1 Наибольший общий делитель, наименьшее общее кратное и их свойства

Определение.
$a_1, ..., a_n \in \mathbb{Z} \setminus \{0\}$

$\{d | \forall i \quad a_i \vdots d\}$ d - общий делитель$(a_1, ..., a_n)$ НОД$(a_1, ...a_n) = max\, d$

$\{s | \forall i \quad s \vdots a_i\}$ s - общее кратное$(a_1, ..., a_n)$ НОК$(a_1, ...a_n) = min\, s$

1.1 Свойства НОД и НОК

Утверждение 1
$$\left.\begin{array}{l} a_1, ..., a_n \in \mathbb{N} \\ m = \text{НОК}(a_1, ..., a_n) \\ c = \text{ОК}(a_1, ..., a_n) \end{array}\right| \Rightarrow c \vdots m$$
Доказательство:
$\urcorner$ c не $\vdots$ на m (от противного)
$c = qm + r$ $0 < r < m$
$\forall i$ $c \vdots a_i$ $m \vdots a_i$
$c - qm \vdots a_i$
$r \vdots a_i$ r - ОК$(a_1, ..., a_n)$

Утверждение 2
$a_1, ..., a_n \in \mathbb{N}$
$d_1, ..., d_k$ - все натуральные ОД $(a_1, ..., a_n)$
НОД$(a_1, ..., a_n) =$НОК$(d_1, ..., d_k)$

Доказательство:
$d_k =$ НОД $(a_1, ..., a_n)$
$a_i \vdots d_j$
$a_i \vdots$ НОК $(d_1, ..., d_k)$
$d_k \geq$ НОК $(d_1, ..., d_k)$
НОК$(d_1, ..., d_k) \vdots d_k$
НОК$(d_1, ..., d_k) \geq d_k$

Следствие 2-1:
$$\left.\begin{array}{l} a_1 \vdots d \\ ... \\ a_n \vdots d \end{array}\right. \Rightarrow \text{НОД } (a_1, ..., a_n) \vdots d$$
Доказательство следствия:
$$\begin{array}{c} \text{НОК}(d_1, ..., d_k) \vdots d_i \\ \| \\ \text{НОД}(a_1, ..., a_n) \end{array}$$
Утверждение 3.

1. $a \vdots d,\ b \vdots d \Rightarrow$ НОД $(a, b) \vdots d$

2. $s \vdots a,\ s \vdots b \Rightarrow s \vdots$ НОК (a, b)
3. НОД (a, b), НОК $(a, b) = ab$
4. $bc \vdots a \quad$ НОД $(a, b) = d \Rightarrow c \vdots \frac{a}{d}$
5. $bc \vdots a \quad$ НОД $(a, b) = 1 \Rightarrow c \vdots a$
6. НОД $(ma, mb) = m$ НОД (a, b)
7. $a \vdots d,\ b \vdots d \Rightarrow$ НОД $(\frac{a}{d}, \frac{b}{d}) = \frac{\text{НОД}(a,b)}{d}$
8. НОД $(a, b) = d \Rightarrow$ НОД $(\frac{a}{d}, \frac{b}{d}) = 1$
9. НОД $(a, b) = b \Leftarrow a \vdots b \quad a, b \in \mathbb{N}$
10. НОД $(a + kb, b) =$ НОД $(a, b) \quad \forall k \in \mathbb{Z}$

Доказательства:

1. - следствие 2-1
2. - утверждение 1
3. $$\left.\begin{array}{l} ab \vdots a \\ \\ ab \vdots b \end{array}\right| \Rightarrow \begin{array}{l} ab \vdots \text{НОК}(a, b) \qquad d = \frac{ab}{\text{НОК}(a,b)} \\ \frac{a}{d} = \frac{\text{НОК}(a,b)}{b} \in \mathbb{Z} \quad \frac{b}{d} = \frac{\text{НОК}(a,b)}{a} \in \mathbb{Z} \end{array}$$
   $\sqsupset d`$ — ОД(a, b)

   $a \vdots d`$

   $b \vdots d`$

   $\frac{ab}{d`} = \frac{a}{d`} b \vdots b \qquad \frac{ab}{d`} = \frac{b}{d`} a \vdots a$

   $\frac{ab}{d`} = k\,\text{НОК}(a, b) = k\frac{ab}{d} \mid \Rightarrow\ d = kd` \vdots d`$

   $|d| \geqslant |d`|$

   $d =$ НОД(a, b)
4. $bc \vdots a \qquad$ НОД$(a, b) = d \qquad$ НОК$(a, b) = \frac{ab}{d}$
   $$\left.\begin{array}{l} bc \vdots a \\ \\ bc \vdots b \\ \\ \end{array}\right| \Rightarrow \begin{array}{l} bc \vdots \text{НОК}(a, b) \\ \\ bc \vdots \frac{ab}{d} \\ c \vdots \frac{a}{d} \end{array}$$
5. без доказательтсва
6. $a \vdots$ НОД(a, b)

   $ma \vdots m\,$НОД(a, b)

   $mb \vdots m\,$НОД(a, b)

   НОД $(ma, mb) \vdots m\,$НОД(a, b)

d — ОД (ma, mb)

$\frac{mab}{d} = \frac{ma}{d}b = \frac{mb}{d}a$

$\frac{mab}{d}$ — ОК (a, b)

$\frac{mab}{d} \vdots$ НОК $(a, b) = \frac{ab}{\text{НОД}(a,b)}$

mab НОД$(a, b) \vdots abd$

m НОД$(a, b) \vdots d$

m НОД$(a, b) =$ НОД(ma, mb)

7. d НОД$(\frac{a}{d}, \frac{b}{d}) =$ НОД(a, b) через 6
8. НОД$(\frac{a}{d}, \frac{b}{d}) = \frac{\text{НОД}(a,b)}{d} = \frac{d}{d} = 1$
9. $a \vdots b$

   $b \vdots b$

   b - ОД (a, b)

   d - ОД (a, b) $\qquad d > b$

   $b \vdots d$ $\qquad\qquad b \geqslant d$ (противоречие)
10. $d =$ НОД(a, b)

    $b \vdots d$

    $a \vdots d$ $\qquad a + kb \vdots d$

    d — ОД$(a + kb, b)$

    d‘ — ОД$(a + kb, b)$

    $a + kb \vdots d$‘

    $b \vdots d$‘

    $a + kb - kb \vdots d$‘

    $a \vdots d$‘ $\Rightarrow$ d‘ — ОД(a, b)

    $d \geqslant d$‘

Утверждение 4.
НОД$(a,$ НОД$(b, c)) =$ НОД(a, b, c)
Доказательство:
НОД$(b, c) = f$
НОД$(a, f) = g$

$a \vdots g$

$b \vdots f \vdots g$

$c \vdots f \vdots g$

$\sqsupset d$ — ОД(a, b, c)

$$\left.\begin{array}{l} b \vdots d \\ c \vdots d \end{array}\right| \Rightarrow \text{НОД}(b, c) = f \vdots d$$

$$\left.\begin{array}{l} a \vdots d \\ f \vdots d \end{array}\right| \Rightarrow \text{НОД}(a, f) = g \vdots d \Rightarrow g = \text{НОД}(a, b, c)$$

Утверждение 5. НОК$(a, \text{НОК}(b, c)) = \text{НОК}(a, b, c)$
Доказательство аналогично доказательству утверждения 4

1.2 Алгоритм нахождения НОД

1.2.1 Способ 1

Поиск всех возможных делителей двух чисел и в выбор наибольшего из них. Пример на числах 12 и 9.
$12 : 1 = 12$
$12 : 2 = 6$
$12 : 3 = 4$
$12 : 4 = 3$
$12 : 5 = 2$ *(2 остаток)*
$12 : 6 = 2$
$12 : 7 = 1$ *(5 остаток)*
$12 : 8 = 1$ *(4 остаток)*
$12 : 9 = 1$ *(3 остаток)*
$12 : 10 = 1$ *(2 остаток)*
$12 : 11 = 1$ *(1 остаток)*
$12 : 12 = 1$
Теперь для числа 9 сделаем то же самое.
$9 : 1 = 9$
$9 : 2 = 4$*(1 остаток)*
$9 : 3 = 3$
$9 : 4 = 2$*(1 остаток)*
$9 : 5 = 1$*(4 остаток)*
$9 : 6 = 1$*(3 остаток)*
$9 : 7 = 1$*(2 остаток)*
$9 : 8 = 1$*(1 остаток)*
$9 : 9 = 1$
Выпишем делите обоих чисел (те, что без остатка).
Делители числа 12 - (1 2 3 4 6 12)
Делители числа 9 - (1 3 9)
Согласно определению, НОДом чисел 12 и 9, является число, на которое 12 и 9 делятся без остатка.
НОДом чисел 12 и 9 является число 3.

1.2.2 Способ 2

Суть данного способа заключается в том, чтобы разложить оба числа на простые множители и перемножить общие из них. Пример на числах 24 и 18.

Разложим оба числа на множители.

