University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012

Exercises from Lecture 1 by Oleksandr Iena

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 28.02.2012, 4 p.m.

Exercise 1: Prove the existence of the division with remainder for integer numbers.

Exercise 2: Prove that $a|b$ and $b|a$ implies $|a| = |b|$.

Exercise 3: Compute $d = \gcd(65, 45)$ and find integers α, β such that

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

Exercise 4: Check whether the following linear Diophantine equations have solutions and find a solution if it is possible.

a) $45x + 65y = 133$;
b) $45x + 65y = 10$;
c) $45x + 65y = -5$.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 2 by KF

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 6.03.2012, 4 p.m.

Exercise 1: Show that the integer solutions of the equation

$$x^2 + y^2 = z^2, \quad x, y, z > 0, \quad \gcd(x, y, z) = 1,$$

so called Pythagorean triples, are all given, up to possible permutation of x and y, by the formulae

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $\gcd(u, v) = 1$, and the numbers u and v are not simultaneously odd.

Hint: *Notice that x and y can not be odd simultaneously. Assume that y is even, write $z^2 - x^2 = y^2$ and notice that x and z have to be odd.*

Exercise 2: Let $x \in \mathbb{Z}[i]$. Recall that the norm defined by

$$N(x) = x \cdot \bar{x} = (\mathrm{Re}(x))^2 + (\mathrm{Im}(x))^2$$

satisfies the following properties:

- $N(xy) = N(x)N(y)$, for all $x, y \in \mathbb{Z}[i]$,
- $x \in (\mathbb{Z}[i])^\times \Leftrightarrow N(x) = 1$, where $(\mathbb{Z}[i])^\times$ is the group of the invertible elements of $\mathbb{Z}[i]$.

1. Show that if $N(x) = p$, where p is a prime number, then x is irreducible in $\mathbb{Z}[i]$.

2. Let $p \in \mathbb{Z}$ be a prime number. Show that p is irreducible in $\mathbb{Z}[i]$ if and only if one can not write it a sum of two squares (equivalent to $p \equiv 3 \mod 4$).

3. Deduce that if $N(x) = N(p)$, where p is a prime number such that $p \equiv 3 \mod 4$, then x is irreducible.

Exercise 3:

1. Give the sequence corresponding to the polynomial $x^7 - 2x^3 + x - 1$.
2. Give the sequence corresponding to the product of polynomials $x^2 - 1$ and $x^2 + 1$.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 3 by RDS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 13.03.2012, 4 p.m.

Exercise 1: Write the rational numbers $\frac{47}{38}$ and $\frac{17}{7}$ as continued fractions.

Exercise 2: a) Write the ratio $\frac{f_n}{f_{n-1}}$ of two consecutive Fibonacci numbers as a continued fraction using the relations

$$f_n = f_{n-1} + f_{n-2}, \quad f_{n-1} = f_{n-2} + f_{n-3}, \quad \dots \quad f_4 = f_3 + f_2, \quad f_3 = 2 \cdot f_2 + 0.$$

b) Show that $\frac{f_n}{f_{n-1}} = \underbrace{[1; 1, 1, \dots, 1]}_{n-1}$.

Exercise 3: Write $\sqrt{5}$ as a continued fraction.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 4 by MS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 27.03.2012, 4 p.m.

Exercise 1: Make a list of all quadratic residues and all non-residues modulo 19.

Exercise 2: A number a is called a cubic residue modulo p if it is congruent to a cube modulo p, i. e.,

$$a \equiv b^3 \mod p$$

for some integer b.

a) Make a list of all cubic residues modulo 11 and modulo 13.

b) Find a and b such that neither of them is a cubic residue modulo 19, but their product ab is a cubic residue.

b) Find a and b such that neither of the numbers a, b, ab is a cubic residue modulo 19.

Exercise 3: Prove that $g = 2$ is a primitive root modulo 19.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises set 5 (Lectures 1–4)

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 27.03.2012, 4 p.m.

Exercise 1: Compute a greatest common divisor of $25-5i$ and $2-4i$ in the ring of Gaussian integers $\mathbb{Z}[i]$. Write down all possible results.

Exercise 2: a) Represent the number $\sqrt{7}$ as a continued fraction.

b) Compute $[\overline{1;7}]$.

Exercise 3: Let p and q be odd prime numbers. Use the formula (quadratic reciprocity theorem)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

to decide whether the following equations have solutions:

a) $x^2 = 3 \mod 67$;

b) $x^2 = 19 \mod 43$.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 5 by AD

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 10.04.2012, 4 p.m.

