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

Agrawal's Conjecture and Carmichael Numbers

(master's thesis)

Tomáš Váňa

advisor:
RNDr. Martin Mačaj, PhD.

Bratislava, 2009

I hereby declare that I wrote this master's thesis 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 how to recognize them apart 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 have some very small probability of giving an incorrect answer. On the other side, they are very fast, not only polynomial with respect to the length of the input, but also practically usable. 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. We will start with a brief evolvement overview of the primality testing algorithms and look at the deterministic test discovered by Indian mathematicians Manindra Agrawal, Neeraj Kayal and Nitin Saxena in august 2002.

Before the test was discovered, the authors formulated the following conjecture which they hoped would bring a deterministic primality test.

Conjecture 1.1 (Agrawal) *Let n,r be relatively prime integers, for which*

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

holds. Then either n is prime, or $n^2 \equiv 1 \pmod{r}$ has to hold.

They have not been successful in proving this conjecture and even now we do not know whether it is true or not. Finally the test they have found is based on some other ideas, however, if true, the conjecture would still provide a significant speed up of the test. In this text we will present our results related to the conjecture and try to give some new ideas that can help with the research.

We will first demonstrate some reasons for the formulation of the conjecture, starting with 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 Chinese 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. In next chapter we will present another choice of parameters where Sophie-Germain prime conjecture comes into play and implies that there is an infinite set of composite numbers satisfying the congruence in the AKS test.

We will then 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.

As a result of further research of the related theory we will demonstrate how to use matrices instead of polynomials to find a connection between the congruence used in AKS test and some special linear recurrent sequences. We will develop a generic way to construct those sequences and demonstrate in the special case that it leads to the well-known Fibonacci sequence. This will give us an alternative way of proving the result of authors of the AKS test where they have shown the numbers satisfying the test with some special parameters actually have to be Fibonacci pseudoprimes. In our text we will additionally show that in some cases we are also dealing with Fermat pseudoprimes to particular bases.

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

Chapter 2

Primality testing

To give the reader a better insight into the motivation of our story, we will mention in this chapter some of the ways to test whether a given integer is a prime number. We will give a brief overview of these methods, but to get a deeper view we strongly recommend the texts [5] and [6], which also contain the original references for all the theorems in this chapter.

First obvious way to find out whether a number is prime, is to follow the definition and simply search the range of possible divisors. This approach is called *trial division* and it comes as no surprise that it is too slow to use for large inputs.

What seems to be necessary to speed up the test, is another characterization of the prime numbers, i.e. some condition equivalent to the primality which is faster to verify. There are such conditions which may seem good candidates at the first sight, the following one is a good example.

Theorem 2.1 (Wilson's theorem) *Let p be an integer, $p > 1$. Then p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.*

However, a closer look tells us that we actually do not know how to calculate the factorial in the congruence in any faster way than the usual iterative multiplication, which means that by using the Wilson's theorem as a primality test we get an even slower algorithm than the trial division. Actually, mathematicians were not very successful in searching for a suitable equivalent condition, but there was another breakthrough idea.

If we consider a necessary condition for primality which is not sufficient in general, we may get much better results in the sense of the speed. Of course this also means that there will be composite numbers passing our test and we have to somehow distinguish them. There is a whole family based on a simple criterion called Fermat's little theorem, we will show some of them in this overview. Apart from the probabilistic tests based on Fermat's little theorem, there are some other methods of primality testing, most notably the Elliptic curve primality proving (ECPP) and the Adleman-Pomerance-Rumely (APR) test, improved by Cohen and Lenstra to get the time complexity $(\log n)^{O(\log\log\log n)}$. These tests are using quite complex results and notions from the number theory, which makes them less intelligible for the general audience.

Theorem 2.2 (Fermat's little theorem) *Let p be a prime number. For any integer a we have $a^p \equiv a \pmod{p}$. Moreover, if a is coprime to p, we have $a^{p-1} \equiv 1 \pmod{p}$.*

There is a fast way to calculate the modular powers which uses the binary representation of the exponent p, which means we have gained speed. Another advantage of this condition is the parameter a. If p is prime, the theorem has to hold for any choice of a, and by choosing more of them we can increase the probability that the result we get is really true. This parameter is usually called a *base* and a composite number that passes the Fermat's test for some base a is called *base-a pseudoprime.* The natural question that arises is whether we can choose a set of bases such that no composite number will pass the test for all of them. If there would be such a set which is small enough, we could turn this into a quickly verifiable sufficient condition as well. Unfortunately, there is no such set, because there are composites which pass the test for any base.

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

It was proved that there are infinitely many Carmichael numbers and the following criterion was found to recognize them.

Theorem 2.3 (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 $p - 1 \mid n - 1$.*

Although the Korselt's criterion characterizes the Carmichael numbers in an alternative way which is very useful for theoretical manipulations, without knowing the prime factorization (which we certainly do not know when testing for primality) it does not help too much to recognize them. On the other side, when we are lucky enough to pick a composite number which is not Carmichael, we have a very high chance of identifying it.

Lemma 2.1 *Let n be an integer. If there is a number a, coprime to n, for which the congruence $a^{n-1} \equiv 1 \pmod{n}$ does not hold, then this congruence holds for at most half of the numbers in set $\{1, \dots, n\}$ coprime to n.*

The real breakthrough idea is to use this fact and pick base a randomly multiple times. In each step we have roughly 50% probability of finding out that the number is composite (if it is not prime or Carmichael). Repeating such a test decreases the probability of wrong decision exponentially and we can bound it with such a low constant that for practical purposes we can be almost sure that the result is correct.

Unfortunately we cannot ignore Carmichael numbers because there are too many of them. What can be done though, is to formulate the necessary condition in a different way.

Theorem 2.4 *Let p be a prime number, $p = 2^s t$, where t is odd. Then for any a coprime to p we have either $a^t \equiv 1 \pmod{p}$ or $a^{2^i t} \equiv -1 \pmod{p}$ for some $i \in \{0, \dots, s-1\}$.*

Once again we can construct a primality test based on this condition. The idea itself was first discovered by Artjuhov and later independently by Selfridge. We call the composite numbers passing the test *base-a strong pseudoprimes* and there is a good reason for calling them strong, because there are no numbers analogous to the Carmichael numbers in this case. In fact, even the probability of getting false positives is lower in this case.

Theorem 2.5 *Let $n > 9$ be an odd integer. If $S(n)$ is the set of all bases $0 \leq a < n$ for which n is a strong pseudoprime, then $|S(n)| \leq \frac{1}{4}\varphi(n)$, where $\varphi(n)$ is Euler's totient function.*

Theorem 2.6 *Let $k \geq 3$ and $T \geq 1$ be integers. Algorithm which generates a prime number by testing validity of the condition 2.4 for a random number $n \in (2^{k-1}, 2^k)$ and a random number $a \in \langle 2, n-2 \rangle$, doing so T times, has a probability of producing composite number less than 4^{-T}.*

These two theorems, proved by Monier and Rabin, provide first variation of the so-called Rabin-Miller test, in this case a probabilistic one which can test or generate prime numbers based on the criterion from theorem 2.4. Another variation, discovered by Miller (which is the reason why he appears in the name of the algorithm) is a deterministic version based on the Extended Riemann hypothesis and the following result.

Theorem 2.7 *If the Extended Riemann hypothesis is true, then the smallest witness of an odd composite number n is less than $2\ln^2 n$.*

Witness is a name for the base which will not make the number a strong pseudoprime, i.e. when the test is performed with this number as a parameter a, it will find out that the number is composite. It is therefore enough to perform the test for all a's from the set $\{1, \ldots, 2\ln^2 n\}$ and we are sure (if we believe that the Extended Riemann hypothesis is true), that the result is correct.

Although both of these approaches have their flaws (the first some non-zero error probability and the second dependency on a conjecture), the variation of this test is widely used for commercial purposes to test and generate prime numbers. The main reason for that is the speed and simplicity. There are many other approaches to probabilistic primality testing, e.g. Solovay-Strassen test dealing with quadratic residues etc. In one of the following chapters we will deal with the Fibonacci test and pseudoprimes, therefore we add it here to our overview.

Theorem 2.8 *Let us denote by f_n the n-th Fibonacci number (starting with $f_0 = 0$, $f_1 = 1$). If n is a prime number, then the following holds*

a) $f_{n-1} \equiv 0 \pmod{n}$ *for* $n \equiv \pm 1 \pmod{5}$

b) $f_{n+1} \equiv 0 \pmod{n}$ *for* $n \equiv \pm 2 \pmod{5}$

Analogously to the previous tests, we call numbers that satisfy this condition in spite of being composite the Fibonacci pseudoprimes.

