FOUNDATIONS OF COMPUTER SECURITY

Mathematical Background

Workbook

Editor: Carolin Hannusch, PhD

UNIVERSITY OF DEBRECEN
FACULTY OF INFORMATICS
2019

Preface

This workbook is mainly inteded to address students of Informatics Sciences. We give some mathematical background for the understanding of encryption and decryption. For more detailed algebraic knowledge one should consider literature about Group Theory and Ring Theory.

In the current workbook we give some examples and also provide exercises. Solutions of the exercises are given in the last chapter.

This work was supported by the construction EFOP-3.4.3-16-2016-00021. The project was supported by the European Union, co-financed by the European Social Fund.

Contents

Chapter 1

Linear Congruences

1.1 Introduction and Notation

Definition 1.1. *Let x and y be two integers. Then we say that x `divides` y if there exists an integer z, such that $y = x \cdot z$, where $\cdot$ denotes the usual multiplication.*
Notation: $x \mid y$

Definition 1.2. *Let x, y and z be arbitrary integers, i.e. $x, y, z \in \mathbb{Z}$. If $z \mid x - y$, then we say that x `is congruent to` y `modulo` z.*
Notation: $x \equiv y \mod z$

Corollary 1.3.

$$x \mid y \Leftrightarrow y \equiv 0 \mod x$$

Example 1.4.

- $17 \equiv 3 \mod 14$
- $5 \mid 20$, *thus* $20 \equiv 0 \mod 5$
- $26 \equiv 0 \mod 13$, *thus* $13 \mid 26$
- $123 \equiv 1 \mod 2$
- $123 \equiv 23 \mod 100$

1.2 Fast computation of powers

In this section we will see a first example for the use of congruences. The following method can be used in order to compute large powers fast.

The steps of the algorithm

Let us assume we want to compute n^k, where n and k are positive integers.

1. Write the power k as the sum of powers of 2 :

$$k = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_t}$$

2. Take the square of n and repeat this step according to the property

$$n^{2^{r+1}} = n^{2^r \cdot 2} = (n^{2^r})^2$$

3. We get the final result by

$$n^k = n^{2^{k_1}} \cdot n^{2^{k_2}} \cdot \ldots \cdot n^{2^{k_t}}$$

Example 1.5. *We want to compute* $3^{123} \mod 51$.
First, we write

$$123 = 2^6 + 2^5 + 2^4 + 2^3 + 2^1 + 2^0.$$

After that we compute

$$\begin{aligned}
3^{2^0} &\equiv 3 \mod 51 \\
3^{2^1} &\equiv 9 \mod 51 \\
3^{2^2} &\equiv 9 \cdot 9 \equiv 30 \mod 51 \\
3^{2^3} &\equiv 30 \cdot 30 \equiv 33 \mod 51 \\
3^{2^4} &\equiv 33 \cdot 33 \equiv 18 \mod 51 \\
3^{2^5} &\equiv 18 \cdot 18 \equiv 18 \mod 51 \\
3^{2^6} &\equiv 18 \cdot 18 \equiv 18 \mod 51
\end{aligned}$$

Finally, we have

$$3^{123} \equiv 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^3} \cdot 3^{2^1} \cdot 3^{2^0} \equiv 18 \cdot 18 \cdot 18 \cdot 33 \cdot 9 \cdot 3 \equiv 24 \mod 51.$$

Exercise 1.6. *Compute the following powers!*

- $6^{75} \mod 78$
- $8^{23} \mod 100$
- $11^{123} \mod 45$
- $7^{49} \mod 10$

1.3 The Chinese Remainder Theorem

Definition 1.7. *Let m and n be two positive integers. We say that g is the greatest common divisor of m and n if g is the largest possible number with $g|m$ and $g|n$.*
Notation: $g = gcd(m,n)$

Definition 1.8. *Let m and n be two positive integers. If $gcd(m,n) = 1$, then m and n are called relatively prime.*

