factor.
$n = a \cdot b$, with b odd.

$$2^n + 1 = (2^a)^b + 1 = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + 2^{a(b-3)} - \ldots + 1)$$

□

Theorem 1.3.8 (Mersenne Numbers):

Mersenne Numbers $M_n = 2^n - 1$ are always composite, when n is composite.

Proof. $n = a \cdot b$, where a and b do not have to be prime.
The *Mersenne Number* $M_{ab} = 2^{ab} - 1$ can be written as

$$2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)$$

[30] □

If p is prime, it does not mean that M_p is also prime. Nevertheless, most of the largest known primes are of this form. // As of 29 April 2018, the largest known Prime Number is a *Mersenne Number*: $M_{77232917}$, found on 26 December 2017 as part of the GIMPS (Great Internet Mersenne Prime Search) project. [12]

1.4. Euler

Leonhard Euler studied Prime Numbers in the 18th century, about 100 years later than Fermat. He generalized 1.3.1 *Fermat's Little Theorem.* Now, the modulus m does not have the condition of being prime any more. Before stating the Theorem, a new function has to be introduced.

Apollo 17 was the last moon landing.

Definition 1.4.1 (Euler φ-function):

The Euler φ-function $\varphi(n)$ for integer $n > 0$ is defined by

$$\varphi(n) = |\{x \in \mathbb{Z} | 1 \leq x \leq n; (x, n) = 1\}|$$

So, $\varphi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n. [30]

Theorem 1.4.2 (Euler's Theorem):

If a positive integer m and $a \in \mathbb{Z}$ with $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Euler's Theorem looks very similar to *Fermat's Little Theorem*. In fact, for $m \in \mathbb{P}$ the Euler ϕ-function $\varphi(m) = m - 1$ is exactly *Fermat's Little Theorem*.

Proof. First, there are exactly $\varphi(m)$ distinct integers r_i with $i \in \{1, 2, \ldots, \varphi(m)\}$ and $1 \leq r_i \leq m \ \forall r_i$ that hold the property $(r_i, m) = 1$.
The next step of the proof is to show the equality $\{r_1, r_2, \ldots, r_{\varphi(m)}\} = \{r_1 \cdot a, r_2 \cdot a, \ldots, r_{\varphi(m)} \cdot a\}$.
If $(r_i \cdot a, m) > 1$ for one i, there is a prime divisor p of $(r_i \cdot a, m)$ with $p | r_i \cdot a$ and $p | m$.
So $p | m$ and eighter $p | r_i$ or $p | a$. This is impossible, because $(r_i, m) = 1$ and $(a, m) = 1$. This means $(r_i \cdot a, m) = 1$.
So far $\{r_1, r_2, \ldots, r_{\varphi(m)}\} \supseteq \{r_1 \cdot a, r_2 \cdot a, \ldots, r_{\varphi(m)} \cdot a\}$.
If $r_i \cdot a = r_j \cdot a$ for some i, j. In addition, a has a unique inverse modulo m, denoted with a'. From $r_i \cdot a \cdot a' = r_j \cdot a \cdot a'$ follows, that $r_i = r_j$ and this means that the the two sets are the same.
So

$$r_1 \cdot a \cdot r_2 \cdot a \cdots r_{\varphi(m)} \cdot a \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \pmod{m}$$

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \pmod{m}$$

So it follows that

$$m | (a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)} - r_1 \cdot r_2 \cdots r_{\varphi(m)})$$

$$m|((a^{\varphi(m)} - 1) \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)})$$

Because $(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$, $m|(a^{\varphi(m)} - 1)$ and it follows that

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

[30]

□

Another property of prime numbers that is based on *Fermat's Little Theorem* and *Wilson's Theorem* is *Euler's Criterion.*

Before the Criterion, the *Legendre Symbol* and the *Jacobi Symbol* must be introduced:

Definition 1.4.3 (Legendre Symbol):

Let p be an odd prime and a an integer with $p \nmid a$.
Then the *Legendre Symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } \exists x \in \mathbb{Z}_p \text{ with } x^2 \equiv a \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

If $\left(\frac{a}{p}\right) = +1$, then a is called a *quadratic residue modulo p*, otherwise a is a *quadratic nonresidue modulo p.*

Definition 1.4.4 (Jacobi Symbol):

Let p be an odd positive integer > 1 with $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and a an integer with $(a, n) = 1$.
Then the *Jacobi Symbol* is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

with $\left(\frac{a}{p_i}\right)$ being *Legendre Symbols.*
If $(a, n) > 1$ then $\left(\frac{a}{n}\right) = 0$.

[41]

In golf, the clubhouse is referred to as the 19th Hole.

Theorem 1.4.5 (Euler's Criterion):

Let p be an odd prime number and a an integer with $p \nmid a$. Then

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

[6][18][41]

Proof. There are two cases. Either $\left(\frac{a}{p}\right) = 1$ or $\left(\frac{a}{p}\right) = -1$.
First assume $\left(\frac{a}{p}\right) = 1$. Then there exists a x with $x^2 \equiv a \pmod{p}$. So

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \pmod{p}$$

Because of *Fermat's Little Theorem*: $x^{p-1} \equiv 1 \pmod{p}$ and thus

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

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

Now to the second case: Assume that $\left(\frac{a}{p}\right) = -1$. Each $i \in \mathbb{Z}_p$ has an inverse $j \in \mathbb{Z}_p$. The inverse is unique and also $i \neq j$ (otherwise $i^2 = a$ and $\left(\frac{a}{p}\right) = 1$). Pairing them up will result in

$$a^{(p-1)/2} \equiv (p-1)! \pmod{p}$$

Because of *Wilson's Theorem* ($(x,p) = 1$): $(p-1)! \equiv -1 \pmod{p}$. So

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

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

[41] □

1.5. The Chinese Remainder Theorem

At first sight, the following Theorem may not be associated with *prime numbers* as much as the other Theorems in this Chapter, but nevertheless, it is crucial for a number of proofs of prime number algorithms.

Theorem 1.5.1 (The Chinese Remainder Theorem):

Let $n_1, n_2, \ldots, n_k$ be pairwise coprime and greater than 1 and $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Then the system of n equations

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ a &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution for a modulo $n_1 \cdot n_2 \cdots n_k$.

Proof. First, let's define $N := n_1 \cdot n_2 \cdots n_k$. Let's show

$$a \equiv \sum_{i=1}^{k} a_i \cdot (N/n_i) \cdot (N/n_i)^{-1} \pmod{N}$$

It is easy to see that $a \equiv a_i \pmod{n_i}$ for all i.
Next, a has to be unique modulo n. Assuming there exists an $a' \not\equiv a \pmod{N}$, but $a' \equiv a_i \pmod{n_i}$, this means $a - a'$ is a multiple of n_i for all i. This implies $a - a'$ is also a multiple modulo N, therefore $a \equiv a' \pmod{N}$. □

[25][36]

2. Prime Numbers and Prime Number Tests

2.1. Prime Number Tests

There are different tests to determine if a number n is prime or not. In general, prime number algorithms can be classified into two groups: *Probabilistic Prime Number Tests* and *Deterministic Prime Number Tests.*

2.1.1. Probabilistic Prime Number Tests

As the name already assumes, *Probabilistic Prime Number Tests* only tell with a certain probability whether a number is prime or composite.

One famous example for a *Probabilistic Prime Number Test* is based on 1.3.1 *Fermat's Little Theorem.* As previously mentioned, composite numbers that pass the test with a certain a are called *Fermat Pseudoprimes* (1.3.4) to base a. If they pass is for all $a > 0$ with $(a, n) = 1$, they are called *Carmichael Numbers* (1.3.6). On the other hand, if the test declares a number as composite, it is for sure composite. Despite this small room for error this test is widely used for primality testing since the errors occur so rarely. For example, for base 2, if $n \to \infty$ the error goes to zero. Although its time complexity is polynomial, the only problem is that it is not deterministic. [2][13]

Algorithm 1 fermat(m: positive integer $>$ 1, a: positive integer $>$ 1)

```
if $a^{m-1} \not\equiv 1 \pmod{m}$ then
  return composite
else
  return probably prime
end if
```

2.1.2. Deterministic Prime Number Tests

More interesting for this paper are *Deterministic Prime Number Tests*, which only have two possible outcomes with no uncertainty regarding a number's primality, thereby preventing the return of *Pseudoprimes*. If the test outputs *prime*, the number is prime; if the test outputs *composite*, the number is composite.

A very easy example is the *Sieve of Eratosthenes*. Moreover, similar algorithms based on the same idea check every number from 2 to $\sqrt{n}$ to determine whether n is prime or composite. The time complexity for this test, however, is $\Theta(\sqrt{n})$. [2]

Algorithm 2 checkprime(m: positive integer > 1)

```
for i=2 to floor(sqrt(m)) do
    if m/i=0 then
        return composite
    end if
end for
return prime
```

Another *Deterministic Prime Number Test* already encountered is based on *Wilson's Theorem*. If one were to multiply $m-1$-times, the algorithm's time complexity explodes, thereby becoming very slow. $\Theta(m)$ is even worse than trivially checking all numbers up to $\sqrt{m}$.

Algorithm 3 wilson(m: positive integer > 1)

```
if $(m-1)! \equiv -1 \pmod{m}$ then
    return prime
else
    return composite
end if
```

While both of those tests are deterministic, they are also inefficient with horrendous time complexities.

These two algorithms are just examples for *Deterministic Prime Number Tests*. The aim has always been to find algorithms that are *deterministic* and have a decent time complexity with the goal of finding one that runs in polynomial time.

23 players are allowed to be on the roster of a rugby game.

2.2. The Compexity Class P

One very important aspect of a prime number algorithm is its time complexity. This is where the *efficiency* of an algorithm comes into play: "[...] an algorithm whose memory requirements are larger than the number of atoms on earth or whose execution takes several billion years would not be very helpful." [33]

The *complexity* of an algorithm depends on how resources depend on an *input*. One aspect of *complexity theory* is very important: the *running time*. The *running time* is defined by the *number of elementary instructions* when an algorithm is applied to an input.

Nowadays, although computers have increasingly more computational power allowing for calculations to be executed faster, the time complexity is independent of the computational power of a computer.

Definition 2.2.1 (Efficient algorithm):

An algorithm is *efficient* or *polynomial* if the time complexity is bounded by $O(n^k)$ for some constant k, where n denotes the input size.
This class of decision problems is called P.

Although *non-efficient* algorithms can have a better running time than *efficient* algorithms for a small input n, this definition is very practical.

In addition to the complexity class P, one important complexity class is NP. In the NP class, the problems are *"verifiable"* in polynomial time. This means, if there is a certificate of a solution, it would take polynomial time to verify it.

There exists a hypothesis that those two complexity classes are in fact the same. The official formulation of the problem is [11]:

Conjecture 2.2.2:

Does $P = NP$?

It is one of seven *Millenium Problems* defined by the Clay Mathematics Institute[1]. Solving it comes with a prize money of 1 Million US Dollars. As of today, only the *Poincaré Conjecture* has been solved and was awarded with a *Fields Medal* while all of the other six problems remain unsolved. [11][13][33]

[1] http://www.claymath.org/millennium-problems

3. Conditional Polynomial Prime Number Tests

In Chapter 2.1.2 *Deterministic Prime Number Tests* two algorithms were introduced. Although they have the advantage of being *deterministic*, thus having no error, they are not desireable because of their poor time complexities.

In the 1970s, two probabilistic algorithms were introduced that could be made deterministic under the assumption of the *Generalized Riemann Hypothesis (GRH)*. In this chapter, the *Riemann Hypothesis (RH)*, the *Generalized Riemann Hypothesis* and the properties needed for the two algorithms are established. After that, the two algorithms are discussed. [2][38]

3.1. The Riemann Hypothesis and the Generalized Riemann Hypothesis

3.1.1. The Riemann ζ-function

The base of the *Riemann Hypothesis* is the *Riemann ζ-function.* Although its definition may seem easy, mathematicians have been studying it for more than a hundred years.

