Department of Computer Science
Faculty of Mathematics, Physics and Informatics
Comenius University, Bratislava

Agrawal's Conjecture and Carmichael Numbers

(student scientific conference)

Tomáš Váňa

advisor:
RNDr.Martin Mačaj, PhD.

Bratislava, 2009

I hereby declare that I wrote this text myself with the help of the referenced literature, under the supervision of my advisor.

.....

Contents

Chapter 1

Introduction

The main interest and high level view of our story will be the prime numbers and recognizing them from composites. This problem was formulated by ancient mathematicians long before there were any notions like time complexity or any practical need of testing large numbers for primality like we know it nowadays in cryptography. Like many problems in number theory, it remained unsolved for hundreds of years, until quite recently there were some significant breakthroughs in this area.

First revolutionary invention were the probabilistic primality tests, which are very fast algorithms based on simple ideas like Fermat's little theorem. These tests are polynomial in respect to the length of the input (i.e. they are polylogarithmic in respect to the input), and give a quite precise result. Of course, if everything you expect as an output of the algorithm is the answer *yes* or *no*, it may seem odd to speak about quite precise result. What this actually means is that the algorithm itself may give a wrong result, but when repeated a few times, the probability of this happening is such small that for *industrial* purposes (e.g. generating primes for cryptography keys), we can use them without worrying too much.

Of course for mathematicians, any probability that the result might be wrong, however small, still makes the solution unsatisfactory. In this text we will speak more about another breakthrough, which was to fill the gap of uncertainty and to construct an algorithm without this small error probability flaw. Anyway, if the reader is interested in the probabilistic algorithms for primality testing, our previous text [11] gives a comprehensive walkthrough of the most ideas used there and also shows some examples of tests based on Riemann hypothesis (another way of trade off which was used

before we had a final solution for the primality test).

In our text we will first have a look at the deterministic AKS test discovered by Indian mathematicians quite recently, after presenting it briefly, we will state some of our related results. We will ask ourselves a question about the choice of parameters made in the test and when can this choice lead to difficulties. To deal with this problem, we will try a combinatoric approach of using binomial theorem and some familiar tricks for manipulating the sums, as an alternative to the algebraic approach using Chineser remainder theorem. In both ways we will prove an interesting result showing that for some choices of parameters the Carmichael numbers are making the same troubles as in other tests

Later we will present some results of our research of the Agrawal's conjecture, a hypothesis stated in the article about the AKS test which might provide a significant speed-up of the algorithm. We will analyze some special cases of the conjecture and develop an algorithm for calculating parameters that can be used to test its validity in a faster way. Along with this algorithm, we will provide an alternative proof for the theorem proposed by Lenstra and Pomerance, which suggest that there is a way to find the counterexample to the conjecture.

We will conclude our story with a set of experimental results which we have collected using the theoretical results from the text and some available records of numbers with special properties, e.g. Carmichael numbers and pseudoprimes. We hope this text presents our ideas and objectives clearly and will be a pleasant tour to make for the reader, possibly inspiring him to a further study of the presented topics or helping with the research.

Chapter 2

AKS & Carmichael numbers

The important step in the development of primality tests was to deliver an algorithm, which would be deterministic (i.e. its result will be guaranteed to be true) and fast enough. When speaking about fast enough, we have once again in mind the polylogarithmic time complexity. Such an algorithm was found in the year 2002 by Indian mathematicians Agrawal, Kayal and Saxena and is called by their names, AKS test. The core idea of the test is the following congruence.

Lemma 2.1 *Let n be an integer, then for all integers a, for which $(a, n) = 1$, the following congruence*

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

holds iff n is prime.

Proof Using the binomial theorem, we can expand the left side of the congruence to a well-known sum

$$(x + a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

We are especially interested in the first and the last member of the expansion, as they are the same degrees as we have on the right side of our congruence. Therefore let us write

$$(x + a)^n = x^n + \sum_{0<k<n} \binom{n}{k} x^k a^{n-k} + a^n$$

Now let us first assume that n is prime. Then we have $a^n \equiv a \pmod{n}$ by Fermat's little theorem, and all we have to show is that the sum in the middle is congruent to zero. This is done quite easily – we just have to realize that the binomial coefficient $\binom{n}{k}$ can be written as $\frac{n^{\underline{k}}}{k!}$, where $n^{\underline{k}} = n \cdot (n-1) \cdots (n-k+1)$. The numerator of this fraction is obviously divisible by n. However, because n is prime, there is no other number which would divide n and be less than n (except for 1 of course, but this is irrelevant). Therefore, there is nothing in the denominator that would cancel out the prime n and the whole number is divisible by n. This means all the terms of the sum are divisible by n and the sum itself is congruent to zero, so we are done. Now let us assume that n is not a prime number and let us take any of its prime divisors p. We will take a look just at the coefficient

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

If the p^α is the highest power of p that divides n, then the numerator is divisible by p^α (only the factor n is divisible by p) and the denominator is divisible by the first power of p (the factor p). Therefore, the whole fraction is divisible only by $p^{\alpha-1}$ and cannot be divisible by n, also the coefficient a^{n-p} which gets multiplied by it won't help, as $(a, p) = 1$. This is just one example of a term from the sum that will not disappear when taken modulo n, which means the congruence cannot hold in this case and we are done with the whole proof. ■

All the primality tests work with some condition that is necessary for primality, but usually checking any condition that is sufficient at the same time, is simply too much time-expensive. What we have in the previous lemma, is such a condition and even this is not an exception – it is a sufficient condition for primality but testing it requires to calculate a polynomial of enormous size, which makes it even slower and more memory consuming than the naive trial division test. If we would stop here, it would be just a curiosity like Wilson's theorem (see [11] or [4]).

The idea that makes the difference is to take the congruence and reduce it modulo some polynomial of a small degree, namely $x^r - 1$, where r is of polylogarithmic size. Because we have already shown that the congruence holds for primes, reducing it further can't break this property and it is still true that

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

for prime n. However, reducing it can cause the opposite effect – the new congruence can hold for some composite n as well. Taking the simplest example of $r = 1$, we have reduced our test to the Fermat's test (see [11]), which is known to be not sufficient for ensuring the primality.

Our goal is therefore to choose r and a in such a way that we gain speed, but don't lose the equivalence with primality condition. Authors of the test have shown that there is indeed a way to choose those parameters that makes it fast and still keep the other direction of the equivalence holding, at least to some extent. We will state their algorithm here, the proof and time-complexity analysis can be found in the original article [8].

Algorithm 1 AKS

- check whether n is a perfect power (i.e. for some $a, b > 1 : n = a^b$)
- find the smallest r such that $o_r(n) > \lg^2 n$
- perform a trial division for n up to r
- check the congruence (2.2) for $a \in \{1, \ldots, \lfloor \sqrt{\varphi(r)} \lg n \rfloor\}$ and r

For simplicity, we will in the following text refer to the congruence (2.2) as $T(a, n, r)$. Instead of presenting the proof, we will now have a look at some aspects of the way to choose the parameters. We have said that putting $r = 1$ reduces testing of the congruence to the Fermat's test. Authors have shown that choosing r in such a way that $o_r(n) > \lg^2 n$ seems to be enough when combined with a suitable set of a's. The question we want to ask is whether there are some choices of r which are so bad that there is no set of a's that would help to distinguish composites from primes. In case of the Fermat's test it is well-known that there are numbers called Carmichael numbers which have exactly this property.

Definition 2.1 *Let n be a composite integer. If for any integer a is true that $a^n \equiv a \pmod{n}$, we call the n a Carmichael number.*

In the next lemma we will show that AKS test is not worse than Fermat's test for any choice of r. What we mean by that is that if it fails for some number n and all choices of a's, then this number n has to be Carmichael.

Lemma 2.2 *Let n and r be some fixed integers and suppose $T(a, n, r)$ holds for any choice of a. Then $a^n \equiv a \pmod{n}$ for all integer a as well.*

As a first step, we have to realize that when

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

holds, then it has to be true that

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

as $x - 1$ is a divisor of the polynomial $x^r - 1$ for any r (it is true that $x^r - 1 = (x-1)(x^{r-1} + \ldots + 1)$). However, this means that for any a we have

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

(we have used the fact $x \equiv 1 \pmod{x - 1}$) and therefore $(1 + a)^n \equiv 1 + a \pmod{n}$. However, this is just a shifted way of saying exactly what we are proving, therefore we are done. ■

Now that we know that when searching for numbers that would fool our test we are only dealing with Carmichael numbers, we should first have a better look at them. Actually, there is a criterion for recognizing Carmichael numbers, the proof can be found for example in our previous text [11].