Next important step in the family of simple algorithms based on variations and generalizations of Fermat's little therorem was an algorithm found in the year 2002 by Indian mathematicians Agrawal, Kayal and Saxena and is called by their names, AKS test. The very basic idea of the algorithm is surprisingly simple, as the next lemma shows.

Lemma 2.2 *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

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

First, let us assume that n is prime. Then by Fermat's little theorem we have $a^n \equiv a \pmod{n}$, 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 p be a prime divisor of n. We will take a look just at the coefficient

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

If 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 will not help, as $(a, p) = 1$. ■

The previous lemma gives us an equivalent condition of primality. We have seen that there are troubles with such conditions and this is not an exception – testing it requires to calculate a polynomial of enormous size, which makes it even slower and more memory consuming than the trial division test.

To make it more than just another curiosity like Wilson's theorem, we 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 shown that the congruence holds for primes, reducing it further cannot 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. For simplicity, we will in the following text refer to this congruence as $T(a, n, r)$. This 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.

Our goal is therefore to choose r and a in such a way that we gain speed, but do not 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 keeps 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 [1].

After the AKS algorithm was discovered, there were many improvements made by other mathematicians and some of them have shifted the time complexity from the original $O(\log^{7.5+\varepsilon} n)$ to $O(\log^{6+\varepsilon} n)$. There are some modifications of the proof that only guarantee the time complexity $O(\log^{12+\varepsilon} n)$, but make the arguments in a more elementary way which is intelligible with basic knowledge of algebra and number theory. However, even these improvements were not enough to make the test practical enough and it still remains just a theoretical result at this time (for practical purposes, probabilistic algorithms are used).

An important questions that remains open will be the main topic of our whole story. We have already mentioned the Agrawal's conjecture in the introduction, this is the direction that authors have been trying to go in the

Algorithm 1 AKS

```
• check whether $n$ is a perfect power (i.e. for some $a, b > 1 : n = a^b$)
  if so, output COMPOSITE

• find the smallest $r$ such that $o_r(n) > \lg^2 n$

• perform a trial division for $n$ up to $r$
  output COMPOSITE if there is a divisor

• check the congruence (2.2) for $a \in \{1, \ldots, \lfloor \sqrt{\varphi(r)} \lg n \rfloor\}$ and $r$
  output COMPOSITE if it does not hold in some case

• otherwise output PRIME
```

article [9] before coming to another way of proof. If true, this conjecture would improve the time complexity of the AKS test to $O(\log^{3+\varepsilon} n)$, simplify it and make it really usable in the practical applications. The initial idea that the conjecture may hold at all came from the experimental searches in the range $n < 10^{10}$, $r < 100$. In the following chapters we will demonstrate some reasons of its formulation and later present our contribution to the search of the counterexample.

Chapter 3

Carmichael numbers

In the previous chapter we have said that putting $r = 1$ in the congruence (2.2) reduces testing of the congruence to the Fermat's test and therefore has all its flaws in that case. Authors have shown that choosing r in such a way that $o_r(n) > \lg^2 n$ seems to be enough to eliminate any flaws when combined with a suitable set of a's. The question we want to ask in this chapter 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, exactly as it was with the Carmichael numbers in case of the Fermat's test.

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 3.1 *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 integers a.*

Substituting $x = 1$ into $T(a, n, r)$ we have directly

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

However, this is just a shift of the congruence we want to prove and we can change a for $a - 1$, therefore we are done. ■

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. 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 3.1 *Let $n = p_1 \cdots p_k$ be a Carmichael number 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 3.2 *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*

$$\sum_{i=0}^{r-1} g^{isk} \equiv \begin{cases} r \pmod p & \textit{when } r \mid k \\ 0 \pmod p & \textit{when } r \nmid k \end{cases}$$

Proof It is easy to see that the condition $r \mid k$ is equivalent to $p - 1 \mid sk$. Because g is the generator of the cyclic group Z_p^*, this is further equivalent to the congruence $g^{sk} \equiv 1 \pmod p$. If it holds, 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 3.3 *Let $n = rq + 1$ be a Carmichael number and let $p = rs + 1$ be a prime divisor of n. Then for any integers a and t we have*

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

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 3.2 to calculate the inner sum. Going from there this sum is always zero modulo p, except for the case when $r \mid n-j+t-1$, in other words when $j \equiv t \pmod{r}$. In this case the value of the sum, according to the lemma 3.2, 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 3.2 once again to calculate the value of both sums. The first one is always zero, except for the case when $r \mid t$, having value r in that case. The second sum is always zero, except for the case when $r \mid t-1$, or $t \equiv 1 \pmod r$, having value r in that case. Summing up what we have learned so far we have

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

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

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

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. ■

Now we are ready to prove the theorem 3.1. 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 :

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

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 3.3 we get that

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

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

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

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

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

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 3.1 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.

Chapter 4

Sophie-Germain primes

Another way of looking at the result from the previous chapter is that we have shown in the case of $r \neq 1$ and $r \mid n-1$, that there are infinitely many composite numbers n for which $T(a,n,r)$ holds. This corresponds to the Agrawal's conjecture which is explicitly saying that this is ok when $r \mid n^2-1$. The question we want to ask now is whether it will help when we restrict the parameters in such a way that $r \nmid n-1$. Will there still be an infinite set of composite numbers n satisfying the congruence ?

We will use simple choices of $r = 4$ and $a = -1$ to show that the situation seems to be similar when $r \mid n+1$. First, let us start with an equivalent characterization of the congruence $T(-1,n,4)$ which will be easier to work with.

Theorem 4.1 *Let n be an integer. 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 :

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

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 the 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

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

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). ■

For the concrete choices of parameters that we have made we no longer have to deal with polynomial congruence, which gives us higher chances of manipulating it successfully. One observation that is quite simple to make, is that by squaring the congruences from 4.1 we immediately see that for a composite number n to satisfy them, it has to be a base-2 Fermat's pseudoprime. Therefore we were able to simply use the existing records of pseudoprimes (up to 10^{15} collected William Galway – see [7]) to give us a feeling of 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 we search for. The next question we want to 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 are 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. However, there are some heuristic arguments and estimations about the expected count of these numbers. 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 are 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 (for more properties see [16]).

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. [5]), 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 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 a number for which the congruence holds, but $r \nmid n - 1$, in fact $r \mid n + 1$, and it seems very probable (based on the mentioned conjectures) that in this case we have infinitely many of them.

Chapter 5

Lenstra-Pomerance heuristic

If we combine the results from the previous two chapters, we see that there seem to be infinite sequences of composite numbers n satisfying the congruence $T(-1, n, r)$ in the case when $r \mid n^2 - 1$. This is a good reason for having this condition in the formulation of the Agrawal's conjecture, but it is not clear whether it covers all the cases. In fact, the scientific community in the area of the number theory researched this problem and formulated several notes (see [12]) 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 5.1 (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 in article [13] 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 auxiliary 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 5.1 *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*

$$(x-1)^{\rho(n)+1} \equiv x-1 \pmod{x^5-1, n} \tag{5.1}$$

The number $\rho(n)$ represents a multiplicative order of the element $x-1$. First, let us show that the definition is correct and the number $\rho(n)$ actually exists in all cases.

