

Теория чисел

Sokolnikov Alex

2025-2026

Содержание

1. Вступление	2
2. Алгоритм Евклида	3
3. Группы, кольца и поля	4
4. Кольцо \mathbb{Z}_m и группа \mathbb{Z}_m^*	7
4.1. Всякие определения	7
4.2. Тест Ферма	11
4.3. Улучшение теста на простоту (Миллер-Рабин)	12
5. Симметричная и асимметричная криптография	14
5.1. Система Полига-Хеллмана (экспоненциальное шифрование)	14
5.2. RSA	15
5.3. Шифровая подпись RSA	15
5.4. я запутался, как это называть уже	15
5.5. Слепая подпись RSA	16
6. КТО	16
7. Изоморфизмы	16
8. Многочлены	18

1. Вступление

Сложность некоторых основных алгоритмов:

- Логарифм

$$q \geq 2$$

$$Lq(n) = \lfloor \log_q n \rfloor + 1$$

$$Lq(0) = 1$$

$$Lq(n) = O(Lq'(n))$$

- Сложение

$$a + b \text{ за } O(\max(L(a), L(b)))$$

- Умножение

$$M(n) = O(n^2) \text{ — столбик}$$

$$M(n) = O(n^{\log_2 3}) \text{ — алгоритм Карацубы}$$

$$M(n) = O_\varepsilon(n^{1+\varepsilon}) \text{ — алгоритм Тома-Кука}$$

$$M(n) = O(n \log n \log \log n) \text{ — алгоритм Шенхаге-Штассена}$$

$M(n) = O(n \log n)$ (2019) — чтобы обогнать предыдущий алгоритм, нужно
число порядка $\log n = 2^{7 \cdot 10^{38}}$

2. Алгоритм Евклида

Определение 2.1

$a_1, \dots, a_n \in \mathbb{Z}$ не равные одновременно 0

Тогда их НОД-ом называется наибольшее число d , которое делит их всех, и обозначается (a_1, \dots, a_n)

$$(a, b) = ?$$

$$a = bq + r, 0 \leq r < b$$

$$(a, b) = (b, r)$$

Остается сделать так несколько раз:

$$\begin{cases} m_0 = a_0m_1 + m_2 \\ m_1 = a_1m_2 + m_3 \\ \dots \\ m_{k-1} = a_{k-2}m_{k-1} + m_k \\ m_{k-1} = a_{k-1}m_k \\ m_k = d \end{cases} \quad m_1 > m_2 > \dots > m_k > 0$$

Лемма 2.2

Пусть $m_0 \geq m_1$, тогда $k = O(\log m_1)$

Действительно: $m_{i-1} = a_{i-1}m_i + m_{i+1} \geq m_i + m_{i+1} \geq 2m_{i+1}$

Нетрудно убедиться, что взятие модуля через деление в столбик занимает $O(L(b) \cdot (L(q) + 1)) = O(L(b)(L(a) - L(b) + 1))$

Теорема 2.3

Сложность алгоритма Евклида, примененного к числам a, b с длинами $L(a), L(b) \leq n$ есть $O(n^2)$

$$\begin{aligned} L(m_1)(L(m_0) - L(m_1) + 1) + L(m_2)(L(m_1) - L(m_2) + 1) + \dots &\leq \\ &\leq L(m_1)(L(m_0) - L(m_1) + 1 + L(m_1) - L(m_2) + 1 + \dots) \leq \\ &\leq L(m_1)(L(m_0) + k) = O(L(m_1)L(m_0)) \end{aligned}$$

Замечание 2.4

Существуют более быстрые варианты алгоритма Евклида

На сегодняшний день известна оценка сложности $O(M(n) \log n)$

С алгоритмом Шенхаге-Штрассена, получим $O(n \log^2 n \log \log n)$

3. Группы, кольца и поля

Определение 3.1: Группа

Множество $(G, *)$ называется группой, если выполняется 3 свойства:

1. $(a * b) * c = a * (b * c)$ — ассоциативность
2. $\exists e : a * e = e * a = a$ — нейтральный элемент
3. $\forall a \in G \exists b : a * b = b * a = e$ — обратный элемент

Пример 3.2

- $G = \{e\}$
- $G = \{\mathbb{Z}, +\}$
- $G = \{R^*, \cdot\}$ — действительные числа без нуля
- $Isom(E^2)$ — движения плоскости ($E^2 = \mathbb{R}^2$ — Евклидова плоскость)
- S_n — множество перестановок

Определение 3.3: Абелева группа

Если $\forall a, b \in G$ верно $a * b = b * a$, группа называется коммутативной или абелевой.