Theorem 2.1 (Korselt's criterion) *Let n be an odd integer. Then n is a Carmichael number if and only if*

a) *It is square-free, i.e. not divisible by any square of a prime number.*

b) *For each of its prime divisors p it is true that $p - 1 \mid n - 1$.*

Korselt's criterion represents a very suitable way of recognizing Carmichael numbers, provided that we have the prime factorization. The next step to answer our question is to ask whether there are choices of r which make the testing of the congruence $T(a, n, r)$ fail for Carmichael numbers and all choices of a. Now that we know what exactly it means to be a Carmichael number we can proceed with the following result giving us the answer. We will start with the combinatoric approach, in order to dig deeper into the structure of the polynomial powers in our congruence, and later we will show the same with a standard algebraic approach, just to see the difference between the methods.

Theorem 2.2 *Let n be a Carmichael number, i.e. let $a^n \equiv a \pmod{n}$ hold for all integers a. So far we know that n is a product of (at least three) distinct primes. Let $n = \prod_{i=1}^{k} p_i$ and $r \mid (p_1 - 1, p_2 - 1, \ldots, p_k - 1)$. Then $T(a, n, r)$ holds for any integer a.*

We will need two lemmas before coming to the proof.

Lemma 2.3 *Let $p = rs + 1$ be a prime number and let g be a generator of the cyclic group Z_p^*. Then for any integer k it is true that*

$$\sum_{i=0}^{r-1} g^{isk} \equiv \begin{cases} r \pmod{p} & \text{when } g^{sk} \equiv 1 \pmod{p} \\ 0 \pmod{p} & \text{when } g^{sk} \not\equiv 1 \pmod{p} \end{cases}$$

Proof In case of $g^{sk} \equiv 1 \pmod{p}$ every summand is 1 modulo p, so it is not hard to see that the sum of r such numbers is exactly r. Let us have a look at the sum in the second case and let us denote its value by S. We have

$$g^{sk} \cdot S \equiv \sum_{i=0}^{r-1} g^{(i+1)sk} = S - g^0 + g^{rsk} \pmod{p}$$

Because $rs = p - 1$, we have $g^{rsk} \equiv g^0 = 1 \pmod{p}$, and therefore

$$g^{sk} \cdot S \equiv S \pmod{p}$$

Another manipulation gives us

$$S(g^{sk} - 1) \equiv 0 \pmod{p}$$

and from the assumption we know that the second factor is not zero, which means p has to divide the first one, i.e. $S \equiv 0 \pmod{p}$, which is the fact we wanted to prove. ■

Lemma 2.4 *Let $n = rq + 1$ be a Carmichael number and let $p = rs + 1$ be a prime number for which $p \mid n$. Then for any integers a and t it is true that*

$$\sum_{\substack{0 \le j \le n \\ j \equiv t \pmod{r}}} \binom{n}{j} a^j \equiv \begin{cases} 1 \pmod{p} & \text{when } t \equiv 0 \pmod{r} \\ a \pmod{p} & \text{when } t \equiv 1 \pmod{r} \\ 0 \pmod{p} & \text{when } t \not\equiv 0, 1 \pmod{r} \end{cases}$$

Proof Let g be a generator of the cyclic group Z_p^*. Let us have a look at the following sum

$$S_1 = \sum_{i=0}^{r-1} (g^{si} + a)^n \cdot g^{si(t-1)}$$

According to the binomial theorem we get

$$S_1 = \sum_{i=0}^{r-1} g^{si(t-1)} \sum_{j=0}^{n} \binom{n}{j} a^j \cdot g^{si(n-j)} = \sum_{i=0}^{r-1} \sum_{j=0}^{n} \binom{n}{j} a^j \cdot g^{si(n-j+t-1)}$$

Changing the order of the summation we further have

$$S_1 = \sum_{j=0}^{n} \sum_{i=0}^{r-1} \binom{n}{j} a^j \cdot g^{si(n-j+t-1)} = \sum_{j=0}^{n} \binom{n}{j} a^j \sum_{i=0}^{r-1} g^{si(n-j+t-1)}$$

Now we are going to use the lemma 2.3 to calculate the inner sum. Going from there this sum is always zero modulo p, except for the case when $g^{s(n-j+t-1)} \equiv 1 \pmod{p}$. Because g is a generator of the group Z_p^*, this condition is equivalent to the fact that $p - 1 \mid s(n - j + t - 1)$, therefore $rs \mid s(rq + 1 - j + t - 1)$, or $r \mid t - j$, in other words that $j \equiv t \pmod{r}$. In this case the value of the sum, according to the lemma 2.3, is exactly r, which means we have

$$S_1 \equiv r \cdot \sum_{\substack{0 \le j \le n \\ j \equiv t \pmod{r}}} \binom{n}{j} a^j \pmod{p}$$

Now let us start with the original sum S_1 and follow a different path of manipulations. We will use the fact that n is a Carmichael number, which means that $(g^{si} + a)^n \equiv g^{si} + a \pmod{n}$, and because $p \mid n$ this also implies that $(g^{si} + a)^n \equiv g^{si} + a \pmod{p}$. Therefore

$$S_1 \equiv \sum_{i=0}^{r-1} (g^{si} + a) \cdot g^{si(t-1)} \pmod{p}$$

and

$$S_1 \equiv \sum_{i=0}^{r-1} g^{sit} + a \cdot \sum_{i=0}^{r-1} g^{si(t-1)} \pmod{p}$$

Now let us use the lemma 2.3 once again to calculate the value of both sums. The first one is always zero, except for the case when $g^{st} \equiv 1 \pmod{p}$, i.e. $p-1 \mid st$, or $rs \mid st$, or $r \mid t$, having value r in that case. The second sum is always zero, except for the case when $g^{s(t-1)} \equiv 1 \pmod{p}$, i.e. $p-1 \mid s(t-1)$, or $rs \mid s(t-1)$, or $t \equiv 1 \pmod{r}$, having value r in that case. Summing up what we have learned so far we have

$$S_1 \equiv \begin{cases} r & \pmod{p} \quad \text{when } t \equiv 0 \pmod{r} \\ ra & \pmod{p} \quad \text{when } t \equiv 1 \pmod{r} \\ 0 & \pmod{p} \quad \text{when } t \not\equiv 0, 1 \pmod{r} \end{cases}$$

Now let us call

$$S_2 = \sum_{\substack{0 \le j \le n \\ j \equiv t \pmod{r}}} \binom{n}{j} a^j$$

We have shown that $S_1 \equiv r \cdot S_2 \pmod{p}$ holds, which means we have

$$r \cdot S_2 \equiv \begin{cases} r & \pmod{p} \quad \text{when } t \equiv 0 \pmod{r} \\ ra & \pmod{p} \quad \text{when } t \equiv 1 \pmod{r} \\ 0 & \pmod{p} \quad \text{when } t \not\equiv 0, 1 \pmod{r} \end{cases}$$

The last step is to cancel out the number r in all the congruences (as $p = rs + 1$, the numbers p and r have to be relatively prime). This gives us the relationship we wanted to prove and we are done. ■

Now we are ready to prove the theorem 2.2. Apart from the fact that n is a product of distinct prime numbers, the Korselt's criterion is telling us that for all of these prime numbers it is true that $p_i - 1 \mid n - 1$. Because r is a common divisor of all terms $p_i - 1$, it has to be true that $r \mid n - 1$ as well. Let us therefore (for a suitable integer q) write $n = rq + 1$. By expanding the left side of the congruence we are proving according to the binomial theorem we get

$$\sum_{i=0}^{n} \binom{n}{i} a^i x^{n-i} \equiv x^n + a \pmod{x^r - 1, n}$$

Now, realizing that $x^r \equiv 1 \pmod{x^r - 1}$, we see that $x^i \equiv x^{i \bmod r} \pmod{x^r - 1}$ for all non-negative exponents i. Let us denote the sum on the left side of the congruence by S_0 and using this fact rewrite it in the following

way :

$$S_0 \equiv \sum_{z=0}^{r-1} \left(x^z \cdot \sum_{\substack{0 \leq j \leq n \\ j \equiv n-z \pmod r}} \binom{n}{j} a^j \right) \pmod{x^r - 1, n}$$