Lemma 5.1 *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 $q(x) = x^4 + x^3 + x^2 + x + 1$. We have

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

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

$$p(x) \cdot (x-1) \equiv 1 - aq(x) \pmod{x^5-1, n} \tag{5.2}$$

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

$$q(x) \cdot (x-1) \equiv 0 \pmod{x^5-1, n} \tag{5.3}$$

Putting them together we have

$$\begin{aligned} p(x)\cdot(x-1)^2 = p(x)\cdot(x-1)\cdot(x-1) \equiv \\ (1-aq(x))\cdot(x-1) = x-1-aq(x)\cdot(x-1) \equiv \\ x-1-a\cdot 0 = x-1 \pmod{x^5-1, n} \end{aligned} \tag{5.4}$$

So we see that $p(x)$ really can be used, in a limited way, as an inverse of $x-1$. Now we will come to the proof of the lemma itself. Because there are only finitely many residue classes modulo x^5-1, there has to be a pair of exponents $k \neq l$ for which

$$(x-1)^k \equiv (x-1)^l \pmod{x^5-1, n} \tag{5.5}$$

If $k = 1$ or $l = 1$, we are already done with the proof. Therefore let us assume, without the loss of generality that $1 < k < l$. To conclude the proof it is enough to multiply the congruence (5.5) by the polynomial $p(x)^{k-1}$ and repeatedly use the relationship (5.4), which gives us

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

and we have found the $r = l-k+1$ we were looking for. ■

Lemma 5.2 *Let k, l be any integers and let ρ be the function we have defined above. Then the congruence $(x-1)^k \equiv (x-1)^l \pmod{x^5-1, n}$ holds if and only if $k \equiv l \pmod{\rho(n)}$ holds.*

Proof The first implication is trivial, it results from the definition of $\rho(n)$. In the other direction we can without loss of generality assume that $k < l$, because in the case $k = l$ there is not much to prove. At the end of the previous proof we have shown that having the congruence (5.5) we know that

$$x-1 \equiv (x-1)^{l-k+1} \pmod{x^5-1, n} \tag{5.6}$$

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 the property (5.1), telling us how often 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. ■

Lemma 5.3 *Let n be an integer for which $(n,5)=1$ and ρ the function defined above. If there exists $\lambda_i(n)$, $i \in \{2,3,4\}$ 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 $\lambda_3(n)^3 \equiv \lambda_2(n) \pmod{\rho(n)}$. In fact, the existence of $\lambda_2(n)$ or $\lambda_3(n)$ implies the existence of the remaining two.

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 5.2 the first congruence we wanted to prove : $\lambda_2(n)^2 \equiv \lambda_4(n) \pmod{\rho(n)}$. The remaining congruences can be obtained in a similar way. ■

Lemma 5.4 *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 5.2). 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 5.3. ■

Now we are ready to prove the Lenstra-Pomerance theorem. We will include the case of $k \equiv 3 \pmod 4$, as stated in the theorem, which solves the exercise proposed by authors of the original proof.

Proof of the theorem 5.1 First, let us 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

$$(x-1)^n \equiv x^3 - 1 \pmod{x^5-1, p_i} \tag{5.7}$$

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

$$(x-1)^{p_i} \equiv x^3 - 1 \pmod{x^5-1, p_i} \tag{5.8}$$

According to the lemma 5.2, congruence (5.7) is equivalent to the relationship

$$n \equiv p_i \pmod{\rho(p_i)} \tag{5.9}$$

Moreover, according to the theorem 5.4 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 (5.9), a following stronger one

$$n \equiv p_i \pmod{10(p_i^2-1)} \tag{5.10}$$

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 is 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 prove the original congruence (5.10) 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

$$(x-1)^n \equiv x^2 - 1 \pmod{x^5-1, p_i} \tag{5.11}$$

Nothing has changed with respect to the congruences (5.8) and once again we can get from the lemma 5.4 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 5.3, 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

$$n \equiv p_i^3 \pmod{\rho(p_i)} \tag{5.12}$$

Using the lemma 5.4 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. ■

Although the theorem shows us that a set of properties identifies the counterexample to the Agrawal's conjecture, it is not clear whether there is any number that could really satisfy all of them. In the next chapter we will show some possible ways to search for the counterexample that could help us find it, if it exists at all.

Chapter 6

Search for counterexample

In the previous chapter we have provided an alternative proof to the theorem of Lenstra and Pomerance which states conditions sufficient for finding a counterexample for the Agrawal's conjecture. Looking at the proof it seems 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), a way to test the conjecture directly.

Lemma 6.1 *Let m and n be any integers such that $\lambda_{n \bmod 5}(m)$ exists. Then the congruence*

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

holds if and only if the congruence $n \equiv \lambda_{n \bmod 5}(m) \pmod{\rho(m)}$ holds.

Proof According to the lemma 5.2, the congruence $n \equiv \lambda_{n \bmod 5}(m)$ $\pmod{\rho(m)}$ is equivalent to the congruence

$$(x-1)^n \equiv (x-1)^{\lambda_{n \bmod 5}(m)} \pmod{x^5 - 1, m}$$

Now from the definition of the function $\lambda_{n \bmod 5}$ we know that

$$(x-1)^{\lambda_{n \bmod 5}(m)} \equiv x^{n \bmod 5} - 1 \pmod{x^5 - 1, m}$$

However, it is obvious that $x^{n \bmod 5} - 1 \equiv x^n - 1 \pmod{x^5 - 1, m}$, therefore we are done. ■

The lemma 6.1 gives us an interesting tool which we can use to test the AKS congruence in a different way. More specifically, let us consider a square-free number $n \equiv \pm 2 \pmod 5$ that is a product of prime numbers p_i with remainders 2 or 3 modulo 5. The reason for requiring the remainder of n is obvious – we are searching for a counterexample to the Agrawal's conjecture, therefore we need that $5 \nmid n^2 - 1$. We will also see why we need the remainders of prime divisors p_i to be as specified.

Because n is square-free, according to the Chinese remainder theorem the congruence $T(-1, n, 5)$ is equivalent to the system of congruences in a form

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

According to lemma 6.1, if the value of $\lambda_{n \bmod 5}(p_i)$ is defined for all of them, it is further equivalent to the system of congruences

$$n \equiv \lambda_{n \bmod 5}(p_i) \pmod{\rho(p_i)}$$

We know according to the lemma 5.3 that it is enough that one of the values $\lambda_2(p_i)$ and $\lambda_3(p_i)$ exists and the second one is not only guaranteed to exist but we also know how to compute it. For $p_i \equiv \pm 2 \pmod 5$ we always have at least one of these values – it is exactly the number p_i (this fact is implied directly by the congruence $T(-1, p_i, 5)$). For the calculation of the second and construction of the equivalent system of congruences we need the value of $\rho(p_i)$. Fortunately, from the theorem 5.4 we have $\rho(p_i) \mid 10(p_i^2 - 1)$, which enables us to search through the divisors and find such a number.

To search through the divisors of some number the well-known method can be used, which takes the prime factorization of the input and decreases the powers of all the prime factors by one until the point where it finds the negative result in all of the cases and it gives the product of decreased powers as a result. The algorithm is based on the fact that the number we are searching for divides all the numbers having the same property (5.1), so it does not really matter which way we choose to go and we always get the correct result.

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 satisfy 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_i for which $\rho(p_i)$ 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 chapters we will show another way of testing this congruence and its relationship to the Fibonacci numbers and Fermat pseudoprimes.

Chapter 7

Fibonacci & matrix approach

In this chapter we will speak about the relationship between the congruence $T(a,n,r)$ and linear recurrent sequences. We will be especially dealing with the case $T(-1,n,5)$, where this recurrent sequence will be the well-known Fibonacci's numbers and we will try to derive a generic way of constructing the sequences for higher values of r. What this means is that we will be searching for matrices defining sequences, and using these matrices to formulate an equivalent condition for our congruence. An inspiration for this approach was the article [9] released by the authors of AKS algorithm before they discovered the AKS test. They have shown the relationship between the congruence $T(-1,n,5)$ and Fibonacci pseudoprimes. We will come to the same result with a different set of tools and show how to generalize the way to obtain similar results for other prime r's.

We want to show that there is a relationship between our congruence, basically dealing with modular polynomial powers, and linear recurrent sequences, which can always be defined by a matrix. To help us transform these notions, we will use the following theorem.

Theorem 7.1 *Let $a(x) = a_0 + a_1x + \ldots + a_{r-1}x^{r-1}$, $b(x) = b_0 + b_1x + \ldots + b_{r-1}x^{r-1}$ be polynomials representing any of the residue classes modulo $(x^r - 1, n)$. Let us construct the matrices $\mathbf{A}$ and $\mathbf{B}$ taking the coefficients of polynomials $a(x)$ and $b(x)$ and arranging them in the following way*

$$\mathbf{A} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{r-1} \\ a_{r-1} & a_0 & \cdots & a_{r-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} b_0 & b_1 & \cdots & b_{r-1} \\ b_{r-1} & b_0 & \cdots & b_{r-2} \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \cdots & b_0 \end{pmatrix}$$

Let $c(x) = c_0 + c_1x + \ldots + c_{r-1}x^{r-1}$ be a polynomial which is the residue of the product $a(x)$ and $b(x)$, i.e. let $a(x) \cdot b(x) \equiv c(x) \pmod{x^r - 1, n}$. Then $\mathbf{A} \cdot \mathbf{B} \equiv \mathbf{C} \pmod{n}$, where

$$\mathbf{C} = \begin{pmatrix} c_0 & c_1 & \cdots & c_{r-1} \\ c_{r-1} & c_0 & \cdots & c_{r-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}$$

and by matrix congruence we mean the system of congruences comparing the entries with the same coordinates.

