Теория чисел
Основной поток

Создал: Низамов Айнур, БПМИ225

Скачать актульную версию можно нажав по ссылке

При обнаружении ошибок просьба писать сюда (не анонимно, но быстро) или сюда (анонимно, но не очень быстро). Для любителей git предлагаю создавать issue на GitHub

Если Вам не нравится ТЧ, жалобы принимаются тут

Версия от 20.02.2023

Содержание:

Лекция 1

1.0. Введение

$\mathbb{N}$ – *натуральные числа*
$\mathbb{Z}$ – *целые числа*
$\mathbb{Q}$ – *рациональные числа*
$\mathbb{R}$ – *вещественные числа*
$\mathbb{C}$ – *комплексные числа*
$\mathbb{A}$ – *алгебраические числа* (не будут затронуты)

Обозначение. $a \mid b$ (реже $b \vdots a$) $\iff \exists c \in \mathbb{Z} : b = ac$ (a *делит* b)

Свойства:

- *Рефлексивность*: $a \mid a$ $(a \neq 0)$
- *Транзитивность*: $a \mid b, b \mid c \implies a \mid c$
- $a \mid b \implies \forall c \in \mathbb{Z}\ a \mid bc$
- $a \mid b, a \mid c \implies a \mid b \pm c$

Теорема 1 (*деление с остатком*). Пусть $a \in \mathbb{Z}, b \in \mathbb{N}$. Тогда $\exists! q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < b$
Доказательство. Возьмем $n \in \mathbb{Z}$, $nb \leq a < (n+1)b$. Положим $q = n, r = a - nb$, тогда $0 \leq r < b$. Теперь докажем единственность: $a = q_1 b + r_1, a = q_2 b + r_2$. Тогда $r_1 - r_2 = (q_2 - q_1)b$. Но $|r_1 - r_2| < b \implies r_1 - r_2 = 0 \implies q_2 - q_1 = 0$

■

Деление с остатком:

1. Однозначное разложение на простые множители (*основная теорема арифметики*)
2. Цепные дроби
3. Вычеты (*арифметика остатков*)

1.1. Алгоритм Евклида

Пусть $a, b \in \mathbb{Z}, |a| + |b| \neq 0$
Тогда $(a, b) = \text{НОД}(a, b)$ – *наибольший общий делитель.*

Определение. a и b *взаимно просты*, если $(a, b) = 1$

Предложение. Пусть $a = qb + r$. Тогда $(a, b) = (b, r)$
Доказательство.

$$\begin{cases} d \mid a, b \Longrightarrow d \mid r \\ d \mid b, r \Longrightarrow d \mid a \end{cases}$$

множество всех общих делителей a и b совпадает с b и r, значит $(a, b) = (b, r)$

■

Алгоритм Евклида. $a \in \mathbb{Z}, b \in \mathbb{N}$
$a = a_0 b + r_0$ $(0 \leq r_0 < b)$
$b = a_1 r_0 + r_1$ $(0 \leq r_1 < r_0)$
$r_0 = a_2 r_1 + r_2$ $(0 \leq r_2 < r_1)$
$\ldots$
$r_{n-3} = a_{n-1} r_{n-2} + r_{n-1}$ $(0 \leq r_{n-2} < r_{n-1})$
$r_{n-2} = a_n r_{n-1} + r_n$ $(r_n = 0)$, то есть $r_{n-1} \mid r_{n-2}$
$(a, b) \to (b, r_0) \to (r_0, r_1) \to \ldots \to (r_{n-3}, r_{n-2}) \to (r_{n-2}, r_{n-1}) = r_{n-1}$

Теорема 2 (*расширенный алгоритм Евклида*).
$\forall a, b \in \mathbb{Z}$ $(|a| + |b| \neq 0)$ $\exists \lambda, \mu \in \mathbb{Z} : (a, b) = \lambda a + \mu b$
Доказательство. $\forall k$ $r_k = r_{k-2} - a_k r_{k-1}$
$r_{n-1} = r_{n-3} - a_{n-1} r_{n-2} = \ldots = \lambda_k r_k + \mu_k r_{k+1} = \ldots = \lambda a + \mu b$

■

Лекция 2

2.0. Введение

Лемма (*важная*). Пусть $a, b, c \in \mathbb{Z}$. Тогда:

$$\begin{cases} a \mid bc \\ (a,b) = 1 \end{cases} \Longrightarrow a \mid c$$

Доказательство. $\exists \lambda, \mu:$

$$\lambda a + \mu b = 1$$

$$\underbrace{\lambda ac}_{a|ac} + \underbrace{\mu bc}_{a|bc} = \underbrace{c}_{a|c}$$

Левое слагаемое делится на a, потому что есть множитель a. Правое слагаемое делится на a по условию. Тогда и сумма делится на a.