Let us now consider any prime number p_i, for which according to the assumption $r \mid p_i - 1$, so there is a suitable s_i so that we can write $p_i = rs_i + 1$. Using the lemma 2.4 we get that

$$\sum_{\substack{0 \leq j \leq n \\ j \equiv n-z \pmod r}} \binom{n}{j} a^j \equiv \begin{cases} 1 \pmod{p_i} & \text{when } n - z \equiv 0 \pmod r \\ a \pmod{p_i} & \text{when } n - z \equiv 1 \pmod r \\ 0 \pmod{p_i} & \text{when } n - z \not\equiv 0, 1 \pmod r \end{cases}$$

Using the fact that $n \equiv 1 \pmod r$ we can easily rewrite that to the form

$$\sum_{\substack{0 \leq j \leq n \\ j \equiv n-z \pmod r}} \binom{n}{j} a^j \equiv \begin{cases} 1 \pmod{p_i} & \text{when } z \equiv 1 \pmod r \\ a \pmod{p_i} & \text{when } z \equiv 0 \pmod r \\ 0 \pmod{p_i} & \text{when } z \not\equiv 0, 1 \pmod r \end{cases}$$

Additionally, as these congruences hold modulo any prime divisor p_i of the number n, they have to hold modulo n as well, namely because n is a product of these distinct primes. This gives us

$$\sum_{\substack{0 \leq j \leq n \\ j \equiv n-z \pmod r}} \binom{n}{j} a^j \equiv \begin{cases} 1 \pmod{n} & \text{when } z \equiv 1 \pmod r \\ a \pmod{n} & \text{when } z \equiv 0 \pmod r \\ 0 \pmod{n} & \text{when } z \not\equiv 0, 1 \pmod r \end{cases}$$

Using this relationship we can easily calculate the value of the sum S_0, we have $S_0 \equiv a + x \pmod{x^r - 1, n}$. To conclude the proof, it is enough to realize that it is true that $x^n \equiv x \pmod{x^r - 1}$, as $n \equiv 1 \pmod r$. Therefore we also have

$$S_0 \equiv a + x^n \pmod{x^r - 1, n}$$

which is already the congruence we wanted to prove in the first place. ■

In addition to the combinatoric proof that we have provided we will now prove the theorem 2.2 in an alternative way, using the Chinese remainder theorem for polynomials. Once again we will start from the fact that $r \mid p_i - 1$

for any prime number p_i and we will show that if we look at the congruence $T(a,n,r)$ modulo p_i, it is true. Knowing that n is a product of distinct primes this is enough to show that $T(a,n,r)$ holds also in the original form, i.e. modulo n.

As a first step, we realize that from $r \mid p_i-1$ we know that $x^r-1 \mid x^{p_i-1}-1$. Namely, for a suitable integer s it has to be true that $p_i = rs+1$, which means $x^{p_i-1}-1 = x^{rs}-1 = (x^r-1)(x^{(s-1)r}+x^{(s-2)r}+\ldots+1)$. Moreover, we have $x^{p_i-1}-1 \mid x^{p_i}-x$ and we know that Z_{p_i} is the splitting field of the polynomial $x^{p_i}-x$. This is implied by the fact that according to the little Fermat's theorem, each member of this field is a root of the polynomial $x^{p_i}-x$ and therefore we can write this polynomial over this field as a product of factors $x^{p_i}-x \equiv x\cdot(x-1)\cdots(x-p_i+1) \pmod{p_i}$. Because the polynomial x^r-1 is its divisor, there has to be a way of writing it analogically as a product of some of these factors (it would be r of them obviously), i.e. $x^r-1 \equiv (x-a_1)\cdots(x-a_r) \pmod{p_i}$, where $a_1,\ldots,a_r$ are distinct members of $Z^*_{p_i}$. Now having the fact that all the polynomials $x-a_j$ are relatively prime we can use the Chinese remainder theorem to simplify our dealing with the congruence $T(a,n,r)$. If we are lucky enough to show that for all $j \in \{1,\ldots,r\}$ it is true that $(x+a)^n \equiv x^n+a \pmod{x-a_j,p_i}$, then knowing that x^r-1 is a product of these relatively prime polynomials and using the Chinese remainder theorem we get $(x-1)^n \equiv x^n-1 \pmod{x^r-1,p_i}$ as well. This would be, according to what has been said so far, enough to show that $T(a,n,r)$ holds for any a. Fortunately, dealing with the congruence modulo $x-a_j$ is very simple, as we have $x \equiv a_j \pmod{x-a_j}$ which effectively means we can substitute a_j for x, getting an equivalent congruence $(a_j-a)^n \equiv a_j^n-a \pmod{p_i}$. From the fact that n is a Carmichael number we immediately have $(a_j-a)^n \equiv a_j^n-a \pmod{n}$, which is even more than we need, as $p_i \mid n$. This means we are done with the proof. ■

We have demonstrated that there are choices of r such that testing the congruence (2.2) can fail for all choices of a. This shows that there are some limitations needed on the parameter r and although the condition $o_r(n) > \lg^2 n$ might not be the tightest and there is still a place for improvements, there is a good reason to limit the r in this way (apart from the fact that it was needed for the proof). More importantly, we have shown an interesting example of two different points of view when dealing with the congruence $T(a,n,r)$. The algebraic approach turned out to be simpler, on the other side by using the sum approach we have gained more insight into

what is happening when we are calculating powers of polynomials. In the next chapters, we will have a look at the conjecture that can lead to a rapid speed-up of the AKS algorithm.

Chapter 3

Agrawal's conjecture

The key idea of the AKS algorithm is to test whether the congruence (2.2) holds for suitable a,r and chosen n. In the article [1], prior to the definitive formulation of the AKS test, proof of its membership in the polynomial algorithms class and final presentation, the authors of the algorithm have dealt with the special case $a = -1$ and proved some connections between primality testing using the congruence $T(-1, n, r)$ and some other probabilistic tests. They have also stated some conjectures, amongst them was the following remarkable statement.

Conjecture 3.1 (Agrawal) *Let n,r be relatively prime integers, for which $T(-1, n, r)$ holds. Then either n is prime, or $n^2 \equiv 1 \pmod{r}$ has to hold.*

If this conjecture were true, it would lead to a different way of finding the polynomial algorithm for primality testing, in principle much easier, even before the AKS test was discovered. However, it wasn't so easy and the authors did not come to any conclusion, neither have they proved nor disproved the conjecture. The initial idea that the conjecture may hold at all came from the experimental searches in the range $n < 10^{10}$, $r < 100$. Later they have found a different way of ensuring that the testing of congruence $T(a, n, r)$ would be an equivalent condition for primality (as presented in the previous chapter). The question of whether the conjecture is true or not still remains interesting though, as if true, the AKS test would become even simpler and faster than its current version.

The scientific community in the area of the number theory researched this problem and formulated several notes to the conjecture, most interesting

being the following theorem, which provides a heuristic way to look for the counterexample for the Agrawal's conjecture.

Theorem 3.1 (Lenstra, Pomerance) *Let $p_1, \ldots, p_k$ be distinct prime numbers and let $n = p_1 \cdots p_k$. If the following conditions hold*

a) $k \equiv 1 \pmod 4$ *or* $k \equiv 3 \pmod 4$

b) $p_i \equiv 3 \pmod{80}$ *for* $i \in \{1, \ldots, k\}$

c) $p_i - 1 \mid n - 1$ *for* $i \in \{1, \ldots, k\}$

d) $p_i + 1 \mid n + 1$ *for* $i \in \{1, \ldots, k\}$

then the congruence $T(-1, n, 5)$ holds, while $n^2 \not\equiv 1 \pmod 5$.

The authors used arguments from analytical number theory to show heuristic reasons for the existence of a number n satisfying the given conditions, and therefore being a counterexample for the Agrawal's conjecture. They did not, however, give any concrete estimation of the size of this number, nor did they give any way to find it. Before we will show that the theorem itself is true, we will prepare some helpful statements. The proof we will give in this text differs slightly from the original proof and from the intermediate lemmas we will later derive a way to verify the congruence $T(-1, n, 5)$ in some special circumstances.

Definition 3.1 *Let n be an arbitrary integer, for which $(n, 5) = 1$. Let us denote by $\rho(n)$ the smallest integer, for which the following is true*

$$(x-1)^{\rho(n)+1} \equiv x - 1 \pmod{x^5 - 1, n} \tag{3.1}$$

First, let us show that the definition is correct and the number $\rho(n)$ actually exists in all cases.