Definition 3.1.1 (Riemann ζ-function):

The Riemann ζ-function for $s \in \mathbb{C}$, is defined as the absolutely convergent series

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

on the half-plane $Re(s) > 1$.

The connection between the function and prime numbers is expressed in the next Theorem.

Theorem 3.1.2 (Euler product of the Riemann ζ-function):

For $s \in \mathbb{C}$ and $Re(s) > 1$ the Riemann ζ-function is

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.1.1}$$

where p in $\mathbb{P}$.

Proof. Because $\zeta(s)$ is absolutely convergent, the factors can be rearranged without changing the limit. Also $|p^{-s}| < 1$ and

$$1 + p^{-s} + (p^2)^{-s} + (p^3)^{-s} + \cdots = \frac{1}{1 - p^{-s}}$$

and because of the uniqueness of the prime factorization

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}$$

[37] □

[7][42][43]

3.1.2. Analytic continuation of the Riemann ζ-function

Analytically continuing $\zeta(s)$ to the complex plane $\mathbb{C}$ gives a meromorphic function with one simple pole at $s = 1$ with residue 1 [43]. Continuing $\zeta(s)$ is neither easy nor straightforward. The first part is to continue the function to the half-plane $Re(s) > 0$:

Proposition 3.1.3:

There exists a meromorphic continuation of $\zeta(s)$ for $Re(s) > 0$.

Proof. First, a real number t can be written as $t = [t] + \{t\}$, where $[t]$ denotes the integer part and $\{t\}$ the fractional part.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} s \int_{n}^{\infty} \frac{1}{t^{s+1}} dt =$$

$$= s \int_{1}^{\infty} \sum_{n \leq t} \frac{1}{t^{s+1}} dt = s \int_{1}^{\infty} \frac{[t]}{t^{s+1}} dt =$$

$$= s \int_{1}^{\infty} \frac{t}{t^{s+1}} dt - s \int_{1}^{\infty} \frac{\{t\}}{t^{s+1}} dt =$$

$$= \frac{s}{s-1} - s \int_{1}^{\infty} \frac{\{t\}}{t^{s+1}} dt \tag{3.1.2}$$

Because $\{t\} \in [0, 1[$, the integral converges for $Re(s) > 0$. So (3.1.2) converges for $Re(0)$ for all points except for $s = 1$. So for $Re(s) > 0$, except $s = 1$, the continuation is analytic and thus unique.
[42] □

Theorem 3.1.4:

The Riemann ζ-function can be analytically continued to the whole complex plane with a single pole at $s = 1$ (with residue 1).
The functional equation is

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{s\pi}{2}\right) \Gamma(1-s)\zeta(1-s) \tag{3.1.3}$$

with $s \neq 0, 1$

Continuing the ζ-function uses a similar idea as Proposition B.0.7.
By using the transformation $s \mapsto 1-s$, the function is defined on the whole complex plane. The center of symmetry is at $s = \frac{1}{2}$ and because of Proposition 3.1.3, $\zeta(s)$ is defined for $Re(s) \geq \frac{1}{2}$. This transformation also defines it for $Re(s) \leq \frac{1}{2}$, which defines $\zeta(s)$ on the whole complex plane.
The idea behind it may sound simple, but the proof of it is definitely not easy.

Proof. For $Re(s) > 0$

$$\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} n^{-s} = \int\limits_0^\infty x^{s-1} e^{-x} \pi^{-s/2} n^{-s} dx$$

Using the Substitution $x = \pi n^2 y$, with n being a positive integer, results in the following integral:

$$\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} n^{-s} = \int\limits_0^\infty y^{s/2-1} e^{-\pi n^2 y} dy$$

Summing over all n nor $Re(s) > 1$ adds up to

$$\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} \int\limits_0^\infty y^{s/2-1} e^{-\pi n^2 y} dy$$

With the identity in Proposition C.0.13:

$$\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} \zeta(s) = \int\limits_0^\infty y^{s/2-1} \cdot \frac{1}{2}(\theta(y) - 1) dy$$

29 is the number of knuts in one sickle.

By just looking at the intervall $[0, 1]$ and substituting $z = \frac{1}{y}$ and using Proposition C.0.13, it follows that

$$\int_0^1 y^{s/2-1} \cdot \frac{1}{2}(\theta(y) - 1)dy =$$

$$= \int_\infty^1 z^{-s/2+1}\frac{1}{2}(\theta\left(\frac{1}{z}\right) - 1)\frac{dz}{-z^2} =$$

$$= \int_1^\infty z^{-s/2-1}\frac{1}{2}(\sqrt{z}\theta(z) - 1)dz =$$

$$= \int_1^\infty z^{-s/2-1}\frac{1}{2}\sqrt{z}\theta(z) - z^{-s/2-1}\frac{1}{2}dz =$$

$$= \int_1^\infty z^{-s/2-1}\frac{1}{2}\sqrt{z}\theta(z) - z^{-s/2-1}\frac{1}{2} + z^{-s/2-1}\frac{\sqrt{z}}{2} - z^{-s/2-1}\frac{\sqrt{z}}{2}dz =$$

$$= \int_1^\infty z^{-s/2-1}\frac{1}{2}\sqrt{z}\theta(z)dz - \frac{1}{s} + \frac{1}{s-1} - \int_1^\infty z^{-s/2-1}\frac{\sqrt{z}}{2}dz =$$

$$= \frac{1}{s(s-1)} + \int_1^\infty z^{-(s+1)/2}\frac{1}{2}(\theta(z) - 1)dz$$

So

$$\Gamma\left(\frac{s}{2}\right)\pi^{-s/2}\zeta(s) = \frac{1}{s(s-1)} + \int_1^\infty z^{-(s+1)/2}\frac{1}{2}(\theta(z) - 1)dz + \int_1^\infty y^{s/2-1} \cdot \frac{1}{2}(\theta(y) - 1)dy =$$

$$= \frac{1}{s(s-1)} + \int_1^\infty (x^{-(s+1)/2} + x^{s/2-1})\frac{1}{2}(\theta(x) - 1)dx$$

Also $\frac{1}{2}(\theta(x) - 1) = O(e^{-\pi x})$ for $x \geq 1$ because

$$\theta(x) = 1 + 2e^{-\pi x} + 2 * e^{-4\pi x} + 2e^{-9\pi x} + \dots$$

$$= 1 + 2e^{-\pi x}(1 + e^{-3\pi x} + e^{-8\pi x} + \dots)$$

The term $1 + e^{-3\pi x} + e^{-8\pi x} + \dots$ is bounded, so

$$\frac{1}{2}(\theta(x) - 1) = O(e^{-\pi x})$$

This is an upper bound, the integral converges uniformly on every bounded domain in $\mathbb{C}$. Thus

$$\frac{1}{s(s-1)} + \int\limits_{1}^{\infty} (x^{-(s+1)/2} + x^{s/2-1})\frac{1}{2}(\theta(z) - 1)dx$$

is an analytic function, invariant under the transformation $s \mapsto 1-s$. This means, $\Gamma\left(\frac{s}{2}\right)\pi^{-s/2}\zeta(s)$ is also an analytic function in $\mathbb{C}\backslash\{0,1\}$ and it is also invariant under $s \mapsto 1-s$. This means

$$\Gamma\left(\frac{s}{2}\right)\pi^{-s/2}\zeta(s) = \Gamma\left(\frac{1-s}{2}\right)\pi^{-(1-s)/2}\zeta(1-s)$$

$$\zeta(s) = \frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\pi^{s-1/2}\zeta(1-s) \tag{3.1.4}$$

With Proposition B.0.8:

$$\frac{1}{\Gamma(\frac{s}{2})} = \frac{\Gamma(1-\frac{s}{2})\sin(\frac{\pi s}{2})}{\pi}$$

(3.1.4) equals

$$\zeta(s) = \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)\sin\left(\frac{\pi s}{2}\right)\pi^{s-3/2}\zeta(1-s)$$

And with Proposition B.0.9:

$$\Gamma\left(1-\frac{s}{2}\right)\Gamma\left(\frac{1-s}{2}\right) = \sqrt{\pi}2^s\Gamma(1-s)$$

$$\zeta(s) = 2^s\pi^{s-1}\sin\left(\frac{s\pi}{2}\right)\Gamma(1-s)\zeta(1-s)$$

[39][42] □

The speed limit in Trenton, Tennessee is 31 miles per hour.

3.1.3. The zeros of the Riemann ζ-function

Looking at (3.1.1) *Euler's product* of $\zeta(s)$ it is easy to see that it has no zeros for $Re(s) > 1$.

For $Re(s) < 0$ the sine-term in the analytic continuation (3.1.3) gives zeros at the negative even integers: $s = -2, -4, -6, \dots$ are called *trivial zeros.* Because $\Gamma(1-s) \neq 0$ for $Re(s) < 0$ those are all zeros for $Re(s) < 0$.

For $0 \leq Re(s) \leq 1$ (called the *critical strip*) it is not easy to calculate the zeros. In fact, it is proven that there are infinitely many zeros in that strip (see [43]), nevertheless only finitely many zeros are known to this point. All of those known zeros have the form $\frac{1}{2} + i \cdot \alpha$ for some $\alpha \in \mathbb{R}$.

This problem is called *The Riemann Hypothesis* and is probably the most famous unsolved problem in Mathematics and one of the seven *Millenium Problems* of the Clay Mathematics Institute; another one is stated on page 24. The official formulation of the problem is [7]:

Conjecture 3.1.5 (The Riemann Hypothesis):

The nontrivial zeros of $\zeta(s)$ have real part equal to $\frac{1}{2}$.

[7][43]

3.1.4. Dirichlet L-Functions

To make it even more complicated, one can extend the Riemann ζ-function to what is called a *Dirichlet L-Function.*

Definition 3.1.6 (Dirichlet character):

Let D be a positive integer. A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a *Dirichlet character modulus D* if
$\chi(mn) = \chi(m)\chi(n)\ \forall m, n \in \mathbb{Z}$,
$\chi(n) = \chi(n + kD)$ with $k \in \mathbb{Z}$ and
$\chi(n) = 0$ iff $(n, D) > 1$.

Definition 3.1.7 (Principal character):

χ_0 is the *principal character modulus D*:

$$\chi_0(n) = \begin{cases} 1, & \text{if } (n, D) = 1 \\ 0, & \text{otherwise} \end{cases}$$

Characters that are not *principal* are called *nonprincipal characters.*

Similar to Defintion 3.1.1 is the Definition of the *Dirichlet L-Series*:

Definition 3.1.8 (Dirichlet L-Series):

Let χ be a Dirichlet character modulus D and $s \in \mathbb{C}$. The Dirichlet L-Series is defined as

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

It is also convergent for $Re(s) > 1$ and if χ is nonprincipal it converges for $Re(s) > 0$.

Similar to Theorem 3.1.2, there exists a product formula, too:

Theorem 3.1.9:

For $s \in \mathbb{C}$ and $Re(s) > 1$

$$L(s, \chi) = \prod_{p} \left(1 - \frac{\chi(n)}{p^s}\right)^{-1}$$

with p in $\mathbb{P}$.

From this, it is easy to see the connection to the *Riemann ζ-function*:

Lemma 3.1.10:

Let χ_0 be the principal character modulus D. Then

$$L(s,\chi_0) = \zeta(s) \prod_{p|D} \left(1 - p^{-s}\right)$$

All Dirichlet L-Series can be analytically continued to the so-called *Dirichlet L-Functions*. If χ is a nonprincipal character, then the series $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges for $Re(s) > 0$, the corresponding function $L(s,\chi)$ is analytic in $\mathbb{C}$. Continuing $L(s,\chi)$ is similar to the continuation of $\zeta(s)$. If χ_0 is the principal character, then $L(s,\chi_0)$ can be continued to a meromorphic function, that has a single pole at $s = 1$ with residue $\varphi(D)/D$.
[14][28][40]

3.1.5. The zeros of the Dirichlet L-Functions

The zeros of $\zeta(s)$ have a great deal to do with the distribution of the primes. Similar to that, the zeros of $L(s,\chi)$ say a lot about the distibution of primes in a residue class. [14]

Conjecture 3.1.11 (The Generalized Riemann Hypothesis):

The zeros of $L(s,\chi)$, with χ being an arbitrary Dirichlet character, in the half plane $Re(s) > 0$ have real part equal to $\frac{1}{2}$.

