

Assignment 0x03

Frank Kaiser – 1742945, Jan Martin – 1796943

January 7, 2018

Contents

1	Explain why the integers \mathbb{Z} form a ring, and the rationals \mathbb{Q} form a field.	2
1.1	Definition: ring	2
2	Task 1: Number Theory and Algebra	2
2.1	Explain why the integers \mathbb{Z} form a ring, and the rationals \mathbb{Q} form a field.	2
2.2	Find the inverses of all elements in \mathbb{Z}_7^* . Why do all numbers between 1 and 6 have an inverse?	2
2.3	As an exercise, calculate the inverse of 331 in \mathbb{Z}_{1234} using the extended euclidean algorithm.	2
2.4	Find all generators of \mathbb{Z}_{11}	3
2.5	Calculate 42^{497} in \mathbb{Z}_{1361} using fast exponentiation and a handheld calculator (not the one running on your computer or a programming language). Document a, e and n for each step.	3
2.6	Definition: field	5
3	Task 2: The RSA cryptosystem	6
3.1	Using that private key, decrypt c	6
3.2	Did Donald choose reasonable parameters? Explain!	6
3.3	Find a value of e for which RSA encryption is the identity function	6

iiiiii HEAD

1 Explain why the integers \mathbb{Z} form a ring, and the rationals \mathbb{Q} form a field.

1.1 Definition: ring

=====

2 Task 1: Number Theory and Algebra

2.1 Explain why the integers \mathbb{Z} form a ring, and the rationals \mathbb{Q} form a field.

A ring is a set R with two operations "+" and "*". $(R, +)$ is an abelian group, that means it is associative, commutative and has a neutral and inverse element. $(R, *)$ is a monoid, that means it is associative and has a neutral element. Lastly multiplication is distributive with respect to addition. If all axioms hold, a set is a ring. And they hold for \mathbb{Z} .

A field is a ring but with the special case that $(R \setminus \{0\}, *)$ is an abelian group. Meaning that associativity and commutativity hold for all elements except 0 and that there also exists a neutral and inverse element for every element of the field.

2.2 Find the inverses of all elements in \mathbb{Z}_7^* . Why do all numbers between 1 and 6 have an inverse?

$$\mathbb{Z}_7^* = 1, 2, 3, 4, 5, 6$$

A number is an inverse, if number mod inverse = 1 (the neutral element)

Number:	1	2	3	4	5	6
Inverse:	1	4	5	2	3	6

If n is a prime, then all numbers between 1 and $n-1$ have an inverse with the modulo-Operation. This is due to n not being a multiple of any of the elements in the set.

2.3 As an exercise, calculate the inverse of 331 in \mathbb{Z}_{1234} using the extended euclidean algorithm.

GCD = 1, if Rest is 0 in the end

$$1234 == 3 * 331 + 241$$

$$331 == 1 * 241 + 90$$

$$241 == 2 * 90 + 61$$

$$90 == 1 * 61 + 29$$

$$61 == 2 * 29 + 3$$

$29 == 9 * 3 + 2$
 $3 == 1 * 2 + 1$
 $2 == 2 * 1 + 0$

Applying the algorithm:

$1 == 3 - 1 * 2$
 $1 == 3 - (29 - 9 * 3)$
 $1 == 10 * 3 - 1 * 29$
 $1 == 10 * (61 - 2 * 29) - 1 * 29$
 $1 == 10 * 61 - 21 * 29$
 $1 == 10 * 61 - 21 * (90 - 1 * 61)$
 $1 == 31 * 61 - 21 * 90$
 $1 == 31 * (241 - 2 * 90) - 21 * 90$
 $1 == 31 * 241 - 83 * 90$
 $1 == 31 * 241 - 83 * (331 - 241 * 1)$
 $1 == 114 * 241 - 83 * 331$
 $1 == 114 * (1234 - 3 * 331) - 83 * 331$
 $1 == 114 * 1234 - 425 * 331$

Inverse of 331 is -425. Since it is not in \mathbb{Z} we add 1234 to it until it is:
 $-425 + 1234 = 809 \Rightarrow 809$ is the inverse of 331 in canonical form.