Делимое	Делитель	Делимое	Делитель
24	2	18	2
12	2	9	3
6	2	3	3
3	3	1	
1			

Теперь перемножим их общие множители. Смотрим на разложение числа 24. Первый его множитель это 2. Ищем такой же множитель в разложении числа 18 и видим, что он там тоже есть.

Снова смотрим на разложение числа 24. Второй его множитель тоже 2. Ищем такой же множитель в разложении числа 18 и видим, что его там второй раз уже нет.

Следующая двойка в разложении числа 24 также отсутствует в разложении числа 18.

Переходим к последнему множителю в разложении числа 24. Это множитель 3. Ищем такой же множитель в разложении числа 18 и видим, что там он тоже есть.

Итак, общими множителями чисел 24 и 18 являются множители 2 и 3. Чтобы получить НОД, эти множители необходимо перемножить: $2 \times 3 = 6$

Значит НОД$(24, 18) = 6$

1.2.3 Способ 3

Суть данного способа заключается в том, что числа подлежащие поиску наибольшего общего делителя раскладывают на простые множители. Затем из разложения первого числа вычеркивают множители, которые не входят в разложение второго числа. Оставшиеся числа в первом разложении перемножают и получают НОД. Рассмотрим на примере чисел 28 и 16.

В первую очередь, раскладываем числа 28 и 16 на простые множители:

Делимое	Делитель	Делимое	Делитель
28	2	16	2
14	2	8	2
7	7	4	2
1		2	2
		1	

Получили два разложения: $2 \times 2 \times 7$ и $2 \times 2 \times 2 \times 2$

Теперь из разложения первого числа вычеркнем множители, которые не входят в разложение второго числа. В разложение второго числа не входит семёрка. Её и вычеркнем из первого разложения.

Теперь перемножаем оставшиеся множители и получаем НОД: $2 \times 2 = 4$

Число 4 является наибольшим общим делителем чисел 28 и 16. Оба этих числа делятся на 4 без остатка:

$28 : 4 = 7$

$16 : 4 = 4$

НОД$(28, 16) = 4$

1.3 Алгоритм нахождения НОК

1.3.1 Способ 1

Можно выписать первые кратные двух чисел, а затем выбрать среди этих кратных такое число, которое будет общим для обоих чисел и маленьким. Рассмотрим на примере числа 9 и 12.

В первую очередь, найдем первые кратные для числа 9. Чтобы найти кратные для 9, нужно эту девятку поочерёдно умножить на числа от 1 до 9. Получаемые ответы будут кратными для числа 9.

$9 \times 1 = 9$

$9 \times 2 = 18$

$9 \times 3 = 27$

$9 \times 4 = 36$

$9 \times 5 = 45$

$9 \times 6 = 54$

$9 \times 7 = 63$

$9 \times 8 = 72$

$9 \times 9 = 81$

Теперь находим кратные для числа 12. Для этого поочерёдно умножим число 12 на все числа 1 до 12:

$12 \times 1 = 12$

$12 \times 2 = 24$

$12 \times 3 = 36$

$12 \times 4 = 48$

$12 \times 5 = 60$

$12 \times 6 = 72$

$12 \times 7 = 84$

$12 \times 8 = 96$
$12 \times 9 = 108$
$12 \times 10 = 120$
$12 \times 11 = 132$
$12 \times 12 = 144$

Теперь выпишем кратные обоих чисел:

9: 9 18 27 36 45 54 63 72 81

12: 12 24 36 48 60 72 84 96 108 120 132 144

Найдём общие кратные обоих чисел.

Общими кратными для чисел 9 и 12 являются кратные 36 и 72. Наименьшим же из них является 36.

Значит наименьшее общее кратное для чисел 9 и 12 это число 36. Данное число делится на 9 и 12 без остатка:

$36 : 9 = 4$
$36 : 12 = 3$

НОК(9 и 12) = 36

1.3.2 Способ 2

Второй способ заключается в том, что числа для которых ищется наименьшее общее кратное раскладываются на простые множители. Затем выписываются множители, входящие в первое разложение, и добавляют недостающие множители из второго разложения. Полученные множители перемножают и получают НОК.

Применим данный способ для предыдущей задачи. Найдём НОК для чисел 9 и 12.

Разложим на множители число 9 и 12:

Делимое	Делитель	Делимое	Делитель
9	3	12	2
3	3	6	2
1		3	3
		1	

Выпишем первое разложение и допишем множители из второго разложения, которых нет в первом разложении. В первом разложении нет двух двоек. Допишем и перемножим: $3 \times 3 \times 2 \times 2 = 36$

Получили ответ 36. Значит наименьшее общее кратное чисел 9 и 12 это число 36. Данное число делится на 9 и 12 без остатка:

$36 : 9 = 4$
$36 : 12 = 3$

НОК (9 и 12) = 36

Говоря простым языком, всё сводится к тому, чтобы организовать новое разложение куда входят оба разложения сразу. Разложением первого числа 9 являлись множители 3 и 3, а разложением второго числа 12 являлись множители 2, 2 и 3.

Наша задача состояла в том, чтобы организовать новое разложение куда входило бы разложение числа 9 и разложение числа 12 одновременно. Для этого мы выписали разложение первого числа и дописали туда множители из второго разложения, которых не было в первом разложении. В результате получили новое разложение 3 × 3 × 2 × 2. Нетрудно увидеть воочию, что в него одновременно входят разложение числа 9 и разложение числа 12.

1.3.3 Способ 3

Он работает при условии, что его ищут для двух чисел и при условии, что уже найден наибольший общий делитель этих чисел.

Данный способ разумнее использовать, когда одновременно нужно найти НОД и НОК двух чисел.

К примеру, пусть требуется найти НОД и НОК чисел 24 и 12. Сначала найдем НОД этих чисел:

Делимое	Делитель	Делимое	Делитель
24	2	12	2
12	2	6	2
6	2	3	3
3	3	1	
1			

Теперь для нахождения наименьшего общего кратного чисел 24 и 12, нужно перемножить эти два числа и полученный результат разделить на их наибольший общий делитель.

Итак, перемножим числа 24 и 12. (288)

Разделим полученное число 288 на НОД чисел 24 и 12. (288 : 12 = 24)

Получили ответ 24. Значит наименьшее общее кратное чисел 24 и 12 равно 24

НОК(24 и 12) = 24.

2 Алгоритм Евклида. Линейное представление НОД(?)

2.1 Алгоритм Евклида

$a, b \in \mathbb{N}$
НОД(a, b) - ?
while $b \neq 0$
    $(a, b) = (b, a\%b)$
return a
НОД$(a, b) =$ НОД$(a + kb, b)$
$k = -[\frac{a}{b}]$
НОД$(a, b) =$ НОД$(a - [\frac{a}{b}]b, b) =$ НОД$(a\%b, b)$
$a \vdots b :$ НОД$(a, b) = b$

2.2 Бинарный алгоритм Евклида

$a, b \in \mathbb{N}$
$i = 0; j = 0;$
while $(!(a\&1))\{$
    $a \gg= 1;$
    $i + +;$
$\}$
while $(!(b\&1))\{$
    $b \gg= 1;$
    $j + +;$
$\}$
if$(a > b)\{t = a; a = b; b = t; \}$
while$(a! = 0)\{$
    $b- = a;$
    while $(!(b\&1))$ $b \gg= 1;$
    if $(a > b)\{$
        t = a;
        a = b;
        b = t;
    $\}$
$\}$
return $b \ll$ std::min(i, j);

2.3 Расширенный алгоритм Евклида

$a, b \in \mathbb{N}$
while $b \neq 0$
  $q = a/b$
  $(a, b) = (b, a - qb)$
  $(x, y) = (y, x - qy)$
  $a-$ НОД
  a, b
  $(x, y, u, v) = (1, 0, 0, 1)$
while $b \neq 0$
  $q = a/b$
  $(a, b) = (b, a - qb)$
  $(x, y, u, v) = (u, v, x - qu, y - qv)$
return (a, x, y)

3 Континуанта

3.1 Определение

Введенные понятия цепной дроби и подходящих дробей оказываются очень полезными для анализа работы алгоритма Евклида. Дадим необходимые обозначения. Рассмотрим трехдиагональный определитель:

$$\begin{vmatrix} q_0 & 1 & 0 & 0 & ... & 0 & 0 \\ -1 & q_1 & 1 & 0 & ... & 0 & 0 \\ 0 & -1 & q_2 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & ... & q_{n-2} & 1 \\ 0 & 0 & 0 & 0 & ... & -1 & q_{n-1} \end{vmatrix} = K_n(q_0, q_1, ..., q_{n-1})$$

Определитель называют континуантой n-го порядка или индекса.

Континуанта индекса n есть многочлен $K_n(x_1, ..., x_n)$

Разложим континуанту n-го порядка по последнему столбцу:

$K_n(x_1, ..., x_n) = x_n K_{n-1}(x_1, ..., x_{n-1}) + K_{n-2}(x_1, ..., x_{n-2})$

Отсюда можно задать континуанту рекуррентным соотношением:

$K_{-1} = 0, K_0 = 1, K_n = x_n K_{n-1} + K_{n-2}$

Соотношение очень напоминает рекуррентные соотношения для числителей и знаменателей подходящих дробей. Это не случайно и две следующие леммы подтверждают предположение о связи континуант и цепных дробей.