Определение 3.4: Кольцо

Множество R с бинарными операциями $+$ и \cdot называется кольцом, если:

1. $(R, +)$ — абелева группа
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ — ассоциативность умножения
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c)a = b \cdot a + c \cdot a$ — дистрибутивность

Пример 3.5

- R — кольцо, тогда $R[x]$ — тоже кольцо
- $R = \{0\}$
- $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot), (M_n(\mathbb{R}), +, \cdot)$
- \mathbb{Z}_m — кольцо вычетов по $\mod m$

- $\mathbb{R}[[x]]$ — кольцо формальных степенных рядов над \mathbb{R}

Определение 3.6

1. Если $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$, то R называют кольцом с единицей
2. Если $\forall a, b \in R a \cdot b = b \cdot a$, то R называют коммутативным кольцом

Пример 3.7

$2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$ — кольцо без 1

Определение 3.8

Если R — кольцо с 1, то $a \in R$ называют обратимым элементом, если $\exists b :$
 $a \cdot b = 1 = b \cdot a$

Определение 3.9: Поле

Если в кольце R с 1 любой ненулевой элемент обратим, то R называют полем

Пример 3.10: Поля

$\mathbb{C}, \mathbb{R}, \mathbb{Q}$

Пример 3.11: Кольца, не являющиеся полями

$M_n(\mathbb{R}), 2\mathbb{Z}, \mathbb{R}[x], \mathbb{R}[[x]]$

Теорема 3.12: Основная теорема арифметики

Произвольное натуральное число $n > 1$ единственным образом (с точностью до порядка сомножителей) раскладывается в произведение простых:

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

Существование несложно показать по индукции: если n не простое, то $n = ab$, где $a, b < n$, после чего применяем предположение индукции.

Единственность покажем от противного. Пусть n — наименьшее число, обладающее двумя разложениями:

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} = q_1^{\beta_1} \cdots q_t^{\beta_t}, \text{ причем } p_i \neq q_j$$

Лемма 3.13: Лемма Евклида

$$a \mid bc, (a, b) = 1 \Rightarrow a \mid c$$

С помощью расширенного алгоритма Евклида (лемма о линейном представлении НОД) получим $au + bv = 1$

$$\begin{aligned} au + bv &= 1 \\ acu + bcv &= c \\ a \mid acu, a \mid bcv &\Rightarrow a \mid c \end{aligned}$$

Используя лемму выше можно “отщепляя” q_j можно доказать, что $p_1 \mid 1$ — противоречие.

Пример 3.14

Не во всех кольцах число раскладывается на простыми единственным способом: например, в $2\mathbb{Z}$ верно $30 \cdot 2 = 60 = 6 \cdot 10$

Определение 3.15

$$m \geq 1$$

Числа a и b называются сравнимыми по модулю m , если $a - b$ делится на m .
Будем обозначать $a \equiv b \pmod{m}$ или $a \equiv b \ (m)$

Определение 3.16

Классом вычетов \bar{a} называется множество (по модулю m)

$$\bar{a} = \{a + mt \mid t \in \mathbb{Z}\}$$

4. Кольцо \mathbb{Z}_m и группа \mathbb{Z}_m^*

4.1. Всякие определения

Определение 4.1

\mathbb{Z}_m — множество классов вычетов

Лемма 4.2: Свойство сравнений

- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$
- $ak \equiv bk \pmod{m}$, $(k, m) = 1 \Rightarrow a \equiv b \pmod{m}$
- $ak \equiv bk \pmod{m}$, $k \mid m \Rightarrow a \equiv b \pmod{m/k}$

Свойства непосредственно следуют из определения.

Следствие 4.3

На \mathbb{Z}_m можно ввести структуру кольца:

$$1. \bar{a} + \bar{b} = \overline{a + b}$$

$$2. \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Получим коммутативное кольцо с 1

Нужно еще проверить корректность (проверяется ручками):

$$1. \bar{a_1} = \overline{a_2}, \bar{b_1} = \overline{b_2}$$

Хотим $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ и $\overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}$.