Lemma 3.1 *Let n be an integer and let $(n, 5) = 1$. Then there is a number $r > 1$, for which*

$$(x-1)^r \equiv x - 1 \pmod{x^5 - 1, n}$$

Proof We will show that if $(n, 5) = 1$ holds, we can in some limited way cancel out the term $x - 1$ from both sides of a congruence, if we have powers of this polynomial at the both sides of it. First of all, from the condition $(n, 5) = 1$ we know that there is an inverse element for the number 5 modulo n. Let us call this inverse element a and consider the following polynomials $p(x) = 2ax^4 + ax^3 - ax - 2a$ and $q(x) = x^4 + x^3 + x^2 + x + 1$. It is true that

$$p(x) \cdot (x - 1) \equiv -ax^4 - ax^3 - ax^2 - ax + 4a \pmod{x^5 - 1, n}$$

what can be written as

$$p(x) \cdot (x - 1) \equiv 5a - aq(x) \pmod{x^5 - 1, n}$$

or by the definition of a

$$p(x) \cdot (x - 1) \equiv 1 - aq(x) \pmod{x^5 - 1, n} \tag{3.2}$$

The next congruence we will use is easy to verify as well

$$q(x) \cdot (x - 1) \equiv 0 \pmod{x^5 - 1, n} \tag{3.3}$$

Now we will come to the proof of the lemma itself. At first we have to realize that the powers like $(x - 1)^k$, $k \geq 1$ are always members of exactly one of just finitely many remainder classes modulo $x^5 - 1$ and n (the overall count of these classes is exactly n^5), therefore it has to come to the situation when some remainder will repeat itself. This means we can find a pair of exponents $k \neq l$, for which

$$(x - 1)^k \equiv (x - 1)^l \pmod{x^5 - 1, n} \tag{3.4}$$

If it would be the case that $k = 1$ or $l = 1$, we are already done with the proof. Therefore let us assume, without the loss of generality that $1 < k < l$. We will show using mathematical induction that following holds

$$p(x) \cdot (x - 1)^{m+1} \equiv (x - 1)^m \pmod{x^5 - 1, n} \tag{3.5}$$

for any positive integer m. For the first step $m = 1$, we have from congruences (3.2) and (3.3), that

$$\begin{aligned} p(x) \cdot (x - 1)^2 = p(x) \cdot (x - 1) \cdot (x - 1) \equiv \\ (1 - aq(x)) \cdot (x - 1) = x - 1 - aq(x) \cdot (x - 1) \equiv \\ x - 1 - a \cdot 0 = x - 1 \pmod{x^5 - 1, n} \end{aligned}$$

The second step is quite trivial, it is enough to multiply the congruence by the polynomial $x - 1$.

To conclude the proof it is enough to multiply the congruence (3.4) by the polynomial $p(x)^{k-1}$ and repeatedly use the relationship (3.5), which gives us

$$\begin{aligned} p(x)^{k-1} \cdot (x-1)^k &\equiv p(x)^{k-1} \cdot (x-1)^l \pmod{x^5 - 1, n} \\ x - 1 &\equiv (x-1)^{l-k+1} \pmod{x^5 - 1, n} \end{aligned}$$

We have found the $r = l - k + 1$ we were looking for, which finally concludes the proof. ■

Lemma 3.2 *Let k, l be arbitrary integers satisfying $(x-1)^k \equiv (x-1)^l \pmod{x^5 - 1, n}$, and let ρ be the function we have defined above. Then the congruence $k \equiv l \pmod{\rho(n)}$ holds.*

Proof The case $k = l$ is trivial, therefore we can without loss of generality assume that $k < l$. At the end of the previous proof we have shown that having the congruence (3.4) we know that

$$x - 1 \equiv (x-1)^{l-k+1} \pmod{x^5 - 1, n} \tag{3.6}$$

in the case $k = 1$ trivially and in the case $k > 1$ after canceling out the terms iteratively. On the other side we have defined the number $\rho(n)$ as the smallest integer with property (3.1), telling us how many times the remainder $x - 1$ will repeat itself in the sequence of powers. Because from this point on the sequence is periodic, every other repetition has to happen exactly for the powers that are further by the multiple of $\rho(n)$. This means that $\rho(n) \mid l - k$ has to hold, but that is only an equivalent way of stating the congruence that we are proving, therefore we are done. ■

Lemma 3.3 *Let n be an integer for which $(n, 5) = 1$ and ρ the function defined above. If there are suitable integers $\lambda_i(n)$, $i \in \{2, 3, 4\}$ for which*

$$(x-1)^{\lambda_i(n)} \equiv x^i - 1 \pmod{x^5 - 1, n}$$

then $\lambda_2(n)^2 \equiv \lambda_4(n) \pmod{\rho(n)}$, $\lambda_2(n)^3 \equiv \lambda_3(n) \pmod{\rho(n)}$, $\lambda_3(n)^2 \equiv \lambda_4(n) \pmod{\rho(n)}$ and $\lambda_3(n)^3 \equiv \lambda_2(n) \pmod{\rho(n)}$.

Proof Let us take first the congruence

$$(x-1)^{\lambda_2(n)} \equiv x^2 - 1 \pmod{x^5 - 1, n}$$

substituting x^2 for x we get

$$(x^2-1)^{\lambda_2(n)} \equiv x^4 - 1 \pmod{x^5 - 1, n}$$

comparing with the original congruence this gives us

$$(x-1)^{\lambda_2(n)^2} \equiv x^4 - 1 \pmod{x^5 - 1, n}$$

from where we already have by the definition of the function ρ and lemma 3.2 the first congruence we wanted to prove : $\lambda_2(n)^2 \equiv \lambda_4(n) \pmod{\rho(n)}$. Let us continue now with further substituting x^2 for x, getting

$$(x^2-1)^{\lambda_2(n)^2} \equiv x^3 - 1 \pmod{x^5 - 1, n}$$

by comparing we get

$$(x-1)^{\lambda_2(n)^3} \equiv x^3 - 1 \pmod{x^5 - 1, n}$$

from where $\lambda_2(n)^3 \equiv \lambda_3(n) \pmod{\rho(n)}$. Analogically starting from congruence

$$(x-1)^{\lambda_3(n)} \equiv x^3 - 1 \pmod{x^5 - 1, n}$$

substituting x^3 for x and comparing we get

$$(x-1)^{\lambda_3(n)^2} \equiv x^4 - 1 \pmod{x^5 - 1, n}$$

or

$$(x-1)^{\lambda_3(n)^3} \equiv x^2 - 1 \pmod{x^5 - 1, n}$$

which gives us the rest of the congruences and concludes the proof. ■

Lemma 3.4 *Let n be an integer and ρ the function defined above. If there are suitable integers $\lambda_i(n)$, $i \in \{2,3,4\}$ such that*

$$(x-1)^{\lambda_i(n)} \equiv x^i - 1 \pmod{x^5 - 1, n}$$

then

$$\rho(n) \mid 10 \cdot (\lambda_i(n)^2 - 1) \text{ for } i \in \{2,3\}$$

and

$$\rho(n) \mid 10 \cdot (\lambda_4(n) - 1)$$

Proof Let us assume that for some integer σ it is true that

$$(x-1)^{\sigma} \equiv x^4 - 1 \pmod{x^5 - 1, n}$$

Then we have

$$(x-1)^{\sigma-1} \equiv x^3 + x^2 + x + 1 \pmod{x^4 + x^3 + x^2 + x + 1, n}$$

or

$$(x-1)^{\sigma-1} \equiv -x^4 \pmod{x^4 + x^3 + x^2 + x + 1, n}$$

Squaring both sides we get

$$(x-1)^{2(\sigma-1)} \equiv x^3 \pmod{x^4 + x^3 + x^2 + x + 1, n}$$

and now by taking both sides to the 5th power we already have

$$(x-1)^{10(\sigma-1)} \equiv 1 \pmod{x^4 + x^3 + x^2 + x + 1, n}$$

It is as well true that

$$(x-1)^{10(\sigma-1)+1} \equiv x - 1 \pmod{x^5 - 1, n}$$

therefore $\rho(n) \mid 10(\sigma - 1)$ (according to the lemma 3.2). To conclude the proof it is enough to realise that we can substitute for the number σ any of the numbers $\lambda_2(n)^2$, $\lambda_3(n)^2$ and $\lambda_4(n)$, in the last case from the lemma itself and in the rest based on the congruences from lemma 3.3. ■

Now we are ready to prove the Lenstra-Pomerance theorem.