3.2 Лемма 1

Континуанта $K_n(q_0, q_1, ..., q_{n-1})$ равна сумме всевозможных произведений элементов $q_0, q_1, ..., q_{n-1}$, одно из которых содержит все эти элементы, а другие получаются из него выбрасыванием одной или нескольких пар сомножителей с соседними номерами (если выброшены все сомножители, то считаем, что осталась 1).

Доказательство. Индукция по n. База индукции:

$K_1(q_0) = q_0, K_2(q_0, q_1) = \begin{vmatrix} q_0 & 1 \\ -1 & q_1 \end{vmatrix} = q_0 q_1 + 1$

и утверждение леммы справедливо для континуант первого и второго порядков. Шаг индукции. Пусть утверждение леммы справедливо для континуант $(n-2)$-го и $(n-1)$-го порядков. Применив разложение , получим требуемое.

Пример

$K_6(q_0,q_1,q_2,q_3,q_4,q_5) = q_0q_1q_2q_3q_4q_5 + q_2q_3q_4q_5 + q_0q_3q_4q_5 + q_0q_1q_4q_5 + q_0q_1q_2q_5 + q_0q_1q_2q_3 + q_4q_5 + q_2q_5 + q_0q_5 + q_2q_3 + q_0q_3 + q_0q_1 + 1$

Явная связь континуант и цепных дробей впервые была установлена Эйлером.

3.3 Лемма Эйлера

Справедливо тождество
$[q_0; q_1, ..., q_{n-1}] = \frac{K_n(q_0,q_1,...,q_{n-1})}{K_{n-1}(q_1,q_2,...,q_{n-1})}$
Доказательство. Индукция по n. База индукции:
$[q_0; q_1] = q_0 + \frac{1}{q_1} = \frac{q_0q_1+1}{q_1} = \frac{K_2(q_0,q_1)}{K_1(q_1)}$

Шаг индукции. Пусть тождество верно для дробей с $n-1$ звеном включительно. Представим n-звенную дробь $(q_0, q_1, ..., q_{n-1})$ дробью с $n-1$ звеном, где последнее звено имеет вид $q_{n-2} + \frac{1}{q_{n-1}}$. Применив к этой дроби индукционное предположение, с учетом разложения , имеем

$[q_0; q_1, ..., q_{n-1}] = [q_0, q_1, ..., q_{n-2}+\frac{1}{q_{n-1}}] = \frac{K_{n-1}(q_0,q_1,...,(q_{n-2}+\frac{1}{q_{n-1}}))}{K_{n-2}(q_1,q_2,...,(q_{n-2}+\frac{1}{q_{n-1}}))} = \frac{(\frac{1}{q_{n-1}})K_{n-2}(q_0,q_1,...,q_{n-3})+K_{n-3}(q_0,q_1,...,q_{n-4})}{(\frac{1}{q_{n-1}})K_{n-3}(q_1,q_2,...,q_{n-3})+K_{n-4}(q_1,q_2,...,q_{n-4})} = \frac{K_{n-1}(q_0,q_1,...,q_{n-2})+\frac{K_{n-2}(q_0,q_1,...,q_{n-3})}{q_{n-1}}}{K_{n-2}(q_1,q_2,...,q_{n-2})+\frac{K_{n-3}(q_1,q_2,...,q_{n-3})}{q_{n-1}}} = \frac{K_n(q_0,q_1,...,q_{n-1})}{K_{n-1}(q_1,q_2,...,q_{n-1})}$

Перейдем к анализу алгоритма Евклида. Нас будет интересовать наихудший случай — когда алгоритм Евклида работает особенно долго. Сформулируем вопрос точнее: для каких двух наименьших чисел надо применить алгоритм Евклида, чтобы он работал в точности заданное число шагов? Ответ на этот вопрос дает следующая теорема.

3.4 Теорема Ламе

Пусть n — произвольное натуральное число, и $a > b > 0$ такие, что алгоритму Евклида для обработки a и b необходимо выполнить точно n шагов (делений с остатком), причем a — наименьшее натуральное число с таким свойством. Тогда

$a = \varphi_{n+2}, b = \varphi_{n+1}$

где φ_k — k-ое число Фибоначчи ($\varphi_0 = 0, \varphi_1 = 1, \varphi_i = \varphi_{i-1} + \varphi_{i-2}$).

Доказательство. Разложим a/b в цепную дробь. Согласно лемме Эйлера получаем,
$\frac{a}{b} = [q_0; q_1, ..., q_{n-1}] = \frac{K_n(q_0,q_1,...,q_{n-1})}{K_{n-1}(q_1,q_2,...,q_{n-1})}$

где $q_0; q_1, ..., q_{n-1}$ — неполные частные из алгоритма Евклида. По условию теоремы, их ровно n. Принимая во внимание несократимость подходящих дробей становится очевидно, что континуанты $q_0; q_1, ..., q_{n-1}$ и $q_1; q_2, ..., q_{n-1}$ взаимно просты. Пусть НОД$(a, b) = d$. Тогда

$$\begin{cases} a = K_n(q_0, q_1, ..., q_{n-1}) \\ b = K_{n-1}(q_1, q_2, ..., q_{n-1}) \end{cases} \tag{1}$$

В силу единственности разложения в цепную дробь, в случае a > b > 0 справедливы неравенства $q_0, q_1, ..., q_{n-2} > 1, q_{n-1} > 2$. Очевидно, что d > 1. По лемме 1, континуанта есть многочлен с неотрицательными коэффициентами от переменных $q_0, q_1, ...$. Его минимальное значение очевидно достигается при $q_0 = q_1 = \cdots = q_{n-2} = 1, q_{n-1} = 2$. Положив d = 1 и подставив эти значения q_i, получим требуемое.

4 Цепные дроби. Наилучшие приближения

4.1 Цепные дроби. Непрерывные дроби

$$[a_0; a_1, a_2, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{... + \cfrac{1}{a_n}}}}; a_0 \in Z; a_1, ..., a_n \in N; a_n > 1$$

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = ... = [q_1; q_2, q_3, ..., q_{k+1}]$$

$-\frac{48}{109} = [-1; 1, 1, 3, 1, 2, 4]$

$-48 = 109(-1) + 61$

$109 = 61 * 1 + 48$

$61 = 48 * 1 + 13$

$48 = 13 * 3 + 9$

$13 = 9 * 1 + 4$

$9 = 4 * 2 + 1$

$4 = 1 * 4$

$\alpha = [a_0; a_1, ..., a_n]$

Подходящая дробь

$\delta_k = [a_0; a_1, ..., a_k]$

$\delta_0 = [-1] = \frac{P_0}{Q_0}$

$\delta_1 = [-1; 1] = \frac{P_1}{Q_1}$

$\delta_2 = [-1; 1, 1] = \frac{P_2}{Q_2}$

$\delta_3 = [-1; 1, 1, 3] = \frac{P_3}{Q_3}$

$P_0 = a_0 \quad Q_0 = 1$

$\delta_0 = [a_0] = \frac{a_0}{1} = \frac{P_0}{Q_0}$

$\delta_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \quad P_1 = a_0 a_1 + 1 \;\; Q_1 = a_1$

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

$$\delta_{k+1} = [a_0; a_1, ..., a_k, a_{k+1}] = [a_0; a_1, ..., a_k + \frac{1}{a_{k+1}}] = \frac{P_k(a_0, ..., a_k + \frac{1}{a_{k+1}})}{Q_k(a_0, .., a_k + \frac{1}{a_{k+1}})} =$$

$$= \frac{(a_k + \frac{1}{a_{k+1}})P_{k-1} + P_{k-2}}{(a_k + \frac{1}{a_{k+1}})Q_{k-1} + Q_{k-2}} = \frac{a_k q_{k+1} P_{k-1} + P_{k-1} + q_{k+1} P_{k-2}}{a_k q_{k+1} Q_{k-1} + Q_{k-1} + q_{k+1} P_{k-2}} = \frac{a_{k+1}(a_k P_{k-1} + P_{k-2}) + P_{k-1}}{a_{k+1}(a_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} =$$

$$= \frac{a_{k+1} P_k + P_{k-1}}{a_{k+1} Q_k + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}} \quad P_{k+1} = a_{k+1} P_k + P_{k-1}; \quad Q_{k+1} = a_{k+1} Q_k + Q_{k-1}$$

$$\delta_2 = [a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}$$

$P_2 = a_0 a_1 a_2 + a_0 + a_3$

$Q_2 = a_1 a_2 + 1$

$[-1; 1, 1, 3, 1, 2, 4]$

k	-1	0	1	2	3	4	5	6
a_n		-1	1	1	3	1	2	4
P_n	1	-1	0	-1	-3	-4	-11	-48
Q_n	0	1	1	2	7	9	25	109

$\delta_0 = -1; \delta_1 = 0; \delta_2 = -\frac{1}{2}; \delta_3 = -\frac{3}{7}; \delta_4 = -\frac{4}{9}; \delta_5 = -\frac{11}{25}; \delta_6 = \alpha = -\frac{48}{109}$