The connection between the *Generalized Riemann Hypothesis* and *Conditional Polynomial Prime Number Tests* is the following:

Theorem 3.1.12:

Assume the *GRH*.
Let G be a nontrivial subgroup of $\mathbb{Z}_D^*$ such that all residue classes x with $(x,D) = 1$ and $x < n$ are contained in G.
Then $n < 2\log^2 D$.

Proof. G is a nontrivial subgroup of $\mathbb{Z}_D^*$ with $x \in G$ for all positive $x < n$.
Without loss of generality, G is maximal.
Then there is a nonprincipal character χ with $G \subset ker(\chi)$ and $\chi(x) = 1$ for all $x < n$.
First, let $D < 1000$. If $D < 3$, there are no nontrivial subgroups of $\mathbb{Z}_D^*$.
For $3 \leq D < 1000$ and $D \in \mathbb{P}$ it has a primitive root $< 1.7 \log^2 D$. [45]
If D is composite, it has a divisor at most $\sqrt{D}$ and $\sqrt{D} < 2\log^2 D$ for $6 \leq D < 1000$.
The harder part of the proof is for $D \geq 1000$.
Now, using Lemma D.0.20 and taking $a = \frac{1}{2}$:

$$\frac{\sqrt{n}}{\left(\frac{3}{2}\right)^2} \leq \frac{1}{2} \cdot (1 + r(n)) \cdot (\log D + t(n)) + s(n)$$

Also, $0 \leq \log D + t(n) \leq \log D$ ([5][1][44]).
Thus

$$\sqrt{n} \leq \frac{9}{8} \cdot (1 + r(n)) \cdot (\log D) + \frac{9}{4} \cdot s(n)$$

$$\sqrt{n} \leq \frac{9}{8} \cdot \left(1 + r(n) + \frac{2 \cdot s(n)}{\log 1000}\right) \cdot (\log D)$$

Also, $r(n) \to 0$ and $s(n) \to 0$ for sufficient large values of n.

$$\sqrt{n} < \sqrt{2} \log D$$

$$n < 2 \log^2 D$$

□

[14]

3.2. The Solovay-Strassen Primality Test

The problem with primality tests based on *Fermat's Little Theorem* are the already discussed *Carmichael Numbers*. An ideal primality test would have no *Pseudoprimes* or at least no composite numbers that fail for a sufficiently small number of bases a.

In the 1970s, *Robert M. Solovay* and *Volker Strassen* developed a randomized polynomial prime number algorithm. Their algorithm can be made deterministic assuming the *Generalized Riemann Hypothesis.* [2] The Primality Test is based on 1.4.5 *Euler's Criterion.*

Theorem 3.2.1:

Let n be an odd positive integer. If there exists an integer a with $(n, a) = 1$ and

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n} \tag{3.2.1}$$

Then n is composite.

Proof. n can either have a prime divisor more than once or n is squarefree.

First, let n be an odd composite number that is squarefree, hence $n = p_1 \cdot p_2 \cdots p_r$ with $r \geq 2$. All p_i are distinct odd primes.

Next, take a $b \in \mathbb{Z}$ that is a *quadratic nonresidue modulo* p_1. So

$$\left(\frac{b}{p_1}\right) = -1$$

With the *Chinese Remainder Theorem* there exists an $a \in \mathbb{Z}$ with

$$a \equiv b \pmod{p_1}$$

and

$$a \equiv 1 \pmod{n/p_1}$$

This means, that a is relatively prime to both p_1 and n/p_1. So $(a, n) = 1$. Furthermore,

$$\left(\frac{b}{p_1}\right) = \left(\frac{a}{p_1}\right) = -1$$

and for $1 < i \leq r$

$$\left(\frac{1}{p_i}\right) = \left(\frac{a}{p_i}\right) = 1$$

This means

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_r}\right) = (-1) \cdot 1 \cdots 1 = -1$$

Let

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

then

$$-1 \equiv a^{(n-1)/2} \pmod{n}$$

Furthermore

$$-1 \equiv a^{(n-1)/2} \pmod{n/p_1}$$

But

$$1 \equiv a \equiv a^{(n-1)/2} \pmod{n/p_1}$$

Now assume that n is of the form $n = p^k \cdot m$ with $p \in \mathbb{P}$, $k \geq 2$ and $(p, m) = 1$.

Because of the *Chinese Remainder Theorem* there exists an a with

$$a \equiv 1 + p \pmod{p^2}$$

and

$$a \equiv 1 \pmod{m}$$

This means $(a, p) = 1$ and $(a, m) = 1$ and it follows, that $(a, n) = 1$.

If

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

Roulette is played using a wheel containing 37 numbered slots.

holds, then (by squaring both sides) also

$$1 \equiv a^{n-1} \pmod{n}$$

which is *Fermat's Little Theorem.*

Also

$$1 \equiv a^{n-1} \equiv (1+p)^{n-1} \equiv 1 + (n-1) \cdot p \pmod{p^2}$$

So

$$0 \equiv (n-1) \cdot p \pmod{p^2}$$

$$n \equiv 1 \pmod{p^2}$$

But n is a multiple of p^2, so there is a contradiction too.
[9] □

This proof also shows that n can only be a *Carmichael Number* if n is squarefree.

3.2.1. The Probabilistic Solovay-Strassen Primality Test

A very effective but probabilistic *Prime Number Test* is based on Theorem 3.2.1. It is easy to show that the number of false positives for a *composite number* n is bounded by $\frac{n-1}{2}$. On that property, there exists a randomized test.

Definition 3.2.2 (Euler Pseudoprime):

n is an *Euler pseudoprime* to a base a if n is an odd composite number with $(n, a) = 1$ and (3.2.1) holds.
The number of all bases a, for which n is an *Euler pseudoprime* is denoted by

$$E(n) := |\{a \,(\text{mod } n) : n \text{ is an Euler pseudoprime to base } a\}|$$

If (3.2.1) fails for a base a, then it is called an *Euler witness.*

Theorem 3.2.3:

Let n be an odd composite integer > 1, then $E(n) < \frac{n-1}{2}$.

Proof. First define three sets:

$$A = \{1 \leq a \leq n-1 : (a,n) = 1 \wedge \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}\}$$

$$B = \{1 \leq a \leq n-1 : (a,n) = 1 \wedge \left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}\}$$

$$C = \{1 \leq a \leq n-1 : (a,n) > 1\}$$

Obviously, $|A| + |B| + |C| = n - 1$ and because of Theorem 3.2.1, B is not empty; additionally, $1 \in A$. Furthermore, because n is composite, C is non-empty too.

Let's take an arbitrary $b \in B$ and look at the set $A \cdot b = \{a \cdot b \pmod{n} : a \in A\}$. For all $a \in A$ the following condition holds: $(a \cdot b, n) = 1$ and

$$(a \cdot b)^{(n-1)/2} \equiv a^{(n-1)/2} \cdot b^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \cdot b^{(n-1)/2} \pmod{n}$$

$a \cdot b$ is either in A or B. If it is in A, then

$$(a \cdot b)^{(n-1)/2} \equiv \left(\frac{a \cdot b}{n}\right) \equiv \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) \pmod{n}$$

It follows that

$$\left(\frac{a \cdot b}{n}\right) \cdot b^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right) \pmod{n}$$

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

This is a contradiction to $b \in B$, therefore $a \cdot b \in B \; \forall a \in A$.

Also, if $a \cdot b \equiv a' \cdot b \mod n$ then $a = a'$. This means, that $|A| = |A \cdot b| \leq |B|$. So

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|$$

Which means that

$$E(n) = |A| < \frac{n-1}{2}$$

[9] □

Theorem 3.2.3 states that more than half of the bases $a \in \{1, 2, \dots n-1\}$ are *witnesses* for the compositeness of n. Based on that Theorem, there exists a randomized probabilistic primality test:

Algorithm 4 probabilisticsolovaystrassen(n: positive odd integer > 1)

```
choose random integer $a \in [2, n-1]$ with $(n, a) = 1$
if $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$ then
    return probably prime
end if
return composite
```

If n is prime, the algorithm always gives *probably prime.* If n is composite, the algorithm gives *probably prime* in less than half the cases. Running the algorithm k times results in a probability of $(\frac{1}{2})^k$ for never finding a witness.

The time complexity of the algorithm is $\tilde{O}(\log^2 n)$ with the right implementation. Running it k times results in a time complexity of $\tilde{O}(k \cdot \log^2 n)$. [16]

3.2.2. The Deterministic Solovay-Strassen Primality Test

To get to the deterministic albeit conditional version of the algorithm, the smallest *Euler witness* has to be further bounded. The only downside is that every proof bounding the smallest *Euler witness* by $c \cdot \ln^2 n$, with c being a constant, requires properties of the still unproven *Generalized Riemann Hypothesis.* The constant c has been proven to be at most 2 by *Eric Bach* in [5].

Theorem 3.2.4:

Assume the *GRH.*
Then every odd composite positive integer n has an *Euler witness* at most $2 \cdot \ln^2 n$.

Proof. With Theorem 3.1.12 a nontrivial subgroup G of $\mathbb{Z}_n^*$ and $x \in G \ \forall x < a'$ exists with $a' < 2\log^2 n$.
Let this subgroup be

$$G = \{a \in \mathbb{Z}_n^* | \left(\frac{a}{n}\right) \equiv a^{(n-1)/2}\}$$

Obviously, G is a subgroup of $\mathbb{Z}_n^*$.
Moreover, G is nontrivial, because $G \neq \mathbb{Z}_n^*$ (for every a there are witnesses) and $G \neq \{\bar{1}\}$.
Thus, there exists an a' with $a' \notin G$ (G is maximal) and $a' < 2\log^2 n$. □

[9]

Now, after at most $2 \cdot \ln^2 n$ steps, a composite number is identified.

Algorithm 5 solovaystrassen(n: positive odd integer >1)

```
$W = min\{\lfloor 2 \cdot \ln^2 n \rfloor, n-1\}$
for a=2 to W do
  if $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod n$ then
    return composite
  end if
end for
return prime
```

The time complexity of this algorithm is at most $O(\log^5 n)$. [36]

3.3. The Miller-Rabin Primality Test

At the same time as *Robert M. Solovay* and *Volker Strassen* published their results, *Gary L. Miller* and *Michael O. Rabin* developed their deterministic but conditional polynomial prime number algorithm.

In 1975, *Gary L. Miller* used *Fermat's Little Theorem* to obtain a deterministic polynomial prime number algorithm assuming the *Generalized Riemann Hypothesis.* His results are in [26]. A few years later, *Michael O. Rabin* modified the algorithm to make it unconditional but randomized while maintaining the polynomial time complexity. His results are in [32].

In contrast to the original order of research, this chapter starts off with the randomized algorithm and finishes with the deterministic one. [2][14]

Theorem 3.3.1:

Let p be an odd prime number with $p-1 = 2^s t$, where t is odd. For $a \in \mathbb{Z}_p^*$

$$\begin{cases} a^t \equiv 1 \pmod{p} \\ a^{2^i t} \equiv -1 \pmod{p} \qquad \text{for some } i \text{ with } 0 \leq i \leq s-1 \end{cases} \tag{3.3.1}$$

Proof. First, let p be an odd prime number.
Let's recall 1.3.1 *Fermat's Little Theorem*:

For $a > 1$ with $(a, p) = 1$

$$a^p \equiv 1 \pmod{p}$$

The first case is that $a^t \equiv 1 \pmod{p}$, which concludes the first part of the proof.