Proof Let us have a look at the way of constructing the matrices. In all cases the pattern is the same – the entry of the matrix with coordinates i, j is the coefficient with index $(j-i) \mod r$, i.e. it is true that $(\mathbf{C})_{i,j} = c_{(j-i) \mod r}$ for any $i, j \in \{1, 2, \ldots, r\}$ and analogically for matrices **A** and **B** we have $(\mathbf{A})_{i,j} = a_{(j-i) \mod r}$, $(\mathbf{B})_{i,j} = b_{(j-i) \mod r}$. Using this relationship we can construct the matrix **C** from the coefficients of polynomial $c(x) = a(x) \cdot b(x) \mod x^r - 1$. We have

$$c(x) = (a_0 + a_1x + \ldots + a_{r-1}x^{r-1}) \cdot (b_0 + b_1x + \ldots + b_{r-1}x^{r-1})$$

and by multiplying those terms we get

$$c(x) = \sum_{k=0}^{2r-2} \left[\left(\sum_{u+v=k} a_ub_v \right) x^k \right] \equiv \sum_{k=0}^{r-1} \left[\left(\sum_{u+v\equiv k \pmod{r}} a_ub_v \right) x^k \right] \pmod{x^r - 1}$$

where in the last step we use the fact that for $k \equiv k' \pmod{r}$ we have $x^k \equiv x^{k'} \pmod{x^r - 1}$. Using this congruence we can calculate the coefficients of polynomial $c(x)$ and putting the result into the formula for constructing the matrix **C** we obtain

$$(\mathbf{C})_{i,j} = \sum_{u+v\equiv j-i \pmod{r}} a_ub_v \tag{7.1}$$

Now let us construct the matrix $\mathbf{C}'$, this time directly as a product of matrices **A** and **B**, i.e. let $\mathbf{C}' = \mathbf{A} \cdot \mathbf{B}$. We will try to derive a formula for the entry of matrix $\mathbf{C}'$ with coordinates i, j using the usual way of matrix multiplication. We have

$$(\mathbf{C}')_{i,j} = (\mathbf{A} \cdot \mathbf{B})_{i,j} = \sum_{k=1}^{r} (\mathbf{A})_{i,k} \cdot (\mathbf{B})_{k,j} = \sum_{k=1}^{r} a_{(k-i) \mod r} \cdot b_{(j-k) \mod r} \quad (7.2)$$

In the set $\{1, 2, \dots, r\}^2$ there are exactly r solutions u, v of the congruence $u + v \equiv j - i \pmod r$, for example if we let the u run through the set $\{1, \dots, r\}$, the v is always determined in exactly one way.

Taking a look at the sum in the equation (7.1) we see that it contains exactly these solutions and for choices $k = 1, \dots, r$ in (7.2) we get exactly the same pairs, because the sum of indexes is always in the residue class $(j - i)$ mod r. With this we have shown that $\mathbf{C} \equiv \mathbf{C}' \pmod n$, which concludes the proof of the original theorem. ■

To illustrate the usage of the matrix approach, shown in the last theorem, we will stop by to take a look at the congruence $T(-1, n, 3)$. It is the simplest case where it makes sense to analyze anything, even though it is too simple to deal with the Agrawal's conjecture. The basic goal is to characterize the congruence using an equivalent statement, in this case in a form of a matrix congruence.

Theorem 7.2 *Let $n \geq 3$ be an integer, then $T(-1, n, 3)$ holds iff n is odd and*

a) $(-3)^{\frac{n-1}{2}} \equiv 1 \pmod n$*, for* $n \equiv 1 \pmod 6$

b) $(-3)^{\frac{n-1}{2}} \equiv -1 \pmod n$*, for* $n \equiv 5 \pmod 6$

c) *n is a power of 3, for* $n \equiv 3 \pmod 6$

Proof Because in the theorem 7.1 the arrangement of polynomial coefficients when put into the matrix is the same for input matrices $\mathbf{A}$ and $\mathbf{B}$, as for the output matrix $\mathbf{C}$, we can use this theorem to do an iterative multiplication, i.e. calculating powers of polynomials. Specifically, in the case of powers of polynomial $x - 1$, which we have in the congruence $T(-1, n, 3)$, we will be dealing with matrix

$$\mathbf{A} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

Before continuing, let us notice the interesting property of this matrix. When taking it to the third power, we get the matrix

$$\mathbf{A}^3 = \begin{pmatrix} 0 & 3 & -3 \\ -3 & 0 & 3 \\ 3 & -3 & 0 \end{pmatrix} = (-3) \cdot \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix} = (-3) \cdot \mathbf{A} \cdot \mathbf{P},$$

where

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

is a permutation matrix, commuting with $\mathbf{A}$ (we will use this fact later). Also notice that

$$\mathbf{P}^0 = \mathbf{I}, \quad \mathbf{P}^1 = \mathbf{P}, \quad \mathbf{P}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{P}^3 = \mathbf{I}, \quad \ldots$$

There is a direct mapping between coefficients of polynomial $(x-1)^n$ and the numbers in the first row of the matrix $\mathbf{A}^n$ (actually only the first row is the source of the information, as all the other rows are always shifted in the same way). In particular class of residues modulo 3, we are able to formulate the congruence $T(-1, n, 3)$ in the form of a matrix congruence. Let us go through all of those classes now.

a) When $n \equiv 1 \pmod 3$, the congruence looks like $x^n - 1 \equiv x - 1 \pmod{x^3 - 1}$, so the resulting matrix $\mathbf{A}^n$ should look exactly like the matrix $\mathbf{A}$. In other words, it has to be true that $\mathbf{A}^n \equiv \mathbf{A} \pmod n$. Let us first assume n is odd. Using the fact $\mathbf{A}^3 = (-3) \cdot \mathbf{A} \cdot \mathbf{P}$ iteratively and knowing that matrices $\mathbf{A}$ and $\mathbf{P}$ commute with one another we get $\mathbf{A}^n = (-3)^{\frac{n-1}{2}} \cdot \mathbf{P}^{\frac{n-1}{2}} \cdot \mathbf{A}$. Because $n \equiv 1 \pmod 3$, we have $\frac{n-1}{2} \equiv 0 \pmod 3$ and $\mathbf{P}^{\frac{n-1}{2}} = \mathbf{I}$, therefore $\mathbf{A}^n = (-3)^{\frac{n-1}{2}} \mathbf{A}$. That means congruence $\mathbf{A}^n \equiv \mathbf{A} \pmod n$ holds iff $(-3)^{\frac{n-1}{2}} \equiv 1 \pmod n$.

In case of even n we get $\mathbf{A}^n = (-3)^{\frac{n-2}{2}} \cdot \mathbf{P}^{\frac{n-2}{2}} \cdot \mathbf{A}^2$ and we have $\frac{n-2}{2} \equiv 1 \pmod 3$, therefore congruence $(-3)^{\frac{n-2}{2}} \cdot \mathbf{P} \cdot \mathbf{A}^2 \equiv \mathbf{A} \pmod n$ has to hold. However, this is not possible because the first two entries of the matrix at the left side are equal, which means it must be the same for the right side, i.e. that $1 \equiv -1 \pmod n$, which is of course a contradiction.

b) When $n \equiv 2 \pmod 3$ and n is odd, the congruence is $x^n - 1 \equiv x^2 - 1 \pmod{x^3 - 1}$. For the equivalent matrix congruence, according to the theorem 7.1, we have :

$$\mathbf{A}^n \equiv \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} = -\mathbf{P}^2 \cdot \mathbf{A} \pmod n$$

Once again taking the relationship $\mathbf{A}^3 = (-3) \cdot \mathbf{A} \cdot \mathbf{P}$ into account we get $\mathbf{A}^n = (-3)^{\frac{n-1}{2}} \cdot \mathbf{P}^{\frac{n-1}{2}} \cdot \mathbf{A}$, while in this case it is true that $\frac{n-1}{2} \equiv 2 \pmod 3$, so $\mathbf{P}^{\frac{n-1}{2}} = \mathbf{P}^2$. By substituting and comparing with the desired congruence we already see that this is equivalent to the congruence $(-3)^{\frac{n-1}{2}} \equiv -1 \pmod n$. Applying the same approach for n which is even we get to the contradiction.

c) In case of odd n divisible by 3, we have $x^n - 1 \equiv 0 \pmod{x^3 - 1}$, which makes the matrix congruence even simpler in this case, it looks like $\mathbf{A}^n \equiv \mathbf{0} \pmod n$, where $\mathbf{0}$ is a zero matrix. Analogically to the previous cases, we can derive the relationship $\mathbf{A}^n = (-3)^{\frac{n-1}{2}} \cdot \mathbf{P}^{\frac{n-1}{2}} \cdot \mathbf{A}$, which now implies (by comparing the coefficients) that it has to be true that $(-3)^{\frac{n-1}{2}} \equiv 0 \pmod n$. However, this congruence means that n has to be a power of 3, namely because a large power of 3 has to be divisible by n (on the other side, when n is a power of 3, it will not have a bigger exponent that $(-3)^{\frac{n-1}{2}}$ has, therefore the congruence will actually hold). In case of even n, we get exactly the same result (n has to be a power of 3), this time leading to contradiction, while a power of 3 is always odd.