As in the lecture the letters correspond to numbers as follows:

$$A \leftrightarrow 11, \quad B \leftrightarrow 12, \quad C \leftrightarrow 13, \quad \ldots \quad Z \leftrightarrow 36.$$

Exercise 1: Which of the following is the numerical equivalent of the message "**exercise**"?

a) 15 34 15 27 13 19 29 15;
b) 15 34 15 28 13 19 13 15;
c) 15 34 15 28 13 19 29 15.

Exercise 2: Which string corresponds to the number sequence 13 25 29 15 11 13 11 29 25

a) "**coseacoso**";
b) "**coseacasa**";
c) "**coseacaso**";
d) "**coseacosa**";

Exercise 3: We want to encipher the message

"**there are more things in heaven and earth**".

We are going to use $e = 79921$ and $n = p \cdot q$, where the prime numbers are $p = 12553$ and $q = 13007$.

a) Convert the message into a string of digits.
b) Which is the encoded message we get?

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 6 by MS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 17.04.2012, 4 p.m.

Exercise 1: Compute the Jacobi symbols $\left(\frac{37}{859}\right)$ and $\left(\frac{10270}{25511}\right)$.

Exercise 2: Show that

$$\left(\frac{41}{51}\right) = 1,$$

but 41 is not a quadratic residue modulo 51.

Exercise 3: Find a solution of the equation

$$x^2 \equiv 56 \mod 113.$$

Hint: *Use the last lemma seen in the class.*

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 7 by KF

Elements of Elementary and Algebraic Number Theory

Primality tests

Due date: Tuesday, 24.04.2012, 4 p.m.

Exercise 1: Use Korselt's Criterion to determine which of the following numbers are Carmichael numbers.

a) 1105;

b) 6601;

c) 10659.

Exercise 2: Let $n = 1105$, so $n - 1 = 2^4 \cdot 69$. Compute the values of

$$2^{69} \mod 1105, \quad 2^{2\cdot 69} \mod 1105, \quad 2^{4\cdot 69} \mod 1105, \quad 2^{8\cdot 69} \mod 1105$$

and use the Rabin-Miller test to conclude that n is composite.

Exercise 3: Find the prime factors of the numbers 29591 and 127433 using Fermat factorisation method.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 8 by RDS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 8.05.2012, 4 p.m.

Exercise 1: a) Find all solutions of the equation

$$x^2 - 2 \equiv 0 \mod 7^k$$

for $k = 1, 2, 3, 4$.

b) Consider the solutions for $k = 4$ as elements of $\mathbb{Z}_7$ and write down their reduced representations.

Exercise 2: Compute $\varepsilon_7(137)$.

Exercise 3: Calculate the reduced forms of the following elements of $\mathbb{Z}_5$.

a) $(3 \cdot 5^0 + 2 \cdot 5^1 + 4 \cdot 5^2) + (4 \cdot 5^0 + 2 \cdot 5^1 + 1 \cdot 5^2)$;

b) $(4 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 4 \cdot 5^3) \cdot (1 \cdot 5^0 + 3 \cdot 5^1)$.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 9 by AD

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 15.05.2012, 4 p.m.

Exercise 1: Represent 178 and 4797 as the sums of two squares as seen in the lecture.

Exercise 2: Find two smallest natural numbers with two different representations as sums of two squares, i. e., $n \in \mathbb{N}$ such that

$$n = a^2 + b^2 = c^2 + d^2, \quad a, b, c, d \in \mathbb{N}, \quad \{a, b\} \neq \{c, d\}.$$

Exercise 3: Find a reason why integers can not be represented as a unique sum of two squares.

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 10 by KF and RDS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 22.05.2012, 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: Apply the algorithm from the lecture in order to solve the equation

$$x^2 \equiv 4 \mod 17.$$

Exercise 3: Solve the equation

$$x^2 \equiv 56 \mod 113.$$

University of Luxembourg
Mathematics Research Unit
Dr. Oleksandr Iena

SS 2012
Exercises from Lecture 11 by AD and MS

Elements of Elementary and Algebraic Number Theory

Due date: Tuesday, 29.05.2012, 4 p.m.

Exercise 1: Find a solution $x \in \mathbb{N}$ of the equation

$$2^x = 7 \mod 37.$$

Exercise 2: Find a solution $x \in \mathbb{N}$ of the equation

$$5^x = 65 \mod 547.$$

Exercise 3: Find a solution $x \in \mathbb{N}$ of the equation

$$5^x = 9 \mod 11.$$