1. Арифметика.

◇ **1.1.** *Доказать, что* $\text{НОК}(a,b)\text{НОД}(a,b) = |ab|$.

◇ **1.2.** *a) Докажите, что если* $\text{НОД}(a,b) = 1$, *то наименьшее натуральное число, представимое в виде* $ax + by$ $x, y \in \mathbb{Z}$, *равно 1.*
b) Докажите, что при этом уравнение $ax+by = 1$ *имеет решение* $(x_0; y_0)$, *у которого* $|x_0| \leq |b/2|$.

◇ **1.3.** *Обобщите теорему о существовании решения уравнения* $ax + by = 1$ *на уравнение с* $n > 2$ *неизвестными.*

◇ **1.4.** *Сформулируйте и обоснуйте алгоритм решения уравнения* $ax + by = 1$ *при помощи цепных дробей.*

◇ **1.5.** *Докажите корректность определения операций сложения и умножения в* $\mathbb{Z}_n$.

◇ **1.6.** *Докажите свойства сложения и умножения остатков:*

$$\begin{array}{llll} 1) & x + (y + z) = (x + y) + z; & 4) & x(yz) = (xy)z \\ 2) & x + y = y + x & 5) & xy = yx \\ 3) & x + \bar{0} = \bar{0} + x = x & 6) & x\bar{1} = \bar{1} + x = x \end{array} \tag{1.1}$$

◇ **1.7.** *Выпишите и рассмотрите внимательно таблицы сложения и умножения в* $\mathbb{Z}_n$, *для* $n = 2,\ 3,\ 4,\ 5,\ 6,\ 7$ *и* 8.

Наименьшее число раз, которое нужно сложить данный остаток $x \in \mathbb{Z}_n$ с собой, чтобы получить $\bar{0}$, называется его *порядком по сложению.*

◇ **1.8.** *Придумайте формулу для вычисления порядка по сложению остатка* $\bar{a} \in \mathbb{Z}_n$. *(Кроме знаков арифметических действий, можно еще использовать функции* НОК *и* НОД.*)*

◇ **1.9.** *При каких значениях* n *в* $\mathbb{Z}_n$ *встречаются делители нуля? Как узнать, является ли* $\bar{a} \in \mathbb{Z}_n$ *делителе нуля?*

Нильпотентными называют остатки, которые при возведении в некоторую степень дают нуль.

◇ **1.10.** *При каких значениях* n *в* $\mathbb{Z}_n$ *встречаются нильпотентные элементы? Как узнать, является ли* $\bar{a} \in \mathbb{Z}_n$ *нильпотентным? Как перечислить все нильпотентные элементы в данном* $\mathbb{Z}_n$*?*

◇ **1.11.** *Докажите, что сумма нильпотентных остатков снова является нильпотентным.*

Идемпотентными называют отличные от $\bar{0}$ и $\bar{1}$ остатки, которые при возведении в квадрат не меняются.

◇ **1.12.** *Докажите, что идемпотентные остатки всегда являются делителями нуля.*

◇ **1.13.** *Докажите, что если* $x \in \mathbb{Z}_n$ *является идемпотентным, то* $\bar{1} - x$ *тоже.*

◇ **1.14.** *При каких значениях* n *в* $\mathbb{Z}_n$ *встречаются идемпотентные элементы? Как перечислить все идемпотентные элементы в данном* $\mathbb{Z}_n$*?*

◇ **1.15.** *Пусть* $\bar{a} \in \mathbb{Z}_n$, *где* a *— целое число от 0 до* $n - 1$. *Укажите формулу для остатка, противоположного к* $\bar{a}$ *(т.е. такого* $\bar{x}$, *что* $\bar{a} + \bar{x} = 0$.