We have analyzed all the residue classes, therefore the proof is done. ■

In the case of $r = 3$ we have reached our goal and found the equivalent characterization of $T(-1, n, 3)$. Actually, in this case we did not even need the matrix congruence, we were able to derive a simpler one containing powers of -3. As a direct consequence (by squaring the congruences) we can see that when $(n, 6) = 1$, in order to be an AKS pseudoprime n has to be a Fermat base-3 pseudoprime (although this is not a sufficient condition).

We will see a similar necessary condition in the case of $r = 5$, but let us now speak more generally and suppose we have any prime $r \geq 5$. In the same way as we have done for $r = 3$ we can construct a square matrix $\mathbf{A}$ of size r, corresponding to the polynomial $x - 1$ according to the transformation described in the theorem 7.1, i.e. $(\mathbf{A})_{i,j} = a_{(j-i) \bmod r}$, where $a_0 = -1$, $a_1 = 1$ and other coefficients are zeros. Let us denote by $\mathbf{J}$ the square matrix of the same size r whose members are all equal to 1, i.e. $(\mathbf{J})_{i,j} = 1$. It can be easily shown that $\mathbf{A} \cdot \mathbf{J} = \mathbf{J} \cdot \mathbf{A} = \mathbf{0}$, the reason for that is that multiplying by $\mathbf{J}$ computes the sum of rows or columns of the matrix $\mathbf{A}$, which are all zeros (there is exactly one member which is 1 and one which is -1 in each row and column of $\mathbf{A}$).

Now let us take the $(r-1)$-th power of matrix $\mathbf{A}$. We will show that one can write

$$\mathbf{A}^{r-1} = r \cdot \mathbf{B} + \mathbf{J} \tag{7.3}$$

for a suitable matrix $\mathbf{B}$. First of all, what is the intended use of this equation? We will use it for the computation of power of matrix $\mathbf{A}$ in the following way : Let us assume we know a better way to compute powers of $\mathbf{B}$ and let us try to compute the power $\mathbf{A}^n$. To do so, let us first write $n = (r-1)q + t$, where $0 < t \leq r - 1$ by Euclidean division, and use the equation (7.3) to write

$$\mathbf{A}^n = \mathbf{A}^{(r-1)q+t} = \mathbf{A}^t \cdot (r \cdot \mathbf{B} + \mathbf{J})^q = r^q \cdot \mathbf{A}^t \cdot \mathbf{B}^q \tag{7.4}$$

In the last step we have used the fact that all the members of the expansion containing matrix $\mathbf{J}$ will multiply to zero matrix with $\mathbf{A}$, therefore we can simply leave them out and only consider the first one. To see why this works also for those members where the matrix $\mathbf{J}$ is not on the left, let us just mention that $\mathbf{J} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{J} = -\frac{1}{r} \cdot \mathbf{J}^2$, as can be easily seen from (7.3).

Now, is there such an *integer* matrix $\mathbf{B}$ which satisfies (7.3)? We have shown that powers of the matrix $\mathbf{A}$ contain the coefficients of $(x-1)^\alpha \bmod (x^r - 1, n)$. Until we actually come to the r-th power and do not consider the members of the matrix modulo n, it contains directly the coefficients of $(x-1)^\alpha$. In other words, for our case of $\mathbf{A}^{r-1}$ what we have in the matrix is some permutation of numbers $(-1)^k\binom{r-1}{k}$ for $k \in \{0, \ldots, r-1\}$. It is therefore enough to show that

$$(-1)^k \binom{r-1}{k} \equiv 1 \pmod{r} \tag{7.5}$$

and we immediately have that $\mathbf{B}$ is an integer matrix. The equation (7.5) is in general only true for prime numbers and this is one of the reasons why we need r to be prime. To prove it, let us write

$$(-1)^k\binom{r-1}{k} = \frac{(r-1)^{\underline{k}}}{(-1)^{\underline{k}}}$$

It is obvious that both the numerator and the denominator of the fraction give the same residue when taken modulo r. Moreover, because r is prime, this residue will not be zero. Whatever this residue is, the fraction will be always congruent to one and that is what we need.

We have shown matrix $\mathbf{B}$ has integers as its members and we know we can use it also for calculating modular powers. The question that remains is whether to power the matrix $\mathbf{B}$ is in any way easier to handle or at least more suitable for other manipulations than that of matrix $\mathbf{A}$. Actually, we will not stop at the matrix $\mathbf{B}$, instead, we will use it to construct a smaller symmetric matrix, more suitable for powering and showing us the relationship with linear recurrent sequences, particularly Fibonacci's sequence in the case of $r = 5$. First let us mention some properties that we will need in order to achieve that.

We have shown in the theorem 7.1 that there is an equivalent transformation between residue classes modulo $(x^r - 1, n)$ and matrices of our form. More specifically we have shown that multiplying those matrices gives us the matrix assigned to the polynomial product. It is not hard to realize that it is the same in case of addition, in fact the proof would be much simpler in that case. Similarly, multiplying the matrix by a constant is equivalent to the mutliplying the polynomial by the same constant and looking at its matrix. What this means is that by doing these operations we still preserve the structure of the matrix and we can still speak about the polynomial assigned to it. This is exactly what we have done with the matrix $\mathbf{B} = \frac{1}{r}(\mathbf{A}^{r-1} - \mathbf{J})$, therefore we know that there are numbers $b_0, \ldots, b_{r-1}$ such that $(\mathbf{B})_{i,j} = b_{(j-i) \bmod r}$. Moreover, these numbers are not some random numbers, they are just the numbers from first row of the matrix $\mathbf{A}^{r-1}$, increased by 1 and divided by r. Because in the first row of matrix $\mathbf{A}^{r-1}$ we had exactly the binomial coefficients $(-1)^k\binom{r-1}{k}$, for which $(-1)^k\binom{r-1}{k} = (-1)^{r-1-k}\binom{r-1}{r-1-k}$, we now have

$$b_{r-1-k} = b_k \tag{7.6}$$

for all suitable k.

This means there is a kind of symmetry involved in the first row of the matrix and we know that all its rows are just cyclic shifts of the first one.

Although this does not mean that the matrix $\mathbf{B}$ itself is symmetric, it is very near to that. What it needs is just to do a suitable number of cyclic shifts of rows (or columns, which is in this case effectively the same). This suitable number is about a half of the matrix size, for prime $r \geq 3$ it would be $\frac{r+1}{2}$. Let us introduce a new name for our shifted matrix, let $\mathbf{C} = \mathbf{B} \cdot \mathbf{P}^{\frac{r+1}{2}}$, where $\mathbf{P}$ is the permutation matrix representing one cyclic shift.

The most important thing for us is that we do not lose any power by taking powers of $\mathbf{C}$ instead of $\mathbf{B}$. This means we should be able to calculate $\mathbf{B}^n$ from $\mathbf{C}^n$ quickly and easily. Fortunately, the permutation matrix did not indeed increase the complexity – it commutes with $\mathbf{B}$, it is true that

$$(\mathbf{B} \cdot \mathbf{P}^{\frac{r+1}{2}})_{i,j} = (\mathbf{P}^{\frac{r+1}{2}} \cdot \mathbf{B})_{i,j} = b_{(\frac{r-1}{2}+j-i) \mod r} \tag{7.7}$$

and we can identify any of its powers easily. This means the only work we have to do when we have got $\mathbf{C}^n$ is to calculate the exponent $(-n \cdot \frac{r+1}{2}) \mod r$ (of the inverse permutation matrix), do one matrix multiplication and we immediately have the desired result, i.e. the matrix $\mathbf{B}^n$.