Proof of the theorem 3.1 Let us first assume that $k \equiv 1 \pmod 4$ and let $k = 4 \cdot k' + 1$. Because $3^4 = 81 \equiv 1 \pmod{80}$ and for all i we have $p_i \equiv 3 \pmod{80}$, it is true that $n = p_1 \dots p_k \equiv 3^{4k'+1} = (3^4)^{k'} \cdot 3 \equiv 3 \pmod{80}$. This means the number n gives the remainder 3 when divided by 5 and the congruence $T(-1, n, 5)$ has the form

$$(x-1)^n \equiv x^3 - 1 \pmod{x^5 - 1, n}$$

in this case. Because n is a product of distinct prime numbers, it is enough to prove the congruence modulo each of these, i.e. to show that it is true that

$$(x-1)^n \equiv x^3 - 1 \pmod{x^5 - 1, p_i} \tag{3.7}$$

for all i. Having $p_i \equiv 3 \pmod 5$ we know that $T(-1, p_i, 5)$ holds, therefore

$$(x-1)^{p_i} \equiv x^3 - 1 \pmod{x^5 - 1, p_i} \tag{3.8}$$

Congruence (3.7) is therefore according to the lemma 3.2 equivalent to the relationship

$$n \equiv p_i \pmod{\rho(p_i)} \tag{3.9}$$

Moreover, according to the theorem 3.4 it is true that $\rho(p_i) \mid 10 \cdot (p_i^2 - 1)$ (for $\lambda_3(p_i) = p_i$). This means that if we are lucky enough to prove, instead of the congruence (3.9), a following stronger one

$$n \equiv p_i \pmod{10(p_i^2 - 1)} \tag{3.10}$$

we would be done with the proof. Let us first have a look at the modulus itself. Because we have $p_i \equiv 3 \pmod{80}$, the number $p_i - 1$ is even, but not divisible by any higher power of two. Additionally, it is not divisible by five. The number $p_i + 1$ is divisible by four, but not by any other higher power of two, and it's not divisible by five as well. In other words, it is true that $10(p_i^2 - 1) = 80 \cdot \frac{p_i - 1}{2} \cdot \frac{p_i + 1}{4}$, while all the factors are relatively prime to one another. To prove the original congruence (3.10) it is enough to prove the congruence taken modulo each of the factors. In the first case this is very easy – we have $n \equiv 3 \pmod{80}$, as well as $p_i \equiv 3 \pmod{80}$. In the second and third case we have to use the conditions c), d) from the theorem itself. These conditions tell us that $n \equiv 1 \pmod{p_i - 1}$ and $n \equiv -1 \pmod{p_i + 1}$. In the first case this means that $n \equiv 1 \pmod{\frac{p_i - 1}{2}}$, while obviously $p_i \equiv 1 \pmod{\frac{p_i - 1}{2}}$. In the second case on the other hand $n \equiv -1 \pmod{\frac{p_i + 1}{4}}$, while obviously $p_i \equiv -1 \pmod{\frac{p_i + 1}{4}}$. We have finished the proof of the given congruence.

Let us take a look at the differences in the case $k \equiv 3 \pmod 4$. Here we can write $k = 4 \cdot k' + 3$, having $n = p_1 \dots p_k \equiv 3^{4k'+3} = (3^4)^{k'} \cdot 3^3 \equiv 27 \pmod{80}$. This means in this case the number n has a remainder of 2 when taken modulo 5 and the congruence we are trying to prove is equivalent to the system of congruences in the following form

$$(x-1)^n \equiv x^2 - 1 \pmod{x^5 - 1, p_i} \tag{3.11}$$

Nothing has changed in respect to the congruences (3.8) and once again we can get from the lemma 3.4 an equivalent formulation of our problem in the form of congruences $n \equiv \lambda_2(p_i) \pmod{\rho(p_i)}$. In this case we will additionally

use the lemma 3.3, which tells us that $\lambda_2(p_i) \equiv \lambda_3(p_i)^3 = p_i^3 \pmod{\rho(p_i)}$, to get the congruence

$$n \equiv p_i^3 \pmod{\rho(p_i)} \tag{3.12}$$

Using the lemma 3.4 once again we will prove the stronger congruence with modulus $10 \cdot (p_i^2 - 1)$ factored to 3 relatively prime factors. We have $n \equiv 27 \pmod{80}$ and $p_i^3 \equiv 27 \pmod{80}$, in case of the first factor the remainders are the same. For the other two we will once again start from the conditions c),d) stated in the theorem, getting $n \equiv 1 \pmod{\frac{p_i-1}{2}}$, while $p_i \equiv 1 \pmod{\frac{p_i-1}{2}}$, and therefore $p_i^3 \equiv 1 \pmod{\frac{p_i-1}{2}}$ as well. Analogically $n \equiv -1 \pmod{\frac{p_i+1}{4}}$, while $p_i \equiv -1 \pmod{\frac{p_i+1}{4}}$, and therefore $p_i^3 \equiv -1 \pmod{\frac{p_i+1}{4}}$ as well. This concludes the proof also in the second case. ■

Looking at the proof it seems to be clear that the conditions we are giving for the counterexample we search are rather strict, which means it is possible that there could be a counterexample that does not satisfy them. On the other hand, the authors provided arguments supporting the confidence that there is a number satisfying these conditions, although it can be actually very large. We intentionally used a slightly different method of proof than the original one given by authors, because this gives us in some special cases (similar to those given by the conditions in the theorem), the way to test the conjecture directly.

More specifically, let us consider a square-free number $n \equiv 2, 3 \pmod 5$ that is a product of prime numbers with remainders 2 or 3 modulo 5. We can consider the congruence $T(-1, n, 5)$ separately modulo the prime factors, while each of the congruences in the form $(x-1)^n \equiv x^n - 1 \pmod{x^5 - 1, p}$ is equivalent to the congruence $n \equiv \lambda_{n \bmod 5}(p) \pmod{\rho(p)}$, where $\lambda_{n \bmod 5}(p)$ is such a number for which $(x-1)^{\lambda_{n \bmod 5}(p)} \equiv x^{n \bmod 5} - 1 \pmod{x^5 - 1, p}$. At the first sight this does not improve anything, because we don't actually know any of the numbers $\lambda_{n \bmod 5}(p)$ or $\rho(p)$. However, because $p \equiv 2, 3 \pmod 5$, we know at least one of the numbers $\lambda_2(p)$, $\lambda_3(p)$ - it is exactly the number p (this fact is implied directly by the congruence $T(-1, p, 5)$). From the theorem 3.4 we then have $\rho(p) \mid 10(p^2 - 1)$. This enables us to search through the divisors, find such a number and then, if it is needed, calculate the missing of the values $\lambda_2(p)$, $\lambda_3(p)$ using the congruence from lemma 3.3.

Let us have a closer look now at the way of searching through the divisors of some number when looking for the value of $\rho(p)$ (this value represents the multiplicative order of the element $x - 1$). Let us denote this number by r

(in our case $r = 10(p^2 - 1)$). We know that $\rho(p) \mid r$, let's assume that we have already found the prime decomposition $r = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and we want, as quickly as possible, find the number $\rho(p)$. Algorithm 2 calculates $\rho(p)$ by testing the congruence (3.1) in such a way that it is decreasing the powers of all the prime factors dividing r by one until the point where it finds the negative result in all of the cases, where it gives the product of decreased powers as a result. The algorithm is based on the fact that the number $\rho(p)$ we are searching for divides all the numbers having the same property (3.1), so it does not really matter which way we choose to go and we always get to the correct result.

Algorithm 2 SEARCH(r)

```
for i = 1 ... k do
    r' ← r / p_i
    if (x − 1)^{r'+1} ≡ x − 1 (mod x^5 − 1, n) then
        return SEARCH(r')
    end if
end for
return r
```

After finding the number $\rho(p)$ and having its prime decomposition, we can create a system of congruences - taking the congruence $n \equiv \lambda_{n \bmod 5}(p) \pmod{\rho(p)}$ modulo all the prime-power divisors (from the decomposition) of the number $\rho(p)$. This system is according to the Chinese remainder theorem equivalent to the original congruence, and therefore to the congruence $T(-1, n, 5)$ as well, if we take the union of those systems for all choices of the prime p.