◇ **1.16.** *Докажите, что при простом* p *в* $\mathbb{Z}_p$ *любое уравнение первой степени* $\alpha x + \beta = \bar{0}$ *при ненулевом* α *имеет единственное решение.*

◇ **1.17.** *Покажите, что если число* n *не простое, то уравнение* $\alpha x + \beta = \bar{0}$ *при ненулевом* α *может как не иметь решений, так и иметь несколько решений. Как по* $\alpha = \bar{a}$, $\beta = \bar{b}$ *и* n *указать число решений этого уравнения?*

◇ **1.18.** *Докажите, что при простом p уравнение $x^2 = \bar{1}$ имеет ровно два решения в $\mathbb{Z}_p$.*

◇ **1.19.** *Докажите, что при $n = 2^k$, $k > 2$, уравнение $x^2 = \bar{1}$ имеет ровно четыре решения в $\mathbb{Z}_n$.*

◇ **1.20.** *Докажите, что для любого натурального N существует такое n, что уравнение $x^2 = \bar{1}$ имеет в $\mathbb{Z}_n$ не менее N решений.*

◇ **1.21.** *Докажите, что при простом $p \neq 2$ ровно половина ненулевых остатков в $\mathbb{Z}_p$ является квадратами.*

◇ **1.22.** *При каких простых p остаток $-\bar{1}$ является квадратом в $\mathbb{Z}_p$?*

◇ **1.23.** *а) Докажите, что при простом p любое квадратное уравнение с коэффициентами из $\mathbb{Z}_p$ имеет в $\mathbb{Z}_p$ не более двух корней.*
б) Объясните, в каком месте доказательство из предыдущего пункта перестает быть верным при не простом p.
в) Верна ли теорема Виета для квадратных уравнений с коэффициентами в $\mathbb{Z}_n$?
г) Объясните, как и в какой мере можно пользоваться в $\mathbb{Z}_n$ школьными формулами для корней квадратного уравнения.

◇ **1.24.** *Придумайте алгебраическое уравнение вида $x^k + a_1x^{k-1} + \ldots a_{k-1}x + a_k = 0$ наименьшей возможной степени k с коэффициентами из $\mathbb{Z}_n$, которое имело бы в $\mathbb{Z}_n$ ровно n различных корней,*
а) для $n = 101$; б) для $n = 111$; в) для $n = 121$.

◇ **1.25.** *1) Верно ли, что если сумма квадратов двух целых чисел делится на 7, то каждое из этих чисел делится на 7?*

2) Верно ли, что если сумма квадратов двух целых чисел делится на 13, то каждое из этих чисел делится на 13?

3) Верно ли, что если сумма кубов трех целых чисел делится на 7, то хоть одно из этих чисел делится на 7?

◇ **1.26.** *Докажите теорему Вильсона: если p простое, то $(p-1)! \equiv -1 \pmod{p}$.*

◇ **1.27.** *а) Вычислите произведение всех ненулевых остатков в в $\mathbb{Z}_p$ при простом p.*
б) Вычислите произведение всех обратимых остатков в $\mathbb{Z}_n$.*

Функцией Эйлера называется

$$\varphi(n) = \text{количество натуральных чисел, меньших } n \text{ и взаимно простых с } n. \tag{1.2}$$

◇ **1.28.** *Вычислите $\varphi(n)$ для $n = 2, 3, 4, \ldots, 10$.*

◇ **1.29.** *Вычислите $\varphi(2^m)$.*

◇ **1.30.** *Вычислите $\varphi(p^m)$, где p — простое число.*

◇ **1.31.** *Докажите, что если числа k и m взаимно просты, то $\varphi(km) = \varphi(k)\varphi(m)$.*

◇ **1.32.** *Докажите, что если остаток обратим в $\mathbb{Z}_n$, то некоторая его степень дает единицу.*

Наименьшая положительная степень, при возведении в которую остаток дает единицу, называется его *порядком по умножению.*

◇ **1.33.** *Докажите, что если обратимый остаток в некоторой степени дает единицу, то эта степень делится на его порядок по умножению.*

◇ **1.34.** *Какие порядки по умножению могут иметь ненулевые остатки в $\mathbb{Z}_p$ при простом p?*

◇ **1.35.** *Какие порядки по умножению могут иметь обратимые остатки в* $\mathbb{Z}_n$*?*

◇ **1.36.** *Докажите Малую теорему Ферма: при простом* p *и* $(a,p)=1$, $a^{p-1}\equiv 1 \pmod p$.

◇ **1.37.** *Докажите, что если* $(a,n)=1$, *то* $a^{\varphi(n)}\equiv 1 \pmod n$.