Theorem 1.9 (Chinese remainder theorem)**.** *Let $m_1, \dots, m_k$ be positive integers, pairwise relatively prime. Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

is solvable for any $a_1, a_2, \dots, a_k$ integers and the solution is one residue class modulo $m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Method to solve such a system of linear congruences:

Let $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$. Then compute $M_i = \frac{M}{m_i}$ for $i = 1, 2, \dots, k$. Let y_i be the solution of $y_i \cdot M_i \equiv 1 \mod m_i$ for $i = 1, 2, \dots, k$. Finally,

$$x \equiv \sum a_i \cdot y_i \cdot M_i \mod M.$$

Example 1.10.

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 4 \mod 7 \end{aligned}$$

Then $M = 2 \cdot 3 \cdot 7 = 42$ and $M_1 = \frac{42}{2} = 21$, $M_2 = \frac{42}{3} = 14$, $M_3 = \frac{42}{7} = 6$.

$$\begin{aligned} 21y_1 \equiv 1 \mod 2 &\Rightarrow y_1 \equiv 1 \mod 2 \Rightarrow y_1 = 1 \\ 14y_2 \equiv 1 \mod 3 &\Rightarrow 2y_2 \equiv 1 \mod 3 \Rightarrow y_2 = 5 \\ 6y_3 \equiv 1 \mod 7 &\Rightarrow y_3 = 6 \end{aligned}$$

Finally,

$$x \equiv 1 \cdot 1 \cdot 21 + 2 \cdot 5 \cdot 14 + 4 \cdot 6 \cdot 6 \mod 42 \equiv 21 + 140 + 144 \mod 42 \equiv 11 \mod 42.$$

Thus $x = 11$ is fulfilling all three congruences.

Exercise 1.11. *Solve the following system of linear congruences!*

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 8 \\ x &\equiv 4 \mod 11 \end{aligned}$$

Chapter 2

Greatest common divisor

2.1 Euclidean algorithm

Given arbitrary integers a and $b \neq 0$ there exist unique numbers q and r such that

$$a = b \cdot q + r,$$

and $0 \leq r <\mid b \mid$.

Proposition 2.1. *Any two integers have a greatest common divisor.*

Proof. Euclidean algorithm:

We divide one number by the second number with remainder. Then we divide the second number by the remainder getting another remainder, etc. We continue dividing the divisor by the remainder until we get remainder 0. The last non-zero remainder will be the greatest common divisor of the two numbers.

Example 2.2. *Let* $a = 155$ *and* $b = 25$. *Then we have*

$$155 = 25 \cdot 6 + 5$$

$$25 = 5 \cdot 5 + 0.$$

Thus $gcd(155, 25) = 5$.

Example 2.3. *Let* $a = 141$ *and* $b = 17$.

k	0	1	2	3	4	5
r_k	141	17	5	2	1	0
q_k		8	3	2	2	

Thus $gcd(a, b) = 1$, *so a and b are relatively prime.*

Exercise 2.4. *Compute the greatest common divisor of a and b in the following cases!*

- $a = 45$, $b = 211$
- $a = 1491$, $b = 23$
- $a = 595$, $b = 867$

2.2 Extended Euclidean algorithm

Theorem 2.5. *Let a and b be two integers. Their greatest common divisor $gcd(a,b)$ can be written in the form of*

$$gcd(a,b) = ax + by$$

for suitable integers x and y.

Proof. Extended Euclidean algorithm:

By definition $x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1$ we will use the following recursive formulae

$$x_{k+1} = x_k \cdot q_k + x_{k-1}$$

and

$$y_{k+1} = y_k \cdot q_k + y_{k-1}.$$

Further, let n be the largest number such that the remainder is non-zero. Thus $n = \max\{k \mid r_k \neq 0\}$. Finally,

$$x = (-1)^n \cdot x_n$$

and

$$y = (-1)^{n+1} \cdot y_n.$$

k	0	1	2	3	4	5
r_k	141	17	5	2	1	0
q_k		8	3	2	2	
x_k	1	0	1	3	7	
y_k	0	1	8	25	58	

Thus $x = (-1)^4 \cdot 7$ and $y = (-1)^5 \cdot 58$ and $gcd(a,b) = ax + by$, which means

$$1 = 7 \cdot 141 - 58 \cdot 17.$$

Exercise 2.6. *Write $gcd(a,b)$ as sum of ax and by in the following cases!*

- $a = 258$, $b = 8$
- $a = 143$, $b = 7$
- $a = 5$, $b = 56$

Chapter 3

Prime tests

3.1 Fermat test

We know by the main theorem of Number Theory that any positive integer can be written as the product of prime numbers. Furthermore, the prime factors of a number n are unique, which means they can only differ in order and can only be extended by the factor 1. If the prime factors differ from the number itself, then we call it composite number. Prime numbers play an important role in Number Theory and Cryptography. We can regard them as the building elements of all numbers.

The Fermat test is a probability test using Fermat's little theorem.

Theorem 3.1. *If $gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \mod p$.*

`Algorithm:`

- Choose a.
- Compute $a^{p-1} \mod p$.
- If $a^{p-1} \not\equiv 1 \mod p$, then p is a composite number.

Example 3.2. *Test if 341 is a prime number!*

First, we use base 2 :

$$2^{340} \equiv 1 \mod 341.$$

Now, we use base 3 :

$$\begin{aligned}
3^{2^0} &\equiv 3 \mod 341 \\
3^{2^1} &\equiv 9 \mod 341 \\
3^{2^2} &\equiv 81 \mod 341 \\
3^{2^3} &\equiv 82 \mod 341
\end{aligned}$$

$$3^{2^4} \equiv 245 \mod 341$$

$$3^{2^5} \equiv 9 \mod 341$$

$$3^{2^6} \equiv 81 \mod 341$$

$$3^{2^7} \equiv 82 \mod 341$$

$$3^{2^8} \equiv 245 \mod 341$$

Since

$$3^{340} \equiv 3^{2^8} \cdot 3^{2^6} \cdot 3^{2^4} \cdot 3^{2^2} \equiv 56 \mod 341,$$

we get that 341 *is not prime number.*

Exercise 3.3.

- *Compute the Fermat test for* 181 *and base* 5 *and* 7!
- *Compute the Fermat test for* 129 *and base* 2 *and* 5!

3.2 Miller-Rabin test

This prime test works for odd numbers greater than 1.

`Algorithm:`

- Compute the values S and d :

$$S = \max\{r \mid 2^r \text{ divides } (n-1)\}$$

$$d = \frac{(n-1)}{2^s}$$

Theorem 3.4. *If n is prime and $gcd(a,n) = 1$, then*

1. $a^d \equiv 1 \mod n$ *or*
2. $\exists r \in \{0,\ldots,S-1\}$ *such that* $a^{d\cdot 2^r} \equiv -1 \mod n$.

Example 3.5. *We want to check if* 567 *is a prime numbers by the Miller-Rabin test. First,*

$$566 = 2 \cdot 283.$$

Thus $S = 1$ and $d = 283$. If 567 *is prime and $gcd(a,567) = 1$, then either* $a^{283} \equiv 1 \mod 567$ *or* $\exists r \in \{0,\ldots,S-1\}$ *such that* $a^{283\cdot 2} \equiv -1 \mod 567$. *Since $S = 1$, we have that $r = 0$ is the only possible value in the second case. Thus if* 567 *is prime, then either*

$$a^{283} \equiv 1 \mod 567$$

or

$$a^{283} \equiv -1 \mod 567.$$

We compute the Miller-Rabin test for bases 5 *and* 7!

