1. Определения

***Определение* 1.1.** Диофантовым уравнение называется уравнение, которое можно решить в $\mathbb{Z}$.

***Определение* 1.2.** a делится на b ($a \vdots b, b|a$), если $\exists c \in \mathbb{Z} : a = bc$.

Теорема 1.1 (О делении с остатком)**.** $a, b \in \mathbb{Z}, \exists!(q, r)$: $\begin{cases} q, r \in \mathbb{Z} \\ a = b \cdot q + r \\ 0 \leqslant r < |b| \end{cases}$

***Определение* 1.3.** Пусть $I \subset \mathbb{Z}$. I называется идеалом, если

$$\begin{cases} m, n \in I \Rightarrow m + n \in I \text{ (замкнутость по сложению)} \\ m \in I \Rightarrow \forall k \in \mathbb{Z}\colon k \cdot m \in I \text{ (замкнутость по домножению)} \\ I \neq \varnothing \end{cases}$$

Теорема 1.2. В $\mathbb{Z}$ любой идеал главный.

***Определение* 1.4.** Пусть $a, b \in \mathbb{Z}$. Тогда d — НОД$(a, b) = \gcd(a, b) = (a, b)$

Теорема 1.3.

1. $\forall a, b\ \exists d = (a, b)$
2. $\exists x, y \in \mathbb{Z} :\ d = ax + by$
3. $ax + by = c$ имеет решение $\iff c \vdots d$.

***Определение* 1.5.** a, b — взаимно просты, если $(a, b) = 1$, то есть $\langle a, b\rangle = \mathbb{Z}$

Лемма. $\begin{cases} ab \vdots c \\ (a, c) = 1 \end{cases} \Rightarrow b \vdots c.$

***Определение* 1.6.** $x \in \mathbb{Z}, x \neq \pm 1$, тогда x — простое число, если $x = x_1 x_2 \iff \left[\begin{array}{l} x_1 = \pm 1 \\ x_2 = \pm 1 \end{array}\right. \quad \forall x_1, x_2$

Свойство *. x — обладает свойством *, $\iff x \neq \pm 1 \wedge ab \vdots x \Rightarrow \left[\begin{array}{l} a \vdots x \\ b \vdots x \end{array}\right.$

Утверждение 1.4. p — простое $\iff$ p — обладает свойством *.

Теорема 1.5 (Основная теорема арифметики)**.** Пусть $n \in \mathbb{Z}, n \neq 0$. Тогда n единственным образом с точностью до перестановки сомножителей, представимо в виде(p_i — простые, $p_i > 0$)

$$n = \varepsilon p_1 p_2 \dots p_k, \varepsilon = \pm 1 = \operatorname{sign}(n).$$

Или, иными словами, существует единственное каноническое разложение:

$$n = \varepsilon p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, \varepsilon = \pm 1 = \operatorname{sign}(n), a_i > 0, p_1 < p_2 < \dots < p_k.$$

***Определение* 1.7.** $n \in \mathbb{Z}, n \neq 0, p$ — простое, тогда степень вхождения ($V_p(n) = k$) p в n — $\max\{k \mid n \vdots p^k\}$

В терминах разложения: $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. $V_p(n) = a_i$, а если p нет в разложении, то $V_p(n) = 0$.

***Определение* 1.8.** m — НОК (LCM, $[a, b]$), если $m \vdots a, m \vdots b$ и $\forall n\ n \vdots a \wedge n \vdots b \Rightarrow n \vdots m$

***Определение* 1.9.** Группой называется пара $(G, *)$, где G — множество, а $* : G \times G \to G$ — бинарная операция, так что выполнены свойства:

1. $\forall a, b, c \in G : (a * b) * c = a * (b * c)$. Ассоциативность.
2. $\exists e \in G : \forall a \in G\ a * e = e * a = a$. Существование нейтрального элемента.
3. $\forall a \in G \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$. Существование обратного элемента.

***Определение* 1.10.** Группа G называется абелевой, если $\forall x, y \in G : x * y = y * x$.

***Определение* 1.11.** Кольцо — тройка $(R, +, \cdot)$ (R — множество, $+, \cdot : R \times R \to R$), такая что:

1–4. $(R, +)$ — абелева группа. Нейтральный элемент обозначается 0, обратный к a — $-a$.

5. $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + b \cdot c$. Дистрибутивность.