■

2.1. Основная теорема арифметики

Теорема. Пусть $n \in \mathbb{N}, n > 1$. Тогда n раскладывается в произведение простых единственным образом с точностью до перестановки множителей.

Доказательство. Если n не имеет *нетривиального разложения*[1], то оно простое. Если $n = mk$, то $m, k < n$. Дальше показывается по индукции, что число можно разложить на такие числа, которые не имеют нетривиального разложения (простые). Теперь докажем единственность. Пусть $n = p_1 \cdot p_2 \cdot \ldots \cdot p_a = q_1 \cdot q_2 \cdot \ldots \cdot q_b$. Сократим все одинаковые множители из первого и второго разложения: $\forall i, j \; p_i \neq q_j$. Тогда $(p_1, q_j) = 1$. По важной лемме:

$p_1 \mid q_2 \cdot q_3 \cdot \ldots \cdot q_b$
$p_1 \mid q_3 \cdot \ldots \cdot q_b$
$\ldots$
$p_1 \mid q_b$

$(p_1, q_b) = 1$, но $p_1 \neq 1$ – противоречие.

■

Пусть $n \in \mathbb{N}, n > 1$. Тогда по основной теореме арифметики: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $p_i \neq p_j \; \forall i \neq j$, где p_i – простое. Это называется *каноническим разложением n на простые.*

Обозначение. $\nu_p(n) = \max\{d \in \mathbb{N} \cup \{0\} : p^d \mid n\}$ – *степень вхождения p в n.*

[1] Разложение $n = mk$ называется нетривиальным, если $m, k < n$ и $m, k \in \mathbb{N}$

С такими обозначениями разложение на простые множители можно записать так: $n = \prod\limits_{p|n} p^{\nu_p(n)} = \prod\limits_{p} p^{\nu_p(n)}$ – с какого-то момента $\nu_p(n)$ будет 0.

2.2. Цепные дроби

Вспомним алгоритм Евклида и разложим $\mathbb{Q}$ в цепную дробь:

$$\begin{array}{c|c}
a = a_0 b + r_0 & \dfrac{a}{b} = a_0 + \dfrac{r_0}{b} = \\
b = a_1 r_0 + r_1 & = a_0 + \dfrac{1}{\frac{b}{r_0}} = a_0 + \dfrac{1}{a_1 + \frac{r_1}{r_0}} = \\
\ldots & \ldots \\
r_{n-2} = a_n r_{n-1} & = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \frac{1}{a_n}}}}
\end{array}$$

Также есть другая, более короткая запись цепной дроби: $[a_0; a_1, \ldots, a_n]$, где $a_0 \in \mathbb{Z}$, $a_1, a_2, \ldots, a_n \in \mathbb{N}, a_n \neq 1$ (последнее видно по алгоритму на предпоследнем шаге: так как $r_{n-1} < r_{n-2}$, то $a_n = \frac{r_{n-2}}{r_{n-1}} \neq 1$).

Обозначение. $[\alpha]$ – целая часть α, $\{\alpha\} = \alpha - [\alpha]$ – дробная доля (часть) α

Пусть $\alpha \in \mathbb{R}$. Положим $\alpha_0 = \alpha$. Реккурента: $\alpha_{k+1} = \frac{1}{\{\alpha_k\}}$, $a_k = [\alpha_k]$, $k \in \mathbb{N} \cup \{0\}$

$\forall n \in \mathbb{N} \cup \{0\}$ верно $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n] = a_0 + \cfrac{1}{a_1 + \cfrac{}{\ddots + \cfrac{1}{a_{n-1} + \frac{1}{\alpha_n}}}}$

Если у цепной дроби есть период, то над каждой a_i (которая в периоде) рисуется черта. Например: $\sqrt{15} = [3; 1, 6, 1, 6, \ldots] = [3; \overline{1, 6}]$

Определение. Пусть $\alpha \sim [a_0; a_1, a_2, \ldots, a_k, \ldots]$. Тогда для $k = 0, 1, 2, \ldots$ дроби $\dfrac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ называются *подходящими дробями* числа α.

Теорема. $\forall k \in \mathbb{N} \cup \{0\}$ верно следующее: $\left|\alpha - \dfrac{p_k}{q_k}\right| \leq \dfrac{1}{q_k q_{k+1}} \leq \dfrac{1}{q_k^2}$

Реккурентные соотношения:

$p_k = a_k p_{k-1} + p_{k-2}$

$q_k = a_k q_{k-1} + q_{k-2}$

Все это будет доказано на следующей лекции.