Because this system of congruences can be calculated for each prime number independently from the actual product n, we can also go the other way - try to combine the prime numbers and their systems of congruences in such a way that we increase the probability that their product (the number n) will be satisfying all of them. In case where the systems are incompatible (asking for a different remainder for the same modulus or its multiple), we can immediately refuse the hypothesis that such a pair of prime numbers can be in a set of prime divisors of our counterexample. The important fact is that this can be concluded without knowing anything about the other prime factors. Intuitively it seems that the optimal choice for the prime divisors of n is to choose such prime numbers p for which $\rho(p)$ is smooth enough (i.e. has

only small prime divisors). In this case the common modulus, derived from the combination of systems of congruences, is not getting such large (as the prime factors are repeating more often). If the prime factors are not repeating at all, the modulus is approximately cubic compared to the product of the primes, and therefore the probability of it satisfying the resulting congruence seems to be very small.

This method is not effective enough for searching in larger ranges, but it gives us a little improvement compared to the naive testing of the congruence $T(-1, n, 5)$ for smaller cases, when the number n satisfies additional conditions. In the following chapter we will present some concrete results of searches done using the theoretical results we have achieved so far.

Chapter 4

Experimental data

In this last chapter we will present some empirical results from experiments we have made based on the theoretical observations from the previous chapters. Our goal was to collect some useful statistics suggesting how near or far are we from finding a counterexample to the Agrawal's conjecture and to collect some data that may help in the future search for the counterexample. Although most of these experiments were based on the proved results, the approach remains rather heuristic as we only have some indications but no evidence that there is any such counterexample.

In the text [1], authors stated that they have made a search up to 10^{11} for a composite n that would satisfy the congruence $T(-1, n, 5)$ and $n \equiv 2, 3 \pmod 5$ at the same time. For other primes $r \leq 100$ they have come up to 10^{10} with the same negative result (i.e. it was always true that $n^2 \equiv 1 \pmod r$). In [14] authors provide a proof for the theorem 3.1, afterwards stating estimations based on heuristic calculations using analytical number theory to conclude that there should be a constant, a lower bound for the range where the counterexamples are frequent enough.

Looking at their result it was not difficult to see that although not explicitly mentioning that, they are dealing with a subset of Carmichael numbers. On the other hand, the Carmichael numbers are a point of interest for many mathematicians, amongst all maybe most significantly Richard Pinch, who has in the last 15 years collected all the Carmichael numbers up to 10^{21} and some lists of pseudoprimes as well (see e.g. [15]). We have used a publicly available subset up to 10^{18} to perform some experiments, of which the results we present here. We also asked Mr. Pinch for the rest of the data and we will continue with the experiments as soon as he delivers it.

As a part of a school project in the course of computer algebra, we have used the software Maple in version 11 to perform some basic search in range $\langle 1, 10^{16} \rangle$ and at first it seemed we have discovered some counterexamples even in this range. After further tests, we have found out that the reason why our algorithm reported those numbers as positive was a bug in the Maple's function *isprime* which uses some randomized primality tests and in the documentation they wrote that

No counterexample is known and it has been conjectured that such a counter example must be hundreds of digits long.

Actually, we have found the following three Carmichael numbers

$$\begin{aligned} 43438471758571 &= 5503 \cdot 8123 \cdot 971759 \\ 54165858332251 &= 14071 \cdot 32831 \cdot 117251 \\ 367826207971951 &= 10531 \cdot 94771 \cdot 368551 \end{aligned}$$

that were falsely identified as prime by Maple. We reported this to the support team and they have admitted this is a bug.

In the version 12 of Maple this bug is already fixed, but we have decided, most importantly for performance reasons, to try out some other frameworks that are more suitable for our purposes. We have found two relevant libraries – LiDIA and NTL (see [16] and [17]) and have decided for the second one as a main tool for our computations. First, let us have a look at the most interesting question – taking the theorem 3.1, how many Carmichael numbers satisfy the individual conditions. As we are dealing with Carmichael numbers, the Korselt's criterion tells us that all of them are square-free and the condition **c)** is satisfied automatically. Therefore it only makes sense to ask about the conditions from **a)**, **b)** and **d)**. The following table shows the results :

Table 1					
range	count of Carmichaels	$k \equiv 1 \pmod 4$	$k \equiv 3 \pmod 4$	b)	d)
$\langle 1, 10^{10} \rangle$	1547	492	337	0	0
$\langle 1, 10^{11} \rangle$	3605	1336	631	0	0
$\langle 1, 10^{12} \rangle$	8241	3156	1262	0	0
$\langle 1, 10^{13} \rangle$	19279	7083	3198	0	0
$\langle 1, 10^{14} \rangle$	44706	14965	8643	0	0
$\langle 1, 10^{15} \rangle$	105212	29452	25293	0	0
$\langle 1, 10^{16} \rangle$	246683	56448	70966	0	0
$\langle 1, 10^{17} \rangle$	585355	109542	191774	0	0
$\langle 1, 10^{18} \rangle$	1401644	223056	496188	1	0

There is not much surprise in those results, it seems that the number of prime factors being of the desired form is not a huge restriction, quite opposite it is the case with conditions **b)** and **d)**. There was only one number which satisfied the condition **b)**, i.e. having all the prime factors with $p_i \equiv 3 \pmod{80}$. It is the number

$$330468624532072027 = 2003 \cdot 574003 \cdot 287432003$$

However, none of its prime factors satisfies the condition $p_i + 1 \mid n + 1$. There is no number in this range which would satisfy this condition **d)** for all its prime factors, too. In order to get a slightly better insight we have tried to count the individual prime factors satisfying conditions **b)** and **d)**. First, in the table 2 we show the counts of Carmichael numbers with a concrete number of prime factors (only those which are satisfying condition **a)** are highlighted there).

Table 2						
range	k = 3	k=5	k=7	k=11	k=13	k=15
$\langle 1, 10^{10} \rangle$	335	492	2	0	0	0
$\langle 1, 10^{11} \rangle$	590	1336	41	0	0	0
$\langle 1, 10^{12} \rangle$	1000	3156	262	0	0	0
$\langle 1, 10^{13} \rangle$	1858	7082	1340	1	0	0
$\langle 1, 10^{14} \rangle$	3284	14938	5359	27	0	0
$\langle 1, 10^{15} \rangle$	6083	29282	19210	170	0	0
$\langle 1, 10^{16} \rangle$	10816	55012	60150	1436	0	0
$\langle 1, 10^{17} \rangle$	19539	100707	172234	8835	1	0
$\langle 1, 10^{18} \rangle$	35586	178063	460553	44993	49	0

The following tables 3 and 4 show the counts of Carmichael numbers with a concrete number of prime factors satisfying the conditions **b)** and **d)**.

Table 3				
range	b) for 1	b) for 2	b) for 3	b) for more than 3
$\langle 1, 10^{10} \rangle$	89	1	0	0
$\langle 1, 10^{11} \rangle$	205	3	0	0
$\langle 1, 10^{12} \rangle$	487	3	0	0
$\langle 1, 10^{13} \rangle$	1149	12	0	0
$\langle 1, 10^{14} \rangle$	2742	39	0	0
$\langle 1, 10^{15} \rangle$	6708	127	0	0
$\langle 1, 10^{16} \rangle$	16077	318	0	0
$\langle 1, 10^{17} \rangle$	39841	832	6	0
$\langle 1, 10^{18} \rangle$	98891	2173	18	0

Table 4				
range	d) for 1	d) for 2	d) for 3	d) for more than 3
$\langle 1, 10^{10} \rangle$	42	3	0	0
$\langle 1, 10^{11} \rangle$	100	4	0	0
$\langle 1, 10^{12} \rangle$	211	5	0	0
$\langle 1, 10^{13} \rangle$	505	8	0	0
$\langle 1, 10^{14} \rangle$	1085	21	0	0
$\langle 1, 10^{15} \rangle$	2462	57	0	0
$\langle 1, 10^{16} \rangle$	5643	124	1	0
$\langle 1, 10^{17} \rangle$	13076	246	3	0
$\langle 1, 10^{18} \rangle$	30648	513	7	0

Looking at the counts of individual prime factors satisfying the conditions we can be a little bit more optimistic as it does not seem to be that rare from this perspective. However, we cannot treat those properties as independent and even the prime factors themselves are not completely independent and therefore the pattern does not necessarily have to hold for larger ranges. Even if it did, the result data suggests that we are still far away from the counterexample proposed by Lenstra and Pomerance and getting to it by an exhaustive search may be impossible.

