Exercises Math 118, Winter 2000, Week 1

Robert Boltje

1. (a) Show that there are infinitely many primes of the form $3k+2$, $k \in \mathbb{N}_0$.
(b) Show that there are infinitely many primes of the form $6k+5$, $k \in \mathbb{N}_0$

2. Determine $U(\mathbb{R})$, $U(\mathbb{R}[x])$, and $U(\mathbb{Z}/6\mathbb{Z})$.

3. Decide which of the rings $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$ is a field.

4. Show that the relation $\sim$ on R, given by $a \sim b$ if and only if $a \cdot u = b$ for some $u \in U(R)$, is an equivalence relation. What is the equivalence class of 0? What is the equivalence class of 1?

5. Let $R = \mathbb{Z}[x]$ and let $I := \{f(x) \in R \mid f(0) \text{ is even}\}$.
(a) Show that I is an ideal of R.
(b) Show that $I = (2, x)$.
(c) Show that I is not a principal ideal.

Exercises Math 118, Winter 2000, Week 2

Robert Boltje

6. Let $R = \mathbb{Z}[\sqrt{5}i]$ and let $N\colon R \to \mathbb{N}_0$ be the function given by

$$N(a + b\sqrt{5}i) := (a + b\sqrt{5}i)(a - b\sqrt{5}i) = a^2 + 5b^2\,,$$

for $a, b \in \mathbb{Z}$.

(a) Show that $N(xy) = N(x)N(y)$ for all $x, y \in R$.

(b) Let $x \in R$. Show that $x \in U(R) \iff N(x) = 1 \iff x \in \{1, -1\}$.

(c) Show that no two of the elements $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ are associate.

(d) Show that the elements $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ are irreducible in R. (Hint: Use the map N.)

7. Let $R = \mathbb{Z}[\sqrt{5}i]$ and N be as in Exercise 6.

(a) Show that none of the elements $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ is a prime element in R. (Hint: Use the two factorizations of the element 6 and the map N.)

(b) Show that 6 cannot be written as a product of prime elements in R. (Hint: Use the map N.)

8. Show that $(1 + i) = (2, 3 + 1)$ in $R := \mathbb{Z}[i]$.

9. Let $R := \mathbb{Z}[i]$ and let $N\colon R \to \mathbb{N}_0$ be defined by

$$N(a + bi) := (a + bi)(a - bi) = a^2 + b^2\,,$$

for $a, b \in \mathbb{Z}$.

(a) Show that $N(xy) = N(x)N(y)$ for all $x, y \in R$.

(b) Let $x \in R$. Show that $x \in U(R) \iff N(x) = 1 \iff x \in \{1, -1, i, -i\}$.

(c) Show that $1 + i$ is a prime element of R. (Hint: Show that $1 + i \mid 2$ and use the map N.)

10. (a) Show that a field R has only two ideals, namely $\{0\}$ and R.

(b) Show that every field is a PID.

Exercises Math 118, Winter 2000, Week 3

Robert Boltje

11. Let R be a domain and let $a_1, \ldots, a_n \in R$. An element $d \in R$ is called a *greatest common divisor* (or gcd) of $a_1, \ldots, a_n$, if d is a common divisor of $a_1, \ldots, a_n$ and if every common divisor of $a_1, \ldots, a_n$ divides d.

(a) Besides $a_1, \ldots, a_n \in R$, let also $b_1, \ldots, b_m \in R$ and assume that $d \in R$ is a gcd of $a_1, \ldots, a_n$ and $e \in R$ is a gcd of $b_1, \ldots, b_m$. Show that if $f \in R$ is a gcd of d and e, then f is a gcd of $a_1, \ldots, a_n, b_1, \ldots, b_m$.

(b) Assume that R is a PID and let $d \in R$. Show that d is a gcd of $a_1, \ldots, a_n$ if and only if $(d) = (a_1, \ldots, a_n)$.

12. Compute a gcd of

$$\begin{aligned} f(x) &= x^4 + 2x^3 - 4x^2 - 2x + 3\,, \\ g(x) &= x^5 + x^4 - 2x^3 + 2x^2 + 2x - 4\,, \\ h(x) &= x^4 + 2x^3 - 2x^2 - 5x - 2\,, \end{aligned}$$

in $\mathbb{Q}[x]$ and express it as a linear combination of $f(x)$, $g(x)$, and $h(x)$.