***Определение* 1.12.** Кольцо R называется ассоциативным, если выполнено

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

***Определение* 1.13.** Кольцо R называется коммутативным, если

7. $a \cdot b = b \cdot a$

***Определение* 1.14.** Кольцо R называется кольцом с 1, если

8. $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$

***Определение* 1.15.** Коммутативное ассоциативное кольцо с 1 называется полем, если выполнена

9. $\forall a \in R \setminus \{0\}\ \exists b \in R\ ab = 1 \wedge 1 \neq 0$

***Определение* 1.16.** Пусть $a, b \in \mathbb{Z}$, говорят, что a сравнимо с b по модулю n ($a \equiv b \pmod n$), если $(a - b) \vdots n$. Эквивалентное определение: a и b имеют одинаковые остатки по модулю n.

***Определение* 1.17.** Фактор множества по отношению $\equiv$ обозначается $\mathbb{Z}/n\mathbb{Z}$.

Теорема 1.6. Пусть $n \in \mathbb{N}$. Тогда класс $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, где $\overline{a} + \overline{b} = \overline{a + b} \wedge \overline{a} \cdot \overline{b} = \overline{a \cdot b}$ — ассоциативное коммутативное кольцо с единицей.

***Определение* 1.18.** Пусть R — коммутативное ассоциативное кольцо с единицей. Тогда $\forall a \in R : a$ — делитель нуля $\Rightarrow \exists b \neq 0 : ab = 0$.

Лемма. $\forall a, b, c \in R$: $ab = ac \wedge a$ — не делитель нуля $\Rightarrow b = c$.

Лемма. $a \in R$: a — обратим $\Rightarrow a$ — не делитель нуля.

Теорема 1.7. $\forall a \in Z : \overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Тогда:

1. $\overline{a}$ — обратим $\iff (a, n) = 1$
2. $\overline{a}$ — делитель нуля $\iff (a, n) \neq 1$.

Следствие. n — простое $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ — поле.

***Определение* 1.19.** $\forall$ ассоциативного кольца с 1 R: R — называется кольцом без делителей нуля (область целостности), если делитель нуля только 0. $ab = 0 \iff a = 0 \vee b = 0$.

***Определение* 1.20.** Гомоморфизмом колец $f : R_1 \mapsto R_2$ называется такое отображение, что $\forall r_1, r_2 \in R_1 : f(r_1 + r_2) = f(r_1) + f(r_2), f(r_1 r_2) = f(r_1) \cdot f(r_2), f(1) = 1$.

***Определение* 1.21.** Гомоморфизмом группы $f : G_1 \mapsto G_2$ называется такое отображение, что $\forall g_1, g_2 \in G_1 : f(g_1 g_2) = f(g_1) \cdot f(g_2)$.

***Определение* 1.22.** R_1, R_2 — кольца. Рассмотрим $(R_1 \times R_2, +, \cdot) : (r_1, r_2) +_{R_1 \times R_2} (r_1' r_2') \coloneqq (r_1 +_{R_1} r_2, r_2 +_{R_2} r_2')$, где $+_{R_1 \times R_2}, +_{R_1}, +_{R_2}$ — операции сложения для соответствующих множеств. Тоже самое для умножения. Тогда $R_1 \times R_2$ — тоже кольцо, т.к. соответствующие свойства операций унаследуются, что можно проверить самостоятельно. Но заметка: если R_1 и R_2 были областями целостности, то их произведение областью целостности почти никогда не будет.

***Определение* 1.23.** Биективный гомоморфизм (групп, колец, ...) (называется изоморфизмом, $\cong$) если каждым a_i задано ровно одно b_j и наоборот.

Теорема 1.8 (Китайская теорема об остатках)**.** Пусть $(m, n) = 1$, тогда $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Теорема 1.9 (КТО 2)**.** $m_1, m_2, m_3, \ldots, m_n \in \mathbb{Z} \wedge (m_i, m_j) = 1 \Rightarrow \mathbb{Z}/m_1, m_2, \ldots, m_n\mathbb{Z} \mapsto \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \ldots$ - изоморфизм колец.

