1. Арифметика.

Задачи этого листка можно сдавать как по пунктам (в любом порядке), так и целиком. Если Вы заявляете, что можете решить какую-то задачу целиком, то преподаватель может зачесть Вам эту задачу, попросив рассказать выборочно (по своему усмотрению) только некоторые пункты. Оценка 10 за этот листок может быть получена, в частности, при сдаче следующего списка задач (без обсуждения остальных): 1.2, 1.4, 1.9, 1.13, 1.14, 1.16, 1.20, 1.22.

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

◇ **1.2.** *В этой задаче нельзя использовать теорему об однозначности разложения целого числа на простые множители.*
а) Докажите, что если $\text{НОД}(a,b) = 1$, *то наименьшее натуральное число, представимое в виде* $ax + by$ $x, y \in \mathbb{Z}$, *равно 1.*
б) Докажите, что если $\text{НОД}(a,b) = 1$, *и* bc *делится на* a, *то* c *делится на* a.
в) Докажите теорему об однозначности разложения целого числа на простые множители.

◇ **1.3.** *а) Докажите, что если* $\text{НОД}(a,b) = 1$, *то уравнение* $ax + by = 1$ *имеет решение* $(x_0; y_0)$, *у которого* $|x_0| \leq |b/2|$.
б) 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.** *а) Докажите корректность определения операций сложения и умножения в* $\mathbb{Z}_n$.
б) Докажите свойства сложения и умножения остатков:

$$\begin{array}{lll} 1) & x + (y + z) = (x + y) + z; & 4) \quad x(yz) = (xy)z \\ 2) & x + y = y + x & 5) \quad xy = yx \\ 3) & x + \overline{0} = \overline{0} + x = x & 6) \quad x\overline{1} = \overline{1} + x = x \\ 7) & x(y + z) = xy + xz; & \end{array} \tag{1.1}$$

◇ **1.6.** *Выпишите и рассмотрите внимательно таблицы сложения и умножения в* $\mathbb{Z}_n$, *для* $n =$ 2, 3, 4, 5, 6, 7 *и* 8. *(Эту задачу следует сдавать только тем, у кого не получаются задачи 1.7 и 1.10.)*

◇ **1.7.** *а) 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* $\bar{a} + \bar{x} = \bar{0}$).
б) Наименьшее число раз, которое нужно сложить данный остаток $x \in \mathbb{Z}_n$ *с собой, чтобы получить* $\bar{0}$, *называется его* **порядком по сложению**. *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.*)*
в) При каких значениях n *в* $\mathbb{Z}_n$ *встречаются делители нуля? Как узнать, является ли* $\bar{a} \in \mathbb{Z}_n$ *делителе нуля?*

◇ **1.8.** *а)* **Нильпотентными** *называют остатки, которые при возведении в некоторую степень дают нуль. При каких значениях* n *в* $\mathbb{Z}_n$ *встречаются нильпотентные элементы?*
б) Как узнать, является ли $\bar{a} \in \mathbb{Z}_n$ *нильпотентным? Как перечислить все нильпотентные элементы в данном* $\mathbb{Z}_n$*?*
в) Докажите, что сумма нильпотентных остатков снова является нильпотентным.

◇ **1.9. Идемпотентными** *называют отличные от* $\bar{0}$ *и* $\bar{1}$ *остатки, которые при возведении в квадрат не меняются (т.е. являются решениями уравнения* $x^2 = x$*).*
а) Докажите, что идемпотентные остатки всегда являются делителями нуля.
б) Докажите, что если $x \in \mathbb{Z}_n$ *является идемпотентным, то* $\bar{1} - x$ *тоже.*
в) При каких значениях n *в* $\mathbb{Z}_n$ *встречаются идемпотентные элементы? Как перечислить все идемпотентные элементы в данном* $\mathbb{Z}_n$*?*

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

◇ **1.11.** *а) Докажите, что при простом p уравнение $x^2 = \bar{1}$ имеет ровно два решения в $\mathbb{Z}_p$.*
б) Докажите, что при простом $p \neq 2$ ровно половина ненулевых остатков в $\mathbb{Z}_p$ является квадратами.

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

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

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

◇ **1.15.** *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) Верна ли теорема Виета для квадратных уравнений с коэффициентами в $\mathbb{Z}_n$ при непростом n?

◇ **1.16.** *Придумайте алгебраическое уравнение вида $x^k + a_1 x^{k-1} + \ldots a_{k-1}x + a_k = 0$ 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 $n = 121$.

◇ **1.17.** *а) Верно ли, что если сумма квадратов двух целых чисел делится на 7, то каждое из этих чисел делится на 7?*
б) Верно ли, что если сумма квадратов двух целых чисел делится на 13, то каждое из этих чисел делится на 13?
в) Верно ли, что если сумма кубов трех целых чисел делится на 7, то хоть одно из этих чисел делится на 7?

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

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

◇ **1.20.** *Функцией Эйлера называется*

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

а) Вычислите $\varphi(n)$ для $n = 2, 3, 4, \ldots, 10$. б) Вычислите $\varphi(2^m)$.
в) Вычислите $\varphi(p^m)$, где p — простое число.
г) Докажите, что если числа k и m взаимно просты, то $\varphi(km) = \varphi(k)\varphi(m)$.

◇ **1.21.** *а) Докажите, что если остаток обратим в $\mathbb{Z}_n$, то некоторая его степень дает единицу.*
б) Наименьшая положительная степень, при возведении в которую обратимый остаток дает единицу, называется его порядком по умножению. Докажите, что если обратимый остаток в некоторой степени дает единицу, то эта степень делится на его порядок по умножению.

◇ **1.22.** *а) Докажите теорему Вильсона: если p простое, то $(p-1)! \equiv -1 \pmod{p}$.*
б) Докажите Малую теорему Ферма: при простом p и $(a,p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$.
в) Докажите теорему Эйлера: если $(a,n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

◇ **1.23.** *а) Найдите остаток от деления $2^{2010} + 3^{2010}$ на 13.*
б) Докажите, что $2^{100} + 3^{100}$ делится на 97.
в) Найдите остаток от деления $2007^{2008^{2009}}$ на 11.