Но это сразу следует из свойств сравнений.

$$2. \bar{0} + \bar{a} = \bar{a} + \bar{0} = \bar{a}$$

$$3. \bar{a} + \overline{-a} = \bar{0}$$

$$4. (\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$$

$$5. \bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$$

$$6. \bar{a}(\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

$$7. \bar{1} \cdot \bar{a} = \bar{a} \cdot \bar{1} = \bar{a}$$

$$8. \bar{a} \cdot (\bar{b} + \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

Определение 4.4

Пусть R — кольцо с 1, то множество

$$R^* = \{a \in R : a\text{ — обратим}\}$$

называется множеством обратимых элементов кольца.

Лемма 4.5

R^* — группа по умножению

Тоже несложно доказывается:

$a, b \in R^*$, хотим $a \cdot b \in R^*$

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

А ассоциативность следует из ассоциативности в кольце.

\mathbb{Z}_m^* — группа обратимых элементов кольца \mathbb{Z}_m

Теорема 4.6

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : (a, m) = 1\}$$

Пусть $\bar{a} \in \mathbb{Z}_m^*$.

Значит $\exists b : ab = 1 + mt \Rightarrow (a, m) = 1$.

Докажем в обратную сторону, пусть $(a, m) = 1$. В таком случае:

$$\exists u, v \in \mathbb{Z} : au + mv = 1$$

Перейдя к сравнению получим, что $au = 1$, то есть \bar{a} — обратим.

Определение 4.7

Полной системой вычетов по модулю m называется набор чисел a_1, \dots, a_m , где из каждого класса вычетов взято ровно одно число.

Понятно, что на таком наборе можно ввести вышеописанную структуру кольца.

Пример 4.8

Зачастую берутся $\{0, 1, \dots, m\}$

Или можно взять наименьшие по модулю: $\left\{-\frac{m-1}{2}, \dots, 0, 1, \dots, \frac{m-1}{2}\right\}$

Определение 4.9

Приведенной системой вычетом по модулю m называется набор чисел, взятых по одному из каждого класса \bar{a} такого, что $(a, m) = 1$.

Аналогично, на этом можно ввести структуру группы.

Определение 4.10

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_6^* = \{1, 5\}$$

Определение 4.11

Функцией Эйлера $\varphi(m)$ называется $|\mathbb{Z}_m^*|$

(количество натуральных чисел $\leq m$, взаимно простых с ним)

Определение 4.12

Функция $f : \mathbb{N} \rightarrow \mathbb{C}$ называется мультипликативной, если:

1. $f(1) = 1$
2. $\forall m, n \in \mathbb{N} : (m, n) = 1$ верно $f(m) \cdot f(n) = f(m \cdot n)$

Замечание 4.13

Пусть $f(mn) = f(m)f(n)$ для всех $m, n \in \mathbb{N}$.

Тогда f называется вполне мультипликативной.

Лемма 4.14

φ — мультипликативная функция

Следствие 4.15

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Докажем лемму:

Пусть $m = m_1 m_2$ и $(m_1, m_2) = 1$

$$|\mathbb{Z}_m^*| = \varphi(m) = \varphi(m_1 m_2)$$

С другой стороны:

$$\forall x \in \mathbb{Z}_m \quad x = ym_1 + z \quad 0 \leq y \leq m_2 - 1, 0 \leq z \leq m_1 - 1$$

$$(x, m) = 1 \Leftrightarrow \begin{cases} (x, m_1) = 1 \\ (x, m_2) = 1 \end{cases}$$

Но $(x, m_1) = 1 \Leftrightarrow (z, m_1) = 1$, поэтому есть $\varphi(m_1)$ способов выбрать z .

Если же y пробегает полную систему вычетов по модулю m_2 , то и $x = ym_1 + z$ тоже пробегает полную систему вычетов по модулю m_2 .

Пусть система не полная, тогда:

$$y_1 m_1 + z \equiv y_2 m_1 + z \pmod{m_2}$$

$$(y_1 - y_2)m_1 \equiv 0 \pmod{m_2}$$

$$y_1 - y_2 \equiv 0 \pmod{m_2}$$

Но все y различны, значит такого не могло быть.

Значит $(x, m_2) = 1$ возможно для $\varphi(m_2)$ значений y .

Но тогда мы выбираем x $\varphi(m_1) \cdot \varphi(m_2)$ способами, что и требовалось доказать.

