University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013

Exercises from Lecture 1 by Oleksandr Iena

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 26.02.2013, 4 p.m.

Exercise 1: 1) Compute $d = \gcd(65, 45)$ and find integers α, β such that

$$\alpha \cdot 65 + \beta \cdot 45 = d.$$

Check whether the following linear Diophantine equations have solutions and find a solution if it is possible.

a) $45x + 65y = 13$;
b) $45x + 65y = 20$;
c) $45x + 65y = 5$.

2) Check whether the following linear Diophantine equations have solutions and find a solution if it is possible.

a) $899x + 203y = 319$;
b) $899x + 203y = 341$.

Exercise 2: 1) In analogy to the definition from the lecture, introduce the notion of $\gcd(a, b, c)$ for three integers $a, b, c \in \mathbb{Z}$. Notice that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ and conclude that

$$\gcd(a, b, c) = \alpha a + \beta b + \gamma c$$

for some integers α, β, and γ.

2) Let a, b, c, d be integer numbers. In analogy to the lecture, develop a criterion to decide whether the Diophantine equation

$$ax + by + cz = d$$

has an integer solution $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Find a constructive way to compute such a solution if it exists.

3) Check whether the following linear Diophantine equations have solutions and find a solution if it is possible.

a) $3x + 6y + 9z = 1$;
b) $3x + 6y + 9z = 3$.

Exercise 3: Let $a_1, \ldots, a_n$ and d be integers. Can you find an efficient way to decide whether the Diophantine equation

$$a_1x_1 + a_2x_2 + \ldots a_nx_n = d$$

has an integer solution? Can you find a solution of such an equation if it exists?

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 2 by PD

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 5.03.2013, 4 p.m.

Remark. *Let me give a precise formulation of the Miller-Rabin test. Let n be a natural odd number. Write $n-1$ in the form $n-1=2^s\cdot d$, where d is an odd natural number and s is a non-negative integer. Take an arbitrary integer a such that $2\leqslant a\leqslant n-1$.*

If n is prime, then

- *either* $a^d\equiv 1 \mod n$
- *or the sequence of numbers*
$$(a^d, a^{2d}, a^{4d}, \dots, a^{2^{s-1}\cdot d})$$
contains -1 modulo n, i. e., is of the form
$$(*, \dots, *, -1, \dots),$$
where $*$ stays for an arbitrary number.

Hence, if $a^d\not\equiv 1 \mod n$ *and* $(a^d, a^{2d}, a^{4d}, \dots, a^{2^{s-1}\cdot d})$ *is not of the form* $(*, \dots, *, -1, \dots)$, *then n is not prime.*

Exercise 1: Apply the Fermat primality test to the number $n=1729$ for $a=2$ and $a=3$.

Exercise 2: Apply the Miller-Rabin test to $n=561$ for $a=2$.

1) In this case $d=35$, $s=4$, and $a^d\equiv 263 \mod 561$.

2) Write down the sequence $(a^d, a^{2d}, a^{4d}, \dots, a^{2^{s-1}\cdot d})$ modulo n. Realize that n can not be prime.

Exercise 3: Apply the Miller-Rabin test to $n=1729$ for two different numbers a of your choice.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 3 by PS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 12.03.2013, 4 p.m.

Exercise 1: Write the rational numbers $\frac{16}{13}$, 5.25, $\frac{23}{7}$ as continued fractions.

Exercise 2: Write $\sqrt{10}$ as a continued fraction. Is $\sqrt{10}$ a rational or an irrational number? Justify your answer.

Exercise 3: i) Find a continued fraction representation of the positive root of the quadratic equation $x^2 - x - 1 = 0$, using continued fractions.

Hint: *Consider* $x = 1 + \frac{1}{x}$.

ii) Find a continued fraction representation of the negative root using the continued fraction representation of the positive root.

Hint: (from Paul) *The negative root is* $\frac{1}{2}(1 - \sqrt{5})$.
Hint: (from Oleksandr) *The sum of the roots is* 1.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 4 by SS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 19.03.2013, 4 p.m.

Exercise 1: Represent 373 and 882 as sums of two squares.

Exercise 2: Determine two consecutive integers whose sum of squares is equal to 613.

Exercise 3: Find the smallest integers which can be represented in two respectively three different ways as sums of two squares. Why isn't the square sum representation for composite numbers in general unique?

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 5 by MR

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 26.03.2013, 4 p.m.

Exercise 1: Bob uses RSA algorithm and publishes his public key $(187, 7)$. Knowing that $\phi(n) = 160$, find Bob's private key.

Exercise 2: (encryption) Using the public key from Exercise 1 and the table $(*)$, encrypt the message "HELLO".

Exercise 3: (decryption) Using the private key that you have found in Exercise 1 and the table $(*)$, decrypt the message $M = 146\ 108\ 115\ 124\ 123$.

Table $(*)$:

Letter	A	B	...	Z	space	.	,	!
Number	1	2	...	26	27	28	29	30

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 6 by MM

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 9.04.2013, 4 p.m.

Letter	A	B	...	Z	0	...	9	,	.	$\approx$	=	*	/
Number	1	2	...	26	27	...	36	37	38	39	40	41	42

Exercise 1: Alice wants Bob to send her a message using the El Gamal algorithm. She chooses

$$p = 263, \quad g = 5, \quad \alpha = 47.$$

1. Give Alice's public key.
2. Encrypt the message "PI" using the table above for $\gamma = 139$.

Exercise 2: Alice and Bob are using the El Gamal algorithm for communication. Alice chose $\alpha = 67$ and published the public key $(257, 5, 201)$. Bob sent her the message $(2, 24047224248)$. Decrypt it.