So assume $a^t \not\equiv 1 \pmod{p}$. To get to $a^p \equiv 1 \mod p$ by only squaring a^t, at one point the square root of $1 \pmod{p}$ has to occur. Because the polynomial $X^2 - 1 \pmod{p}$ has only two solutions: ± 1, at one point the sequence $a^{2^i t}$ has to be -1. This concludes the second part of the proof.

So if p is prime, one of the conditions has to hold.
[15] □

3.3.1. The Probabilistic Miller-Rabin Primality Test

The conversion of Theorem 3.3.1 does not necessarily hold:

Definition 3.3.2 (Strong Pseudoprime):

n is a *strong pseudoprime* to a base a if n is an odd composite number and (3.3.1) holds. The number of all bases a, for which n is a *strong pseudoprime* is denoted by

$$S(n) := |\{a \pmod{n} : n \text{ is a strong pseudoprime to base } a\}|$$

[14]

Theorem 3.3.3:

Let n be an odd composite integer with $n > 9$, then $S(n) \leq \frac{1}{4} \cdot \varphi(n)$.

Proof. [14] or [10] □

Theorem 3.3.3 states, that for at least $\frac{3}{4}$ of all bases $a \in \{1, 2, \ldots n-1\}$ n is not a *strong pseudoprime.* a is called a *witness* for an odd composite number n.

The following algorithm is very similar to the Solovay-Strassen randomized algorithm:

Algorithm 6 probabilisticmillerrabin(n: positive odd integer > 3)

```
find $s, t$ with $n - 1 = 2^s t$ and $t$ odd
choose random integer $a \in [2, n-1]$ with $(n, a) = 1$
if $a^t \equiv 1 \pmod{n}$ then
  return probably prime
else
  for i=0 to s-1 do
    if $a^{2^i t} \equiv -1 \pmod{n}$ then
      return probably prime
    end if
  end for
end if
return composite
```

Barbie and Ken broke up after 43 years.

It is easy to see that a is not a witness for an odd composite n in less than $\frac{1}{4}$ of the cases. Running the algorithm k times results in a probability to never choose a witness of $\left(\frac{1}{4}\right)^k$.

Using special fast multiplication techniques to implement the algorithm results in a time complexity $\tilde{O}(\log^2 n)$. Running the algorithm k times gives a time complexity of $\tilde{O}(k \cdot \log^2 n)$ [38].

3.3.2. The Deterministic Miller-Rabin Primality Test

Similar to the *Deterministic Solovay-Strassen Primality Test*, there also exists a *deterministic version* of the *Miller-Rabin Primality Test.* The two algorithms also have a number of commonalities. Every *Euler witness* for the *Solovay-Strassen Test* is also a *witness* for the *Miller-Rabin Test.* The conversion does not hold, which is also consistent with at least 50% being *Euler witnesses* and 75% *witnesses* for the *Miller-Rabin Test.*

Lemma 3.3.4:

For an odd positive integer > 1, an Euler witness is a witness for the Miller-Rabin primality test.

Proof. It is easier to prove: if an integer a is not a *Miller-Rabin witness*, then it is also not an *Euler witness.*

This means, if

$$a^t \equiv 1 \pmod{p}$$

or

$$a^{2^i t} \equiv -1 \pmod{p} \qquad \text{for some } i \text{ with } 0 \leq i \leq s-1$$

for some $a \in \mathbb{Z}_n^*$ and $n - 1 = 2^s t$ with t odd, then

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

Because

$$a^{(n-1)/2} = a^{2^s t/2} = a^{2^{s-1}t}$$

it follows that

$$a^{(n-1)/2} \equiv \pm 1 \pmod{n}$$

Let's consider 2 cases.

First, $s = 1$. So

$$a^{(n-1)/2} \equiv a^t \equiv \pm 1 \pmod{n}$$

Because $(n-1)/2$ is odd

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

If $a^{(n-1)/2} \equiv 1 \pmod{n}$, then

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

If $a^{(n-1)/2} \equiv -1 \pmod{n}$, then

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

Because $s = 1$, $(n-1)/2$ is odd.

So

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

This concludes the proof of the first case, namely where $s = 1$.

The second case is $s > 1$. If $a^{2^{s-1}t} \equiv -1 \pmod{n}$, then $a^{(n-1)/2} \equiv -1 \pmod{n}$. Otherwise $a^{2^{s-1}t} \equiv a^{(n-1)/2} \equiv 1 \pmod{n}$, because either $a^t \equiv 1$ or $a^{2^i t} \equiv -1$

(mod n) with $i < s - 1$. If $a^k \equiv 1 \pmod{n}$ and k is odd, then

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

The next step is to count all powers of 2 in each $p-1$, where p is a prime divisor of n.

Let $p - 1 = 2^{s_p} t_p$ with $s_p \geq 1$ and t_p odd. Because $a^{2^i t} \equiv -1 \pmod{n}$, $(a^t)^{2^i} \equiv -1$ (mod p). So the order of a^t (mod p) is 2^{i+1}. It follows, that $2^{i+1} | (p-1)$. This means, that $i < s_p$ and

$$p \equiv 1 \pmod{2^{i+1}} \tag{3.3.2}$$

Because p is prime

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

Because t is odd

$$\left(\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right)^t \equiv a^{2^{s_p-1}2t_p} \equiv a^{(2^i t_p)(2^{s_p-1-i}t_p)} \equiv (-1)^{2^{s_p-1-i}} \pmod{p}$$

If $i = s_p - 1$, then $2^{s_p-1-i} = 1$, otherwise 2^{s_p-1-i} is even. So $\left(\frac{a}{p}\right) = -1$ if $i = s_p - 1$ and $\left(\frac{a}{p}\right) = 1$ if $i < s_p - 1$.

With (3.3.2) follows

$$p \equiv 1 + c \cdot 2^{i+1} \pmod{2^{i+2}}$$

with $c \in \{0, 1\}$. $c = 0$ if $i < s_p - 1$ and 1 if $i = s_p - 1$.
Then

$$\left(\frac{a}{p}\right) = (-1)^c$$

Now, $n = p_1 \cdot p_2 \cdots p_r$.

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right) = \prod_{j=1}^{r} (-1)^{c_j} = (-1)^{\sum c_j} \tag{3.3.3}$$

Also,

$$n \equiv \prod_{j=1}^{r} p_j \equiv \prod_{j=1}^{r}(1 + c_j \cdot 2^{i+1}) \equiv 1 + \left(\sum_{j=1}^{r} c_j\right) \cdot 2^{i+1} \pmod{2^{i+2}}$$

Let $\tilde{c} = \sum_{j=1}^{r} c_j = |\{j : i = s_{p_j} - 1\}|$.
So because of (3.3.3) it follows that

$$\left(\frac{a}{n}\right) = (-1)^{\tilde{c}} \tag{3.3.4}$$

and

$$n \equiv 1 + \tilde{c} \cdot 2^{i+1} \equiv 2^s t + 1 \pmod{2^{i+2}}$$

If $i = s - 1$ (recall: $a^{(n-1)/2} \equiv -1$), then $2^{i+2} = 2^{s+1}$ and

$$1 + \tilde{c} \cdot 2^{i+1} \equiv 2^s t + 1 \pmod{2^{s+1}}$$

So $t \equiv \tilde{c} \pmod 2$, which means that $\tilde{c}$ is odd.

Because of (3.3.4)

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

If $i < s - 1$ (recall: $a^{(n-1)/2} \equiv 1$), then $i + 2 \leq s$, so $2^s \equiv 0 \pmod{2^{i+2}}$. So

$$\tilde{c} \cdot 2^{i+1} \equiv 0 \pmod{2^{i+2}}$$

This means, that $\tilde{c}$ is even and because of (3.3.4)

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

[10] □

In the television series *Alias*, the number 47 is of significant importance.

Theorem 3.3.5:

Assume the *GRH*.
The *smallest witness* for an odd composite positive integer n is at most $2 \cdot \ln^2 n$.

Proof. It follows directly from Lemma 3.3.4. □

Now, if the *GRH* holds, the smallest witness for an odd composite n is bounded by $2 \cdot \ln^2 n$. This means only bases smaller or equal to this bound have to be checked.

Algorithm 7 millerrabin(n: positive odd integer > 1)

```
$W = min\{\lfloor 2 \cdot \ln^2 n \rfloor, n-1\}$
find $s, t$ with $n - 1 = 2^s t$ and $t$ odd
for a=2 to W do
  if $a^t \not\equiv 1 \pmod{n}$ then
    if $a^{2^i t} \not\equiv -1 \pmod{n}\ \forall i : 0 \le i \le s-1$ then
      return composite
    end if
  end if
end for
return prime
```

The time complexity for the deterministic version of the *Miller-Rabin Primality Test* was first stated and proven in [26]; it is $\tilde{O}(\log^4 n)$.

4. Deterministic Polynomial Prime Number Tests

All of the algorithms mentioned in chapter 2 are either probabilistic or inefficient due to the time complexity. Algorithms mentioned in chapter 3 are both of that, assuming the *Generalized Riemann Hypothesis* is true. In this chapter, an unconditional deterministic prime number algorithm is indroduced that runs in polynomial time. In 2002, *Manindra Agrawal*, *Neeraj Kayal* and *Nitin Saxena* presented the *AKS prime number algorithm* in a paper simply called *PRIMES is in P*. [2][38]

4.1. Generalization of Fermat's Little Theorem

The algorithm is based on one simple Theorem, a generalization of 1.3.1 *Fermat's Little Theorem.*

Theorem 4.1.1 (Fermat for polynomials):

Let p be a prime number. Then

$$(P(X))^p \equiv P(X^p) \pmod{p}$$

holds for all polynomials P with integer coefficients.

Proof. The proof is done by using induction over the degree d of P.
For $d = 0$ it is simply *Fermat's Little Theorem.*
Let's suppose the Theorem is true for degree at most d. Let Q be such a polynomial with degree at most d and $P = aX^{d+1} + Q$ a polynomial with degree $d + 1$ and integer coefficient a.

$$(P(X))^p = (aX^{d+1}+Q(X))^p = (aX^{d+1})^p+\sum_{k=1}^{p-1}\binom{p}{k}(aX^{d+1})^k(Q(X))^{p-k}+(Q(X))^p \tag{4.1.1}$$

Because

$$(aX^{d+1})^p = a^p(X^{d+1})^p = a^p(X^p)^{d+1}$$

and because of 1.3.1 *Fermat's Little Theorem*

$$a^p(X^p)^{d+1} \equiv a(X^p)^{d+1} \pmod p$$

it follows that

$$(aX^{d+1})^p \equiv a(X^p)^{d+1} \pmod p$$

The sum in (4.1.1) is equivalent to $0 \pmod p$ because $\binom{p}{i} = \frac{p!}{i!\cdot(p-i)!} \equiv 0 \pmod p$. Moreover, $(Q(X))^p \equiv Q(X^p) \pmod p$ as it has degree at most d.
It therefore follows that

$$(P(X))^p \equiv a(X^p)^{d+1} + Q(X^p) = P(X^p) \pmod p$$

[33] □

Taking $P(X) = X + a$ with integer a relatively prime to the modulo even gives an "if and only if" criterion:

Theorem 4.1.2:

Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, $(a, n) = 1$.
Then n is prime iff

$$(X + a)^n \equiv X^n + a \pmod n \tag{4.1.2}$$

Proof. Let's examine $(X + a)^n - (X^n + a)$: for $0 < i < n$, the coefficient of x^i is $\binom{n}{i}a^{n-i}$.
If n is prime $\binom{n}{i} = \frac{n!}{i!\cdot(n-i)!} \equiv 0 \pmod n$ and all the coefficents are zero.