Лекция 3

3.0. Введение

Давайте разложим $5+\dfrac{1}{3}$ в цепную дробь следующим образом: $5+\dfrac{1}{2+\frac{1}{1}}$. Запретим такие $\dfrac{1}{1}$, потому что можно отщепить 1 из числителя и получить исходное число разложение: $5+\dfrac{1}{2+1}=5+\dfrac{1}{3}$.

3.1. K-я подходящая дробь

Вспомним прошлую лекцию и дополним определение. Дробь вида $\dfrac{p_k}{q_k}=[a_0;a_1,\ldots,a_k]$, $p_k,q_k\in\mathbb{Z},q_k>0,(p_k,q_k)=1$ называется *k-й подходящей дробью.* Докажем некоторые факты, которые остались недоказанными в прошлый раз.

Теорема (*о реккурентных соотношениях для числителей и знаменателей подходящих дробей*). Пусть заданы последовательности α_k (*хвосты*), a_k (*неполные частные*). Тогда последовательности p и q заданы следующей реккурентной формулой:

$$p_k=a_kp_{k-1}+p_{k-2}$$

$$q_k=a_kq_{k-1}+q_{k-2}$$

Для удобства можно положить:

$$\begin{pmatrix}p_{-1} & p_{-2}\\ q_{-1} & q_{-2}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

Теперь последовательности p и q определены $\forall k\geq 0$

Теорема (*о континуантах*). Пусть $x_0,x_1,\ldots,x_k$ – независимые переменные. Положим:

$$\begin{pmatrix}P_{-1} & P_{-2}\\ Q_{-1} & Q_{-2}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

А также определим последовательности многочленов ($\forall k\geq 0$):

$$P_k(x_0,\ldots,x_k)=x_kP_{k-1}(x_0,\ldots,x_{k-1})+P_{k-2}(x_0,\ldots,x_{k-2})$$

$$Q_k(x_0,\ldots,x_k)=x_kQ_{k-1}(x_0,\ldots,x_{k-1})+Q_{k-2}(x_0,\ldots,x_{k-2})$$

Обозначение. Сокращенная запись P_k предполагает $P_k(x_0,\ldots,x_k)$ (аналогично и для Q_k).

Утверждения:

1. $\dfrac{P_k}{Q_k} = [x_0, \dots, x_k]$

2. $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$

3. $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k \cdot x_k$

Доказательство.

1. Докажем по индукции по k:

   База: $k = 0:$

   $$P_0(x_0) = x_0 P_{-1} + P_{-2} = x_0$$
   $$Q_0(x_0) = x_0 Q_{-1} + Q_{-2} = 1$$
   откуда $\dfrac{P_0(x_0)}{Q_0(x_0)} = x_0 = [x_0]$ (цепная дробь) – верно

   Переход: пусть верно $\forall k < n$, докажем для $k = n$:

   $$[x_0; \dots, x_{n-2}, x_{n-1}, x_n] = [x_0; \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n}]^{2} = \frac{P_{n-1}(x_0, \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n})}{Q_{n-1}(x_0, \dots, x_{n-2}, x_{n-1} + \frac{1}{x_n})} =$$
   $$= \frac{(x_{n-1} + \frac{1}{x_n})P_{n-2}(x_0, \dots, x_{n-2}) + P_{n-3}(x_0, \dots, x_{n-3})}{(x_{n-1} + \frac{1}{x_n})Q_{n-2}(x_0, \dots, x_{n-2}) + Q_{n-3}(x_0, \dots, x_{n-3})} = \frac{(x_{n-1} + \frac{1}{x_n})P_{n-2} + P_{n-3}}{(x_{n-1} + \frac{1}{x_n})Q_{n-2} + Q_{n-3}} =$$
   $$= \frac{x_n}{x_n} \cdot \frac{(x_{n-1} + \frac{1}{x_n})P_{n-2} + P_{n-3}}{(x_{n-1} + \frac{1}{x_n})Q_{n-2} + Q_{n-3}} = \frac{x_n(x_{n-1}P_{n-2} + P_{n-3}) + P_{n-2}}{x_n(x_{n-1}Q_{n-2} + Q_{n-3}) + Q_{n-2}} = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}} =$$
   $$= \frac{P_n}{Q_n} = \frac{P_n(x_0, x_1, \dots, x_n)}{Q_n(x_0, x_1, \dots, x_n)} = [x_0; x_1, \dots, x_n] \text{ – верно}$$

2. Докажем по индукции по k:

   База: $k = -1 : P_{-1}Q_{-2} - P_{-2}Q_{-1} = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^{-1-1} = (-1)^{-2}$ – верно

   Переход: пусть верно для $\forall k < n$, докажем дял $k = n$:

   $P_n Q_{n-1} - P_{n-1} Q_n = (x_n P_{n-1} + P_{n-2}) Q_{n-1} - P_{n-1}(x_n Q_{n-1} + Q_{n-2}) = x_n P_{n-1} Q_{n-1} +$
   $+ P_{n-2} Q_{n-1} - x_n P_{n-1} Q_{n-1} - P_{n-1} Q_{n-2} = P_{n-2} Q_{n-1} - P_{n-1} Q_{n-2} = -(P_{n-1} Q_{n-2} -$
   $- P_{n-2} Q_{n-1}) = -(-1)^{n-2} = (-1)^{n-1}$ – верно

3. Возьмем определитель:

   $$\begin{vmatrix} P_k & P_{k-2} \\ Q_k & Q_{k-2} \end{vmatrix} = \begin{vmatrix} P_k - P_{k-2} & P_{k-2} \\ Q_k - Q_{k-2} & Q_{k-2} \end{vmatrix} = \begin{vmatrix} x_k P_{k-1} & P_{k-2} \\ x_k Q_{k-1} & Q_{k-2} \end{vmatrix} = x_k \begin{vmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{vmatrix} =$$
   $$= x_k(P_{k-1} Q_{k-2} - P_{k-2} Q_{k-1}) = (-1)^{k-2} \cdot x_k = (-1)^k \cdot x_k$$

■

Доказательство теоремы (*о реккурентных соотношениях для числителей и знаменателей подходящих дробей*). Положим $x_0 = a_0, \dots, x_k = a_k$:

[2] Ключевой ход: $x_{n-1} + \frac{1}{x_n} = [x_{n-1}, x_n] = [x_{n-1} + \frac{1}{x_n}]$ – по алгоритму построения цепной дроби

$$\frac{P_k(a_0, \ldots, a_k)}{Q_k(a_0, \ldots, a_k)} = [a_0; a_1, \ldots, a_k]$$

Заметим, что:

- $P_k(a_0, \ldots, a_k), Q_k(a_0, \ldots, a_k) \in \mathbb{Z}$
- $Q_k(a_0, \ldots, a_k) \in \mathbb{N}$
- $(P_k(a_0, \ldots, a_k), Q_k(a_0, \ldots, a_k)) = 1$ – следствие пункта 2 из теоремы о континуантах.

Стало быть $p_k = P_k(a_0, \ldots, a_k),\ q_k = Q_k(a_0, \ldots, a_k)$
То есть $p_k = a_k p_{k-1} + p_{k-2},\ q_k = a_k q_{k-1} + q_{k-2}$, так как P_k и Q_k удовлетворяли этому.

■

Лекция 4

4.0. Введение

Вспомним 3 утверждения с прошлой лекции:

- $\dfrac{P_k}{Q_k} = [x_0, \ldots, x_k]$
- $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}$
- $P_k Q_{k-2} - P_{k-2} Q_k = (-1)^k \cdot x_k$

Следствие из теоремы о континуантах.

1. Справедливы $p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$
2. $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$
3. $p_k q_{k-2} - p_{k-2} q_k = (-1)^k \cdot a_k$

Доказательство. 1 доказывали на прошлой лекции, 2 и 3 мгновенно получаются из утверждений, которые тоже были доказаны на прошлой лекции

■

Предложение.

1. $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \ldots < \dfrac{p_{2k}}{q_{2k}} < \ldots \leq \alpha \leq \ldots < \dfrac{p_{2k+1}}{q_{2k+1}} < \ldots < \dfrac{p_3}{q_3} < \dfrac{p_1}{q_1}$
2. $\dfrac{p_k}{q_k} - \dfrac{p_{k-1}}{q_{k-1}} = \dfrac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \dfrac{(-1)^{k-1}}{q_k q_{k-1}}$
3. $\dfrac{p_k}{q_k} - \dfrac{p_{k-2}}{q_{k-2}} = \dfrac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}} = \dfrac{(-1)^k \cdot a_k}{q_k q_{k-2}}$
4. $q_k \geq 2 q_{k-2}$ $(\forall k \geq 1)$
5. $\left|\alpha - \dfrac{p_k}{q_k}\right| \leq \dfrac{1}{q_k q_{k+1}} \leq \dfrac{1}{q_k^2}$
6. $\left|\alpha - \dfrac{p_k}{q_k}\right| \geq \dfrac{a_{k+2}}{q_k q_{k+2}}$

Доказательство.

1. $\forall i = 2n, j = 2m+1$ $\dfrac{p_i}{q_i} < \dfrac{p_j}{q_j}$ следует из пункта 2 предложения. $\forall i = 2n$ $\dfrac{p_i}{q_i} < \dfrac{p_{i+2}}{q_{i+2}}$ по пункту 3 предложения верно (знаменатель всегда положительный, а числитель положительный так как $(-1)^k$ положительный при четном k). Аналогично показывается для нечетных индексов.