13. Compute a gcd of $\alpha = 13 - i$, $\beta = -2 + 4i$, and $\gamma = 3 + i$ in $\mathbb{Z}[i]$ and express it as a linear combination of α, β, and γ.

14. Decompose $-30 + 24i$ into a product of prime elements in $\mathbb{Z}[i]$.

15. Show that the ring

$$R = \mathbb{Z}[\sqrt{2}i] := \{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\}$$

is a euclidean domain.

Exercises Math 118, Winter 2000, Week 4

Robert Boltje

16. Find an integer a satisfying the congruences

$$\begin{aligned} a &\equiv 13 \mod 27 \\ a &\equiv 27 \mod 64 \\ a &\equiv 64 \mod 125 \end{aligned}$$

Is $a + 216000\mathbb{Z}$ a unit in $\mathbb{Z}/216000\mathbb{Z}$?

17. Show that 2 is the only prime number which is divisible in $\mathbb{Z}[i]$ by π^2 for some prime element π of $\mathbb{Z}[i]$.

18. Show that if π is a prime element in $\mathbb{Z}[i]$, then also $\bar{\pi}$ is a prime element.

19. Find all primitive roots modulo 23.

20. Assume that in some strange country there only exist coins of 35 and 64 units of their currency. Is it possible to pay for any number of units of this currency just using these coins (and allowing to get change)? How can you pay for a piece of bread which costs 11 units?

Exercises Math 118, Winter 2000, Week 6

Robert Boltje

21. Compute the following Legendre symbols:
(a) $\left(\frac{393}{1009}\right)$,
(b) $\left(\frac{86}{513}\right)$.

22. For what prime numbers p is
(a) 3,
(b) 5,
(c) 6,
a quadratic residue modulo p.

23. Let p be a prime number.
(a) Show that, if $p \equiv 1 \mod 3$, then for exactly $(p-1)/3$ of the numbers $a \in \{1, \ldots, p-1\}$ there exists a solution of the congruence $x^3 \equiv a \mod p$.
(b) Show that, if $p \equiv 2 \mod 3$, then for every $a \in \{1, \ldots, p-1\}$ there exists a solution of the congruence $x^3 \equiv a \mod p$.

24. Does $x^2 - 5x + 3 \equiv 7 \mod 233$ have a solution?

25. Let I and J be ideals in a commutative ring R. Show that

$$I + J := \{a + b \mid a \in I, b \in J\},$$
$$I \cdot J := \{a_1 b_1 + \ldots + a_n b_n \mid a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\},$$

and $I \cap J$ are again ideals of R and that they satisfy

$$I \cdot J \subseteq I \cap J \subseteq I \subseteq I + J.$$

Exercises Math 118, Winter 2000, Week 7

Robert Boltje

26. Let R be a commutative ring and let $\alpha \in R$. For $r, s \in R$ we write $r \equiv s \mod \alpha$ (r is congruent to s modulo α) if $\alpha \mid r - s$.

(a) Show that being congruent modulo α defines an equivalence relation on R.

(b) Let $r_1, r_2, s_1, s_2 \in R$ such that

$$r_1 \equiv s_1 \mod \alpha \quad \text{and} \quad r_2 \equiv s_2 \mod \alpha .$$

Show that

$$r_1 + r_2 \equiv s_1 + s_2 \mod \alpha \quad \text{and} \quad r_1 \cdot r_2 \equiv s_1 \cdot s_2 \mod \alpha .$$

(c) Try to formulate the definition of $r \equiv s \mod \alpha$ using the ideal (α) and generalize the definition by replacing (α) by an arbitrary ideal. Show that again (a) and (b) hold.

For the exercises 27–30 we introduce the following notation:
Let $\zeta := (-1 + \sqrt{3}i)/2$ and set

$$K := \{a + b\zeta \mid a, b \in \mathbb{Q}\} \quad \text{and} \quad R := \{a + b\zeta \mid a, b \in \mathbb{Z}\} .$$

Moreover consider the function

$$N \colon K \to \mathbb{Q}, \quad a + b\zeta \mapsto (a + b\zeta)(\overline{a + b\zeta}) .$$

27. (a) Show that $1 + \zeta + \zeta^2 = 0$, $\zeta^3 = 1$, and

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta)$$

for all $\alpha, \beta \in \mathbb{C}$.

(b) Show that R is a commutative ring.

(c) Show that K is a field.

28. (a) Let $\alpha = a + b\zeta \in K$. Show that $N(a + b\zeta) = a^2 - ab + b^2 \geq 0$.

