

# Some slides for 6th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences  
Aalborg University  
Denmark

21-09-2011

You are welcome to use Maple for computations.

To get some help type in Maple:

- `>?mod`
- `>?isprime` (or `nextprime`)
- `>?ifactor`
- `>?igcdex`

Do not forget that we use  $\&\wedge$  to apply the repeated squaring algorithm in Maple. Type:

- `>185705890543 mod 37;`
- `>18&wedge5705890543 mod 37;`

- $N = p \cdot q$ ,  $p$  and  $q$  primes.
- $e$  a number for encryption,  $d$  a number for decryption.
- Public:  $N, e$ . Private:  $d$ .
- Message:  $X, 0 \leq X < N$ .
- Encryption:  $f(X) = [X^e]_N$   
 Decryption:  $g(X) = [X^d]_N$ .  
 $g(f(X)) = X$ .

How do we choose  $e$  and  $d$ ?

We know:

$$g(f(X)) = [[X^e]^d] = [X^{ed}] = X \text{ if and only if } X \equiv X^{ed} \pmod{N}$$

$$\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

Let  $X$  be any integer and  $k$  a natural number. Then

$$X^{k(p-1)(q-1)+1} \equiv X \pmod{N}$$

Proof:

- It is enough to prove that  $X^{k(p-1)(q-1)+1} \equiv X \pmod{p}$ .
- If  $p \mid x$ . Thus,  $[X]_p = 0 = [X^{k(p-1)(q-1)+1}]_p$ , we have  $X^{k(p-1)(q-1)+1} \equiv X \pmod{N}$ .
- If  $p \nmid x$ . Thus,  $\gcd(p, x) = 1$ , by Euler Theorem  $X^{\varphi(p)} = X^{p-1} \equiv 1 \pmod{p}$  and

$$X^{k(p-1)(q-1)} \equiv (X^{p-1})^{k(q-1)} \equiv 1 \pmod{p}$$

- Multiply the previous congruence with  $X$

# Encryption and decryption exponents



# Finding astronomical prime numbers

## Fermat's little theorem

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

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

## 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

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

- $\gcd(a, N) \neq 1 \Rightarrow N$  cannot be a pseudoprime relative to  $a$  (EX 1.41).
- Carmichael numbers (or pseudoprimes).

### Lemma 1.9.4

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

Proof:

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

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

$$a^q \equiv 1 \pmod{N}$$

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

$$a^{2^i q} \equiv -1 \pmod{N},$$

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

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

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

$$a^{2^i q} \equiv -1 \pmod{p}.$$

Proof:

- Let  $a_i = a^{2^i q}$ ,  $i = 0, \dots, k$ .
- By Fermat's th:  $a_k \equiv 1 \pmod{p}$  and  $a_{i+1} = a_i^2$ , for  $i = 0, \dots, k - 1$ .
- Therefore,  $a_0 \equiv 1 \pmod{p} \Leftrightarrow a_k \equiv 1 \pmod{p}$  for every  $i$ .

- Let  $a_i = a^{2^i q}, i = 0, \dots, k$ .
- By Fermat's th:  $a_k \equiv 1 \pmod{p}$  and  $a_{i+1} = a_i^2$ , for  $i = 0, \dots, k - 1$ .
- Therefore,  $a_0 \equiv 1 \pmod{p} \Leftrightarrow a_i \equiv 1 \pmod{p}$  for every  $i$ .
- If  $a_0 \not\equiv 1 \pmod{p}$ , then  $\exists a_i, i \geq 0$ , such that  $a_i \not\equiv 1 \pmod{p}$ .
- Let  $j$  be the largest index with this property.
- Since  $j < k$  and  $a_j^2 \equiv a_{j+1} \equiv 1 \pmod{p}$ , we get  $a_j \equiv -1 \pmod{p}$  (by previous lemma).

### 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

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