◇ **1.38.** *1) Найдите остаток от деления* $2^{2010}+3^{2010}$ *на* 13.

2) Докажите, что $2^{100}+3^{100}$ *делится на* 97.

3) Найдите остаток от деления $2007^{2008^{2009}}$ *на* 11.

2. Поля и кольца. Знакомство.

◇ **2.1.** *Покажите, что если множество* X *содержит больше одного элемента, то операция композиции на множестве отображений множества* X *в себя не коммутативна.*

◇ **2.2.** *Придумайте коммутативную, но не ассоциативную операцию.*

◇ **2.3.** *Придумайте ассоциативную, но не коммутативную операцию.*

◇ **2.4.** *Сколькими различными способами можно расставить скобки в произведении* $a_1 * a_2 * \ldots a_n$, *так чтобы порядок выполнения действий был определен однозначно? (Менять порядок сомножителей нельзя!)*

◇ **2.5.** *Докажите, что если операция ассоциативна, то все различные способы расстановки скобок в произведении* $a_1 * a_2 * \ldots a_n$ *дают один и тот же результат. (Менять порядок сомножителей по-прежнему нельзя!)*

◇ **2.6.** *Докажите, что в любом множестве с бинарной операцией имеется не более одного нейтрального элемента.*

◇ **2.7.** *Существует ли нейтральный элемент для следующих операций на множествах:*

1) Операция композиции на множестве отображений множества X *в себя;*

2) Операция $\min(a,b)$ *на множестве неотрицательных действительных чисел* $[0;+\infty)$*;*

3) Операция $\min(a,b)$ *на множестве всех действительных чисел* $\mathbb{R}$*;*

4) Операция НОД(a,b) *на множестве натуральных чисел* $\mathbb{N}$*;*

5) Операция НОК(a,b) *на множестве натуральных чисел* $\mathbb{N}$*;*

6) Операция умножения на множестве всех периодических функций из $\mathbb{R}$ *в* $\mathbb{R}$, *имеющих период* 2π*;*

7) Операция объединения множеств на множестве всех подмножеств данного множества Ω*;*

8) Операция пересечения множеств на множестве всех подмножеств данного множества Ω*;*

9) Операция симметрической разности множеств $(A \oplus B = (A \setminus B) \cup (B \setminus A))$ *на множестве всех подмножеств данного множества* Ω.

◇ **2.8.** *1) Докажите, что в произвольном поле* $(-a)b=-ab$. *В частности,* $(-1)a=-a$.
2) Докажите, что в произвольном поле если $ab=0$, *то либо* $a=0$, *либо* $b=0$.
3) Докажите, что в произвольном поле умножение на ноль всегда дает ноль: $a0=0$.

◇ **2.9.** *Докажите, что в* $\mathbb{Q}$ *нет меньших подполей.*

◇ **2.10.** *1) Докажите, что множество действительных чисел вида $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ является подполем в $\mathbb{R}$.*
2) Является ли множество действительных чисел вида $a + b\sqrt[3]{2}$, $a, b \in \mathbb{Q}$ подполем в $\mathbb{R}$? Как описать наименьшее подполе в $\mathbb{R}$, содержащее все такие числа?
3) Описать наименьшее подполе в $\mathbb{R}$, содержащее $\sqrt{2}$ и $\sqrt{3}$.
4) Найдите все подполя поля из п. 3.

Рассмотрим евклидову плоскость и зафиксируем на ней единичный отрезок. Множество E будет состоять из длин всех отрезков, которые можно построить циркулем и линейкой, нуля и всех противоположных им чисел.

◇ **2.11.** *1) Докажите, что E является подполем в $\mathbb{R}$.*
2) Докажите, что если $x \in E$, $x > 0$, то $\sqrt{x} \in E$.
**3) Докажите, что $E \neq \mathbb{R}$.*

◇ **2.12.** ** 1) Докажите, что $\overline{\mathbb{Q}}_{\mathbb{R}}$ является подполем в $\mathbb{R}$.*
2) Докажите, что E является подполем в $\overline{\mathbb{Q}}_{\mathbb{R}}$.

◇ **2.13.** *Докажите, что при простом p $\mathbb{Z}_p$ является полем.*

Для этих полей имеется другое общепринятое обозначение $\mathbb{F}_p$, которое мы будем использовать чаще, чем $\mathbb{Z}_p$.