Далее $\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}]$. Рассмотрим последние 3 неполных частных: $a_{k-1} + \cfrac{1}{a_k + \cfrac{1}{\alpha_{k+1}}}$. Если обрубим α_{k+1} (получим $[a_0; a_1, \ldots, a_k]$), то знаменатель $a_k + \frac{1}{\underbrace{\alpha_{k+1}}_{>0}}$ уменьшится, значит дробь $\cfrac{1}{a_k + \cfrac{1}{\alpha_{k+1}}}$ увеличится. Следующий знаменатель увеличится, а дробь уменьшится и так далее. Из этого следует:

- $\alpha \geq \frac{p_{2k}}{q_{2k}}$
- $\alpha \leq \frac{p_{2k+1}}{q_{2k+1}}$

Выходит, что все четные не больше α, а нечетные – не меньше.

2. Даром из следствия 2 из теоремы о континуантах.

3. Даром из следствия 3 из теоремы о континуантах.

4. $q_k = \underbrace{a_k}_{\geq 1} q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} \geq 2q_{k-2}$

5. $\frac{p_k}{q_k} \begin{matrix} \leq \\ \geq \end{matrix} \alpha \begin{matrix} \leq \\ \geq \end{matrix} \frac{p_{k+1}}{q_{k+1}}, \quad \begin{matrix} \text{если } k \text{ – четное} \\ \text{если } k \text{ – нечетное} \end{matrix}$. Вычитаем $\frac{p_k}{q_k}$ и получаем что надо.

6. $\alpha \begin{matrix} \geq \\ \leq \end{matrix} \frac{p_{k+2}}{q_{k+2}} \begin{matrix} > \\ < \end{matrix} \frac{p_k}{q_k}, \quad \begin{matrix} \text{если } k \text{ – четное} \\ \text{если } k \text{ – нечетное} \end{matrix}$. Вычитаем $\frac{p_k}{q_k}$ и получаем что надо.

$\blacksquare$

Еще одно **следствие** из теоремы о континуантах. Пусть $\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha_k]$.
Тогда $\alpha = \frac{P_k(a_0, \ldots, a_{k-1}, \alpha_k)}{Q_k(a_0, \ldots, a_{k-1}, \alpha_k)} = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}$

Пример. $\varphi = \frac{1 + \sqrt{5}}{2}$

$$\varphi^2 = \varphi + 1$$

$$\varphi = 1 + \frac{1}{\varphi}$$

$\varphi = [1; \bar{1}]$ – самая простая цепная дробь для числа из $\mathbb{R}$

Пусть F_k – k-е число Фибоначчи. Положим $p_k = F_k$, $q_k = F_{k-1}$. Тогда $\lim\limits_{k \to \infty} \frac{p_k}{q_k} = \varphi$

Приложения *к линейным диофантовым уравнениям.*
$a, b \in \mathbb{N}$, $(a, b) = 1$. Как решить уравнение $ax + by = c$?

Пусть $\frac{a}{b} = [a_0; a_1, \ldots, a_{k-1}, a_k]$. Тогда $\frac{p_k}{q_k} = \frac{a}{b}$, $\frac{p_{k-1}}{q_{k-1}} = [a_0; a_1, \ldots, a_{k-1}]$

Следовательно $aq_{k-1} + b(-p_{k-1}) = (-1)^{k-1}$

Значит $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = (-1)^{k-1} \cdot c \cdot \begin{pmatrix} q_{k-1} \\ -p_{k-1} \end{pmatrix}$ – частичное решение уравнения $ax + by = c$

4.1. Сравнения и вычеты

Определение. Пусть $m \in \mathbb{N}, m \geq 2$ – *модуль*. Есть $a, b \in \mathbb{Z}$. Тогда a и b *сравнимы по модулю* m если $m \mid a - b$

Обозначение. $a \equiv b \pmod{m}$. Реже пишут как $a \underset{m}{\equiv} b$

Свойства:

1. Отношение сравнения является отношением *эквивалентности*.
2. Пусть выполняются $\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases}$. Тогда верно и $\begin{cases} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \\ ac \equiv bd \pmod{m} \end{cases}$
3. $a \equiv b \pmod{m}, \forall c \in \mathbb{N} \Longrightarrow ac \equiv bc \pmod{mc}$
4. $a \equiv b \pmod{m}, \forall c \in \mathbb{Z}\ (c, m) = 1 \Longrightarrow ac \equiv bc \pmod{m}$
5. Пусть $f(x) \in \mathbb{Z}[x]$[3], $a \equiv b \pmod{m}$. Тогда $f(a) \equiv f(b) \pmod{m}$

Доказательство.