We have actually tried some approaches to get to some much bigger numbers, where there is no way of performing an exhaustive search but the Lenstra and Pomerance suggest that the density of counterexamples

may grow there. First approach is based on the algorithm from chapter 3. There we have found a way of constructing a set of congruences which together form the necessary and sufficient condition for a prime p to be able to form (with some other factors) the counterexample for Agrawal's conjecture. These congruences are telling us the required remainders of n when taken modulo some prime powers. For example, if we have a prime $p = 113$ and constructing $n \equiv 3 \pmod 5$, the congruences are as follows

$$\begin{aligned} n &\equiv 49 \pmod{2^6} \\ n &\equiv 3 \pmod 5 \\ n &\equiv 1 \pmod 7 \\ n &\equiv -1 \pmod{19} \end{aligned}$$

Adding the congruence $n \equiv 0 \pmod{113}$ we have a complete set which we can use for combining with sets of another prime numbers. If we find a considerable *compatibility* of these sets of congruences, we can try to use the Chinese remainder theorem to formulate just one congruence for the result and search its solutions for numbers having only desired form. In this way it is possible to construct numbers with many prime factors satisfying the equivalent condition $n \equiv \lambda_{n \bmod 5} \pmod{\rho(p)}$. Of course, the problem in this approach is to find a suitable last factor that would be compatible with all the previous congruences and would therefore satisfy the equivalent condition. It shows us that the fact of having some, but not all prime factors satisfying any property seems to have almost no real value for us as we can construct any number of such examples as we like.

In order to be able to manipulate and combine the sets of congruences for the particular prime numbers, we have decided to collect this data for all the prime numbers up to 10^8. The file is available on request from the author of this text and contains the value of $\rho(p)$ for all $p \equiv 2, 3 \pmod 5$ within the range, with their prime factorization and the desired remainders for each of the prime power factor. One way of searching good candidates for combination could be a restriction for smoothness (suggested also in [13]). The table 5 shows some counts of m-smooth numbers between the values of $\rho(p)$ within our range. Files containing only those primes with smooth $\rho(p)$ are also available on request from the author of this text.

Table 5	
m	count of primes p within $\langle 1, 10^8 \rangle$ with $\rho(p)$ being m-smooth
30	44
50	134
100	670
500	20524
1000	54270

Another interesting question in the connection to the Agrawal's conjecture is the choice of the congruence $n^2 \equiv 1 \pmod{r}$. It seems at first that it would be enough to take just the first power, i.e. the congruence $n \equiv 1 \pmod{r}$, as the cases where this more specific congruence doesn't hold are quite rare. To express the *rare* word in more quantitative form, we have tried to collect some useful data based on the pre-calculated pseudoprimes list by William Galway (see [18]). We will state another result here and show that for the special case $r = 4$, the pseudoprimality of n is a necessary condition for the AKS congruence to hold.

Theorem 4.1 *Let n be a natural number. The congruence $T(-1, n, 4)$ holds iff*

a) $2^{\frac{n-1}{2}} \cdot (-1)^{\frac{n-1}{4}} \equiv 1 \pmod{n}$ *for* $n \equiv 1 \pmod{4}$

b) $2^{\frac{n-1}{2}} \cdot (-1)^{\frac{n+1}{4}} \equiv 1 \pmod{n}$ *for* $n \equiv 3 \pmod{4}$

Proof Let $n = 4k + 3$. It can be easily shown by induction that

$$2^{2k} \cdot ((-2^{2k+1} + (-1)^k) + (2^{2k+1} + (-1)^k)x +$$
$$(-2^{2k+1} - (-1)^k)x^2 + (2^{2k+1} - (-1)^k)x^3)$$

is congruent to $(x-1)^n$ in $(x^4 - 1, n)$. In the first step, taking $k = 0$, the expression evaluates to $x^3 - 3x^2 + 3x - 1$, which is exactly $(x-1)^3$. In the induction step we just multiply the expression by $(x-1)^4 = 2(-2x^3 + 3x^2 - 2x + 1)$ and we get the desired result for $k + 1$. To derive the equivalent property for $T(-1, n, 4)$, we just have to compare the coefficients of desired result $(x-1)^n$, which should be the same as $x^3 - 1$, to what we have in our expression. This gives us the following congruences :

$$2^{2k}(2^{2k+1} - (-1)^k) \equiv 1 \pmod{n}$$
$$2^{2k}(2^{2k+1} + (-1)^k) \equiv 0 \pmod{n}$$

When we subtract these we get directly the congruence $2^{2k+1} \cdot (-1)^{k+1} \equiv 1 \pmod{n}$, which we wanted to prove in the first place. To get the other direction of equivalence, it is enough to realize that $(n, 2) = 1$ and by multiplying the congruence by 2^{-1} and squaring both sides we can easily derive both of the congruences equivalent to $T(-1, n, 4)$, which concludes the proof. In case of $n = 4k + 1$, the proof is exactly the same, first we show by induction that

$$2^{2k-1} \cdot ((-2^{2k} + (-1)^{k-1}) + (2^{2k} - (-1)^{k-1})x + \\ (-2^{2k} - (-1)^{k-1})x^2 + (2^{2k} + (-1)^{k-1})x^3)$$

is in the same class of residues as $(x - 1)^n$, then we compare the coefficients with the desired result, in this case the polynomial $x - 1$. This way we get congruences

$$2^{2k-1}(2^{2k} - (-1)^{k-1}) \equiv 1 \pmod{n} \\ 2^{2k-1}(2^{2k} + (-1)^{k-1}) \equiv 0 \pmod{n}$$

Subtracting them gives us the congruence $2^{2k} \cdot (-1)^k \equiv 1 \pmod{n}$, which we wanted to prove (the other direction is done once again with squaring both sides). ■

As a direct consequence (by squaring the proved congruences) we have the fact that n has to be a pseudoprime. Therefore we were able to simply use the existing records of pseudoprimes (up to 10^{15}) to find out how often the congruence $T(-1, n, 4)$ holds. From the overall count of 1801533 pseudoprimes in the range we searched through, there were 867198 such that $T(-1, n, 4)$ holds and $n \equiv 1 \pmod{4}$, and only 89913 were such that $T(-1, n, 4)$ holds and $n \equiv 3 \pmod{4}$. The reason seems to be that there is about 10 times more pseudoprimes with residue 1 than with residue 3 and for both of them about a half satisfies the condition needed for $T(-1, n, 4)$ to hold.

It all looks like for $r = 4$ there is a lot of examples showing why stating the Agrawal's conjecture for $n \equiv 1 \pmod{4}$ was definitely not enough. The next question we could ask is whether this pattern holds also for large numbers and whether we can find an infinite sequence of numbers with $T(-1, n, 4)$ and $n \equiv 3 \pmod{4}$. We will show that if the widely believed Sophie-Germain primes conjecture is true, such a sequence can be easily constructed. First of all, let us introduce some necessary basics.

Definition 4.1 *Let p be a prime number. We say that p is a Sophie-Germain prime if $2p+1$ is a prime number as well.*

The conjecture says that there is infinitely many Sophie-Germain primes. Some very large examples were actually found (e.g. $p = 8069496435 \cdot 10^{5072} - 1$), but no proof was yet given. There are some heuristic arguments and estimations about the expected count of these numbers, however. The next theorem tells us about the connection between Sophie-German primes and composite Mersenne numbers, which we will need for our proof. Mersenne numbers are numbers in form $2^n - 1$, especially interesting when the exponent n is prime.

Lemma 4.1 *If $M_n = 2^n - 1$ is prime, then n has to be a prime.*

Proof If the n is composite, we can write $n = ab$ $(a, b > 1)$ and $2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + \ldots + 1)$, therefore $2^n - 1$ is composite as well. ■

While p has to be prime for $2^p - 1$ to be prime as well, the converse is not true and actually there are many such Mersenne numbers with prime exponents that are composite. It is not even known whether there is infinitely many such composite or infinitely many such prime Mersenne numbers with prime exponents. We will now show the connection between such numbers and Sophie-Germain primes.

Theorem 4.2 *Let $p > 3$ be a Sophie-Germain prime for which $p \equiv 3 \pmod 4$. Then the number $M_p = 2^p - 1$ is composite.*

Proof Let $q = 2p + 1$, we know that this number is prime. In addition, because $p \equiv 3 \pmod 4$, we know that $q \equiv 7 \pmod 8$. This implies (calculating the Legendre's symbol, see e.g. [11]), that the number 2 is a quadratic residue $\pmod q$, which by Euler's criterion for quadratic residues means that $2^{\frac{q-1}{2}} = 2^p \equiv 1 \pmod q$. Therefore, we have shown that $M_p = 2^p - 1$ has a non-trivial factor of $q = 2p+1$, and has to be composite. ■

Now we know that relying on a fact of having enough Sophie-Germain primes (with the desired residue mod 4), there is enough composite Mersenne numbers with prime exponents as well. To finish our reasoning we will use

these numbers to construct the sequence of numbers which we were looking for.