If n is composite, there exists a prime q with $q|n$. Let $q^k|n$ and $q^{k+1} \nmid n$. Then (with $n = q^k \cdot m$)

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

$$= \frac{(q^k \cdot m) \cdot (n-1) \cdots (n-q+1)}{q!} =$$

$$= \frac{(q^{k-1} \cdot m) \cdot (n-1) \cdots (n-q+1)}{(q-1)!}$$

Because q does not divide any number between $n-q+1$ and $n-1$ $q^k \nmid \binom{n}{q}$, it follows that $\binom{n}{q} \not\equiv 0 \pmod{n}$. Also, $(a^{n-q}, n) = 1$, so $a^{n-q} \not\equiv 0 \pmod{n}$.
So, $\binom{n}{q}a^{n-q}$, the coefficient of X^q, is not zero and $(X+a)^n - (X^n + a)$ does not vanish over $\mathbb{Z}_n$. [2] □

Although Theorem 4.1.2 is a deterministic prime number test, the time complexity is not desirable. In the worst case, n coefficients have to be checked, so the time complexity is $O(n)$. A simple solution to improve time complexity (and thereby also the running time) is to reduce the number of coefficients. Instead of comparing the coefficients modulo n, comparing them in the ring $Z_n[x]/(X^r - 1)$ with an appropriately small r would do exactly that. [2]

Definition 4.1.3:

Let $f(X)$, $g(X)$ be integer polynomials. Then the notation

$$f(X) \equiv g(X) \pmod{h(X), n}$$

means $f(X) \equiv g(X)$ in the ring $Z_n[X]/(h(X))$.

Lemma 4.1.4:

If n is prime, then

$$(X+a)^n \equiv X^n + a \pmod{X^r - 1, n} \tag{4.1.3}$$

Proof. It follows immediately from Theorem 4.1.2 that all values of a and r satisfy the equation. [2] □

A problem with which the algorithm has to contend is that a few composite numbers may, in fact, satisfy equation (4.1.3) for some a and r, too. *Agrawal*, *Kayal* and *Saxena* already have a solution for that: "we show that for appropriately chosen r if the equation (4.1.3) is satisfied for several a's, then n must be a prime power. The number of a's and the appropriate r are both bounded by a polynomial in $\log n$ and therefore, we get a deterministic polynomial time algorithm for testing primality." [2]

4.2. The AKS Prime Number Algorithm

Algorithm 8 aks(n: positive integer > 1)

```
Step 1
    if $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$ then
        return composite
    end if
Step 2
    Find the smallest $r$ such that $o_r(n) > \log^2 n$
Step 3
    if $1 < (a, n) < n$ for some $a \le r$ then
        return composite
    end if
Step 4
    if $n \le r$ then
        return prime
    end if
Step 5
    for $a = 1$ to $\lfloor \sqrt{\varphi(r)} \log n \rfloor$ do
        if $(X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$ then
            return composite
        end if
    end for
Step 6
    return prime
```

Theorem 4.2.1:

The algorithm $aks(n)$ returns prime iff n is prime.

Proving this Theorem requires some more work:

Lemma 4.2.2:

If n is prime, the algorithm $aks(n)$ returns prime.

Proof. If n is *prime* steps 1 and 3 cannot return *composite*. Also, 5 never returns *composite* because of Lemma 4.1.4, thus the algorithm returns *prime*.
The algorithm returning *prime* in step 4 means the input n has to be prime, otherwise there would be a non-trivial factor of n identified in step 3.
The only remaining case to check is step 6. This means, check if all *composite numbers* have been identified by either step 1, 3 or 5. □

Lemma 4.2.3:

lcm(n) is the *least common multiple* for the first n numbers. For $n \geq 9$:

$$lcm(n) \geq 2^n$$

Proof. First, consider the integral for $1 \leq m \leq n$

$$I = I(m,n) = \int_0^1 x^{m-1}(1-x)^{n-m}dx =$$

$$= \int_0^1 x^{m-1} \sum_{k=0}^{n-m} \binom{n-m}{k} (-x)^k dx =$$

$$= \int_0^1 \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k x^{k+m-1} dx =$$

$$= \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k \int_0^1 x^{k+m-1} dx =$$

$$= \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k \frac{1}{k+m}$$

Because every denominator in the sum is at most n, $I \cdot lcm(n) \in \mathbb{Z}$.

53 players are allowed to be on the roster of an NFL game.

Repeatedly integrating I by parts gives

$$I = I(m,n) = \int\limits_0^1 x^{m-1}(1-x)^{n-m}dx =$$

$$= \frac{n-m}{m}\int\limits_0^1 x^m(1-x)^{n-m-1}dx =$$

$$= \frac{(n-m)(n-m-1)}{m(m+1)}\int\limits_0^1 x^{m+1}(1-x)^{n-m-2}dx =$$

$$\vdots$$

$$= \frac{(n-m)\cdots(n-m-(n-m-1))}{m\cdots(m+(n-m-1))}\int\limits_0^1 x^{m+(n-m-1)}(1-x)^{n-m-(n-m-1)-1}dx =$$

$$= \frac{(n-m)(n-m-1)\cdots 1}{m(m+1)\cdots(n-1)}\int\limits_0^1 x^{n-1}dx =$$

$$= \frac{(n-m)(n-m-1)\cdots 1}{m(m+1)\cdots(n-1)n} =$$

$$= \frac{(n-m)!\cdot m!}{m\cdot n!} = \frac{1}{m\cdot\binom{n}{m}}$$

It follows that $m\cdot\binom{n}{m}|lcm(n)\ \forall m,\ 1\le m\le n$.

Also

$$n\cdot\binom{2n}{n}|lcm(2n) \text{ and } (2n+1)\cdot\tbinom{2n}{n} = (n+1)\cdot\tbinom{2n+1}{n+1}|lcm(2n+1)$$

Because $lcm(2n)|lcm(2n+1)$, both $n\cdot\binom{2n}{n}$ and $(2n+1)\cdot\binom{2n}{n}$ divide $lcm(2n+1)$.

From $(2n+1,n)=1$ it follows that $n\cdot(2n+1)\cdot\binom{2n}{n}|lcm(2n+1)$.

$$lcm(2n+1)\ge n(n+1)\binom{2n}{n}\ge n\cdot\sum_{k=0}^{2n}\binom{2n}{k} = n\cdot(1+1)^{2n}\ge 2^{2n+1}$$

The last inequality holds for $n \geq 2$. For even numbers the inequality also holds, because if $n \geq 4$ $lcm(2n+2) \geq lcm(2n+1) \geq 2^{2n+2}$. So

$$lcm(n) \geq 2^n$$

for $n \geq 9$. [27] □

Lemma 4.2.4:

There exists a $r \leq \max\{3, \lceil \log^5 n \rceil\}$ such that $o_r(n) > \log^2 n$.

Proof. $r = 3$ satisfies all the conditions for $n = 2$: $o_3(2) = 2 > \log^2 2 = 1$, thus assume $n \geq 3$.
First, consider r as the smallest number that does not divide the product

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) \tag{4.2.1}$$

with $B := \lceil \log^5 n \rceil$.

(r, n) cannot be divisible by all the prime divisors of r because r does not divide $n^{\lfloor \log B \rfloor}$. So it follows that $\frac{r}{(r,n)}$ does not divide (4.2.1) either. Because r is the smallest number not dividing (4.2.1), $(r, n) = 1$ and $o_r(n)$ exists.
r also does not divide any $n^i - 1$ for $1 \leq i \leq \lfloor \log^2 n \rfloor$, so

$$o_r(n) > \log^2 n$$

Second,

$$n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) <$$

$$< n^{\lfloor \log B \rfloor + \frac{1}{2} \log^2 n \cdot (\log^2 n - 1)} \leq=$$

$$\leq n^{\log^4 n} =$$

$$= (2^{\log n})^{\log^4 n} =$$

$$= 2^{\log^5 n} \leq$$

$$\leq 2^B \tag{4.2.2}$$

Because $\lceil \log^5 n \rceil > 10$ Lemma 4.2.3 can be applied, the *least common multiple* of the first B numbers is at least 2^B.

Let's assume that $r > B$, then for all $1 \leq i \leq B$, i divides (4.2.1). Then

$$lcm(B) \leq n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1)$$

But because of (4.2.2) it is not true, so $r \leq B$. [2] □

Now that $o_r(n) > 1$, there must be a prime divisor p of n, such that $o_r(p) > 1$. In order to get to step 5, $p > r$, otherwise step 3 or 4 would terminate the algorithm. For the same reason, $(n, r) = 1$ and therefore $p, n \in \mathbb{Z}_r^*$.
Also, define $l := \lfloor \sqrt{\varphi(r)} \log n \rfloor$.
In step 5 of the algorithm, l equations are checked. For the algorithm to proceed to step 6, all l of them have to be equivalent:

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

for $0 \leq a \leq l$.

It follows that

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, p} \tag{4.2.3}$$

for $0 \leq a \leq l$.

Because p is prime and Theorem 4.1.2

$$(X + a)^p \equiv X^p + a \pmod{X^r - 1, p} \tag{4.2.4}$$

for $0 \leq a \leq l$.

From (4.2.3) and (4.2.4) it follows that

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

Substituting X with $X^{\frac{1}{p}}$ gives ($X^{\frac{1}{p}}$ is unique)

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

for $0 \leq a \leq l$.

Because of this, n and $\frac{n}{p}$ both behave like prime, a property we will term *introspective.* [2][8]

Definition 4.2.5:

Let $f(X)$ be a polynomial and $m \in \mathbb{N}$, then m is *introspective* for $f(X)$ if

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

It is easy to see that both n and $\frac{n}{p}$ are *introspective* for $X + a$ with $0 \leq a \leq l$. The next two Lemma show some properties about *introspective numbers*:

Lemma 4.2.6:

Introspective numbers are closed under multiplication. So if m and m' are *introspective* for $f(X)$, so is $m \cdot m'$.

Proof. m is *introspective*, so

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

$$[f(X)]^{m \cdot m'} \equiv [f(X^m)]^{m'} \pmod{X^r - 1, p} \tag{4.2.5}$$

For m':

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

Replacing X with X^m gives

$$[f(X^m)]^{m'} \equiv f(X^{m \cdot m'}) \pmod{X^{m \cdot r} - 1, p}$$

$X^r - 1$ divides $X^{m \cdot r} - 1$, so

$$[f(X^m)]^{m'} \equiv f(X^{m \cdot m'}) \pmod{X^r - 1, p} \tag{4.2.6}$$

From (4.2.5) and (4.2.6) it follows that

$$[f(X)]^{m \cdot m'} \equiv f(X^{m \cdot m'}) \pmod{X^r - 1, p}$$

[2] □

Lemma 4.2.7:

The set of polynomials for which a number m is *introspective* is closed under multiplication. So if m is *introspective* for $f(X)$ and $g(X)$, then m is also *introspective* for $f(X) \cdot g(X)$.

Proof.

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

[2] □

Because of Lemma 4.2.6 and Lemma 4.2.7, every number in the set

$$I = \{\left(\frac{n}{p}\right)^i \cdot p^j | i, j \in \mathbb{N}\}$$

is *introspective* for every polynomial

$$P = \{\prod_{a=0}^{l} (X + a)^{e_a} | e_a \in \mathbb{N}\}$$

The next step is to define a group G, which is the set of all residues of numbers in I modulo r. Because $(n, r) = 1$, it is also a subgroup of $\mathbb{Z}_r^*$. Let $t := |G|$. Because G is generated by $\frac{n}{p}$ and p modulo r and because of Lemma 4.2.4: $o_r(n) > \log^2 n$, $t > \log^2 n$. [2][8]

In order to define the second group crucial for the final steps of the proof, a few properties about *Cyclotomic Polynomials over finite fields* have to be stated:

Definition 4.2.8 (Cyclotomic Polynomial):

A cyclotomic polynomial $C_r(X)$ divides $X^r - 1$ but not $X^k - 1$ for $k \in \{1, 2, \dots r-1\}$.

Cyclotomic Polynomials are irreducible over $\mathbb{Z}$. In the finite field $\mathbb{F}_p$, *Cyclotomic Polynomials* $Q_r(X)$ do not have to be irreducible. In fact, there exists an irreducible factor $h(X)$ of $Q_r(X)$ with degree $o_r(p)$ ([8]) because $o_r(p) > 1$, the degree of $h(X)$ is also greater than one.