(b) Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in K$.

(c) Show that N is a euclidean norm for R.

29. (a) Let $\alpha \in R$. Show that

$$\alpha \in U(R) \iff N(\alpha) = 1 \iff \alpha \in \{\pm 1, \pm\zeta, \pm\zeta^2\} .$$

(b) Show that $1 - \zeta$ is a prime element in R and compute all the elements that are associated to it.

30. Let $\theta := \sqrt{3}i$. Show that modulo θ, every element in R is congruent to 0, to 1, or to -1. Show also that 0, 1, and -1 are pairwise not congruent modulo θ.

Exercises Math 118, Winter 2000, Week 8

Robert Boltje

31. Let $n \in \mathbb{N}$. Show that if n is of the form $n = 4^a(8b+7)$ with $a, b \in \mathbb{N}_0$, then n cannot be written as a sum of 3 squares. (By a theorem due to Gauss, also the converse is true.)

32. Let $d \in \mathbb{N}$ be not a square and let $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$ be solutions to the equation

$$X^2 - dY^2 = 1\,. \tag{E}$$

(a) Show that $x_1 + y_1\sqrt{d} > 1$, $x_1 - y_1\sqrt{d} = 1/(x_1 + y_1\sqrt{d})$, and $0 < x_1 - y_1\sqrt{d} < 1$.

(b) Show that the following are equivalent:

(i) $x_1 < x_2$.

(ii) $y_1 < y_2$.

(iii) $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$.

33. Let $d \in \mathbb{N}$ be not a square. Assume that $(x_1, y_1) \in \mathbb{N}^2$ is a fundamental solution for (E) (i.e., with minimal x_1), and assume that $(x, y) \in \mathbb{N}^2$ is any solution to (E). Show that $(x + y\sqrt{d}) = (x_1 + y_1\sqrt{d})^n$ for some $n \in \mathbb{N}$.

34. (a) Show that if $d = c^2 - 1$ for some $c \in \mathbb{N}$ with $c \geq 2$, then $(c, 1)$ is a fundamental solution of (E).

(b) Show that if $d = c(c+1)$ for some $c \in \mathbb{N}$, then $(2c+1, 2)$ is a fundamental solution of (E).

(c) Find fundamental solutions of (E) in the cases $d = 5, 6, 7, 8, 10$.

35. Let $\alpha \in \mathbb{Q}$. Show that there are only finitely many relative coprime $x, y \in \mathbb{Z}$ with $y \neq 0$ such that

$$|\alpha - \frac{x}{y}| < \frac{1}{y^2}\,.$$

Exercises Math 118, Winter 2000, Week 9

Robert Boltje

36. Let $d \in \mathbb{N}$ be not a square and consider the equation

$$X^2 - dY^2 = -1\,. \tag{F}$$

Assume that $(x, y), (x', y') \in \mathbb{N}^2$ are solutions to (F). Show that

$$x \leq x' \iff y \leq y' \iff x + \sqrt{d}y \leq x' + \sqrt{d}y'\,.$$

(A solution $(x, y) \in \mathbb{N}^2$ is called a *fundamental solution to (F)* if $x \leq x'$ for any solution $(x', y') \in \mathbb{N}^2$.)

37. Let $d \in \mathbb{N}$ be not a square and consider besides (F) the equation

$$X^2 - dY^2 = 1\,. \tag{E}$$

Assume that Equation (F) is solvable in $\mathbb{N}^2$ and that $(x, y) \in \mathbb{N}^2$ is a fundamental solution to (F). For $n \in \mathbb{N}$, define $(x_n, y_n) \in \mathbb{N}^2$ by $x_n + \sqrt{d}y_n = (x + \sqrt{d}y)^n$. Show the following statements:

(a) The pair (x_2, y_2) is a fundamental solution to (E).

(b) The pairs (x_n, y_n), $n \in \mathbb{N}$ even, form the set of solutions to (E) in $\mathbb{N}^2$.

(c) The pairs (n_n, y_n), $n \in \mathbb{N}$ odd, form the set of solutions to (F) in $\mathbb{N}^2$.

(Hint: Use the norm map.)

38. Show that (F) has no solution for $d = 34$.

39. Compute the continued fraction expansion of $87/101$, $\sqrt{2}$, and $\sqrt{5}$.

40. Compute the continued fraction expansion of $\sqrt{13}$ and find a fundamental solution to (E) for $d = 13$. Find a fundamental solution to (F) if possible.