Утв. $\dfrac{P_s}{Q_s} - \dfrac{P_{s-1}}{Q_{s-1}} = \dfrac{(-1)^{s+1}}{Q_sQ_{s-1}}$

Док-во: $\dfrac{P_s}{Q_s} - \dfrac{P_{s-1}}{Q_{s-1}} = \dfrac{P_sQ_{s-1} - P_{s-1}Q_s}{Q_sQ_{s-1}}$

$h_s = P_sQ_{s-1} - P_{s-1}Q_s = (a_sP_{s-1} + P_{s-2})Q_{s-1} - P_{s-1}(a_sQ_{s-1} + Q_{s-2}) = P_{s-2}Q_{s-1} - P_{s-1}Q_{s-2} =$
$= -(P_{s-1}Q_{s-2} - P_{s-2}Q_{s-1}) = -h_{s-1} = h_{s-2} = -h_{s-3} = ... = (-1)^{s-1}h_1 = (-1)^{s-1}(P_1Q_0 - P_0Q_1) =$
$(-1)^{s-1}(a_0a_1 + 1 - a_0a_1) = (-1)^{s-1}$

Следствие: НОД$(P_s, Q_s) = 1$ (все подходящие дроби несократимы/ взаимно просты)

Следствие: $\lim\limits_{s\to\infty}\left|\dfrac{P_s}{Q_s} - \dfrac{P_{s-1}}{Q_{s-1}}\right| = 0$ (последовательность подходящих дробей фундаментальна)

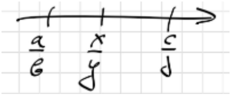
4.2 Наилучшие приближения

$\left|\alpha - \dfrac{x}{y}\right|$

Опр. $\dfrac{a}{b}$ - наилучш. приближ. к числу α, если не сущ. другой дроби $\dfrac{x}{y}$: $\begin{cases}\left|\alpha - \dfrac{x}{y}\right| \le \left|\alpha - \dfrac{a}{b}\right| \\ 0 < y < b\end{cases}$

Утв. $\dfrac{x}{y} \in \left(\dfrac{a}{b}; \dfrac{c}{d}\right)$ и $bc - ad = 1 \Rightarrow y > b$ и $y > d$

Доказательство: $\dfrac{c}{d} - \dfrac{a}{b} = \dfrac{bc - ad}{bd} = \dfrac{1}{bd}$ (по услов.)

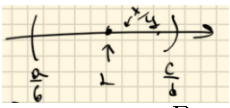


$\dfrac{bx - ay}{by} = \dfrac{x}{y} - \dfrac{a}{b} \le \dfrac{1}{bd}| \cdot bdy; \quad xbd - ady \le y; \quad d \le (bx - ay)d < y$

$xbd \le (ad + 1)y; \quad y \ge \dfrac{xbd}{ad + 1}; \quad cy - dx \ge 1$

$0 < \dfrac{c}{d} - \dfrac{x}{y} < \dfrac{1}{bd}; \quad 0 < \dfrac{cy - dx}{dy} < \dfrac{1}{bd}(\dfrac{cy - dx}{dy} \le \dfrac{1}{dy}); \quad \dfrac{1}{dy} < \dfrac{1}{bd}; b < y$

Следствие: $\alpha \in (\dfrac{a}{b}; \dfrac{c}{d})$ и $dc - ad = 1 \to$ та из $(\dfrac{a}{b}, \dfrac{c}{d})$, кто ближе к α - наилучшее приближение.



Следствие: $\dfrac{P_s}{Q_s}$ - наил. прибл к α

$\dfrac{P_{s-1}}{Q_{s-1}}$ и $\dfrac{P_s}{Q_s}$: $P_{s-1}Q_s - P_sQ_{s-1}$

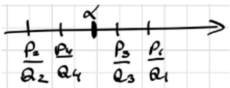
4.3 Бесконечные цепные дроби

$\alpha = [a_0, a_1, ..., a_n, ...]$

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{... + \cfrac{1}{a_n + \cfrac{1}{a_{n+1} + ...}}}} = \alpha$$

$\eta_n = a_n + \dfrac{1}{a_{n+1} + ...}$

$\eta_n = [a_n; a_{n+1}, a_{n+1}, ...] \to \alpha = [a_0; a_1, ..., \eta_n]$

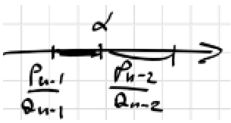


Утверждение α между $\dfrac{P_s}{Q_s}$ и $\dfrac{P_{s+1}}{Q_{s+1}}$

Доказательство:

$\alpha = \dfrac{P_n}{Q_n} = \dfrac{\eta_n P_{n-1} + P_{n-2}}{\eta_n Q_{n-1} + Q_{n-2}}$

1. $\alpha - \dfrac{P_{n-1}}{Q_{n-1}} = \dfrac{\eta_n P_{n-1} + P_{n-2}}{\eta_n Q_{n-1} + Q_{n-2}} - \dfrac{P_{n-1}}{Q_{n-1}} = \dfrac{\eta_n P_{n-1} Q_{n-1} + P_{n-2} Q_{n-1} - \eta_n P_{n-1} Q_{n-1} - P_{n-1} Q_{n-2}}{Q_{n-1}(\eta_n Q_{n-1} + Q_{n-2})} = \dfrac{(-1)^{n-1}}{Q_{n-1}(\eta_n Q_{n-1} + Q_{n-2})}$
2. $\alpha - \dfrac{P_{n-2}}{Q_{n-2}} = \dfrac{\eta_n P_{n-1} + P_{n-2}}{\eta_n Q_{n-1} + Q_{n-2}} - \dfrac{P_{n-2}}{Q_{n-2}} = \dfrac{\eta_n P_{n-1} Q_{n-2} + P_{n-2} Q_{n-2} - \eta_n P_{n-2} Q_{n-1} - P_{n-2} Q_{n-2}}{Q_{n-2}(\eta_n Q_{n-1} + Q_{n-2})} =$
$= \dfrac{\eta_n (P_{n-1} Q_{n-2} - P_{n-2} Q_{n-1})}{Q_{n-2}(\eta_n Q_{n-1} + Q_{n-2})} = \dfrac{\eta_n (-1)^{n-2}}{Q_{n-2}(\eta_n Q_{n-1} + Q_{n-2})}$
3. $\left.\begin{array}{l} \left|\alpha - \dfrac{P_{n-1}}{Q_{n-1}}\right| = \dfrac{Q_{n-2}}{\eta_n Q_{n-1}} \left|\alpha - \dfrac{P_{n-2}}{Q_{n-2}}\right| \\ \dfrac{Q_{n-2}}{\eta_n Q_{n-1}} < 1 \\ Q_{n-2} < Q_{n-1} \le \eta_n Q_{n-1} \end{array}\right| \Rightarrow \left|\alpha - \dfrac{P_{n-1}}{Q_{n-1}}\right| < \left|\alpha - \dfrac{P_{n-2}}{Q_{n-2}}\right|$



$\Rightarrow$ Следствие:$|\alpha - \dfrac{P_n}{Q_n}| < \dfrac{1}{Q_n^2}$

Доказательство: $|\alpha - \dfrac{P_n}{Q_n}| \le |\dfrac{P_{n+1}}{Q_{n+1}} - \dfrac{P_n}{Q_n}| = \dfrac{1}{Q_n Q_{n+1}} < \dfrac{1}{Q_n^2}$

$Q_{n+1} > Q_n$

$\dfrac{1}{Q_{n+1}} < \dfrac{1}{Q_n}$

Пример: $\sqrt{28} = 5 + (\sqrt{28} - 5) = 5 + \dfrac{1}{\dfrac{1}{\sqrt{28}-5}} = 5 + \dfrac{1}{\dfrac{\sqrt{28}+5}{3}} = 5 + \dfrac{1}{3 + \dfrac{\sqrt{28}-4}{3}} = 5 + \dfrac{1}{3 + \dfrac{1}{\dfrac{3}{\sqrt{28}-4}}}$

$\dfrac{3}{\sqrt{28}-4} = \dfrac{3(\sqrt{28}+4)}{12} = 2 + \dfrac{\sqrt{28}-4}{4} = |\dfrac{4}{\sqrt{28}-4} \dfrac{\sqrt{28}+4}{3} = 3 + \dfrac{\sqrt{28}-5}{3}|$

$\dfrac{3}{\sqrt{28}-5} = \sqrt{28} + 5 = 10(\sqrt{28} - 5)$... итого: $\sqrt{28} = [5; 3, 2, 3, 10] = [5; (3, 2, 3, 10)]$

5 Простые числа. Основная теорема арифметики.

5.1 Определение

$p \in \mathbb{N}$ простое, если есть ровно 2 натуральных делителя.