Теорема 4.16: Теорема Эйлера

$$m \in \mathbb{N}, (a, m) = 1 \Rightarrow a^{\varphi}(m) \equiv 1 \pmod{m}$$

Теорема 4.17: Малая теорема Ферма

Это частный случай предыдущей теоремы

$$p — \text{простое}, (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Пусть $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ — приведенная система вычетов по модулю m . Умножим каждое на a , тогда $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ тоже является приведенной системой вычетов по модулю m :

$$ar_1 \equiv ar_2 \pmod{m}$$

$$\Updownarrow$$

$$r_1 \equiv r_2 \pmod{m}$$

В таком случае:

$$r_1 \cdot r_2 \cdots r_{\varphi(m)} \equiv (ar_1) \cdot (ar_2) \cdots (ar_{\varphi(m)}) \pmod{m}$$

$$\Updownarrow$$

$$1 \equiv a^{\varphi(m)} \pmod{m}$$

Замечание 4.18

Обратное к МТФ утверждение неверно.
Например, $2^{340} \equiv 1 \pmod{341}$, но $341 = 31 \cdot 11$

Теорема 4.19: Теорема Вильсона

Если p — простое, то $(p - 1)! \equiv -1 \pmod{p}$

Доказывается тем, что обратимые элементы (кроме ± 1) разбиваются на пары.

Замечание 4.20

На самом деле верно утверждение и в обратную сторону.

Определение 4.21

Пусть $b > 1$ — натуральное. Тогда составное число m называется псевдопростым по основанию b , если $b^{m-1} \equiv 1 \pmod{m}$.
(псевдопростым Ферма по основанию b)

Пример 4.22

91 является псевдопростым по основанию 3

4.2. Тест Ферма

Вход: n

Выход: “ n — составное” или “ n вероятно простое”

1. $b \in_R \{2, 3, \dots, n - 2\}$ и проверяем $b^{n-1} \equiv 1 \pmod{n}$
2. Если сравнение нарушается, то n — составное, иначе “ n вероятно простое”

Определение 4.23

Если n — составное и $\forall a \in \mathbb{Z}_n^*$ выполнено $a^{n-1} \equiv 1 \pmod{n}$, то такое число называется числом Кармайкла или абсолютно псевдопростым.

Пример 4.24

Первое число Кармайкла — 561

4.3. Улучшение теста на простоту (Миллер-Рабин)

Пусть n — нечетное простое. Разложим в виде $n - 1 = 2^s \cdot d$, $(d, 2) = 1$, $s \geq 1$

$$\begin{aligned} a^{n-1} - 1 &\equiv 0 \pmod{n} \\ a^{2^s d} - 1 &= (a^{2^{s-1} d} + 1) \cdot (a^{2^{s-2} d} + 1) \dots (a^d + 1)(a^d - 1) \equiv 0 \pmod{n} \end{aligned}$$

Получили лемму:

Лемма 4.25

Пусть $p > 2$ — простое, $p - 1 = 2^s d$, d — нечетно.

Тогда:

1. Либо $a^d \equiv 1 \pmod{p}$
2. Либо $\exists r : 0 \leq r \leq s - 1$, что $a^{2^r d} \equiv -1 \pmod{p}$.

,

Определение 4.26

Если n составное, но выполнено одно из условий выше, то оно называется сильно псевдопростым по основанию a .

Такая идея доводится до теста Миллера-Рабина:

Вход: n

Выход: “ n — составное” или “ n вероятно простое”

1. $b \in_R \{2, 3, \dots, n - 2\}$ и проверяем $b^{n-1} \equiv 1 \pmod{n}$

Проверим два вышеописанных условия на p .

2. Если оба условия неверны, то n — составное, иначе “не удалось определить”
3. Повторить 1-й шаг несколько раз. Если везде “не удалось определить”, то возвращаем “ n вероятно простое”

Замечание 4.27

Среди первых $25 \cdot 10^9$ есть 13 чисел, которые являются сильно псевдопростыми по основаниям 2, 3, 5.

Если добавить 7, 11, то все числа определяются корректно.

Теорема 4.28: (Рабин)

$$G_n = \{b \in \mathbb{Z}_n^* : n \text{ — сильно не простое по основанию } b\}$$

$$\Downarrow$$

$$|G_n| \leq \frac{\varphi(n)}{4}$$

Теорема 4.29

Для доказательства того, что n — простое (если n простое), то нужно проверить сильную псевдопростоту для простых оснований $b \leq 2 \ln^2 n$ при условии GRH (расширенная гипотеза Римана).

Теорема 4.30

\mathbb{Z}_m — поле $\Leftrightarrow m$ — простое
Обычно обозначают \mathbb{F}_p или $GF(p)$

Доказательство тривиально.