Theorem 4.3 *If $p > 3$ is a prime number and $M_p = 2^p - 1$, then $T(-1, M_p, 4)$ holds.*

Proof According to the theorem 4.1, we need to check the equivalent congruence to know whether $T(-1, M_p, 4)$ holds. The residue mod 4 is in this case obviously 3, so we have to prove that

$$2^{\frac{M_p-1}{2}} \cdot (-1)^{\frac{M_p+1}{4}} \equiv 1 \pmod{M_p}$$

The exponent of -1 disappears immediately, as $\frac{M_p+1}{4} = 2^{p-2} \equiv 0 \pmod 2$. The congruence is equivalent to

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

Now we will use the fact that p is prime and by Fermat's theorem $p \mid 2^{p-1}-1$. This means that the exponent is divisible by p and can be written in a form $p \cdot k$ for some k. This gives us the conclusion that $2^{2^{p-1}-1} = 2^{p \cdot k} = (2^p)^k \equiv 1^k = 1 \pmod{2^p - 1}$ and the proof is done. ■

From the theorem we now see the reason why we needed the Mersenne numbers to be composite - in the case of composite M_p we directly have an example of AKS pseudoprime for which $n \not\equiv 1 \pmod 4$, and it seems very probable (based on the mentioned conjectures) that in this case we have infinitely many of them.

Although we have not made any significant discovery, we consider our approaches quite promising because according to the results of exhaustive searches it seems there is no other way to directly find the counterexample except for aiming at very large numbers. After performing all the experiments we strongly believe that if the counterexample exists and will be found, it would be with some sophisticated method for generating large possible counterexamples. We will continue with an occasional research with these methods and try to look for some more ways in the future.

Chapter 5

Conclusion

A couple of years ago the best where we could get with the solution for the problem of primality testing was probabilistic tests and tests based on various conjectures, most notably Riemann hypothesis. Although these algorithms were not perfect from a strict point of view, they were very elegant and easily understandable, which made them intelligible and usable both to mathematicians and computer scientists. After all, only a couple of decades has passed from the discovery of RSA which launched the heavy usage of number theory in cryptography and made it attractive to the computer scientists, not only as a theoretical tool, but for very practical reasons, too.

The year 2002 has brought a breakthrough in this area, the algorithm AKS which is almost as elegant and easy to understand as the previous tests and does not have any theoretical drawbacks. The only problem still present is that although being a satisfactory solution for computer scientists, it is not much of a use for practical applications, e.g. for generating primes for keys. The reason for that is of course that even though it is polynomial, the large exponent still makes it too slow. In our text we have tried to research some of its aspects in order to make it faster or show that some of the suggested ways to make it faster do not work and we should look somewhere else.

We have demonstrated the use of combinatoric methods to deal with modular sums in the binomial expansion. In our particular problem this approach was an interesting way of how to prove the theorem and gain a better insight to the structure of objects we are dealing with. We have also provided the algebraic proof as an alternative, just to compare and see the differences. The method itself is the most valuable result that we have come to, but the theorem itself is interesting as well.

We have also presented the Agrawal's conjecture and Lenstra-Pomerance heuristic, which were the main points of interest throughout the story. As a first step, we have provided an alternative proof for the theorem that is a base of the heuristic, adding case $k = 3$, which was mentioned as an exercise in the original article. The way of proving it also provided us with an algorithm to search for parameters needed to test the AKS congruence directly in the case of $r = 5$.

As a conclusion, we have made some concrete experiments to try out the approaches that we have invented and provide some statistics which would give us a feeling of how far away is the answer to the questions we have asked at the begining. We have collected some data that can be used as a basis of further research in this area.

We believe that we have opened some new possibilities and brought new ideas which could eventually lead to the discovery of the counterexamples or proofs of the mentioned conjecture or some other interesting results related to the AKS test and hope that they were inspiring for the reader. We look forward to any advances in this area and will try to contribute to it in the future.

Bibliography

[1] Kayal N., Saxena N.: *Towards a deterministic polynomial-time Primality Test.* Indian Institute of Technology, Kanpur, India, 2002.

[2] Bernstein D.: *Detecting perfect powers in essentially linear time.* Mathematics of computation 223, 1998, p.1253-1283.

[3] Stay M.: *Primes is in P, slowly.* (unpublished)
http://math.ucr.edu/∼mike/primes.ps

[4] Crandall R., Pomerance C.: *Prime Numbers - A computational perspective.* Springer-Verlag, New York, 2001.

[5] Dietzfelbinger M.: *Primality testing in polynomial time.* Springer-Verlag, Berlin, 2004.

[6] Kolibiar M., et al.: *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992. ISBN 80-05-00721-3.

[7] Kominers S.D.: *Further improvements of lower bounds for the least common multiples of arithmetic progressions.* arXiv:0811.4769v1 [math.NT] 28 Nov 2008.

[8] Agrawal M., Kayal N., Saxena N.: *PRIMES is in P.* Annals of Mathematics 160(2), 2004, p. 781–793.

[9] Ribenboim P.: *The new book of prime number records.* Springer-Verlag, New York, 1996.

[10] Nair M.: *On Chebyshev-type inequalities for primes.* Amer. Math. Monthly 89, 1982, p. 126–129.

[11] Váňa T.: *Silné pseudoprvočísla.* bachelor thesis, FMFI UK, 2007.

[12] Š. Znám: *Teória čísel*. Alfa, vydavateľstvo technickej a ekonomickej literatúry, 1986.

[13] Lenstra H. W. Jr., Pomerance C.: *Future directions in algorithmic number theory. Problems.* (unpublished) http://www.aimath.org/WWN/primesinp/articles/html/38a

[14] Lenstra H. W. Jr., Pomerance C.: *Remarks on Agrawal's conjecture.* (unpublished) http://www.aimath.org/WWN/primesinp/articles/html/50a

[15] Pinch R.: *The Carmichael numbers up to* 10^{18}. arXiv:math.NT/0604376 April 2006.

[16] Hamdy S.: *LiDIA - A library for computational number theory.* (unpublished) ftp://ftp.informatik.tu-darmstadt.de/pub/TI/systems/LiDIA/current/LiDIA.pdf

[17] Shoup V.: *NTL : A Library for doing Number Theory.* (unpublished) http://www.shoup.net/ntl/

[18] Galway W.: *Pseudoprimes up to* 10^{15}. (data file) http://oldweb.cecm.sfu.ca/pseudoprime

[19] Anderson P.: *Fibonacci pseudoprimes up to 2217967487.* (data file) http://www.cs.rit.edu/usr/local/pub/pga/fibonacci_pp

[20] Shoup V.: *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press, 2008.

Abstract

The text deals with the AKS - deterministic primality test, the choices of the parameters of the congruence used in this test, as well as the Agrawal's conjecture leading to the speed-up of the algorithm. It shows that for some fixed choices of parameter r, the Carmichael numbers are passing whatever is the choice of the parameter a, doing so in two ways, algebraic and combinatoric, manipulating with the sums of binomial coefficients. Further it presents the heuristic of Lenstra and Pomerance as a potential way of the disproof of the Agrawal's conjecture. It gives a new alternative proof of it, along with the algorithm derived from a method used in this proof. In the end it presents the results of experiments using this algorithm and some other results from previous chapters, contributing to the intuition about the size and existence of the counterexample to the Agrawal's conjecture.

Práca sa zaoberá deterministickým testom prvočíselnosti AKS, voľbou parametrov v kongruencii používanej v tomto teste a hypotézou Agrawala vedúcou k jej urýchleniu. Ukazuje, že pri niektorých fixných voľbách parametra r prechádzajú testom Carmichaelove čísla bez ohľadu na voľbu parametra a, a to dvoma spôsobmi, algebraickým a kombinatorickým, s využitím manipulácie súm binomických koeficientov. Ďalej predstavuje heuristiku Lenstru a Pomerance-a ako možný spôsob vyvrátenia Agrawalovej hypotézy, spolu s novým, alternatívnym dôkazom, ako aj algoritmom získaným z metódy použitej pri dôkaze. Nakoniec predstavuje výsledky experimentov s využitím tohoto algoritmu a ďalších výsledkov z predchádzajúcich kapitol, ktoré prispievajú k intuitícii o veľkosti a existencii protipríkladu na Agrawalovu hypotézu.