$7^{283}:$				$5^{283}:$			
7^{2^0}	$\equiv$	7	mod 567	5^{2^0}	$\equiv$	5	mod 567
7^{2^1}	$\equiv$	49	mod 567	5^{2^1}	$\equiv$	25	mod 567
7^{2^2}	$\equiv$	133	mod 567	5^{2^2}	$\equiv$	58	mod 567
7^{2^3}	$\equiv$	112	mod 567	5^{2^3}	$\equiv$	529	mod 567
7^{2^4}	$\equiv$	70	mod 567	5^{2^4}	$\equiv$	310	mod 567
7^{2^5}	$\equiv$	364	mod 567	5^{2^5}	$\equiv$	277	mod 567
7^{2^6}	$\equiv$	385	mod 567	5^{2^6}	$\equiv$	184	mod 567
7^{2^7}	$\equiv$	238	mod 567	5^{2^7}	$\equiv$	403	mod 567
7^{2^8}	$\equiv$	511	mod 567	5^{2^8}	$\equiv$	247	mod 567

Then we have

$$7^{283} \equiv 511 \cdot 70 \cdot 112 \cdot 49 \cdot 7 \equiv 511 \mod 567$$

and

$$5^{283} \equiv 247 \cdot 310 \cdot 529 \cdot 25 \cdot 5 \equiv 320 \mod 567.$$

Thus the result of the Miller-Rabin test is that $n = 567$ is a composite number.

Exercise 3.6. *Check by the help of the Miller-Rabin test if n is a prime number!*

- $n = 197$, *base* 7 *and* 11
- $n = 243$, *base* 12 *and* 14
- $n = 397$, *base* 2 *and* 3

Chapter 4

RSA algorithm

4.1 Introduction

The RSA algorithm was invented by Rivest, Shamir and Adleman in 1976. It is still today the most widely used cryptographic system in the world.

The RSA algorithm is an asymmetric cryptosystem, which means it consists of a public key and a private key. Encryption is possible by the knowledge of the public key. Decryption is only possible by the knowledge of the private key, so the private key has to be kept secret.

Definition 4.1. *Let n be a positive integer. We define $\varphi(n)$ as the number of integer k in the range $1 \leq k \leq n$, such that $gcd(k,n) = 1$. This function φ is called the Euler's phi-function.*

Remark 4.2. *If n is a prime number, then $\varphi(n) = n - 1$.*

Remark 4.3. *If p and q are prime numbers, then $\varphi(pq) = (p-1)(q-1)$.*

4.2 Encryption

1. Choose two arbitrary large prime numbers p and q.
2. Compute $n = p \cdot q$.
3. Choose a small odd number e, which is relatively prime to $\varphi(n)$.
4. Search for a number d, for which $d \cdot e \equiv 1 \mod \varphi(n)$.

`Public Key:` the pair (e,n)

The set of messages is $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$.

Encrypting message m :

$$Enc(m) = m^e \mod n$$

4.3 Decryption

`Private Key:` the pair (d,n)

Decrypting message $y = m^e \mod n$:

$$Dec(y) = y^d \mod n$$

since $(m^e)^d \equiv m \mod n$.

4.4 Decryption by using Chinese Remainder Theorem and Euclidean Algorithm

Let c be the encrypted message and d the secret exponent. Further we know the two prime numbers p and q. Then using the Chinese remainder theorem we have

$$c_1 \equiv c^{d \mod (p-1)} \mod p$$

$$c_2 \equiv c^{d \mod (q-1)} \mod q$$

Further $M = p \cdot q$. Then $M_1 = q$ and $M_2 = p$. We know that $gcd(p,q) = 1$. Now we use the extended Euclidean algorithm in order to find solutions x and y for the equation

$$1 = x \cdot q + y \cdot p.$$

Finally, the decrypted message m can be computed:

$$m = c_1 \cdot x \cdot M_1 + c_2 \cdot y \cdot M_2.$$

Example 4.4. *Given $p = 5$, $q = 11$ primes, $c = 18$ encrypted message, $e = 7$ encrypting exponent, $d = 23$ decrypting exponent we compute*

$$c_1 \equiv 18^{23 \mod 4} \equiv 18^3 \equiv 2 \mod 5$$

$$c_2 \equiv 18^{23 \mod 10} \equiv 18^3 \equiv 2 \mod 11$$

Then $M_1 = 11, M_2 = 5, M = 55$. We need to solve $1 = 11x + 5y$.