Now let us see what the cyclic shift has actually brought us. First of all, putting (7.6) and (7.7) together we see that

Lemma 7.1 *Matrix* $\mathbf{C} = \mathbf{B} \cdot \mathbf{P}^{\frac{r+1}{2}}$ *is symmetric.*

Proof We know from (7.7) that

$$(\mathbf{C})_{i,j} = b_{(\frac{r-1}{2}+j-i) \mod r}$$

and

$$(\mathbf{C})_{j,i} = b_{(\frac{r-1}{2}+i-j) \mod r}$$

Without loss of generality let us assume that $j \geq i$ and consider two following cases :

a) In the case of $\frac{r-1}{2} \geq j - i$ we can write $(\mathbf{C})_{i,j} = b_{\frac{r-1}{2}+j-i}$ and $(\mathbf{C})_{j,i} = b_{\frac{r-1}{2}+i-j}$. Using the equation (7.6) we see that those are the same numbers and we are done.

b) In the case of $\frac{r-1}{2} < j - i$ we have $(\mathbf{C})_{i,j} = b_{j-i-\frac{r+1}{2}}$ and $(\mathbf{C})_{j,i} = b_{\frac{3r-1}{2}+i-j}$. Once again using (7.6) we see that these are the same. ■

Moreover, there is another symmetry still involved in the matrix $\mathbf{C}$:

Lemma 7.2 *Let us call $c_i^{(n)}$ the coefficients of polynomial assigned to the matrix $\mathbf{C}^n$, i.e. $c_i^{(n)} = (\mathbf{C}^n)_{1,i+1}$ and because of the structure of the matrix $\mathbf{C}^n$ also the other way $(\mathbf{C}^n)_{i,j} = c^{(n)}_{(j-i) \mod r}$. Then for any integers $n \geq 1$ and $i \in \{1, \dots, r-1\}$ it is true that $c^{(n)}_{r-i} = c^{(n)}_i$.*

Proof To improve the readability, let us write c_i instead of $c_i^{(1)}$ where appropriate. Before getting to the general case of n, as a first step let us show that $(\mathbf{C})_{1,r-i+1} = (\mathbf{C})_{1,i+1}$. The way is essentially the same as the previous proof. We will compare both values according to the (7.7), getting the desired equality $b_{(\frac{r-1}{2}+r-i) \mod r} = b_{(\frac{r-1}{2}+i) \mod r}$. To prove this, we consider the two cases $i \leq \frac{r-1}{2}$ and $i > \frac{r-1}{2}$, in each of them using (7.6) to conclude the proof. For the general case, let us write

$$(\mathbf{C}^n)_{1,r-i+1} = \sum_{k=1}^{r} (\mathbf{C}^{n-1})_{1,k} \cdot (\mathbf{C})_{k,r-i+1} = \sum_{k=1}^{r} (\mathbf{C}^{n-1})_{k,1} \cdot (\mathbf{C})_{r-i+1,k}$$

using the symmetry of matrices $\mathbf{C}$ and $\mathbf{C}^{n-1}$ (lemma 7.1). Further manipulations give us the following result

$$= \sum_{k=1}^{r} c^{(n-1)}_{(1-k) \mod r} \cdot c_{(k+i-1) \mod r} = c_0^{(n-1)} \cdot c_i + \sum_{k=2}^{r} c^{(n-1)}_{(1-k) \mod r} \cdot c_{(k+i-1) \mod r}$$

Now we change the order of summation, we will substitute $r+2-k$ for k, getting

$$= c_0^{(n-1)} \cdot c_i + \sum_{k=2}^{r} c^{(n-1)}_{(k-1) \mod r} \cdot c_{(i+1-k) \mod r} = \sum_{k=1}^{r} c^{(n-1)}_{(k-1) \mod r} \cdot c_{(i+1-k) \mod r}$$

and as a last step we get back to the matrices

$$= \sum_{k=1}^{r} (\mathbf{C}^{n-1})_{1,k} \cdot (\mathbf{C})_{k,i+1} = (\mathbf{C}^n)_{1,i+1}$$

which concludes the proof. ■

As a direct consequence of the previous lemma we have that

$$c^{(n)}_{-i \mod r} = c^{(n)}_{i \mod r} \tag{7.8}$$

which we will use extensively later. We have shown that the matrix $\mathbf{C}$ has some nice properties and symmetries, but we would like to use these symmetries to make it easier to calculate its powers. The next step of transforming the matrix will be the last one, giving us a matrix of less than half the size of $\mathbf{C}$ (exactly $\frac{r-1}{2}$), which will still be symmetric and we can use it to calculate powers effectively. We will call it the matrix $\mathbf{R}$ and define it in the following way :

$$(\mathbf{R})_{i,j} = (-1)^{i+j} \cdot \left(c_{(j-i) \mod r} - c_{(i+j) \mod r}\right) \tag{7.9}$$

Before progressing any further, let us have a look at the case $r = 5$ and the matrices we have constructed so far. We have started with the

$$\mathbf{A} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix} \text{ and } \mathbf{B} = \begin{pmatrix} 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 \end{pmatrix}$$

further using permutation matrix

$$\mathbf{P}^3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \text{ to get } \mathbf{C} = \begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 1 \end{pmatrix}$$

and ended up with

$$\mathbf{R} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

In this case the matrix $\mathbf{R}$ is the well-known Fibonacci matrix, we have

$$\mathbf{R}^n = \begin{pmatrix} f_{2n-1} & f_{2n} \\ f_{2n} & f_{2n+1} \end{pmatrix} \tag{7.10}$$

where f_n is the n-th Fibonacci number (starting with $f_0 = 0$, $f_1 = 1$). This means that if we will successfully reach our goal, we can calculate Fibonacci numbers instead of powering polynomials in the case of $r = 5$.

After reviewing what we will gain, let us continue with the most important question which we have to ask once again – is the transformation from the $\mathbf{C}$

to $\mathbf{R}$ reversible in the sense that we can easily calculate $\mathbf{C}^n$ from $\mathbf{R}^n$? Here it is not so obvious even in the simplest case $n = 1$. However, it is enough to realize two things :

a) Thanks to the lemma 7.2 we know that the source of the information in the matrix $\mathbf{C}^n$ is basically just the half of the first row, i.e. the numbers $c_i^{(n)}$ for $i \in \{0, \ldots, \frac{r-1}{2}\}$, all the other members depend on them and can be calculated from them.

b) We do not actually need to reconstruct the matrix $\mathbf{C}^n$, it is quite enough to get to some matrix $\mathbf{C}^n + m \cdot \mathbf{J}$ for any integer m. The reason is that in the reverse transformation we will get $\mathbf{B}^n + m \cdot \mathbf{J}$ instead of $\mathbf{B}^n$, which is still acceptable because in (7.4) the additional multiple of $\mathbf{J}$ does not make any difference – it will get lost when multiplied by $\mathbf{A}$ anyway. Because the matrix $\mathbf{R}$ only contains the differences between the coefficients of $\mathbf{C}$, we can fix one of them to any number we like (this will only shift all of them by some constant m which we might not know but also do not need to know).

Using these two facts we can put $c_0 := 0$ and calculate the rest of the coefficients from the diagonal of $\mathbf{R}$ using the formula (7.9), constructing the (shifted) matrix $\mathbf{C}$ once again. This works for the matrix $\mathbf{R}$, but what about its powers ? The following lemma shows us that it is exactly the same in the case of $\mathbf{R}^n$.

Lemma 7.3 *For any integer $n \geq 1$ and integers i, j from the set $\{1, \ldots, \frac{r-1}{2}\}$ it is true that*

$$(\mathbf{R}^n)_{i,j} = (-1)^{i+j} \cdot \left(c^{(n)}_{(j-i) \mod r} - c^{(n)}_{(i+j) \mod r} \right)$$

Proof To provide a proof, we will use the mathematical induction. The first step ($n = 1$) just states the definition of the matrix $\mathbf{R}$. For the second step let us write

$$(\mathbf{R}^n)_{i,j} = \sum_{k=1}^{\frac{r-1}{2}} (\mathbf{R}^{n-1})_{i,k} \cdot (\mathbf{R})_{k,j}$$

Using the induction hypothesis we have

$$= \sum_{k=1}^{\frac{r-1}{2}} (-1)^{i+k} \left(c^{(n-1)}_{(k-i) \mod r} - c^{(n-1)}_{(i+k) \mod r} \right) \cdot (-1)^{k+j} \left(c_{(j-k) \mod r} - c_{(k+j) \mod r} \right)$$

$$= (-1)^{i+j} \cdot \sum_{k=1}^{\frac{r-1}{2}} \left(c^{(n-1)}_{(k-i) \mod r} - c^{(n-1)}_{(i+k) \mod r} \right) \cdot \left(c_{(j-k) \mod r} - c_{(k+j) \mod r} \right)$$