5.2 Определение

$a \in \mathbb{N}$ составное, если есть $>$ 2 натуральных делителей

5.3 Утверждение

p - простое, $ab \vdots p \Rightarrow a \vdots p$ или $b \vdots p$

5.3.1 Доказательство

Пусть a не делится на p, НОД(a, p) = 1 $\Rightarrow b \vdots p$

5.4 Утверждение

НОД$(a, b, c) = 1 \Leftrightarrow$ НОД$(a, b) = 1$ и НОД$(a, c) = 1$

5.4.1 Доказательство

| => / НОД(a, b) = d

$a \vdots d$

$bc \vdots b \vdots d$

НОД(a, b, c) $\vdots d$

$1 \vdots d$

$d = 1$

| <= | НОД$(a, b, c) = d$

$a \vdots d \vdots f \qquad a \vdots d \vdots \frac{d}{f}$

$bc \vdots d$

НОД$(b, d) = f \qquad c \vdots \frac{d}{f}$

$b \vdots f$

НОД$(a, b) \vdots f$

$1 \vdots f \qquad \frac{d}{f} = 1$

$f = 1 \qquad d = 1$

5.5 Утверждение

НОД$(b, c) = 1$

$a \vdots b,\ a \vdots c \ \Rightarrow\ a \vdots bc$

5.5.1 Доказательство

$a \vdots$ НОК$(b, c) = \frac{bc}{\text{НОД}(b,c)} = bc$

5.6 Утверждение

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

5.6.1 Доказательсто

НОД(НОД(a, b), НОД(a, c)) = d

$b \vdots$ НОД$(a, b) \vdots d$

$c \vdots$ НОД$(a, c) \vdots d$

НОД$(b, c) \vdots d$

$d = 1$

$bc \vdots \text{НОД}(a,b), bc \vdots \text{НОД}(a,c) \Rightarrow bc \vdots \text{НОД}(a,b)\text{НОД}(a,c)$

$f-\text{ОД}(a,bc) \qquad a \vdots f \qquad bc \vdots f$

$\text{НОД}(a,b) = g, \text{НОД}(\frac{b}{g}, \frac{f}{g}) = 1 \qquad c \vdots \frac{f}{g}$

$a \vdots f \vdots g \qquad b \vdots g \qquad \text{НОД}(a,b) \vdots g$

$a \vdots f \vdots \frac{f}{g}, c \vdots \frac{f}{g} \Rightarrow$ НОД(a, c) $\vdots \frac{f}{g}$

$\text{НОД}(a,b)\text{НОД}(a,c) \vdots f$

5.7 Утверждение

$\forall a \in \mathbb{N},\ a > 1 \Rightarrow \exists\, p$ простое $a \vdots p$

5.7.1 Доказательство

$1, d_1, ..., d_k$ - делители a

d_1 простое $d_1 \vdots f \qquad a \vdots d_1 \vdots f$

5.8 Утверждение(основная теорема арифметики)

$\forall a \in \mathbb{N},\ a > 1, \qquad a = p_1^{\alpha_1}...p_k^{\alpha_k}, \quad \alpha_i = 0$

5.8.1 Доказательство

$a = a \qquad a = bc \qquad a = bc = p_1^{\beta_1}...p_1^{\beta_1}p_3^{\beta_3}...p_k^{\beta_k}$
$a = p_1^{\alpha_k}...p_k^{\alpha_k} = q_1^{\beta_1}...q_l^{\beta_l}$
$p_1 = q_1 a = p_2^{\alpha_2}...p_n^{\alpha_n} = q_1^{\beta_1 - 2}...q_l^{\beta_l}$

5.9 Утверждение

$\alpha = p_1^{\gamma_1}...p_k^{\gamma_k} \qquad \beta = p_1^{\delta_1}...p_k^{\delta_k}$
$\gamma_i \geq 0 \qquad \delta_i \geq 0 \qquad p_i-$ простое
$\text{НОД}(\alpha,\beta) = p_1^{min(\gamma_1,\delta_1)}...p_k^{min(\gamma_k,\delta_k)}$
$\text{НОК}(\alpha,\beta) = \prod_{i=1}^{k} p_i^{max(\gamma_i,\delta_l)}$

5.9.1 Доказательство

$]d = \prod_{i=1}^{k} p_i^{min(\gamma_i,\gamma_i)}$

$\alpha \vdots d,\ \beta \vdots d,\ ]d' - \text{ОД}(\alpha,\beta)$

$\alpha \vdots q_1^{\epsilon_1}...q_s^{\epsilon_s}$
$]|q_1 \neq p_1,\ q_1 \neq p_2, ..., q_1 \neq p$

$p_1^{\gamma_1}...p_k^{\gamma_k} \vdots q_1, \text{НОД}(p_1^{\gamma}, q_1) = 1 \Rightarrow\ p_2^{\gamma_2}...p_k^{\gamma_k} \vdots q_1 \Rightarrow p_k^{\gamma_k} \vdots q_1$
$d' = p_1^{\epsilon_1}...p_k^{\epsilon_k}$

$]|\epsilon_1 > \gamma_1 \quad \alpha \vdots d' \vdots p_1^{\epsilon_1} \quad p_1^{\gamma_1} \vdots p_1^{\epsilon}$
$p_1^{\gamma_1 - \epsilon} \in \mathbb{Z} \quad \gamma_1 - \epsilon \geq 0 \quad \epsilon_1 \leq \gamma_1 \quad \epsilon_1 \leq \delta_1 \quad \epsilon_1 \leq min(\gamma_1, \delta_1) \quad d' \leq d$
$\text{НОД}(\alpha,\beta)\text{НОК}(\alpha,\beta) = \alpha\beta$
$\text{НОК}(\alpha,\beta) = \frac{\alpha\beta}{gcd(\alpha,\beta)} = \prod_{i=1}^{k} \frac{p_i^{\gamma_i} p_i^{\delta_i}}{min(\gamma_i,\delta_i)} = \prod_{i=1}^{k} p_i^{max(\gamma_i,\delta_i)}$

5.9.2 Пример

$24 = 2^3 * 3 * 5^0$
$90 = 2 * 3^2 * 5$
НОД$(24, 90) = 2^{min(3,1)} 3^{min(1,2)} 5^{min(0,1)} = 2^1 * 3^1 * 5^0 = 6$

6 Кольца вычетов. Полная система вычетов. Теорема о кольцах вычетов по простому модулю

6.1 Кольца вычетов

$< x, +, * >$

$$\text{Кольцо} \begin{cases} \text{Абелева группа} \begin{cases} \text{Группа} \begin{cases} \text{Полугруппа} \begin{cases} 1^\circ \quad (a+b)+c = a+(b+c) \end{cases} \\ 2^\circ \quad \exists 0 : a+0 = a \\ 3^\circ \quad \forall a \quad \exists(-a) : a+(-a) = 0 \end{cases} \\ 4^\circ \quad a+b = b+a \end{cases} \\ 5^\circ \quad \begin{cases} (a+b)*c = (a*c)+(b*c) \\ c*(a+b) = (c*a)+(c*b) \end{cases} \end{cases}$$

6.1.1 Свойства колец

- Кольцо ассоциативно: $(a * b) * c = a * (b * c)$
- Кольцо коммутативно: $a * b = b * a$
- Кольцо с единицей: $\exists 1 : 1 * a = a$
- Область целостности: $\exists a \neq 0, b \neq 0 \Rightarrow a * b \neq 0$

6.1.2 Примеры колец

- Кольцо целых чисел $\mathbb{Z}$, кольцо рациональных чисел $\mathbb{Q}$, кольцо вещественных чисел $\mathbb{R}$
- Кольцо $\mathbb{Z}[i]$ целых гауссовых чисел вида $a + bi$, где $a, b \in \mathbb{Z}$
- Кольцо $\mathbb{Z}[\sqrt{2}]$ вещественных чисел вида $a + b\sqrt{2}$ с целыми a, b

6.1.3 Поле

Поле - коммутативное ассоциативное кольцо с единицей в котором $\forall a \neq 0 \quad \exists a^{-1} : a * (a^{-1}) = 1$

6.1.4 Множество классов вычетов

Множество классов вычетов (обозначают $\mathbb{Z}_m$) является ассоциативным коммутативным кольцом с единицей

6.1.5 Примеры полей

- Числовые поля $\mathbb{Q}, \mathbb{R}$
- Поле $\mathbb{Q}[i]$ рациональных чисел вида $a + bi$, где $a, b \in \mathbb{Q}$
- Поле $\mathbb{Z}[\sqrt{2}]$ вещественных чисел вида $a + b\sqrt{2}$ с рациональными a, b

6.2 Полная система вычетов

Классом вычетов по модулю m называют множество чисел с одинаковым остатком при делении на m

6.2.1 Определение

Если взять по одному представителю из каждого класса вычетов, то эти m чисел образуют полную систему вычетов по модулю m

6.2.2 Примеры простейших полных систем вычетов

- $\{0, 1, 2, \ldots, m-1\}$ наименьшие положительные вычеты
- $\{0, -1, -2, \ldots, -(m-1)\}$ наименьшие отрицательные вычеты
- для произвольного $a \in \mathbb{Z} \quad \{a, a+1, a+2, \ldots, a+(m-1)\}$
- если $D(a, m) = 1$, то $\{0, a, 2a, \ldots, (m-1)a\}$

6.3 Теорема о кольцах вычетов по простому модулю

Китайская теорема об остатках утверждает, что система сравнений с попарно взаимно простыми модулями $m_1, m_2, \ldots, m_k$:

$$\begin{cases} x \equiv c_1 (\text{mod}\, m_1) \\ x \equiv c_2 (\text{mod}\, m_2) \\ \ldots \\ x \equiv c_k (\text{mod}\, m_k) \end{cases}$$

всегда разрешима и имеет единственное решение по модулю $(m_1 m_2 \ldots m_k)$

Другими словами, китайская теорема об остатках утверждает, что кольцо вычетов по модулю произведения нескольких попарно взаимно простых чисел является прямым произведением соответствующих множителям колец вычетов

6.3.1 Теорема

Если модуль m - составное число, то $\mathbb{Z}_m$ не является полем

Доказательство

Пусть $\quad m = p_1 p_2, \qquad 1 < p_1, p_2 < m$

Будем считать, что $P_1, P_2 \in \mathbb{Z}_m$ - классы вычетов, которым принадлежат p_1, p_2. Тогда:

$P_1 P_2 = 0, \quad P_1, P_2 \neq 0 \quad$ и элементы P_1, P_2 необратимы.