◇ **2.14.** *Докажите, что в $\mathbb{F}_p$ нет меньших подполей.*

◇ **2.15.** *Докажите, что при изоморфизме полей $\varphi(-a) = -\varphi(a)$, $\varphi(0) = 0$ и $\varphi(1) = 1$.*

◇ **2.16.** *Докажите, что в любом поле*

$$(\underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{n}) + (\underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{m}) = \underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{n+m}; \tag{2.1}$$

$$(\underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{n}) \cdot (\underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{m}) = \underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{nm}. \tag{2.2}$$

◇ **2.17.** *Докажите, что если среди кратностей единичного элемента поля $\mathbb{K}$ нет повторений, то $\mathbb{K}$ содержит подполе, изоморфное $\mathbb{Q}$.*

◇ **2.18.** *Докажите, что если среди кратностей единичного элемента поля $\mathbb{K}$, имеются повторения, то $\mathbb{K}$ содержит подполе, изоморфное $\mathbb{F}_p$.*

Характеристикой поля $\mathbb{K}$ (обозначается $\operatorname{char}\mathbb{K}$) называется наименьшее положительное число p, такое, что $\underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{p} = \mathbf{0}$. Если же такого числа p не существует, то полагают по определению $\operatorname{char}\mathbb{K} = 0$.

◇ **2.19.** *1) Докажите, что $\operatorname{char}\mathbb{K}$ является простым числом (или 0).*
2) Докажите, что при определении характеристики вместо единицы можно было взять любой ненулевой элемент поля. Другими словами, требуется доказать, если a — любой ненулевой элемент поля характеристики ноль, то любая его кратность отлична от нуля, а если a — любой ненулевой элемент поля характеристики $p > 0$, то $\underbrace{a + a + \ldots + a}_{m} = 0$ равносильно тому, что m кратно p.

◇ **2.20.** *Докажите, что в поле характеристики $p > 0$ $(a + b)^p = a^p + b^p$.*

В этом листке мы будем работать **только с коммутативными ассоциативными кольцами с единицей**, которые мы будем для краткости называть просто **кольцами**.

◇ **2.21.** *1) Докажите, что в произвольном кольце* $(-a)b = -ab$. *В частности,* $(-1)a = -a$.
2) Докажите, что в произвольном кольце умножение на ноль всегда дает ноль: $a0 = 0$.

◇ **2.22.** *Верно ли, что*

1) *произведение двух обратимых элементов является обратимым элементом?*

2) *если произведение двух элементов является обратимым элементом, то хотя бы один сомножитель является обратимым элементом?*

3) *если произведение двух элементов является обратимым элементом, то оба сомножителя являются обратимыми элементами?*

4) *если произведение двух элементов является делителем нуля, то оба сомножителя являются делителями нуля?*

5) *если произведение двух элементов является делителем нуля, то хотя бы один сомножитель является делителем нуля?*

6) *произведение двух нильпотентных элементов является нильпотентным элементом?*

7) *если произведение двух элементов является нильпотентным, то хотя бы один сомножитель является нильпотентным?*

8) *произведение любого элемента на нильпотентный является нильпотентным?*

9) *произведение двух идемпотентных элементов, является идемпотентным?*

10) *сумма двух обратимых элементов снова является обратимым?*

11) *сумма двух делителей нуля снова является делителем нуля?*

12) *сумма двух нильпотентных элементов снова является нильпотентным?*

13) *сумма двух идемпотентных элементов снова является идемпотентным?*

◇ **2.23.** *Докажите, что идемпотентные элементы всегда являются делителями нуля.*

◇ **2.24.** *Докажите, что если элемент кольца* x *является идемпотентным, то* $1 - x$ *тоже является идемпотентным.*

◇ **2.25.** *Докажите, что следующие множества с заданными на них операциями сложения и умножения являются кольцами (коммутативными ассоциативными и с единицей!). Найдите в них все делители нуля, нильпотентные и идемпотентные элементы (если таковые есть).*

1) *Множество всех непрерывных функций из* $\mathbb{R}$ *в* $\mathbb{R}$ *с обычными операциями сложения и умножения функций.*