1. Чтобы отношение сравнения было отношением эквивалентности, должны выполняться 3 условия. Проверим каждый:
   - *Рефлексивность*: $a \equiv a \pmod{m}$
   - *Симметричность*: $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$
   - *Транзитивность*: $a \equiv b \pmod{m},\ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$
2. $\begin{cases} m \mid a - b \\ m \mid c - d \end{cases} \Longrightarrow m \mid (a - b) + (c - d) \Longrightarrow m \mid (a + c) - (b + d) \Longrightarrow a + c \equiv$

   $\equiv b + d \pmod{m}$. Аналогично для вычитания.

   Для умножения:

   $\begin{cases} m \mid a - b \\ m \mid c - d \end{cases} \Longrightarrow \begin{cases} m \mid c(a - b) \\ m \mid b(c - d) \end{cases} \Longrightarrow m \mid c(a - b) + b(c - d) \Longrightarrow m \mid ac - bc +$

   $+bc - bd \Longrightarrow m \mid ac - bd \Longrightarrow ac \equiv bd \pmod{m}$

[3] $\mathbb{Z}[x]$ – многочлен с целыми коэффициентами от x

3. $m \mid a - b \Longleftrightarrow mc \mid (a-b)c$

4. С одной стороны: $m \mid a - b \Longrightarrow m \mid c(a-b)$

   С другой стороны: $m \mid c(a-b) \Longrightarrow m \mid a-b$ (по важной лемме, так как $(m, c) = 1$)

5. Не доказывалось на лекции.

$\blacksquare$

Лекция 5

5.0. Введение

Вспомним что такое сравнимость по модулю: $a \equiv b \pmod{m} \iff m \mid a - b$

Определение. Множество $a + m\mathbb{Z} = \{a + mt \mid t \in \mathbb{Z}\}$ называется *классом вычетов* числа a по модулю m. Еще обозначают как $\bar{a} = a + m\mathbb{Z}$

Обозначение. $\mathbb{Z}_m = \{a + m\mathbb{Z} \mid a \in \{0, 1, \dots, m-1\}\}$ – множество всех классов вычетов по модулю m. Также обозначают $\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}}$

5.1. Арифметические операции

Для $\bar{a}, \bar{b} \in \mathbb{Z}_m$ полагаем:

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \cdot \bar{b} = \overline{ab}$

Предложение. Операции корректно определены, то есть $\forall a_1, a_2, b_1, b_2$ таких, что $a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m}$ верно следующее:

$$\begin{cases} a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \\ a_1 b_1 \equiv a_2 b_2 \pmod{m} \end{cases}$$

Теперь (при наличии m) $a \equiv b \pmod{m} \iff \bar{a} = \bar{b}$

Определение. Пусть $m \in \mathbb{N}$, $m \geq 2$. Набор из m чисел $a_1, a_2, \dots, a_m$ называется *полной системой вычетов*, если $a_1, a_2, \dots, a_m$ – представители всех различных m классов вычетов.

Замечание. Если $a \equiv b \pmod{m}$, то $(a, m) = (b, m)$. Поэтому можно говорить о свойстве $\bar{a}$ быть взаимно простым с m.

Определение. Пусть $m \in \mathbb{N}$ $m \geq 2$. Набор $a_1, a_2, \dots, a_k$ называется *приведенной системой вычетов*, если $a_1, a_2, \dots, a_k$ – представители всех классов вычетов, взаимно простых с m.

Определение. *Функция Эйлера*: $\varphi(m) = |\{a \in \mathbb{Z} \mid 1 \leq a < em, (a, m) = 1\}|$

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

5.2. Много теорем

Теорема (*о полной и приведенной системах вычетов*). Пусть:

$$\begin{cases} m \in \mathbb{N},\ m \geq 2 \\ a \in \mathbb{Z},\ (a, m) = 1 \end{cases}$$

1. Если $b_1, \dots, b_m$ – полная система вычетов по модулю m, а также $c \in \mathbb{Z}$. Тогда $ab_1 + c, \dots, ab_m + c$ – тоже полная система вычетов.

2. Если $b_1, \dots, b_k$ – приведенная система вычетов по модулю m, а также $k = \varphi(m)$. Тогда $ab_1, \dots, ab_k$ – тоже приведенная система вычетов.

Доказательство. $\forall i \neq j\ b_i \not\equiv b_j \pmod m$. Следовательно, $ab_i \not\equiv ab_j \pmod m$, $(a, m) = 1$ (так как $ab_i \equiv ab_j \pmod m \iff b_i \equiv b_j \pmod m$ по 4 свойству сравнений и вычетов).
Далее, $\forall c \in \mathbb{Z}$ при $ab_i \not\equiv ab_j \pmod m$ имеем также $ab_i + c \not\equiv ab_j + c \pmod m$

1. Числа $ab_1 + c, \dots, ab_m + c$ – представители m различных классов вычетов.