Следовательно, $\mathbb{Z}_m$ - не поле

7 Линейные сравнения

Теорема: Если НОД$(a, b) = d$, то уравнение $a * x \equiv b \pmod m$ имеет решение тогда и только тогда, когда $b \vdots d$.
Доказательство ———————————————————

$\Rightarrow ax \equiv b \pmod{m}$, то $ax - b \vdots m \vdots d$, так как $ax \vdots d$ и $b \vdots d$.
$\Leftarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$
НОД $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ и $\left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)} \equiv 1 \pmod{\frac{m}{d}}$.

$\left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)} x \equiv \left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)-1} \frac{b}{d} \pmod{m}$

$x \equiv \left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)-1} \frac{b}{d} \pmod{\frac{m}{d}}$

$\left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)-1} \cdot \frac{b}{d} \equiv d \cdot \left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)} \cdot \frac{b}{d} \pmod{m} = d\left[k\frac{m}{d} + 1\right] \frac{b}{d} = [km + d]\frac{b}{d} \equiv d\frac{b}{d} \pmod{m} = b.$

---

1)$ax \equiv b \pmod{m}$
НОД$(a, m) = 1$! решение$\Rightarrow x \equiv a^{\phi(m)-1}b \pmod{m}$

2) НОД$(a, m) = d; b \vdots d$
$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$
$x \equiv \left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)-1} \frac{b}{d} \pmod{\frac{m}{d}}$, где $\left(\frac{a}{d}\right)^{\phi\left(\frac{m}{d}\right)-1} \frac{b}{d} = x_0$

d реш: $\left[\begin{array}{l} x \equiv x_0 \pmod{m} \\ x \equiv x_0 + \frac{m}{d} \pmod{m} \\ x \equiv x_0 + (d-1)\frac{m}{d} \pmod{m} \end{array}\right.$

3) НОД$(a, m) = d; b \not\vdots d$ => $\emptyset$

4)$ax \equiv b \pmod{m}$
$ax - b \vdots m$
$ax - b = my$
$b = ax - my$
$x = x_0 + t\frac{m}{d}$

Утв: p-простое, $a < p$
Решение $x \equiv \frac{C_p^a}{p} * b * (-1)^k \pmod{m}$,где k = a -1
Доказательство:
$C_p^a = \frac{p!}{a!(p-a)!} = \frac{p(p-1)....(p-a+1)}{1*2...a}$
$\frac{C_p^a}{p} == \frac{p(p-1)....(p-a+1)}{1*2...(a-1)a}$
$(p-1)(p-2)...(p-a+1) \equiv (-1)(-2)....(-a+1) = (-1)^k * 1 * 2.... * (a-1)$,где k=a-1
$a\frac{C_p^a}{p} \equiv (-1)^k \pmod{p}$,где k=a-1
$ab\frac{C_p^a}{p} * (-1)^k \equiv b \pmod{p}$,где k=a-1

Теорема Критерий Вильсона
p-простое <=> $(p-1)! \equiv -1 \pmod{p}$
Доказательство:
$|$ => $|(p-1)! = 1(p-1)$
$a^2 \equiv 1 \pmod{p}$
$a^2 - 1 \vdots p$
$(a-1)(a+1) \vdots p$

$$\left[\begin{array}{l} a-1 \vdots p \\ a+1 \vdots p \end{array}\right.$$

$\left[\begin{array}{l} a \equiv 1 \pmod p \\ a \equiv -1 \pmod p \end{array}\right. \quad | <= |p$- не простое $p = mn$

$(p-1)! \vdots m$
$(p-1)! \equiv -1 \pmod p$
$(p-1)! + 1 \vdots m \vdots p$

Теорема Китайскаяя теорема об остатках
$m_1, .., m_n$- попарно взаимно простые

d имеет ! реш: $\begin{cases} x \equiv C_1 \pmod{m1} \\ \text{.............................} \\ \text{.............................} \\ x \equiv C_n \pmod{m_n} \\ . \end{cases}$

$x \equiv C \pmod M$, где$M = m_1, ...m_n$

Доказательство:
$M_i = \frac{M}{m_i}$

НОД$(M_i, m_i) = 1$

$x * M_i \equiv 1 \pmod{m_i} => x \equiv a_i \pmod{m_i}$

$x = \sum_{i=1}^{n} M_i * a_i * C_i \equiv M_i * a_i * C_i \pmod{m_i} \equiv C_i \pmod{m_i}$
$|!| x \not\equiv y \pmod M$
$x \equiv C_i \pmod{m_i} \equiv y \pmod{m_i}$
$x - y \vdots m_i => x - y \vdots M$
$x = (C_1, ...C_n)$-китайский код числа X
$y = (d_1, ..d_n)$
$x + y = (C_1 + d_1, ...C_n + d_n)$

8 Функция Эйлера и её свойства

8.1 Определение

Функция Эйлера $\varphi(n)$ ставит в соответствие каждому натуральному n количество чисел, меньших n и взаимно простых с n. Будем полагать $\varphi(1) = 1$.

8.2 Свойства

1. $p \in P : \varphi(p) = p - 1$, - Функция Эйлера для простого числа
2. $p \in P : k \in N : \varphi(p^k) = p^k - p^{k-1}$, - Функция Эйлера для простого числа в степени
3. $\exists$НОД$(a, b) = 1 => \varphi(ab) = \varphi(a)\varphi(b)$, при $a, b \in \mathbb{N}$ - мультипликативность функции Эйлера

8.3 Утверждение

Для простого p значение функции Эйлера задаётся формулой:

$$\varphi(p) = p - 1,$$

которая следует из определения. Если p - простое, то все числа, меньшие p, взаимно просты с ним, а их ровно $p - 1$ штук.

Для вычисления функции Эйлера от степени простого числа используют следующую формулу:

$$\varphi(p^n) = p^n - p^{n-1}.$$

Доказательство. Подсчитаем количество чисел от 1 до p^n, которые не взаимно просты с p^n. Все они, очевидно, кратны p, то есть, имеют вид: $p, 2p, 3p, \ldots, p^{n-1}p$. Всего таких чисел p^{n-1}. Поэтому количество чисел, взаимно простых с p^n, равно $p^n - p^{n-1}$.

8.4 Следствие

Если НОД$(a, b) = 1$, тогда $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. В полной системе вычетов по модулю a существует $\varphi(a)$ значений x, таких, что НОД$(a, x) = 1$. Также и для полной системы вычетов по модулю b существует $\varphi(b)$ значений y, таких, что НОД$(b, y) = 1$. Следовательно, всего имеется $\varphi(a)\varphi(b)$ значений z, взаимно простых с ab. Но значения z образуют полную систему вычетов по модулю ab, и чисел, взаимно простых с ab, в ней $\varphi(ab)$.

8.4.1 Пример

Для иллюстрации доказательства следствия составлена таблица 1 величин (x,y) при $a = 4$ и $b = 5$. Возможные значения для x - числа $0, 1, 2, 3$, возможные значения для y - числа $0, 1, 2, 3, 4$. Из них для x имеется два значения (1 и 3) взаимно простых с a (так как $\varphi(4) = 2$). Соответственно для y также есть четыре значения (1,2,3 и 4) взаимно простых с b (так как $\varphi(5) = 4$). Эти значения помещены в кружочки, как и соответствующие им значения $z = ay + bx$.

Выделенные значения z дают 8 чисел, меньших 20 и взаимно простых с ним, Таким образом:

$$\varphi(20) = \varphi(4)\varphi(5) = 2 * 4 = 8.$$

	y				
x	0	1	2	3	4
0	0	4	8	12	16
1	5	9	13	17	1
2	10	14	18	2	6
3	15	19	3	7	11

Таблица 1: **Доказательство мультипликативности**

8.5 Следствие

Всякое натуральное число n>1 представляется в виде:

$$n = p_1^{\alpha_1} * \cdots * p_k^{\alpha_k},$$

где $p_1 < \cdots < p_k$ - простые числа, $\alpha_1 < \cdots < \alpha_k$ - натуральные числа.