Let's define another group H as the set of all residues of polynomials in P modulo p and $h(X)$. H is generated by its elements $X, X+1, X+2, \dots, X+l$ in the field $\mathbb{F} := \mathbb{F}_p[X]/h(X)$. [2][8][33]

The next step of the proof is putting an upper and a lower bound on $|H|$.

Lemma 4.2.9:

If n is not a power of p, then $|H| \leq n^{\sqrt{t}}$.

Proof. First, take a look at the subset I' of I:

$$I' := \{\left(\frac{n}{p}\right)^i \cdot p^j | i, j \in \{0, 1, \dots, \lfloor\sqrt{t}\rfloor\}\}$$

Since n is not a power of p, I' has $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ distinct numbers. Moreover, because $|G| = t$, there have to be two numbers in I' that are equal modulo r. Let m_1 and m_2 be those numbers and without loss of generality let $m_1 > m_2$.

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

Let $f(X)$ be an arbitrary polynomial in P.

$$[f(X)]^{m_1} \equiv f(X^{m_1}) \equiv f(X^{m_2}) \equiv [f(X)]^{m_2} \pmod{X^r - 1, p}$$

Because of this

$$[f(X)]^{m_1} \equiv [f(X)]^{m_2} \pmod{X^r - 1, p}$$

is in $\mathbb{F}$.

It follows that $f(X) \in H$ is a root of the polynomial $Q(Y) = Y^{m_1} - Y^{m_2}$ in the field $\mathbb{F}$. Thus, $Q(Y)$ has at least $|H|$ distinct roots in F. Because the degree of $Q(Y)$ is $m_1 \leq (\frac{n}{p} \cdot p)^{\lfloor \sqrt{t} \rfloor} \leq n^{\sqrt{t}}$, $|H| \leq n^{\sqrt{t}}$. [2][8] □

Lemma 4.2.10:

$$|H| > n^{\sqrt{t}}$$

Proof. The first step is to show that two arbitrary polynomials $f(X)$ and $g(X) \in P$, with degree smaller than t, map to different elements in H. Let $f(X) \equiv g(X)$ in $\mathbb{F}$ and let $m \in I$. It follows that

$$[f(X)]^m \equiv [g(X)]^m$$

in $\mathbb{F}$.

Because $m \in I$, it is introspective for $f(X)$ and $g(X)$ and also $h(X)$ divides $X^r - 1$:

$$f(X^m) \equiv g(X^m)$$

in $\mathbb{F}$.

It follows that X^m is a root of the polynomial $Q(Y) = f(Y) - g(Y)$ $\forall m \in G$.
G is a subgroup of $\mathbb{Z}_r^*$, so $(m, r) = 1$ and X^m is a primitive r^{th} root of unity. This implies that there are $|G| = t$ distinct roots of $Q(Y)$ in $\mathbb{F}$, but the degree of $Q(X)$ is smaller than t because of the degree of $f(X)$ and $g(X)$. This contradicts $f(X) \equiv g(X)$ in $\mathbb{F}$, so $f(X) \not\equiv g(X)$ in $\mathbb{F}$.
Additionally, because $i \neq j$ in $\mathbb{F}_p$ for $1 \leq i \neq j \leq l$ and $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor < \sqrt{r} \log n < r < p$, $X, X+1, \ldots, X+l$ are distinct in $\mathbb{F}$.
Furthermore, the degree of $h(X)$ is greater than one, so $X, X+1, \ldots, X+l \neq 0$ in $\mathbb{F}$. Because of this, there are at least $l+1$ distinct polynomials of degree one in H.

So there exist at least (number of combinations with repetition)

$$\sum_{i=0}^{t-1} \binom{l+1}{i} = \sum_{i=0}^{t-1} \binom{l+1+i-1}{i} = \sum_{i=0}^{t-1} \binom{l+i}{i} = \binom{l+t-1+1}{t-1} = \binom{t+l}{t-1}$$

distinct polynomials of degree smaller than t in H.

So

$$|H| \geq \binom{t+l}{t-1}$$

Because $t > \log^2 n >$, $t > \sqrt{t} \log n$ and therefore $t \leq \lfloor \sqrt{t} \log n \rfloor + 1$

$$|H| \geq \binom{\lfloor \sqrt{t} \log n \rfloor + 1 + l}{\lfloor \sqrt{t} \log n \rfloor + 1 - 1}$$

Also, $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor \geq \lfloor \sqrt{t} \log n \rfloor$:

$$|H| \geq \binom{2 \cdot \lfloor \sqrt{t} \log n \rfloor + 1}{\lfloor \sqrt{t} \log n \rfloor}$$

Because

$$\sum_{i=0}^{2 \cdot \lfloor \sqrt{t} \log n \rfloor + 1} \binom{2 \cdot \lfloor \sqrt{t} \log n \rfloor + 1}{i} = 2^{2 \cdot \lfloor \sqrt{t} \log n \rfloor + 1}$$

it follows that

$$|H| > 2^{\lfloor \sqrt{t} \log n \rfloor + 1} \geq n^{\sqrt{t}}$$

[2][8] □

Lemma 4.2.11:

If the algorithm aks(n) returns prime, then n is prime.

Proof. Because of Lemma 4.2.11 $|G| > n^{\sqrt{t}}$, but Lemma 4.2.2 states that if n is not a prime power $|G| \leq n^{\sqrt{t}}$. So n has to be a power of p: $n = p^k$ for $k \in \mathbb{N}^+$. For $k > 1$, the alogrithm returns *composite* in step 1, therefore $k = 1$ and n is prime. [2] □

Proof of Theorem 4.2.1. Because of Lemma 4.2.2 and Lemma 4.2.11, the algorithm returns prime iff n is prime. □

Some minutes have 61 seconds.

4.2.1. Time Complexity

Theorem 4.2.12:

The asymptotic time complexity of the *AKS Prime Number Algorithm aks*(n) is $\tilde{O}(\log^{21/2} n)$.

Proof. **Step 1:** If n is a perfect power a^b then $n = \lfloor (n^{\frac{1}{b}})^b \rfloor$, where b runs up to $\log n$. The time complexity is $\tilde{O}(\log^3 n)$.

Step 2: In this step, the smallest r with the condition $o_r(n) > \log^2 n$ is found. Checking if the order is bigger than the limit can be done in $\tilde{O}(r \cdot \log^2 n)$ because only $n^k \neq 1 \pmod r$ for all $k \leq \log^2 n$ needs to be checked. Also, the numbers of r are bounded by $O(\log^5 n)$ (Lemma 4.2.4), so the time complexity in this step is $\tilde{O}(\log^7 n)$.

Step 3: The computation of a *greatest common divisor* has the time complexity of $O(\log n)$. Because r of them are checked, it is $O(r \cdot \log n)$, which results in $O(\log^6 n)$ because of Lemma 4.2.4.

Step 4: This step does not require a great deal of time, merely $O(\log n)$.

Step 5: The *for-loop* runs at most $\sqrt{\varphi(r)} \log n$ times. In every cycle, there is an *if-condition* that requires $O(\log n)$ multiplications of degree r polynomials with coefficients of the size $O(\log n)$. In total, it makes $\tilde{O}(r \cdot \log^2 n)$. This translates into a total time complexity of $\tilde{O}(r \cdot \sqrt{\varphi(r)} \log^3 n) = \tilde{O}(r^{\frac{3}{2}} \log^3 n) = \tilde{O}(\log^{21/2} n)$.

Step 6: This step only returns *prime*, thus the time compexity is $O(1)$.

Step 5 dominates all others which results in a time complexity of $\tilde{O}(\log^{21/2} n)$ for the whole algorithm. [2] □

This proves that the time complexity of the *AKS prime number algorithm* is polynomial. Nevertheless, it is still desirable to get to an even better time complexity. This can be done by bounding r even more. The best case would be $r = O(\log^2 n)$, bringing the total time complexity down to $\tilde{O}(\log^6 n)$.

5. Recent Developments

Since the paper *Primes is in P* was published, there have been several attempts to improve the time complexity from $\tilde{O}(\log^{21/2} n)$ to $\tilde{O}(\log^{6} n)$ or even further. There are two conjectures, *Artin's Conjecture* and *Sophie-Germain Prime Density Conjecture*, that support the possibility of such a time complexity. The first conjecture even holds under the *Generalized Riemann Hypothesis.*

Conjecture 5.0.13 (Artin's Conjecture):

For all $n \in \mathbb{N}$, where $\sqrt{n} \notin \mathbb{N}$, the number of primes $q \leq m$ for which $o_q(n) = q - 1$ is asymptotically $A(n) \cdot \frac{m}{\ln m}$.
$A(n)$ is Artin's constant with $A(n) > 0.35$.

Conjecture 5.0.14 (Sophie-Germain Prime Density Conjecture):

The number of primes $q \leq m$ with $2q + 1 \in \mathbb{P}$ is asymptotically $\frac{2C_2 m}{\ln^2 m}$.
C_2 is the twin prime constant and estimated to be approximately 0.66.

Another conjecture would improve the time complexity to $\tilde{O}(\log^3 n)$.

Conjecture 5.0.15:

If $r \in \mathbb{P}$ and r does not divide n and if

$$(X-1)^n \equiv X^n - 1 \pmod{X^r - 1, n} \tag{5.0.1}$$

then either n is prime or $n^2 \equiv 1 \pmod{r}$.

If this conjecture is true, the algorithm can be modified to first search for an r, where r does not divide $n^2 - 1$. Such an r can be found in the interval $[2, 4 \log n]$ [4]. With this r, the congruence (5.0.1) can be verified in $\tilde{O}(\log^2 n)$. This gives a time complexity of $\tilde{O}(\log^3 n)$.

Although the conjecture is true for $r \leq 100$ and $n \leq 10^{10}$ [21], in 2003, *Hendrik Lenstra* and *Carl Pomerance* have given an heuristic argument that suggests that the conjecture is false. [2]

Without using any conjecture, a Lemma provided in [19] does not rely on an unproven hypothesis; with this, the time complexity can be improved to $\tilde{O}(\log^{15/2} n)$:

Lemma 5.0.16:

There exist constants $c > 0$ and n_0 such that, for all $x \geq n_0$:

$$|\{q | q \in \mathbb{P}, q \leq x \wedge P(q-1) > q^{2/3}\}| \geq c \cdot \frac{x}{\ln x}$$

Theorem 5.0.17:

The time complexity of $aks(n)$ is $\tilde{O}(\log^{15/2} n)$.

Proof. With Lemma 5.0.16, step 2 of the algorithm finds an $r = O(\log^3 n)$ with $o_r(n) > \log^2 n$. This results in a time comlexity of $\tilde{O}(\log^{15/2} n)$. □

[2][19]

5.1. Primality testing with Gaussian periods

In 2009, *Hendrik Lenstra* and *Carl Pomerance* modified the algorithm $aks(n)$ to get an improved time complexity of $\tilde{O}(\log^6 n)$. They are also performing computations in a ring extension of $\mathbb{Z}_n$. Instead of generating their rings by roots of unity, they are using *Gaussian Periods.* [2][24]

Conclusion

Time complexity has always been a significant concern when attempting to differentiate prime numbers from composite numbers. Although there are tests that are sufficiently fast, most of them are, unfortunately, probabilistic, which means that there is room for error. Until 2002, mathematicians assumed that the Prime Number Problem is, in fact, polynomial but thus far had been unable to prove it. With the paper *PRIMES is in P* ([2]), Agrawal, Kayal and Saxena provided the proof that had thus far been missing. They were able to develop an algorithm, based on *Ferman's Little Theorem*, that can deterministically distinguish primes from composites with a time complexity of $\tilde{O}(\log^{21/2} n)$. Their algorithm was further improved upon by *Carl Pomerance*, reducing the time complexity to $\tilde{O}(\log^{15/2} n)$.