Test: $331 * 809 = 267779$

$267779 \% 1234 = 1$

So the calculations are correct.

2.4 Find all generators of \mathbb{Z}_{11}

	1	2	3	4	5	6	7	8	9	10	
1	1	1	1	1	1	1	1	1	1	1	
2	2	4	8	5	10	9	7	3	6	1	TRUE
3	3	9	5	4	1	3	9	5	4	1	FALSE
4	4	5	9	3	1	4	5	9	3	1	FALSE
5	5	3	4	9	1	5	3	4	9	1	FALSE
6	6	3	7	9	10	5	8	4	2	1	TRUE
7	7	5	2	3	10	4	6	9	8	1	TRUE
8	8	9	6	4	10	3	2	5	7	1	TRUE
9	9	4	3	5	1	9	4	3	5	1	FALSE
10	10	1	10	1	10	1	10	1	10	1	TRUE

ExcelFormula = MOD((linke Spalte^Obere Zeile);11)

The marked lines (2, 6, 7, 8) are generators.

2.5 Calculate 42^{497} in \mathbb{Z}_{1361} using fast exponentiation and a handheld calculator (not the one running on your computer or a programming language). Document a, e and n for each step.

Fastexp(a=42, n=497)

1st Iteration:

$e = 1$
 n is odd:
 $e = (42 * 1) \bmod 1361 = 42$
 $a = 42 \bmod 1361 = 1764 \bmod 1361 = 403$
 $n = 497 / 2 = 248$

2):

$e = 42$
 n is even:
 $a = 403 \bmod 1361 = 450$
 $n = n/2 = 124$

3)

$e = 42$
 n is even:
 $a = 450 \bmod 1361 = 1072$
 $n = 124 / 2 = 62$

4)

$e = 42$
 n is even:
 $a = 1072 \bmod 1361 = 500$
 $n = 62 / 2 = 31$

5)

$e = 42$
 n is odd:
 $e = (500 * 42) \bmod 1361 = 585$
 $a = 500 \bmod 1361 = 937$
 $n = 31 / 2 = 15$

6)

$e = 1072$
 n is odd:
 $e = (937 * 585) \bmod 1361 = 1023$
 $a = 937 \bmod 1361 = 124$
 $n = 15 / 2 = 7$

7)

```

    e = 46
n is odd:
e = (124 * 1023) mod 1361 = 279
a = 124 mod 1361 = 405
n = 7 / 2 = 3

```

8)

```

    e = 260
n is odd:
e = (405*279) mod 1361 = 32
a = 405 mod 1361 = 705
n = 3 / 2 = 1

```

9)

```

    e = 503
n is odd:
e = (705*32) mod 1361 = 784
a = 705 mod 1361 = 260
n = 1 / 2 = 0

```

10)

```

n = 0 => return e = 784

```

```

=> 42497 mod 1361 = 784

```

```

lllllll 621161c88ec086a6b093522fd76a88451fabbb7a

```

```

iiiiiii HEAD

```

2.6 Definition: field

```

===== lllllll 621161c88ec086a6b093522fd76a88451fabbb7a

```

3 Task 2: The RSA cryptosystem

3.1 Using that private key, decrypt c

$$PHI(n) = (p - 1)(q - 1) = (17 - 1) * (23 - 1) = 16 * 22 = 352$$

$$e = 17; Z_{352}^* \\ (e * d) \bmod 352 = 1$$

Using Excel we found the inverse using the formula above: $d = 145$

$$m = c^d \bmod n = 282^{145} \bmod 391 = 197$$

3.2 Did Donald choose reasonable parameters? Explain!

When $e = 1$, the message itself is encrypted just by applying the modulo with the public Key part N . Resulting in $c = m \bmod N$, which means that if m is smaller than N , the encrypted message is just the plain message $\Rightarrow c = m$

3.3 Find a value of e for which RSA encryption is the identity function