2. Числа $ab_1, \dots, ab_k$ – представители k различных классов вычетов. При этом $(ab_i, m) = (b_i, m) = 1$ (по важной лемме).

■

Теорема (*Эйлера*). Пусть:

$$\begin{cases} m \in \mathbb{N},\ m \geq 2 \\ a \in \mathbb{Z},\ (a, m) = 1 \end{cases}$$

Тогда $a^{\varphi(m)} \equiv 1 \pmod m$
Доказательство. Пусть $b_1, \dots, b_k$ – приведенная система вычетов, тогда $ab_1, \dots, ab_k$ – тоже приведенная система вычетов (по теореме о приведенной системе вычетов). Это значит, что $\forall i \in \{1, \dots, k\}\ \exists! j \in \{1, \dots, k\} : b_i \equiv ab_j \pmod m$. Следовательно:

$$\prod_{i=1}^{k} b_i \equiv \prod_{j=1}^{k} ab_j \pmod m$$

$$\prod_{i=1}^{k} b_i \equiv a^k \prod_{j=1}^{k} b_j \pmod m$$

.
Но $\forall l \in \{1, \dots, k\}\ (b_l, m) = 1$, поэтому можно сократить. Остается $1 \equiv a^k \pmod m$, где $k = \varphi(m)$

■

Следствие (*Малая теорема Ферма*). Пусть p – простое, $a \in \mathbb{Z}$, $p \nmid a$. Тогда $a^{p-1} \equiv$ $\equiv 1 \pmod p$

Доказательство. При $m = p$ – простом, $\varphi(m) = p - 1$. Дальше просто применяем теорему Эйлера.

$\blacksquare$

Теорема (*об обратимых вычетах по умножению*). Пусть $m \in \mathbb{N}$, $m \geq 2$, $a \in \mathbb{Z}$. Тогда сравнение $ax \equiv 1 \pmod{m}$ имеет решение $\iff (a, m) = 1$

Примечание. Такое a называется *обратимым* по модулю m, а найденный x – *обратным* к a.
Доказательство. Сравнение $ax \equiv 1 \pmod{m}$ имеет решение $\iff \exists b \in \mathbb{Z} : ab \equiv 1 \pmod{m} \iff \exists c \in \mathbb{Z} : ab - 1 = mc \iff ab - mc = 1$. Получили линейное диофантово уравнение, так как $(a, m) = 1$

$\blacksquare$

Следствие. Пусть $\bar{a} \in \mathbb{Z}_m$ (кольцо). Тогда $\bar{a}$ обратим по умножению (то есть $\exists \bar{b} : \bar{a}\bar{b} = \bar{1}$) $\iff \bar{a} \in \mathbb{Z}_m^*$

Замечание. Если $\bar{a} \in \mathbb{Z}_m^*$, то обратный по умножению элемент определен однозначно, то есть $\exists! \bar{b} : \bar{a}\bar{b} = \bar{1}$
Доказательство. Пусть $ab_1 \equiv 1 \pmod{m}$ и $ab_2 \equiv 1 \pmod{m}$. Тогда $a(b_1 - b_2) \equiv 0 \pmod{m}$. Но $(a, m) = 1$, значит $b_1 - b_2 \equiv 0 \pmod{m}$, то есть $b_1 \equiv b_2 \pmod{m}$

$\blacksquare$

Теорема (*Вильсона*). Пусть p – простое. Тогда $(p-1)! \equiv -1 \pmod{p}$
Доказательство. $\forall a \in \{1, 2, \ldots, p-1\}\ \exists! b \in \{1, 2, \ldots, p-1\} : ab \equiv 1 \pmod{p}$
Но в некоторых случаях может случиться $b = a$. Тогда:

$$a^2 \equiv 1 \pmod{p} \iff p \mid a^2 - 1 = (a-1)(a+1) \iff \left[\begin{array}{l} p \mid a-1 \\ p \mid a+1 \end{array}\right. \iff a \equiv \pm 1 \pmod{m}$$

Получается, что $2, 3, \ldots, p-2$ разбиваются на пары так, что каждая в произведении дает 1.
Следовательно, $(p-1)! = 1 \cdot \underbrace{1 \cdot \ldots \cdot 1}_{\text{пары}} \cdot (p-1) = (p-1) \iff (p-1)! \equiv -1 \pmod{p}$

$\blacksquare$

Лекция 6

6.0. Введение

Вспомнили, что $\mathbb{Z}_m = \{a + m\mathbb{Z} \mid a \in \{0, 1, \dots, m-1\}\}$ называется классом вычетов числа a по модулю m. А также все другие теоремы.