Why is this paper so significant? Firstly, it provides additional to the heat of the discussion whether $P = NP$. Actually having proof of a problem being polynomial that has otherwise thus far been officially categorized as NP for ages might provide new insight into other current NP problems.

Moreover, the *Generalized Riemann Hypothesis*, despite not yet having been proven, says that a deterministic algorithm might be polynomial. Even though the GRH remains unsolved to this day and the AKS algorithm is not based on the GRH, having a deterministic polynomial time algorithm gives an indication that it might indeed be true.

In number theory, this algorithm is groundbreaking as it is the very first deterministic polynomial prime number test in history. Furthermore, it also opens up a lot of potential and providing insight into reexamining famous conjectures, such as the *Riemann Hypothesis*. Nonetheless, while being a significant finding, it remains theoretical due to it still having a higher time complexity than some based on the *Riemann Hypothesis*, thus making it unattractive for real world prime number tests. Instead, probabilistic or deterministic algorithms based on the Riemann Hypothesis remain better tools for determining primality outside of theoretical work. Despite the risks inherent with this approach, it is worth it since the errors are virtually non-existent.

Jupiter has 67 confirmed moons.

Appendices

A. Asymptotic Growth of Functions

In order to characterize the efficiency of an algorithm, several types of asymptotic notations are introduced. They make it easier to compare similar alogrithms and give information about their running time. The *asymtotic efficiency* gives information on how the running time increases when the size of the input increases. An algorithm that is asymptotically more efficient than another algorithm means that with a large enough input, it will have the better running time than the other; for a very small input, it may be the other way around. [13] The first notation gives an asymptotic upper bound for a function $f(n)$:

Definition A.0.1 (Big O-notation):

$$f(n) = O(g(n)) :\Leftrightarrow \exists c, n_0 > 0 : 0 \leq f(n) \leq c \cdot g(n) \; \forall n \geq n_0$$

In chapter 4 another notation is used [2]:

Definition A.0.2:

$$\tilde{O}(t(n)) := O(t(n) \cdot poly(\log t(n)))$$

with $t(n)$ being a function of n.

Another notation gives the asymptotic lower bound for a function $f(n)$:

Definition A.0.3 (Big Ω-notation):

$$f(n) = \Omega(g(n)) :\Leftrightarrow \exists c, n_0 > 0 : 0 \leq c \cdot g(n) \leq f(n) \; \forall n \geq n_0$$

A much tighter bound is the next notation, it gives both an upper and a lower bound for a function $f(x)$:

Definition A.0.4 (Big Θ-notation):

$$f(n) = \Theta(g(n)) :\Leftrightarrow \exists c_1, c_2, n_0 > 0 : 0 \leq c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n) \; \forall n \geq n_0$$

[13][33][34]

B. The Gamma function

Definition B.0.5 (Γ-function):

For $Re(s) > 0$, the Γ-function is defined as

$$\Gamma(s) = \int\limits_0^\infty x^{s-1}e^{-x}dx$$

A few properties of the Γ-function are:

Proposition B.0.6:

$$\Gamma(s+1) = s\Gamma(s)$$

Proof.

$$\Gamma(s+1) = \int\limits_0^\infty x^s e^{-x}dx = -e^{-x}x^s|_0^\infty + \int\limits_0^\infty sx^{s-1}e^{-x}dx = s\Gamma(s)$$

□

Proposition B.0.7:

$\Gamma(s)$ can be analytically continued to the whole complex plane with simple poles at the negative integers (including 0).

Proof. Because of Proposition B.0.6, Γ can be continued to $-1 < Re(s) \leq 0$ exept for $s = 0$. Repeating that for the negative half-plane gives an analytic continuation with simple poles at $0, -1, -2, \ldots$. □

The Hubble constant is approximately 71 km/s/Mpc.

Proposition B.0.8 (Formula of complements):

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$$

A proof can be found in [20].

Proposition B.0.9 (Duplication formula of Legendre):

$$\Gamma(s)\Gamma\left(s+\frac{1}{2}\right) = \sqrt{\pi}2^{1-2s}\Gamma(2s)$$

A proof can be found in [20].

C. Fourier transformation

Definition C.0.10 (Fourier transformation):

The *Fourier transformation* $\hat{f}$ of an integrable function f on R is defined as

$$\hat{f}(x) = \int\limits_{-\infty}^{+\infty} f(y)e^{-2\pi ixy}dy$$

Proposition C.0.11 (Poisson Summation):

If g is infinitely differentiable, then

$$\sum_{m=-\infty}^{\infty} g(m) = \sum_{m=-\infty}^{\infty} \hat{g}(m)$$

Proof. First, let's define $h(x) := \sum_{k=-\infty}^{\infty} g(x+k)$.
The Fourier series is

$$h(x) = \sum_{m=-\infty}^{\infty} c_m e^{2\pi imx}$$

with c_m defined as

$$c_m := \int\limits_{0}^{1} h(x)e^{-2\pi imx}dx$$

$$= \int\limits_{0}^{1} \sum_{k=-\infty}^{\infty} g(x+k)e^{-2\pi imx}dx$$

Sheldon Cooper's favorite number is 73.

$$= \sum_{k=-\infty}^{\infty} \int_{0}^{1} g(x+k)e^{-2\pi imx}dx$$

$$= \int_{-\infty}^{\infty} g(x+k)e^{-2\pi imx}dx$$

$$= \hat{g}(m)$$

This means that

$$\sum_{k=-\infty}^{\infty} g(k) = h(0)$$

$$= \sum_{k=-\infty}^{\infty} c_k e^{-2\pi im\cdot 0}$$

$$= \sum_{k=-\infty}^{\infty} c_k = \sum_{k=-\infty}^{\infty} \hat{g}(k)$$

[39] □

Proposition C.0.12:

For $f(x) := e^{-\pi x^2}$

$$f(x) = \hat{f}(x)$$

A proof can be found in [39].

Proposition C.0.13:

For $f(\sqrt{u}x) = e^{-\pi ux^2}$ with $u > 0$, $\hat{f}(\sqrt{u}x) = e^{-\pi x^2/u}u^{-1/2}$.
Also, for $\theta(u) := \sum_{n\in\mathbb{Z}} e^{-\pi n^2 u}$

$$\theta(1/u) = \sqrt{u}\theta(u) \tag{C.0.1}$$

Proof.

$$f(\sqrt{u}x) = e^{-\pi ux^2} = e^{-\pi(\sqrt{u}x)^2}$$

$$\hat{f}(\sqrt{u}x) = \int\limits_{-\infty}^{\infty} e^{-2\pi ixy} e^{-\pi(\sqrt{u}x)^2} dx =$$

$$= \int\limits_{-\infty}^{\infty} e^{-2\pi ixy/\sqrt{u}} e^{-\pi x^2} \frac{dx}{\sqrt{u}} =$$

$$= \frac{1}{\sqrt{u}} \hat{f}\left(\frac{y}{\sqrt{u}}\right) \overset{Prop. C.0.12}{=}$$

$$= \frac{1}{\sqrt{u}} f\left(\frac{x}{\sqrt{u}}\right) =$$

$$= \frac{1}{\sqrt{u}} e^{-\pi x^2/u}$$

In conclusion,

$$\hat{f}(\sqrt{u}x) = \frac{1}{\sqrt{u}} e^{-\pi x^2/u} \tag{C.0.2}$$

(C.0.1) holds because:

$$\theta(u) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 u} =$$

$$= \sum_{n\in\mathbb{Z}} f(\sqrt{u}n) \overset{Prop. C.0.11}{=}$$

$$= \sum_{n\in\mathbb{Z}} \hat{f}(\sqrt{u}n) \overset{(C.0.2)}{=}$$

$$= \frac{1}{\sqrt{u}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/u} =$$

$$= \frac{\theta(1/u)}{\sqrt{u}}$$

[39] □

D. Lemma for Theorem 3.1.12

Definition D.0.14 (ψ-function):

Let $\psi(x)$ be the logarithmic derivative of the Gamma function.

$$\psi(x) = \frac{\Gamma'(x)}{\Gamma(x)}$$

Definition D.0.15:

$$\psi_\zeta(s) := \frac{1}{2}\psi\left(\frac{s}{2}\right) - \frac{n \log \pi}{2}$$

Definition D.0.16:

$$\psi_L(s) := \frac{\alpha}{2}\psi\left(\frac{s}{2}\right) + \frac{\beta}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n \log \pi}{2}$$

with $\beta = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{otherwise} \end{cases}$ and $\alpha = 1 - \beta$.

Definition D.0.17 (Mangoldt function):

$$\Lambda(x) = \begin{cases} \log p & \text{for } n = p^k \\ 0 & \text{else} \end{cases}$$

Lemma D.0.18:

$$\frac{\zeta'(s)}{\zeta(s)} = B + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) - \frac{1}{s} - \frac{1}{s-1} - \psi_{\zeta}(s)$$

Lemma D.0.19:

$$\frac{L'(s)}{L(s)} = B_{\chi} + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) - \frac{1}{2} A_{\chi} - \psi_L(s)$$

In both Lemma, ρ denotes a nontrivial zero of either $\zeta(s)$ or $L(s,\chi)$. B, B_{χ} and A_{χ} are constants. $B = -\sum_{\rho} Re\left(\frac{1}{\rho}\right) = \frac{1}{2}\log(4\pi) - 1 - \frac{\gamma}{2} = -0.02309...$ $(\gamma = 0.57732...)$.

Lemma D.0.20:

Assume the *GRH*.
Let χ be a nonprincipal character on $\mathbb{Z}_D^*$ and $\chi(x) = 1$ for all $n < x$.
For $0 < a < 1$

$$\frac{\sqrt{n}}{(a+1)^2} \leq \frac{1}{2a+1} \cdot (1 + r(n)) \cdot (\log(D) + t(n)) + s(n)$$

with

$$r(n) = \frac{(a+2) \cdot \log n + 1}{n^{a+1/2}}$$

$$s(n) = \frac{5/2 \cdot \log n + 1}{n^{a+1/2}} + \frac{\beta}{(a-2)^2 \cdot n^{5/2}}$$

$$t(n) = -\log \pi + \psi\left(\frac{a+\beta+1}{2}\right) + (2a+1) \cdot (\gamma + 2 - \log(4\pi)) + 2\frac{\zeta'}{\zeta}(1+a) + 4\sum_{x \geq n} \frac{\Lambda(x)}{x^{1+a}}$$

$$\beta = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{otherwise} \end{cases}$$

Outline of the proof for Lemma D.0.20. The inequality in D.0.20 starts off with a more easy to prove equality that does not assume the *Generalized Riemann Hypothesis*:

$$\frac{n}{(a+1)^2} = \sum_{\rho} \pm n^{\rho}(\rho+a)^2 + I_0 + I_- + \sum_{x<n} \Lambda(x)(1-\chi(x)) \left(\frac{x}{n}\right)^a \log\left(\frac{n}{x}\right) \quad \text{(D.0.1)}$$

In the first sum of (D.0.1), there is a plus if ρ is a primitive root of $\zeta(s)$ and minus if it is a primitive root of $L(s,\chi)$. The exact value of I_- is not important and it can be estimated very easily and without assuming the *Generalized Riemann Hypothesis.*

$$I_- \leq \frac{\beta}{(a-2)^2 n^2} \quad \text{(D.0.2)}$$

I_0 needs a little more attention than I_-:

$$I_0 = (\beta-1)\frac{1}{a^2} + \frac{\log n}{n^a}\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(-a) + \frac{1}{n^a}\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)'(-a) - \frac{\beta}{n(a-1)^2}$$

Estimating I_0 involves the *GRH.*

If $\beta = 0$ then

$$I_0 = -\frac{1}{a^2} + \frac{\log n}{an^a} + \frac{1}{a^2 n^a} + \frac{\log n}{n^a}\left(\sum_{\rho} \pm \left(\frac{1}{-a-\rho} - \frac{1}{2-\rho}\right) + \right.$$
$$\left.\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(2) + \frac{3}{2}\right) + \frac{1}{n^a}\left(\sum_{\rho} \mp \frac{1}{(\rho+a)^2} + \frac{1}{(a+1)^2}\right)$$

The next step involves using definitions and rearanging terms, so it is rather easy.

