Some slides for Mini-project in Algebra (2)

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

27-10-2010

What are the exercises in the problemkatalog about?:

- Opgave 1: Estimates the number of iterations in the Euclidean algorithm
- Opgave 2 and Opgave 3: Lemmas for proving other results.

Problems for multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$:

- Opgave 4: We prove that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$. We are using this when we are working with ElGamal.
- Opgave 5: We prove that $(\mathbb{Z}/p^2\mathbb{Z})^*$ is also a cyclic group. We will use it later (in opgave 7).

Finding astronomical prime numbers

We will recall some theory we saw in Lecture 4: For RSA and ElGamal we need to have a huge prime. But, how do we know if a number is prime or not?

Fermat's little theorem

Let p be a prime number and a an integer with $gcd(a, p) = 1$. Then

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

Consider $N \in \mathbb{N}$ odd. Is it prime?:

- Choose $0 < a < N$ randomly
- Compute $\gcd(a, N)$. If it is different from 1, then N is not prime.
- If $\gcd(a, N) = 1$, then compute $[a^{N-1}]_N$. If $[a^{N-1}]_N \neq [1]_N$ then it is not prime.
- If $[a^{N-1}]_N = [1]_N$ then we are not sure. It can be prime or not. Therefore, we start again for another value for a.

Definition 1.9.3

Let N be a composite natural number and a an integer. Then N is called a pseudoprime relative to the base a if

$$a^{N-1} \equiv 1 (\mathrm{mod}\ N)$$

We wonder: What is the probability of finding a "helpful" base a?, we see this in opgave 6:

- Opgave 6: If N is composite and there is a such that $[a^{N-1}]_N \neq [1]_N$, then the probability to find a basis b such that $[b^{N-1}]_N \neq [1]_N$ is $1/2$ (50%) (half of the elements in $(\mathbb{Z}/N\mathbb{Z})^*$).

So, this is nice. We repeat the previous algorithm k times, and therefore, given a composite number N, the probability to fail is: $(1/2)^k$. A small number for a not so large k.

But there is something that may happen...

Carmichel numbers (or pseudoprimes)

A Carmichel number is composite integer N such that the equation in Fermat's little theorem holds for every $a \in (\mathbb{Z}/N\mathbb{Z})^*$)

There are infinity Carmichael numbers, the first one is $561 = 3 \cdot 11 \cdot 17$. But exercise 7 tell us something about them:

- Opgave 6a: If N is divisible by p^2 for some prime p, then it cannot be a Carmichael number.

This is nice, but it is still risky. How do we improve it?

Lemma 1.9.4

Let p be a prime number and $x \in \mathbb{Z}$. If $x^2 \equiv 1 (\mathrm{mod}\ p)$ then $x \equiv 1 (\mathrm{mod}\ p)$ or $x \equiv -1 (\mathrm{mod}\ p)$

Proof:

- $p \mid (x^2 - 1) = (x + 1)(x - 1)$.
- Then $p \mid (x + 1)$ or $p \mid (x - 1)$

Therefore, if we have

$$a^{N-1} \equiv 1 (\mathrm{mod}\ N)$$

we "extract roots" of this congruence until we have

$$a^{\frac{N-1}{2^s}}$$

with $\frac{N-1}{2^s}$ odd and the previous proposition tell us that the first residue class we get other than 1 must be -1 if N is prime.

In practice one does this computation as in page 28 in [Lau] (it is a good idea that you read and understand the example for $N = 341$). You can include this in the project if you like. Thus:

An odd composite N is called a strong pseudoprime relative to the base a if either

$$a^q \equiv 1 (\mathrm{mod}\ N)$$

or there exists $i = 0, \ldots, k-1$ such that

$$a^{2^i q} \equiv -1 (\mathrm{mod}\ N),$$

where $N - 1 = 2^k q$ and $2 \nmid q$.

Proposition 1.9.6

Let p be an odd prime number and suppose that

$$p - 1 = 2^k q,$$

where $2 \nmid q$. If $a \in \mathbb{Z}$ and $gcd(a, p) = 1$ then either

$$a^q \equiv 1 (\mathrm{mod}\ p)$$

or there exists $i = 0, \ldots, k - 1$ such that

$$a^{2^i q} \equiv (\mathrm{mod}\ p).$$

The situation has improved, the probability of being unlucky performing this second test is lower than before. But, what is this probability?, that is, how many pseudoprimes are there? This is bounded by Rabin's result:

Theorem 1.9.7 (Rabin)

Suppose that $N > 4$ is an odd composite integer and let B be the number of bases a ($1 < a < N$) such that N is a strong pseudoprime relative to a. Then

$$B < \varphi(N)/4 \leq (N-1)/4$$

The rest of the exercises, 7–11, are the path of lemmas to the proof of this result.

- Opgave 8, opgave 9, opgave 10: They are lemmas for Opgave 7 and Opgave 11.
- Opgave 7: If $p^2|N$ for some prime p. It bounds the number of pseudoprimes (and therefore the number of strong pseudoprimes)
- Opgave 11: Bounds the number of strong pseudoprimes in the general case.

So, now, you can try to give the proof of Rabin's theorem. Try it to do it for $p^2|N$ for some prime p and then the general case. The computations are a little bit messy.

$$B < \frac{\text{Bound for Pseudoprimes}}{\text{Possible cases}}$$

The structure of the project SHOULD NOT be the description of the 3 cryptosystems + a sequence of exercises.

You should introduce the results from the Projektkatalog. In particular, the exercises with green color (1, 4, 6, 6a, 7, 11) should have a nice introduction.