5. Симметричная и асимметричная криптография

5.1. Система Полига-Хеллмана (экспоненциальное шифрование)

$m \in \mathbb{Z}_p$, p — простое.

m — message

$k = (e, d)$ — key

При этом $ed \equiv 1 \pmod{p-1}$

c — cyphertext (зашифрованный текст)

Enc (encryption), Dec (decryption)

$c = Enc_e(m) = m^e \pmod{p}$

$m = Dec_d(c) = c^d \pmod{p}$

Хотелось бы $m = Dec_d(Enc_e(m))$ (и еще желательно $c = Enc_e(Dec_d(c))$)

Очевидно, что эти равенства выполняются по МТФ.

В общем случае:

- M — множество сообщений
- C — множество шифротекстов
- K — множество всех ключей
- Enc_k и Dec_k — функции шифрования такие, что:

$$Enc_k(Dec_k(c)) = c$$

$$Dec_k(Enc_k(m)) = m$$

5.2. RSA

p, q — различные простые.

Найдем $n = pq$ и посчитаем $\varphi(n) = (p - 1)(q - 1)$

Выберем пару экспонент (d, e) такую, что $de \equiv 1 \pmod{\varphi(n)}$

Пара (n, e) служит открытым ключом, а число d является секретным ключом.

Аналогично $m, c \in \mathbb{Z}_n$, $Enc_e(m) = m^e \pmod{n}$ и $Dec_d(c) = c^d \pmod{n}$.

Хотим:

$$m^{ed} = m^{1+\varphi(n)t} \equiv m \pmod{n}$$

Если $(m, n) = 1$, то верно по теореме Эйлера.

Иначе (m, n) равен одному из трех чисел: p, q, pq .

Последний случай тривиален, теперь разберем оставшиеся.

Не умаляя общности, пусть $m \equiv 0 \pmod{p}$, но $m \not\equiv 0 \pmod{q}$:

$$\begin{aligned} m^{1+(p-1)(q-1)t} &\equiv 0 \equiv m \pmod{p} \\ m^{1+(p-1)(q-1)t} &\equiv m \pmod{q} \quad (\text{МТФ}) \end{aligned}$$

Замечание 5.1

Систему можно взломать, если мы можем разложить n на простые множители, но человечество не умеет быстро такое делать.

5.3. Шифровая подпись RSA

A — Алиса, создала (n, e, d) , (n, e) — в открытом доступе.

$m \in \mathbb{Z}_n$ — сообщение для Боба

Алисы посыпает пару $(m, Sign_d(m))$

По определению $Sign_d(m) = Dec_d(m) = m^d \pmod{n}$

Для проверки подписи необходимо проверить, что $(Sign_d(m))^e \equiv m \pmod{n}$.

Если сообщение слишком длинное, то можно заменить $Dec_d(m)$ на $Dec_d(Hash(m))$

5.4. я запутался, как это называть уже

Определение 5.2

Биективное отображение f_k называется односторонней функцией с секретом, если:

1. \exists полиномиальный алгоритм вычисления f_k .
2. \exists полиномиальный алгоритм вычисления f_k^{-1} при известном k
3. \nexists полиномиального алгоритма вычисления f_k^{-1} , если k неизвестно.

Определение 5.3

Биективное отображение f называется односторонней функцией, если:

1. \exists существует полиномиальный алгоритм вычисления f
2. \nexists не существует полиномиального алгоритма вычисления f^{-1}

5.5. Слепая подпись RSA

Алиса (банк) знает: (n, e, d) — набор RSA, H — хэш-функция

Боб: выбирает $r \in_R \mathbb{Z}_n^*$ и посыпает Алисе $m' = H(m)r^e \pmod{n}$

Алиса: вычисляет $\sigma' = (m')^d \pmod{n}$ и посыпает Бобу.

Боб: $\sigma = \sigma'r^{-1} \equiv H^d(m) \pmod{n}$

Проверка подписи: $\sigma^e \equiv H(m) \pmod{n}$

6. КТО

Семиклассники доказывают, и вы справитесь.

7. Изоморфизмы**Определение 7.1**

Группы (G_1, \cdot) и $(G_2, *)$ изоморфны, если существует биективное отображение $\varphi : G_1 \rightarrow G_2$, такое, что $\varphi(g \cdot h) = \varphi(g) * \varphi(h)$.