Now the part where the *Generalized Riemann Hypothesis* comes into play:

$$\left|\sum_{\rho} \pm \left(\frac{1}{-a-\rho} - \frac{1}{2-\rho}\right)\right| \leq \sum_{\rho} \left|\frac{1}{a+\rho} + \frac{1}{2-\rho}\right| \leq$$
$$\sum_{\rho} \frac{2+a}{|(\rho+a)(\rho-2)|} \leq \sum_{\rho} \frac{2+a}{|\rho+a|^2}$$

An estimation for the second sum is similar. For $\beta = 1$ it involves estimations on $\psi(x)$. It follows that

$$I_0 \leq \frac{\log n}{n^a} \left(\sum_{\rho} \frac{2+a}{|\rho+a|^2} + \frac{5}{2}\right) + \frac{1}{n^a} \left(\sum_{\rho} \frac{1}{|\rho+a|^2} + 1\right) \tag{D.0.3}$$

Probably the most crucial step is the next one:
Assuming the *GRH*

$$\begin{aligned} &\sum_{\rho} \frac{1}{|\rho+a|^2} = \sum_{\rho} \left(\frac{1}{2a+1} \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right)\right) \leq \\ &\frac{1}{2a+1} \left(\log \frac{D}{\pi^2} + 2\left(\frac{1}{a} + \frac{1}{a+1}\right) + \psi\left(\frac{a+1}{2}\right) + \right. \\ &\quad \left. \psi\left(\frac{a+\beta+1}{2}\right) + 2\frac{\zeta'}{\zeta}(1+a) + 2Re\frac{L'}{L}(1+a)\right) \end{aligned} \tag{D.0.4}$$

The equality is true if $Re(\rho) = \frac{1}{2}$.
Theorem 3.1.12 follows with using (D.0.1) and the estimations for I_- and I_0 and (D.0.4). □

[5][22][23]
A full proof can be found in [5].

The atomic number of gold is 79.

E. The distribution of prime numbers

E.1. The prime number theorem

While it is of great interest to assign numbers into two groups, primes and composites, lately, finding patterns in the distribution of prime numbers has grown in significance.

Definition E.1.1:

Let $x \in \mathbb{R}$ with $x > 0$ and the function

$$\pi(x) = |\{p|p \in \mathbb{P}, 1 < p \leq x\}|$$

Then $\pi(x)$ denotes the number of primes less or equal than x.

The idea is to find functions that behave approximately like $\pi(x)$. It should be easy to do calculations with those functions.

In 1793, *Carl Friedrich Gauss* conjectured that $\pi(x)$ behaves approximately like $\frac{x}{ln(x)}$ for large values of x. About 100 years later, two independent proofs were found.

Theorem E.1.2 (Prime Number Theorem):

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

[41]

Even though the *Prime Number Theorem* is the most famous one for approximating $\pi(x)$, there are others, too.

Theorem E.1.3:

$$\pi(x) \sim Li(x) = \int_{2}^{x} \frac{dt}{log(t)}$$

$Li(x)$ is called the *Eulerian Logarithmic Integral Funtion.*[30] The following table compares $\pi(x)$ with two of its approximations: $\frac{x}{ln(x)}$ and $Li(x)$. $\frac{x}{ln(x)}$ and $Li(x)$ have been rounded to its nearest integer.

x	$\pi(x)$	$\frac{x}{ln(x)}$	$Li(x)$
10^1	7	4	5
10^2	25	22	29
10^3	168	145	177
10^4	1229	1086	1245
10^5	9592	8686	9629
10^6	78498	72382	78627
10^7	664579	620421	664917
10^8	5761455	5428681	5762208

List of Symbols

$\mathbb{N}$	the natural numbers including 0
$\mathbb{N}^+$	the natural numbers not including 0
$\mathbb{Z}$	the integer numbers
$\mathbb{R}$	the real numbers
$\mathbb{C}$	the complex numbers
$\mathbb{P}$	the prime numbers
$\mathbb{Z}_n$	the ring of residue classes modulo n
$\mathbb{Z}_n^*$	$\{a \in \mathbb{Z}_n \mid (a,n) = 1\}$
$Re(s)$	the real part of a complex number
$x \equiv y \pmod{n}$	$x = y + nk$ with $k \in \mathbb{Z}$
(x, y)	the greatest common divisor of x and y
$lcm(x, y)$	the least common multiple of x and y
$x!$	$x! = \prod_{k=1}^{x} k$
$\lvert A \rvert$	the number of elements in the set A
$\lceil x \rceil$	the smallest $n \in \mathbb{Z}$ with $n \geq x$
$\lfloor x \rfloor$	the largest $n \in \mathbb{Z}$ with $n \leq x$
$[x]$	the integer part of x
$\{x\}$	the fractional part of x
$\binom{n}{k}$	$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$
$ker(f)$	$ker(f) = \{x \mid f(x) = 0\}$

Barney Stinson’s made-up statistics always include the number 83.

Bibliography

[1] M. Abramowitz and I. A. Stegun. *Handbook of mathematical functions.* Dover, New York, 1965.

[2] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. *PRIMES is in P.* Annals of Mathematics 160, pages 781-793, Kanpur, India, 2004.

[3] W R Alford, Andrew Granville, and Carl Pomerance. *There are infinitely many Carmichael numbers.* Annals of Mathematics 139, pages 703-722, 1994.

[4] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer, 1997.

[5] Eric Bach. *Explicit bounds for primality testing and related problems.* Mathematics of computation Volume 55, Number 191, pages 355-380, 1990.

[6] M. W. Baldoni, C. Ciliberto, and G. M. Piacentini Cattaneo. *Elementary Number Theory, Cryptography and Codes.* Springer, 2009.

[7] E. Bombiere. *Problems of the Millenium: The Riemann Hypothesis.* Institute for Advanced Study, Princeton `http://www.claymath.org/sites/default/files/official_problem_description.pdf`. [last visit 2018-05-09].

[8] Oliver Braun and Sebastian Schönnenbeck. *Der AKS-Primzahltest.* `http://www.math.rwth-aachen.de/~Gabriele.Nebe/Vorl/pros/AKS.pdf`, 2009.

[9] Keith Conrad. *The Solovay-Strassen Test.* `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/solovaystrassen.pdf`, 2016.

[10] Keith Conrad. *The Miller-Rabin Test.* `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/millerrabin.pdf`, 2017.

[11] Stephen Cook. *The P vs NP problem.* Institute for Advanced Study, Princeton `https://www.claymath.org/sites/default/files/pvsnp.pdf`. [last visit 2018-05-09].

[12] C Cooper, G Woltman, Kurowski S, A Blosser, and et al. *GIMPS Project Discovers Largest Known Prime Number.* `https://www.mersenne.org/primes/press/M77232917.html`. [last visit 2018-05-09].

[13] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Stein Clifford. *Introduction to Algorithms.* The MIT Press, 3 edition, 2009.

[14] Richard Crandall and Carl Pomerance. *Prime Numbers A Computational Perspective.* Springer, 2 edition, 2005.

[15] Volker Diekert, Manfred Kufleitner, and Gerhard Rosenberger. *Diskrete algebraische Methoden.* De Gruyter Studium, 2013.

[16] Martin Dietzfelbinger. *Primality Testing in Polynomial Time.* Springer, 2004.

[17] Euclid. *Elements.* `https://mathcs.clarku.edu/~djoyce/java/elements/toc.html`, circa 300 BC. [last visit 2017-05-03].

[18] Otto Forster. *Algorithmische Zahlentheorie.* vieweg, 1996.

[19] E. Fouvry. *Theoreme de Brun-Titchmarsh; application au theoreme de Fermat.* Invent. Math. 79, pages 383-407, 1985.

[20] Alexander O. Gogolin, Elena G. Tsitsishvili, and Andreas Komnik. *Lectures on Complex Integration, Hypergeometric Series with Applications, pages 63-111.* Undergraduate Lecture Notes in Physics, 2013.

[21] Neeraj Kayal and Nitin Saxena. *Towards a deterministic polynomial time test.* IIT Kanpur `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.9281&rep=rep1&type=pdf`, 2002.

[22] Elena A. Kudryavtseva, Saidak Filip, and Zvengrowski Peter. *Riemann and his zeta function.* Morfismos, Volume 9, Number 2, pages 1-48, 2005.

[23] Youness Lamzouri, Xiannan Li, and Kannan Soundararanjan. *Conditional bounds for the least quadratic non-residue and related problems.* Mathematics of Computation, Volume 84, Number 295, pages 2391-2412, 2015.

[24] H. W. Lenstra jr. and Carl Pomerance. *Primality testing with Gaussian periods.* `https://www.math.dartmouth.edu/~carlp/aks080709.pdf`, 2009.

[25] Ben Lynn. *The Chinese Remainder Theorem.* `https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html`. [last visit 2017-05-09].

[26] Gary L. Miller. *Riemann's Hypothesis and Tests for Primality.* Journal of Computer and System Sciences Volume 13, Number 3, pages 300-317, 1976.

[27] M. Nair. *On Chebyshev-Type Inequalities for Primes.* The American Mathematical Monthly Volume 89, pages 126-129, 1982.

[28] W. Narkiwics. *The Development of Prime Number Theory.* Springer, 2010.

[29] J J O'Connor and E F Robertson. *Prime numbers.* `http://www-history.mcs.st-andrews.ac.uk/HistTopics/Prime_numbers.html`, 2009. [last visit 2016-03-22].

[30] Oystein Ore. *Number theory and its history.* McGraw-Hill Book Company, Inc., 1948.

[31] Carl Pomerance, Selfridge J. L., and Samuel S. Wagstraff Jr. *The Preudoprimes to* $25 \cdot 10^9$. Mathematics of Computation Volume 35 Number 151, pages 1003-1026, 1980.

[32] Michael O. Rabin. *Probabilistic Algorithm for Testing Primality.* Journal of Number Theory Volume 123, pages 128-138, 1980.

[33] Lasse Rempe-Gillen and Rebecca Waldecker. *Primality Testing for Beginners.* American Mathematical Society, 2014.

[34] Lasse Rempe-Gillen and Rebecca Waldecker. *Primzahltests für Einsteiger.* Springer, 2 edition, 2016.

[35] Paolo Ribenboim. *The Litte Book of Bigger Primes.* Springer, 2 edition, 2004.

[36] Paulo Ribenboim. *Die Welt der Primzahlen.* Springer, 2 edition, 2011.

[37] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie.* Springer, 2007.

[38] René Schoof. *Four primality testing algorithms.* Cambridge University Press, `https://arxiv.org/pdf/0801.3840.pdf`, 2004.

[39] Andreas Steiger. *Riemann's second proof of the analytic continuation of the Riemann Zeta function.* https://www2.math.ethz.ch/education/bachelor/seminars/ws0607/modular-forms/Riemanns_second_proof.pdf, 2006.

[40] Jörn Steuding. *An Introduction to the Theory of L-functions.* http://www.mathematik.uni-wuerzburg.de/~steuding/seminario0.pdf, 2005.

[41] James K Strayer. *Elementary Number Theory.* Waveland Press, 2002.

[42] Gérald Tenenbaum and Michel Mendès France. *The Prime Numbers and Their Distribution.* American Mathematical Society, 2001.

[43] E. C. Titchmarsh. *The Theory of the Riemann zeta-function.* Clarendon Press, Oxford, 2 edition, 1986.

[44] A. Walther. *Anschauliches zur Riemann Zetafunktion.* Acta Math. 48, pages 393-400, 1926.

[45] A. E. Western and Miller J. C. P. *Tables of indices and primitive roots.* Royal Society, Cambridge, 1968.