Теорема 1.10 (КТО без колец)**.** $\forall m_1, \ldots, m_n \in \mathbb{Z} : \forall i, j (m_i, m_j) = 1, \forall a_1, \ldots, a_n \Rightarrow \exists x_0 \in Z : x \equiv a_1 \pmod{m_1} \wedge \ldots \wedge x \equiv a_n \pmod{m_n} \iff x \equiv x_0 \pmod{\prod_i m_i}$

***Определение* 1.24.** Пусть C — группа ($a \in C$), тогда порядок элемента a: $\operatorname{ord}(a) = \{\min k \in \mathbb{N} \mid a^k = 1\}$. А если такого k нет, то $\operatorname{ord}(a) = \infty$

Лемма. Пусть G — группа ($a \in G$). $\langle a \rangle = \{a, a^2, \ldots; a^{-1}, (a^{-1})^2, \ldots, e\} = \{a^k \mid k \in \mathbb{Z}\}$.Тогда $(\langle a \rangle, *)$ — группа.

***Определение* 1.25.** $\langle a \rangle$ называется циклической группой, порожденной a. G — циклическая группа $\iff \exists a \in G \colon G \cong \langle a \rangle$

Теорема 1.11 (О классификации циклических групп)**.** $\operatorname{ord} a = \infty \Rightarrow \langle a \rangle \cong (\mathbb{Z}, +)$. $\operatorname{ord} a = k \in \mathbb{N} \Rightarrow \langle a \rangle \cong (\mathbb{Z}/k\mathbb{Z}, +)$

Теорема 1.12 (Теорема Лангранжа)**.** Пусть G — группа. $\forall G$ — n-элементная группа, тогда $\forall a \in G : n \vdots \operatorname{ord} a$

Следствие. G — конечная группа ($a \in G$) $\Rightarrow a^{|G|} = e$

Утверждение 1.13. G — группа ($|G| = n$). G — циклическая $\iff \exists a \in G : \operatorname{ord} a = n$. МТФ: $\overline{a}, \overline{a}^2, \ldots$ — периодична с периодом $p - 1$. Утверждение: $\exists \overline{a} : p - 1$ — наименьший период этой последовательности.

***Определение* 1.26.** R — ассоциативное кольцо, тогда $R^* = \{a \in R | \exists a^{-1}\}$ — группа обратимых элементов.

Теорема 1.14 (Теорема Эйлера)**.** $\forall b \in (\mathbb{Z}/n\mathbb{Z})^* = b^{\varphi(n)} = 1$

Теорема 1.15 (Теорема Эйлера)**.** $\forall a \in \mathbb{Z} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Теорема 1.16 (Теорема о первообразном корне)**.** $p \in \mathbb{Z}$ — простое $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ — циклическая.

***Определение* 1.27.** Подгруппа группы G — пара $(H, *)$, где $H \subset G$, $*$ — замкнуто относительно H. Обозначается $\leqslant$.

***Определение* 1.28.** Подгруппа группы G порожденная множеством S ($S \subset G$) — наименьшая по включению подгруппа G, содержащая все элементы S.

$$\langle S\rangle = \bigcap_{H\leqslant G, S\subset H} H.$$

Теорема 1.17. $\forall S \subset G\colon \langle S\rangle = \{a_1^{\varepsilon_1}\dots a_k^{\varepsilon_k} \mid \forall i \in I a_i \in S \wedge \varepsilon_i = \pm 1\}$

Теорема 1.18. $(\mathbb{Z}/n\mathbb{Z})^*$ — циклическая $\iff \begin{cases} n = p^k & p > 2 \text{ — простое} \\ n = 2p^k & \text{см. выше} \\ n = 2 \vee n = 4 \end{cases}$.

Теорема 1.19. $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Тогда $x^2 = a$ имеет решение $\iff a^{\frac{p-1}{2}} = 1$

Теорема 1.20. $\pi(n)$ — количество простых на $[1, n]$. Тогда $\lim_{n\to+\infty} = \frac{\pi(n)}{\frac{n}{\ln n}} = 1$.

Следствие. Случайное число на $1, n$ — простое с вероятностью $\frac{1}{\ln n}$

Теорема 1.21 (Тест Люка)**.** Пусть $b \in \mathbb{Z}$, такое что $b^{n-1} = 1 \pmod n$ и $b^{\frac{n-1}{p_i}} \neq 1 \pmod n$. Тогда b — простое.

***Определение* 1.29.** Если n — составное, но $a^{n-1} \equiv 1 \pmod n$, то a — свидетель простоты.