2) *Множество всех непрерывных функций из* $\mathbb{R} \setminus \{0\}$ *в* $\mathbb{R}$ *с обычными операциями сложения и умножения функций.*

3) *Множество всех подмножеств данного множества* Ω*; в качестве операции сложения берется симметрическая разность двух множеств, а в качестве умножения — пересечение.*

4) *Множество всех линейных функций из $\mathbb{R}$ в $\mathbb{R}$ (т.е. всех $f(x) = kx + b$, $k, b \in \mathbb{R}$); в качестве сложения берется обычное сложение функций, а умножение определяется следующим геометрическим способом. Две линейные функции перемножаются обычным образом, получается квадратный трехчлен, графиком которого является парабола (или прямая, если один из сомножителей был константой). К полученному графику проводится касательная в точке его пересечения с осью ординат; уравнение полученной прямой виде $f(x) = kx + b$ и называется произведением двух исходных функций в этом кольце.*[1]

5) *Множество векторов плоскости, на которой введена прямоугольная система координат. В качестве сложения берется обычное сложение векторов, а умножение (которое мы в этой задаче, чтобы не создавать путаницы, будем обозначать звездочкой) определяется следующим образом. Если два вектора $\vec{u}$ и $\vec{v}$ имеют координаты $\vec{u} = (a; b)$ то $\vec{v} = (c; d)$ то $\vec{u} * \vec{v} = (ac; bd)$.*

6) *Изменим в условиях предыдущей задачи закон умножения: $\vec{u} * \vec{v} = (ac - bd; ad + bc)$.*

7) *Докажите, что кольца из последних трех пунктов попарно не изоморфны друг другу.*

◇ **2.26.** *Докажите, что при изоморфизме колец $\varphi(-a) = -\varphi(a)$ и $\varphi(0) = 0$.*

◇ **2.27.** *1) Докажите, что любое кольцо из двух элементов изоморфно $\mathbb{Z}_2$.*
2) Докажите, что любое кольцо из трех элементов изоморфно $\mathbb{Z}_3$.
3) Перечислите (с точностью до изоморфизма) все кольца, состоящие из четырех элементов.

◇ **2.28.** * *Заметим, что примеры колец из п. 5 и 6 задачи 2.25 построены похожим образом. Естественно спросить, какие еще кольца можно так получить. Зафиксируем какие-нибудь действительные числа α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 и определим закон умножения на множестве векторов плоскости следующим образом: $\vec{u} * \vec{v} = (\alpha_1 ac + \beta_1 bc + \gamma_1 ad + \delta_1 bd; \alpha_2 ac + \beta_2 bc + \gamma_2 ad + \delta_2 bd)$. (Здесь, как и в 2.25, $\vec{u} = (a; b)$ то $\vec{v} = (c; d)$.) Интересно выяснить, при каких значениях α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 получится коммутативное ассоциативное кольцо с единицей. Отметим, что нужно уточнить вопрос, поскольку в кольцах из п. 5 и 6 задачи 2.25 получились разные единичные элементы. Выберем в качестве основного вариант п. 6: потребуем, чтобы единичным элементом был вектор $(1; 0)$.*

1) *При каких значениях констант α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 получится коммутативное ассоциативное кольцо, единичным элементом которого будет вектор $(1; 0)$?*

2) *Найдутся ли среди полученных колец кольца, изоморфные кольцу из п. 4 задачи 2.25?*

3) *Найдутся ли среди полученных колец кольца, изоморфные кольцу из п. 5 задачи 2.25?*

4) *Найдутся ли среди полученных колец кольца, не изоморфные кольцам из п. 4, 5 и 6 задачи 2.25?*

---

[1] Этот пример не является искусственным, как это может показаться на первый взгляд. Если нас интересуют только очень близкие к нулю значения переменной x, то при вычислениях естественно пренебрегать слагаемыми, в которые входит x во второй (и большей) степени. Докажите, что это приводит как раз к умножению, введенному в первой части задачи. Если же нас интересуют более точные вычисления, мы можем рассматривать квадратичные по x выражения и пренебрегать слагаемыми начиная с третьего порядка малости. Опишите получающееся таким образом кольцо.