Теорема. (*китайская теорема об остатках*). Пусть есть $m_1, \dots, m_k \in \mathbb{N}$, $m_1, \dots, m_k \geq$ ≥ 2, $\forall i \neq j$ $(m_i, m_j) = 1$, а также $a_1, \dots, a_k \in \mathbb{Z}$. Тогда система:

$$(*) \begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

имеет решение и, более того, $(*) \iff x \equiv x_0 \pmod{M}$, где

$$M = \prod_{i=1}^{k} m_i$$
$$M_i = \frac{M}{m_i}$$
$$x_0 = \sum_{i=1}^{k} b_i M_i$$
$$b_i \in \mathbb{Z} : b_i M_i \equiv a_i \pmod{m_i}$$

Доказательство. Поскольку $\forall i \neq j$ $(m_i, m_j) = 1$ имеем также $(m_i, M_i) = 1$. Следовательно, $\forall i$ коэффициент b_i корректно определен (то есть существует) по $\pmod{m_i}$.

Наблюдения:

1. x_0 удовлетворяет $(*)$: $x_0 = \sum\limits_{i=1}^{k} b_i M_i \equiv_{m_j} b_j M_j$[4] $\equiv_{m_j} a_j$ – верно для всех j.
2. Если $x_1 \equiv x_0 \pmod{M}$, то x_1 также удовлетворяет (*): $\forall j$ $x_1 \equiv_{m_j} x_0 \equiv_{m_j} a_j$
3. Если x_1 удовлетворяет $(*)$, то $x_1 \equiv x_0 \pmod{M}$. $\forall j$:

$$\begin{cases} x_1 \equiv a_j \pmod{m_j} \\ x_0 \equiv a_j \pmod{m_j} \end{cases} \implies x_1 - x_0 \equiv 0 \pmod{m_j}$$

Но $m_1, \dots, m_k$ попарно взаимно просты. Следовательно $x_1 - x_0 \equiv 0 \pmod{M}$

■

[4]Ключевой переход: $\sum\limits_{i=1}^{k} b_i M_i \equiv b_j M_j \pmod{m_j}$. Так как $\forall i \neq j$ $(M_i, m_j) = m_j$, то по модулю m_j любой $b_i M_i$ обнуляется

6.1. Группы, кольца, поля

Определение. Пусть G – множество, замкнутое относительно операции "$\circ$" ($\forall a, b \in G\ \exists! c \in G : a \circ b = c$). G называется группой (относительно операции "$\circ$"), если:

1. Операция *ассоциативна*: $\forall a, b, c, \in G$ верно $(a \circ b) \circ c = a \circ (b \circ c)$
2. Существует *нейтральный элемент*: $\exists e \in G : \forall a \in G$ верно $a \circ e = e \circ a = a$
3. Существует *обратный элемент*: $\forall a \in G\ \exists b \in G : a \circ b = b \circ a = e$

Определение. Если $\forall a, b \in G\ a \circ b = b \circ a$, то G называется *коммутативной* (или *абелевой*) группой.

Определение. Пусть R – множество, замкнутое относительно операций "$+$" и "$\cdot$". Тогда R называется кольцом, если:

1. $(R, +)$ – абелева группа.
2. Умножение *дистрибутивно:* $\forall a, b, c \in R$:

$$\begin{cases} (a+b)c = ac + bc \\ c(a+b) = ca + bc \end{cases}$$

Замечание. Иногда требуют в определении кольца еще ассоциативность умножения.

Определение. Ассоциативное, коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется *полем.*

Определение. Пусть $(G_1, \circ)$, $(G_2, *)$ – группы. Тогда $G_1 \cong G_2$ (*изоморфны*), если $\exists f : G_1 \to G_2$ такое, что:

1. f – биекция
2. $\forall a, b \in G_1\ f(a \circ b) = f(a) * f(b)$

Пример. $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$. Пусть отображение $f : \mathbb{R} \xrightarrow{\exp} \mathbb{R}_{>0}$, где:

- $a \in \mathbb{R} : f(a) = e^a$ – инъекция в одну сторону.
- $a \in \mathbb{R}_{>0} : f(a)^{-1} = \ln a$ – инъекция в другую сторону.
- $a, b \in \mathbb{R} : e^{a+b} = f(a+b) = f(a) \cdot f(b) = e^a \cdot e^b$

Инъекции в обе стороны говорят о том, что функция f является биекцией (по теореме Кантора-Бернштейна).

Определение. Пусть R_1, R_2 – кольца. Тогда $R_1 \cong R_2$, если $\exists f : R_1 \to R_2$ такое, что:

1. f – биекция
2. $f(a + b) = f(a) + f(b)$
3. $f(a \cdot b) = f(a) \cdot f(b)$

Замечание. Если $R_1 \cong R_2$ и f реализует *изоморфизм*, то $a \in R_1$ обратим $\iff$ $f(a) \in R_2$ обратим.