Exercise 3: Suppose that Eve eavesdropped the exchange between Bob and Alice and knows they use the El Gamal algorithm.

1. Knowing that Eve knows m and the encrypted message m', prove that Eve can decrypt any further message n' provided γ stays unchanged in the next exchanges.
Hint: Compute $n'(m')^{-1}$ modulo p.

2. Using the keys and the result from Exercise 1 and your formula from the previous question, decrypt $O' = (193, 12611026)$ and use the table to find the associated message.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 7 by SK

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 16.04.2013, 4 p.m.

Exercise 1: Notice that 2 and 4 are invertible 5-adic integers. Compute the first four coefficients a_i of the power series $\sum_{i \geqslant 0} a_i \cdot 5^i$ of the following numbers in $\mathbb{Z}_5$:

$$\frac{1}{2} = 2^{-1}, \quad \frac{7}{4} = 7 \cdot 4^{-1}, \quad \frac{11}{2} = 11 \cdot 2^{-1}.$$

Exercise 2: Find all solutions of the congruence

$$x^3 - 3x - 5 \equiv 0 \mod 7^4.$$

Exercise 3: Characterize the solutions of the equations

$$x^4 - 3x^2 + 27 \equiv 0 \mod 5^k$$

and

$$x^4 - x^3 - 8 \equiv 0 \mod 5^k.$$

Compute the solutions for $k = 5$.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 8 by SS & PS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 23.04.2013, 4 p.m.

Exercise 1: Calculate the following Legendre and Jacobi symbols.

$$\left(\frac{85}{87}\right), \quad \left(\frac{20}{25}\right), \quad \left(\frac{101}{211}\right).$$

Exercise 2: Decide whether or not the following equations have solutions. Find the solutions if they exist.

$$x^2 \equiv 101 \mod 211, \quad x^2 \equiv 130 \mod 157.$$

Exercise 3: Provide an example (different from the one given in the lecture) of a and n such that $\left(\frac{a}{n}\right) = 1$ but a is a quadratic non-residue modulo n.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 9 by MM & MR

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 30.04.2013, 4 p.m.

Exercise 1: 1) Write the golden number

$$\frac{1+\sqrt{5}}{2}$$

as a continued fraction.

2) What can you deduce comparing the result to the continued fraction seen during the lecture.

Exercise 2: 1) Let p be a prime number. Prove that

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \mod 5; \\ -1, & \text{if } p \equiv \pm 2 \mod 5. \end{cases}$$

2) Compute $F_{163} \mod 163$ and $F_{1129} \mod 1129$.

Exercise 3: 1) Prove that $F_{2q-1} = F_q^2 + F_{q-1}^2$ for all $q \geqslant 1$.
Hint: *use the Assertion from the lecture.*

2) Is it true that also for even n the n-th Fibonacci number F_n can be written as a sum of two squares of Fibonacci numbers?

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercises from Lecture 10 by SK

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 7.05.2013, 4 p.m.

Exercise 1: Find the solutions of the equation

$$x^2 \equiv 3 \mod 13$$

using $z = 5$ as a quadratic non-residue.

Exercise 2: Find the solutions of the equations

$$x^2 \equiv 6 \mod 43.$$

Exercise 3: Find the solutions of the equation

$$x^2 \equiv 2 \mod 41.$$

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercise sheet 11

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 14.05.2013, 4 p.m.

Exercise 1: Find the solutions of the equation

$$x^2 + 6x + 6 \equiv 0 \mod 13^2.$$

Exercise 2: Find the solutions of the equations

$$y^4 + 2y^2 + 38 \equiv 0 \mod 43.$$

Exercise 3: From Exercise 3 from Lecture 7 we know that for every $k \geqslant 3$ the equation

$$x^4 - x^3 - 8 \equiv 0 \mod 5^k.$$

has 10 solutions. We also know that only two of them can be lifted to solutions modulo 5^{k+1}. This means that the equation

$$x^4 - x^3 - 8 = 0$$

has two solutions in $\mathbb{Z}_5$. One of these solutions is $2 \in \mathbb{Z}$ (recall that $\mathbb{Z}$ is naturally a subring of $\mathbb{Z}_5$).

(1) Present a solution of the equation

$$x^4 - x^3 - 8 \equiv 0 \mod 5^{555437}$$

that is different from 2.

(2) Can you say whether the second solution of

$$x^4 - x^3 - 8 = 0$$

in $\mathbb{Z}_5$ is an integer?

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercise sheet 12

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 21.05.2013, 4 p.m.

Exercise 1: Check whether the equation

$$9^x \equiv 15 \mod 35$$

is solvable. Find a solution if the equation is solvable.

Exercise 2: Check whether the equation

$$5^x \equiv 460 \mod 547$$

is solvable and find a solution if possible.

Exercise 3: Check whether the equations are solvable and find their solutions, if possible.

$$x^2 \equiv 6 \mod 89, \quad x^2 \equiv 7 \mod 89, \quad x^2 \equiv 8 \mod 89.$$

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2013
Exercise sheet 13

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 04.06.2013, 4 p.m.

Exercise 1: Solve the equation

$$27^x \equiv 4 \mod 157.$$

Exercise 2: Solve the equation

$$x^2 \equiv 122 \mod 157.$$

Exercise 3: Let us use the RSA algorithm and the following table for communication.

Symbol	A	B	...	Z	space	.	,	!
Number	1	2	...	26	27	28	29	30

You have published your public key $(143, 7)$. I used it and encrypted my message for you:

117 1 138 48 53 47 94 117 115 138 6 1 53 47 94 3 1 109 12 94 46 47 12 117 1 94 46 22 47 53 63.

Decrypt it.