Now we split the sum by multiplying out the second factor :

$$= (-1)^{i+j} \cdot \left(\sum_{k=1}^{\frac{r-1}{2}} c_{(j-k) \mod r} \cdot \left(c^{(n-1)}_{(k-i) \mod r} - c^{(n-1)}_{(i+k) \mod r} \right) + \sum_{k=1}^{\frac{r-1}{2}} c_{(k+j) \mod r} \cdot \left(c^{(n-1)}_{(i+k) \mod r} - c^{(n-1)}_{(k-i) \mod r} \right) \right)$$

Now, if we replace k for $-k$ in the second sum and use (7.8) to adjust the indices, we are actually able to merge those sums together again, getting further to

$$= (-1)^{i+j} \sum_{k=1}^{r-1} c_{(j-k) \mod r} \cdot \left(c^{(n-1)}_{(k-i) \mod r} - c^{(n-1)}_{(k+i) \mod r} \right)$$

As a next step we notice from (7.8) that for $k = 0$ the terms of second factor are equal, therefore the whole summand is in this case zero. This means we are free to include the $k = 0$ into the summation range. Moreover, we will do a substitution $k := (j + 1 - k) \mod r$, basically shifting the summation range modulo r, something that we can do because k is only used in modular expressions in the summands. We get

$$= (-1)^{i+j} \sum_{k=0}^{r-1} c_{(k-1) \mod r} \cdot \left(c^{(n-1)}_{(j+1-i-k) \mod r} - c^{(n-1)}_{(j+1+i-k) \mod r} \right)$$

Another shift of summation range by 1 (without changing the expression) and multiplying out the second factor gives us

$$= (-1)^{i+j} \left(\sum_{k=1}^{r} c_{(k-1) \mod r} \cdot c^{(n-1)}_{(j+1-i-k) \mod r} + \sum_{k=1}^{r} c_{(k-1) \mod r} \cdot c^{(n-1)}_{(j+1+i-k) \mod r} \right)$$

To conclude the proof, we just need to read the last expression in the right way :

$$= (-1)^{i+j}\left(\sum_{k=1}^{r}(\mathbf{C})_{1,k}\cdot(\mathbf{C}^{n-1})_{k,j-i+1}+\sum_{k=1}^{r}(\mathbf{C})_{1,k}\cdot(\mathbf{C}^{n-1})_{k,j+i+1}\right)$$

which is of course

$$= (-1)^{i+j}\cdot\left(c^{(n)}_{(j-i)\mod r}-c^{(n)}_{(i+j)\mod r}\right)$$

■

We have chosen the matrix $\mathbf{R}$ in such a way that the pattern of its dependency to the matrix $\mathbf{C}$ holds also for their powers, therefore the transformation is reversible where we need it. This gives us a generic way to calculate the powers of $\mathbf{A}$, and to use them to test the congruence $T(-1,n,r)$. The time complexity does not improve drastically by this, actually we have only made a constant speed-up relying on the fact that we have precomputed some matrices needed for a particular r. However, what is interesting about this result is that we can use it to derive some interesting properties of numbers satisfying the congruence $T(-1,n,r)$. As a demonstration of this approach, we will in the rest of this chapter deal with the case $r=5$ and show the already suggested connection to the Fibonacci numbers.

The method we have designed gives us a technique of constructing properties equivalent to the congruence $T(-1,n,r)$. The way to get to them is to start with the congruence $\mathbf{A}^n \equiv \mathbf{A}' \pmod{n}$ for our matrix $\mathbf{A}$ assigned to the polynomial $x-1$ and the matrix $\mathbf{A}'$ assigned to the polynomial $x^{n \mod r}-1$. From this congruence we follow the path to the powers of matrices $\mathbf{B}$, $\mathbf{C}$ and $\mathbf{R}$, returning back to construct the equivalent matrix congruence for the power of the matrix $\mathbf{R}$.

As an example, let us consider $n \equiv 3 \pmod{20}$ and $r=5$. In this case

$$\mathbf{A}' = \begin{pmatrix} -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

From (7.4) we have that $\mathbf{A}^n = 5^{\frac{n-3}{4}}\cdot\mathbf{A}^3\cdot\mathbf{B}^{\frac{n-3}{4}}$. When we continue to the matrix $\mathbf{C}$, we realize that $\mathbf{C}^{\frac{n-3}{4}} = (\mathbf{B}\cdot\mathbf{P}^3)^{\frac{n-3}{4}} = \mathbf{B}^{\frac{n-3}{4}}$, as $\frac{n-3}{4} \equiv 0 \pmod{5}$

and therefore $\mathbf{P}^{\frac{n-3}{4}} = \mathbf{I}$. Now let us denote the diagonal entries of $\mathbf{R}^{\frac{n-3}{4}}$ by a and b. Putting $c_0 := 0$ we get the (possibly shifted) matrix

$$\mathbf{C}^{\frac{n-3}{4}} + k \cdot \mathbf{J} = \begin{pmatrix} 0 & -b & -a & -a & -b \\ -b & 0 & -b & -a & -a \\ -a & -b & 0 & -b & -a \\ -a & -a & -b & 0 & -b \\ -b & -a & -a & -b & 0 \end{pmatrix}$$

Comparing the entries of the product $5^{\frac{n-3}{4}} \cdot \mathbf{A}^3 \cdot \mathbf{C}^{\frac{n-3}{4}}$ and the matrix $\mathbf{A}'$ we finally get to the system of congruences

$$\begin{aligned} 5^{\frac{n-3}{4}}(a-4b) &\equiv 0 \pmod{n} \\ 5^{\frac{n-3}{4}}(2a-3b) &\equiv 1 \pmod{n} \end{aligned}$$

giving us the resulting equivalent congruence

$$5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \begin{pmatrix} -4 & 3 \\ 3 & -1 \end{pmatrix} \pmod{n}$$

Progressing the same way for the rest of the residue classes we learn that in cases where $(n,4) > 1$ and $5 \nmid n$ we get directly to the contradiction and in all other cases we can specify the equivalent congruences. This gives us the following result :

Theorem 7.3 *$T(-1,n,5)$ holds iff $(n,4) = 1$ or $5 \mid n$ and*

a) $5^{\frac{n}{4}} \cdot \mathbf{R}^{\frac{n-4}{4}} \equiv \mathbf{0} \pmod{n}$ *for* $n \equiv 0 \pmod{20}$

b) $5^{\frac{n-1}{4}} \cdot \mathbf{R}^{\frac{n-1}{4}} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}$ *for* $n \equiv 1 \pmod{20}$

c) $5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \begin{pmatrix} -4 & 3 \\ 3 & -1 \end{pmatrix} \pmod{n}$ *for* $n \equiv 3 \pmod{20}$

d) $5^{\frac{n-1}{4}} \cdot \mathbf{R}^{\frac{n-1}{4}} \equiv \mathbf{0} \pmod{n}$ *for* $n \equiv 5 \pmod{20}$

e) $5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \begin{pmatrix} 4 & -3 \\ -3 & 1 \end{pmatrix} \pmod{n}$ *for* $n \equiv 7 \pmod{20}$

f) $5^{\frac{n-1}{4}} \cdot \mathbf{R}^{\frac{n-1}{4}} \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \pmod{n}$ *for* $n \equiv 9 \pmod{20}$

g) $5^{\frac{n-2}{4}} \cdot \mathbf{R}^{\frac{n-2}{4}} \equiv \mathbf{0} \pmod{n}$ *for* $n \equiv 10 \pmod{20}$

h) $5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \begin{pmatrix} -3 & 1 \\ 1 & -2 \end{pmatrix} \pmod{n}$ *for* $n \equiv 11 \pmod{20}$

i) $5^{\frac{n-1}{4}} \cdot \mathbf{R}^{\frac{n-1}{4}} \equiv \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix} \pmod{n}$ *for* $n \equiv 13 \pmod{20}$

j) $5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \mathbf{0} \pmod{n}$ *for* $n \equiv 15 \pmod{20}$

k) $5^{\frac{n-1}{4}} \cdot \mathbf{R}^{\frac{n-1}{4}} \equiv \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \pmod{n}$ *for* $n \equiv 17 \pmod{20}$

l) $5^{\frac{n+1}{4}} \cdot \mathbf{R}^{\frac{n-3}{4}} \equiv \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix} \pmod{n}$ *for* $n \equiv 19 \pmod{20}$

Using the equation (7.10) we can read directly from the matrix congruences which we have just proved the congruences involving Fibonacci numbers. This gives us the possibility of proving the following theorem, a very useful tool for recognizing AKS pseudoprimes.