k	0	1	2	
r_k	11	5	1	0
q_k	$-$	2	5	
x_k	1	0	1	
y_k	0	1	2	

Thus $x = 1$ and $y = -2$. Now the can compute the original message

$$m = 2 \cdot 1 \cdot 11 + 2 \cdot (-2) \cdot 5 \equiv 2 \mod 55.$$

Exercise 4.5. *Generate a public and a private key for RSA cryptographic system with the following two prime numbers:* 463 *ad* 547 *and the encrypting exponent is one of* $12, 47, 76, 93$ *fulfilling the conditions!*

Exercise 4.6. *Decrypt RSA-encrypted* 85 *by Chinese Remainder Theorem and knowing the two primes* 7 *and* 13 *and the decrypting exponent* 47!

Exercise* 4.7. *Prove that we can compute a message knowing the public information, if the message is encrypted by RSA with the pairs* (n,e) *and* (n,f), *where e and f are relatively prime!*

4.5 Some more background from Mathematics

Does there always exist d, **such that** $d \cdot e \equiv 1 \mod \varphi(n)$?

The answer to this question is yes, and the reason for that lies in the structure of $\mathbb{Z}_n$.

Recall, that $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$ is the set of residue classes modulo n. This set has the algebraic structure of a `ring` under the operations of addition and multiplication, i.e.

- addition is commutative, associative, and has a neutral element
- multiplication is distributive: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$
- there exists a multiplicative neutral element: $1 \cdot a = a \cdot 1 = a$

If n is a prime number, then $\mathbb{Z}_n$ is not only a ring, but it is also a `field`. That means there exists an inverse element for each number due to multiplication, i.e. $a \cdot a^{-1} = a^{-1} \cdot a = 1$. If n is not a prime, then such inverse does not exist for all nonzero elements.

Example 4.8. *Consider* $\mathbb{Z}_4 = \{0,1,2,3\}$ *under classical addition and multiplication. Then* $3 \cdot 3 = 9 \equiv 1 \mod 4$, *thus the inverse of* 3 *is* 3 *itself. But* $3 \cdot 2 = 6 \equiv 2 \mod 4$. *and* $2 \cdot 2 = 4 \equiv 0 \mod 4$. *Thus* 2 *has no inverse in* $\mathbb{Z}_4$.
Consider now $\mathbb{Z}_5 = \{0,1,2,3,4\}$. *Then we have* $2 \cdot 3 \equiv 1 \mod 5$ *and* $4 \cdot 4 \equiv 1 \mod 5$. *Thus every element of* $\mathbb{Z}_5$ *has a multiplicative inverse.*

The elements which have multiplicative inverse in $\mathbb{Z}_n$ are exactly those elements, which are relatively prime to n. The set of these elements if called the `multiplicative group` of $\mathbb{Z}_n$. The multiplicative group has $\varphi(n)$ elements. Therefore we choose e as relatively prime to $\varphi(n)$. So there always exist d such that $d \cdot e \equiv 1 \mod \varphi(n)$.

Chapter 5

The problem of discrete logarithm

5.1 Discrete logarithm and primitive roots

Let p be a prime number and let us denote the multiplicative group of $\mathbb{Z}_p$ by $\mathbb{Z}_p^\star$. Then $\mathbb{Z}_p^\star = \{1,2,\dots,p-1\}$. Let a be an arbitrary element in this multiplicative group. The `order` of a is the smallest number k such that $a^k \equiv 1 \mod p$. If this order is equal to $\varphi(p)$, then a is called a `primitive root` of $\mathbb{Z}_p$.