Пример 7.2

1. $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$
2. $Sym(\Delta) \cong s_3$

Определение 7.3

Кольца $(R_1, +, \cdot)$ и (G_2, \oplus, \odot) изоморфны, если существует биективное отображение $\varphi : R_1 \rightarrow G_2$, такое, что:

1. $\varphi(g + h) = \varphi(g) \oplus \varphi(h)$.
2. $\varphi(g \cdot h) = \varphi(g) \odot \varphi(h)$.

Определение 7.4

Прямое произведение групп $(G_1, \cdot), (G_2, \circ)$ это $G_1 \times G_2$ с $(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot x_2, y_1 \circ y_2)$

Определение 7.5

Прямое произведение колец $(R_1, +_1, \cdot_1), (R_2, +_2, \cdot_2)$ это $R_1 \times R_2$ с $(x_1, x_2) + (y_1, y_2) = (x_1 +_1 x_2, y_1 +_2 y_2)$

Теорема 7.6

m_1, \dots, m_n — попарно взаимнопростые $m = m_1 \cdot \dots \cdot m_n$

Тогда $F : x \in \mathbb{Z}_m \rightarrow (x \pmod{m_1}, \dots, x \pmod{m_n}) \in \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_n}$

Следствие 7.7

$$\begin{aligned}\mathbb{Z}_m^* &\cong \mathbb{Z}_{m_1}^* \times \dots \times \mathbb{Z}_{m_n}^* \\ \varphi(m) &= \varphi(m_1) \cdot \dots \cdot \varphi(m_n)\end{aligned}$$

8. Многочлены

Определение 8.1

Пусть R — кольцо $a, b \in R$, $a, b \neq 0$ и $ab = 0$. В таком случае a и b называются делителями нуля.

Это будет мешать жить, поэтому многочлены нужно рассматривать над полем. Если F — поле, $P(x), Q(x) \in F[x]$, то $\deg P(x)Q(x) = \deg P(x) + \deg Q(x)$

Теорема 8.2

$$P(x), Q(x) \in F[x], F \text{ — поле}, \deg Q(x) > 0$$

$$\exists! T(x), R(x) \in F(x) : P(x) = Q(x)T(x) + R(x) \quad \deg R(x) < \deg Q(x)$$

Доказательство:

- Существование

Делим в столбик.

- Единственность

$$Q(x)T_1(x) + R_1(x) = Q(x)T_2(x) + R_2(x)$$

$$Q(x)(T_1(x) - T_2(x)) = R_2(x) - R_1(x)$$

$$\deg Q(x)(T_1(x) - T_2(x)) \geq \deg Q(x) > \deg R_2(x) - R_1(x)$$

Теорема 8.3: (Безу)

$$P(x) \mod (x - a) = P(a)$$

Делим с остатком, ура, сошлось.

Следствие 8.4

Многочлен степени n над полем имеет не более n корней.

Определение 8.5

F — поле, $P(x), Q(x) \in F[x]$

НОД многочленов $P(x)$ и $Q(x)$ называется общий делитель $T(x)$, который делится на все их общие делители.

Теорема 8.6

F — поле, $P(x), Q(x) \in F[x]$, $P(x), Q(x)$ не равны 0 одновременно.
Тогда:

1. Корректно определен НОД $P(x), Q(x)$ $D(x)$
2. $\exists U(x), V(x) \in F[x] : D(x) = P(x)U(x) + Q(x)V(x)$

1. Доказывается алгоритмом Евклида. Поскольку множество общих делителей не меняется, а в конце мы можем получить НОД, НОД существует и для первоначальной пары.
2. Доказывается тоже алгоритмом Евклида, как и для чисел.

Определение 8.7

F — поле, $P(x) \in F[x]$

$P(x)$ называют неприводимым, если его нельзя представить в виде $P(x) = P_1(x)P_2(x)$, где $P_1(x), P_2(x)$ не константы.

Теорема 8.8

Произвольный многочлен над произвольным полем единственным образом раскладывается на произведение неприводимых.

Определение 8.9

F — поле $m_1(x), \dots, m_n(x) \in F[x]$, любые два взаимнопросты.

Тогда $\forall a_1(x), \dots, a_n(x) \in F[x] \exists! p(x) : p(x) \equiv a_i(x) (m_i(x))$ и $\deg p(x) < \deg m_1(x) + \dots + \deg m_n(x)$.

Доказывается, например, по индукции, как и обычная КТО.