Theorem 7.4 *Let* n *be a composite integer, for which* $(n, 10) = 1$ *and assume that* $T(-1, n, 5)$ *holds. Then* n *is a Fibonacci pseudoprime and a base-*5 *Fermat pseudoprime at the same time.*

Proof Simply by taking the theorem 7.3 and squaring all the congruences, in some cases multiplying them by the matrix $\mathbf{R}$, in some cases canceling out the number 5 (which we can do as $(n, 5) = 1$) we always get to the congruence

$$5^{\frac{n-1}{2}} \cdot \mathbf{R}^{\frac{n-1}{2}} \equiv \mathbf{I} \pmod{n} \tag{7.11}$$

in the case of $n \equiv 1, 4 \pmod{5}$ and to the congruence

$$5^{\frac{n-1}{2}} \cdot \mathbf{R}^{\frac{n+1}{2}} \equiv \mathbf{I} \pmod{n} \tag{7.12}$$

in the case of $n \equiv 2, 3 \pmod{5}$. Now comparing with the (7.10) we immediately see that $5^{\frac{n-1}{2}} \cdot f_{n-1} \equiv 0 \pmod{n}$ or in the second case

$5^{\frac{n-1}{2}} \cdot f_{n+1} \equiv 0 \pmod{n}$. However, because $(n, 5) = 1$, this means that $f_{n-1} \equiv 0 \pmod{n}$ or $f_{n+1} \equiv 0 \pmod{n}$ respectively, and that is exactly what we wanted to prove in the first place. For the second part of our proof we will use the determinant of the matrix $\mathbf{R}$. Its value is exactly 1, that means also any power of $\mathbf{R}$ has a determinant of 1. What this means is that the following equation is true

$$f_{2k-1} \cdot f_{2k+1} = f_{2k}^2 + 1 \tag{7.13}$$

for any k. Now, comparing the entries of matrices in (7.11) we see that $5^{\frac{n-1}{2}} \cdot f_{n-2} \equiv 1 \pmod{n}$, as well as $5^{\frac{n-1}{2}} \cdot f_n \equiv 1 \pmod{n}$. Multiplying these together and using (7.13) we see that $5^{n-1} \equiv 1 \pmod{n}$, i.e. the number n is a base-5 Fermat pseudoprime. Analogically comparing the entries of matrices in (7.12) we have $5^{\frac{n-1}{2}} \cdot f_n \equiv 1 \pmod{n}$, as well as $5^{\frac{n-1}{2}} \cdot f_{n+2} \equiv 1 \pmod{n}$, which multiplies to $5^{n-1} \equiv 1 \pmod{n}$ when taking (7.13) into consideration. ■

The last theorem showed us that when searching for AKS pseudoprimes for $r = 5$, we can start with Fibonacci pseudoprimes and base-5 Fermat pseudoprimes, which means we can further investigate their properties and maybe derive a faster method than we would have just for AKS pseudoprimes. Unfortunately, we have used congruence squaring and multiplying in the proof and therefore lost the equivalence, which means that finding such a number n that $n \equiv 2, 3 \pmod{5}$ and n is Fibonacci pseudoprime and base-5 pseudoprime at the same time may not necessarily bring us to the counterexample for the Agrawal's conjecture, on the other way if there is no such number we know that at least for $r = 5$ we do not have to search any longer.

Chapter 8

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 [9], 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 [13] authors provide a proof for the theorem 5.1, 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, results of which 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 provides them.

As a part of a school project in the course of computer algebra, the author of this work has 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 [8] and [18]) 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 5.1, 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 6. 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 [12]). 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

For $r = 5$ we have another set to search in, because as we have shown in chapter 7, congruence $T(-1, n, 5)$ implies that n is a base-5 Fermat pseudoprime and a Fibonacci pseudoprime at the same time. Actually, even these loosened conditions are not satisfied at the same time for small numbers. We have done a search in the set of Fibonacci pseudoprimes up to $2 \cdot 10^9$ (using records from Anderson, see [2]), where we have found only 25 base-5 Fermat pseudoprimes with $n \equiv 4 \pmod 5$. There were none such pseudoprimes for residue classes 2 and 3, but on the other hand there were 782 base-5 pseudoprimes in the residue class 1, of which 264 were actually AKS pseudoprimes.

Using Fibonacci numbers and the result from chapter 7 we were able to try another approach for creating very large examples of numbers that could form a counterexample for Agrawal's conjecture. In this case we were working with loosened conditions, generating very big Fibonacci pseudoprimes and testing them for base-5 pseudoprimality. For the purpose of generating we have used a result from Lehmer, who has shown that if $p > 5$ is any prime number, then f_{2p}, i.e. the $(2p)-$th Fibonacci number, is a Fibonacci pseudoprime as well.

Although we have not made any significant discovery, we consider this and similar 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 9

Conclusion

A couple of years ago the problem of primes recognition was still not known to belong into the polynomial class of algorithms. Even then we already had a lot of algorithms for primality testing, using very sophisticated ideas and some of them were really fast. Each of them had some flaw – from some small error probability, depending on an unproved conjecture to being polynomial only on some inputs or being slightly more than polynomial on all of them.

Although these algorithms were not perfect from a strict point of view, some of them 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 also an elegant and easy to understand 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 thesis 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 started with an overview of primality testing algorithms including the AKS algorithm in order to give the reader some feeling about it and prepare some necessary terms. We presented the Agrawal's conjecture as a central point of interest for the following story. As a next step 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 difference.

The main idea of these chapters was to explore the choices of the parameters in the AKS congruence and in some way show the reason for the formulation of the Agrawal's conjecture. In addition to the Carmichael numbers, we have shown that Mersenne numbers of special form, which existence is guaranteed by the Sophie-Germain prime conjecture, may possibly represent an infinite sequence of numbers making troubles to the AKS congruence.

We have then presented the Lenstra-Pomerance heuristic as an argument against Agrawal's conjecture, 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 $r = 5$.

In the next chapter, we have developed tools involving matrix exponentiation and transformations into smaller symmetric matrices of recurrent sequences, giving us yet another way of testing the congruence, in this case more generic one which works also without knowing the prime factorization of the input or putting any restrictions to it. More importantly, we have generalized the previously known way of expressing the relationship between the recurrent sequences (e.g. Fibonacci numbers) and the AKS congruence.

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

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

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

[4] Bernstein D.: *Distinguishing prime numbers from composite numbers: the state of the art in 2004.* (unpublished) http://cr.yp.to/papers.html#prime2004

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Abstract

In the text we investigate the AKS 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. We show that for some choices of parameter r, the Carmichael numbers are passing for all choices of the parameter a, providing two different proofs of this fact. We demonstrate that if the widely believed Sophie-Germain primes conjecture is true, there is another infinite class of composite numbers satisfying the congruence. Further we present the heuristic of Lenstra and Pomerance as a potential way of the disproof of the Agrawal's conjecture. We give an alternative proof of it, along with the algorithm derived from a method used in this proof. We use the matrix approach to generalize a known result about the relationship between Fibonacci pseudoprimes and AKS congruence. Finally we present the empiric results contributing to the intuition about the size and existence of the counterexample to the Agrawal's conjecture.

V práci sa zaoberáme testom AKS, voľbou parametrov v kongruencii používanej v tomto teste a hypotézou Agrawala vedúcou k jeho urýchleniu. Ukazujeme, že pri niektorých voľbách parametra r prechádzajú testom Carmichaelove čísla bez ohľadu na voľbu parametra a a tento fakt dokazujeme dvoma rôznymi spôsobmi. Demonštrujeme, že v prípade platnosti všeobecne akceptovanej hypotézy o Sophie-Germainovej prvočíslach vieme nájsť ďalšiu nekonečnú triedu zložených čísel vyhovujúcich kongruencii. Ďalej predstavujeme heuristiku Lenstru a Pomerance-a ako možný spôsob vyvrátenia Agrawalovej hypotézy, spolu s alternatívnym dôkazom, ako aj algoritmom získaným z metódy použitej pri dôkaze. Používame prístup využívajúci matice na zovšeobecnenie známeho výsledku o súvislosti medzi Fibonacciho pseudoprvočíslami a kongruenciou z algoritmu AKS. Nakoniec predstavujeme empirické výsledky prispievajúce k intuitícii o veľkosti a existencii protipríkladu na Agrawalovu hypotézu.