Remark 5.1. *A primitive root generates the whole multiplicative group.*

Example 5.2. 2 *is a primitive root of* $\mathbb{Z}_5^\star$*, since*

$$2^1 \equiv 2 \mod 5,\ 2^2 \equiv 4 \mod 5,\ 2^3 \equiv 3 \mod 5,\ 2^4 \equiv 1 \mod 5.$$

Thus the order of 2 *is* 4 *and* $4 = \varphi(5)$.

If a is a primitive root of $\mathbb{Z}_p$, then any element of $\mathbb{Z}_p$ can be written as the power of a. That means $A \in \mathbb{Z}_p \Rightarrow A \equiv a^k \mod p$ for suitable integer k.

Let us now assume that we know A, p and a. We want to compute the exponent k. For large prime numbers p this is a difficult problem and no algorithm is known to compute k in polynomial time. This problem is called the `discrete logarithm problem`.

5.2 Diffie-Hellmann key exchange

We assume that `Alice` and `Bob` want to use a symmetric crptographic system in order to send messages. They can share a secret key by the Diffie-Hellmann key exchange:

`Algorithm:`

1. Choose a large prime number p. This will be public.
2. Choose a primitive root a of $\mathbb{Z}_p^\star$. This will also be public.
3. Alice chooses $s \in \{2,\dots,p-1\}$ randomly. This is kept in secret.

4. Bob chooses $t \in \{2, \dots, p-1\}$ randomly. This is kept in secret.

5. Alice computes $a^s \mod p$ and sends it to Bob.

6. Bob computes $a^t \mod p$ and sends it to Alice.

7. Alice computes $(a^t)^s \mod p$, which is the symmetric key.

8. Bob computes $(a^s)^t \mod p$, which is the symmetric key.

Exercise 5.3. *Compute a protocol of Diffie-Hellmann key exchange, if the public prime is* 149 *and primitive root is* 21. *If necessary, give further parameters.*

Exercise 5.4. *Given the public prime* 47 *and primitive root* 11. *Further* $s = 12$ *and* $t = 23$. *Compute the protocol of a Diffie-Hellmann key exchange.*

Chapter 6

Solutions

Exercise 1.6:

- 60
- 12
- 26
- 7

Exercise 1.11: 26

Exercise 2.4:

- 1
- 1
- 17

Exercise 2.6:

- $2 = 258 - 32 \cdot 8$
- $1 = -2 \cdot 143 + 41 \cdot 7$
- $1 = -11 \cdot 5 + 56$

Exercise 3.3:

- $5^{180} \equiv 1 \mod 181$ and $7^{180} \equiv 1 \mod 181$, thus 181 can be prime (indeed, it is).
- $2^{128} \equiv 4 \mod 129$ and $5^{128} \equiv 25 \mod 129$, thus 129 cannot be prime.

Exercise 3.6:

- $7^{149} \equiv -1 \mod 197$ and $11^{49 \cdot 2} \equiv -1 \mod 197$, thus 197 can be prime (indeed, it is).

- $12^{121} \equiv 0 \mod 243$ and $14^{121} \equiv 32 \mod 243$, thus 243 cannot be prime.
- $2^{99\cdot 2} \equiv -1 \mod 397$ and $3^{99} \equiv -1 \mod 397$, thus 397 can be prime (indeed, it is).

Exercise 4.5: Public key $(47, 253261)$, Private key $(166379, 253261)$

Exercise 4.6: 15

Exercise 5.3:

- Alice chooses 3, computes $21^3 \mod 149$ and sends 23 to Bob
- Bob chooses 2, computes $21^2 \mod 149$ and sends 143 to Alice
- Alice computes $143^3 = 82 \mod 149$
- Bob computes $23^2 = 82 \mod 149$
- Now they can use the private key 82.

Exercise 5.4:

- Alice sends $11^{12} = 6 \mod 47$ to Bob
- Bob sends $11^{23} = 46 \mod 47$ to Alice
- Alice computes $11^{23^{12}} \mod 47$
- Bob computes $11^{12^{23}} \mod 47$
- Now they can use the private key 1.