Тогда $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) * p_2^{\alpha_2 - 1}(p_2 - 1) * \cdots = n\left(1 - \dfrac{1}{p_1}\right) * \left(1 - \dfrac{1}{p_2}\right)$

8.5.1 Пример

Для доказательства следствия приведён пример вычисления:

1. $\varphi(49) = \varphi(7^2) = 7^2 - 7 = 42$,
2. $\varphi(30) = \varphi(2 * 3 * 5) = \varphi(2)\varphi(3)\varphi(5) = (2-1)(3-1)(5-1) = 8$,
3. $\varphi(60) = 60\left(1 - \dfrac{1}{2}\right) * \left(1 - \dfrac{1}{3}\right) * \left(1 - \dfrac{1}{5}\right) = 16$.

8.6 Следствие

Функция Эйлера $\varphi(n)$ принимает только чётные значения при $n > 2$. Причём, если n имеет k различных нечётных простых делителей, то $2^k \mid \varphi(n)$.

Доказательство. Если $\exists p > 2$ и p - простое число, тогда

$$\varphi(n) \vdots (p-1) \vdots 2.$$

Тогда если $n = 2^k$, то

$$\varphi(n) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1} \vdots 2.$$

8.7 Теорема Формула Гаусса

8.8 Определение

Пусть d пробегает все делители числа m. Тогда

$$m = \sum_{d|m} \varphi(d).$$

Доказательство. $\sqsupset$ p - простое число. Тогда

$$\varphi(p^n) = p^{n-1}(p-1).$$

Таким образом

$$1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^\alpha) = 1 + (p-1) + \cdots + (p^\alpha - p^{\alpha-1}) = p^\alpha$$

Пусть $m = p_1^{\alpha_1} * \cdots * p_k^{\alpha_k}$, тогда

$$\prod_{i=1}^{k}(1 + \varphi(p_i) + \cdots + \varphi(p_i^{\alpha_i})) = \prod_{i=1}^{k} p_i^{\alpha_i} = m.$$

Исходя из этого

$$\prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\varphi(p_i^j) = \sum_{\substack{0 \le j_1 \le \alpha_1 \\ \vdots \\ 0 \le j_k \le \alpha_k}} \varphi(p_1^{j_1}) * \varphi(p_2^{j_2}) * \cdots * \varphi(p_k^{j_k}) = \sum_{\substack{0 \le j_1 \le \alpha_1 \\ \vdots \\ 0 \le j_k \le \alpha_k}} \varphi(p_1^{j_1} * \cdots * p_k^{j_k}) = \sum_{d|m}\varphi(d)$$

8.8.1 Пример

$$\sum_{d|30}\varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 1+1+2+4+2+4+8+8 = 30$$

8.9 Теорема Эйлера

Пусть НОД$(a, m) = 1$, тогда $a^{\varphi(m)} \equiv_m 1$.

Доказательство. Пусть НОД$(a, m) = 1$. Тогда классов вычетов взаимно простых с m будет $\varphi(m)$. Пусть $\{x_1, x_2, \dots, x_{\varphi(m)}\}$ - представители классов, то $\{ax_1, ax_2, \dots, ax_{\varphi(m)}\}$ будут также взаимно просты с m. Также, если $ax_i \equiv_m ax_j$, то $x_i \equiv_m x_j$. Следовательно, числа ax_i - также представители классов вычетов, взаимно простых с m. Тогда каждое ax_i сравнимо с одним и только одним a_j.

$$x_i * \dots * x_{\varphi(m)} \equiv_m ax_i * \dots * ax_{\varphi(m)}.$$

После сокращения получаем нужное сравнение:

$$1 \equiv_m a^{\varphi(m)}.$$

8.10 Следствие: Малая теорема Ферма

Если p - простое число, то $a^p \equiv_p a$

Доказательство.

Если НОД$(a, p) = 1$, то $a^{\varphi(p)} \equiv_p 1$, $a^{p-1} \equiv_p 1$, $a^p \equiv_p a \equiv_p 0$.

Если $a \vdots p$, то $a \equiv_p 0$, $a^p \equiv_p a \equiv_p 0$.

8.11 Следствие

Если p - простое число, то $(a + b)^p \equiv_p a^p + b^p$

Доказательство. $(a + b)^p \equiv_p a + b \equiv_p a^p + b^p$

8.12 Следствие

Если

$$\left.\begin{aligned} a \equiv_m b \\ c \equiv_{\varphi(m)} d \\ \text{НОД}(a, m) = 1 \end{aligned}\right| \Rightarrow a^c \equiv_m b^d$$

Доказательство. $a^c \equiv_m b^c \equiv_m b^{k\varphi(m)+d} = (b^{\varphi(m)})^k * b^d \equiv_m b^d$

$c \equiv_{\varphi(m)} d \Rightarrow c = k\varphi(m) + d$

НОД$(a, m) = 1 \Rightarrow$ НОД$(b, m) = 1$

НОД$(a, m) =$ НОД$(a - \widetilde{k}m, m)$

8.12.1 Пример

$25^{11^{35}} \equiv_{34} (-9)^3 = 81 * (-9) \equiv_{34} -13 * 9 = -117 \equiv_{34} 19$

НОД$(25, 34) = 1$

$11^{35} \equiv_{16} 11^3 \equiv_{16} (-5)^3 = -125 \equiv_{16} 3$

$\varphi(34) = 34\left(1 - \dfrac{1}{2}\right) * \left(1 - \dfrac{1}{17}\right) = 16$

НОД$(11, 16) = 1$

$\varphi(16) = 8$

$35 \equiv_8 3$

9 Система шифрования RSA

Определение 1: Функция f называется односторонней, если для любого x существует эффективный алгоритм вычисления $f(x)$, но не существует эффективного алгоритма решения уравнения $f(x) = a$.

Определение 2: Функция $f_k(x)$ называется функцией с секретом, если для любого k и x существует эффективный алгоритм вычисления $f_k(x)$, такой что $f_k(x) = a$, но не существует эффективного алгоритма решения уравнения $f_k(x) = a$. Однако, если значение k известно, то существует эффективный алгоритм решения уравнения $f_k(x) = a$.

RSA, разработанная Райвестом, Шамиром и Адлеманом, определяется функцией $f(x) = x^e \mod m$, где m - произведение двух больших простых чисел p и q. Для выбора открытого ключа e необходимо выбрать число, взаимно простое с функцией Эйлера $\varphi(m) = (p-1)(q-1)$. Закрытый ключ d находится из уравнения $e \cdot d \equiv 1 \mod \varphi(m)$.

Для шифрования сообщения x отправитель (Алиса) использует открытый ключ (m, e) получателя (Боба) и преобразует сообщение в зашифрованное сообщение c с помощью формулы $c \equiv x^e \mod m$. Зашифрованное сообщение c отправляется Бобу.

Для расшифровки сообщения Боб использует свой закрытый ключ d и преобразует зашифрованное сообщение c обратно в исходное сообщение x с помощью формулы $x \equiv c^d \mod m$.

RSA также может использоваться для создания электронных подписей. Электронная подпись используется для подтверждения подлинности и целостности данных. Она создается путем хеширования сообщения и шифрования полученного хеша закрытым ключом отправителя. Получатель может проверить подлинность сообщения, расшифровав подпись с помощью открытого ключа отправителя и сравнив полученный хеш с хешем исходного сообщения.

10 Определение деления многочленов с остатком. Теорема Безу. Схема Горнера

10.1 Определение деления многочленов с остатком:

10.2 Определение:

Для любых двух многочленов $f(x)$ и $g(x)$, $g(x) \neq 0$ существуют $q(x)$ и $r(x)$, такие что: $f(x) = g(x)q(x) + r(x)$, при этом степень $r(x)$ строго меньше степени $g(x)$

10.3 Свойства:

- $f(x) \div g(x), g(x) \div h(x) \Rightarrow f(x) \div h(x)$
- $f(x) \div g(x), g(x) \div h(x) \Rightarrow f(x) \pm g(x) \div h(x)$
- $f(x) \div h(x) \Rightarrow f(x)g(x) \div h(x)$
- $f(x) \div c, c \neq 0$
- $f(x) \div g(x) \Rightarrow f(x) \div cg(x), c \neq 0$

10.4 Теорема Безу:

10.4.1 Теорема:

Остаток от деления многочлена $P(x)$ на $x - a$ равен значению многочлена $P(a)$

10.4.2 Доказательство:

$P(x) = (x - a)Q(x) + r$, следовательно, $P(a) = r$

10.4.3 Следствие:

$P(x)\vdots(x-a) \Rightarrow P(a) = 0$

10.5 Схема Горнера:

10.5.1 Определение:

$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$
$P(x) = (x - b)Q(x) + r$
$Q(x) = C_{n-1}x^{n-1} + C_{n-2}x^{n-2} + ... + C_1 x + C_0$
$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = (x - b)(C_{n-1}x^{n-1} + ... + C_0) + r$
$x^n : a_n = C_{n-1}$
$x^{n-1} : a_{n-1} = C_{n-2} - bC_{n-1}$
$x^{n-2} : a_{n-2} = C_{n-3} - bC_{n-2}$
.
.
.
$x : a_1 = C_0 - bC_1$
$x^0 : a_0 = r - bC_0$
$C_{n-1} = a_{n-1}$
$C_i = bC_{i+1} + a_{i+1}$
.
.
.
$r = bC_0 + a_0$

10.5.2 Пример:

Найти остаток от деления $p(x) = x^4 - 3x^2 + x - 5$ на $x - 2$
$b = 2$

a_n	a_4	a_3	a_2	a_1	a_0
b	C_3	C_2	C_1	C_0	r

Далее подставив значения мы можем найти $C_{n-1}...C0$ и r

a_n	1	0	-3	1	-5
2	C_3	C_2	C_1	C_0	r

Используя формулу $C_{n-1} = b * C_{n-1} + a_{n-1}, C_{n-1} = a_n$ получим

a_n	1	0	-3	1	-5
2	1	2	1	3	1

Ответ $p(x) = (x_3 + 2x_2 + x + 3)(x - 2) + 1$

11 Интерполяционная формула Лагранжа

11.1 Формула Лагранжа

$L(x) = \sum_{i=0}^{n} y_i l_i(x)$
$l_i(x) = \frac{x-x_0}{x_i-x_0} \times \frac{x-x_1}{x_i-x_1} \times ... \times \frac{x-x_{i-1}}{x_i-x_{i-1}} \times \frac{x-x_{i+1}}{x_i-x_{i+1}}$

11.2 Пример

Найти многочлен $P(x)$ минимальной степени, используя формулу Лагранжа:
$P(-3) = -36$
$P(0) = -9$
$P(5) = -44$
Для удобства пронумеруем многочлены от 0 до 2, где $P_0(-3)$, $P_1(0)$, $P_2(5)$
$l_0(x) = \frac{x-x_1}{x_0-x_1} \times \frac{x-x_2}{x_0-x_2} = \frac{x-0}{-3-0} \times \frac{x-5}{-3-5} = \frac{x(x-5)}{(-3)*(-8)} = \frac{x(x-5)}{24}$
$l_1(x) = \frac{x-x_0}{x_1-x_0} \times \frac{x-x_2}{x_1-x_2} = \frac{x+3}{0+3} \times \frac{x-5}{0-5} = \frac{(x+3)(x-5)}{3*(-5)} = \frac{(x+3)(x-5)}{-15}$
$l_2(x) = \frac{x-x_0}{x_2-x_0} \times \frac{x-x_1}{x_2-x_1} = \frac{x+3}{5+3} \times \frac{x-0}{5-0} = \frac{x(x+3)}{5*8} = \frac{x(x+3)}{40}$
Обозначим многочлен минимальной степени $L(x)$:
$L(x) = -36\frac{x(x-5)}{24} + (-9)\frac{(x+3)(x+5)}{-15} + (-44)\frac{x(x+3)}{40}$
Чтобы найти многочлен минимальной степени, преобразуем многочлен к стандартному виду:
$L(x) = -\frac{3}{2}x(x-5) + \frac{3}{5}(x+3)(x-5) - \frac{11}{10}x(x+3) =$
$= -\frac{3}{2}(x^2 - 5x) + \frac{3}{5}(x^2 + 3x - 5x - 15) - \frac{11}{10}(x^2 + 3x) =$
$= -\frac{3}{2}x^2 + \frac{15}{2}x + \frac{3}{5}x^2 - \frac{6}{5}x - 9 - \frac{11}{10}x^2 - \frac{33}{10}x =$
$= \frac{-15+6-11}{10}x^2 + \frac{75-12-33}{10}x - 9 = -2x^2 + 3x - 9$
Итоговый вид многочлена: $L(x) = -2x^2 + 3x - 9$

12 (Билет 12) Разложение многочленов на свободные от квадратов множетели.

12.1 Определение:

Пусть K - поле
$P(x) \in K[x]$ **неприводим** if не $\exists$ нетривиальный делитель: не $\exists$ $Q(x) \in K[x] : 0 < deg(Q) < deg(P)$ и $P(x) \vdots Q(x)$;
$P(x) \vdots$ C
$P(x) \vdots cP(x)$
$x^2 - 2$ над $\mathbb{Q}$
$\exists| \; x^2 - 2 \vdots x - a$
$a^2 - 2 = 0$
$a^2 = 2$
$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$
То есть
$x^2 + 1$ над $\mathbb{Q}$ **неприводим**!
над $\mathbb{R}$ **неприводим**!
$x^2 + 1 = (x - i)(x + i)$ над $\mathbb{C}$
$x^2 + 1 = (x^2 + 1)$ над $\mathbb{Z}$

12.2 Определение: $P(x)$ свободный от квадратов

не $\exists$ $Q(x)$: $deg(Q) > 0$
$P(x) \vdots Q(x)^2$
$P(x) = P_1(x)P_2(x)^2P_3(x)^3...P_n(x)^n$
$P_1(x)$,...,$P_n(x)$ попарно взаимно/пр. и свободны от квадратов

12.3 Утверждение: $P(x) = Q(x)^k M(x)$

$NOD(Q(x), M(x)) = 1$ и $Q(x)$ неприводим => $P'(x) = Q(x)^{k-1}N(x)$
$NOD(Q(x), N(x)) = 1$
Доказательство:
$P'(x) = kQ(x)^{x-1}Q'(x)M(x) + Q(x)M'(x)$
$P'(x) = Q(x)^{x-1}(kQ'(x)M(x) + Q(x)M'(x))$
$kQ'(x)M(x) = N(x) - Q(x)M'(x) \vdots Q(x)$
$kQ'(x) \vdots Q(x)$?! Противоречие
Это работает при Z_k k характ поля, p - характ. k if $\forall a \in K a + a + ... + a = 0$
K-поле характеристики ноль

12.4 Следствие:

$P(x) = Q_1(x)^{k_1}...Q_m(x)^{k_n}$,$Q_i$- неприводимы => $P'(x) = Q_1(x)^{k_1-1}...Q_m(x)^{k_n-1}$,$Q$ вз./пр. с Q_i
Доказательство:
$P'(x) = \sum_{i=1}^{m} K_i Q_1(x)^{k_1}...Q_m(x)^{k_n}Q'_i(x) = Q_1(x)^{k_1-1}...Q_m(x)^{k_m-1}\sum_{i=1}^{n} \frac{k_i Q_1(x)...Q_m(x)}{Q_i(x)}Q'_i(x)$
$NOD(Q_1, Q_i) \neq 1$
$NOD(Q_1, Q_i) = Q_i$
$Q \vdots Q_i$
$Q(x) = k_1 Q_2 Q_3 ... Q_m Q'_1 + k_2 Q_1 Q_3 ... Q_m Q'_2 + ... + ... Q_{m-1} Q'_m \vdots Q_i$
$k_i Q'_i \vdots Q_i$
$Q'_i \vdots Q_i =>$ Противоречие

12.5 Алгоритм разложения на свободные от квадратов множ.:

На языке программирования питон:
$j = 1$
$while\ degP > 0$
$p' = diff(P)$
$S = NOD(P, P')$
$r = \frac{P}{S}$
$t = NOD(r, P')$
$P_j = \frac{r}{t}$
$P := \frac{P}{r}$
$j++$
$return\ P_1 P_2^2 ... P_{j-1}$

Где:

$P = P_1 P_2^2 P_3^3 ... P_n^n$
$P' = P_2 P_3^2 ... P_n^{n-1}$
$NOD(P, P') = P_2 P_3^2 ... P_n^{n-1}$
$r = \frac{P}{NOD(P,P')} = P_1 P_2 ... P_n$
$NOD(r, P') = P_2 ... P_n$
$\frac{r}{NOD(r,P')} = P_1$

Пример:
$P(x) = x^3 + x^2 - x - 1$
$P'(x) = 3x^2 + 2x - 1$

$NOD(P(x), P'(x)) = x + 1 = S(x)$
$r(x) = P/S = x^2 - 1$
$NOD(r, P') = x + 1 = t(x)$
$P_1 = x - 1$
new $P = x + 1$
$P' = 1$
$S = 1$
$r = x + 1$
$t = 1$
$P_2 = x + 1$
$P(x) = P_1(x)P_2(x)^2P_3(x)^3...P_n(x)^n$
$P_1(x), ..., P_n(x)$ попарно вз./пр. и свободные от квадратов множетели

12.6 $P(x) \in \mathbb{Z}P(x) \vdots x - \frac{p}{q}$ $NOD(p, q) = 1 => a_n \vdots q$, где $p(v) = a_n(x^n) + ... + a_0$

12.7 Теорема Безу

$P(x) \vdots x - \frac{p}{q} => p(\frac{p}{q} = 0)$
Доказательство:
$\frac{a_nP^n}{q_n} + \frac{a_{n-1}P^{n-1}}{q^{n-1}} + \frac{a_1P}{q} + a_0 = 0$
$a_nP^n + a_{n-1}P^{n-1}q + ... + a_nPq^{n-1} + a_0q^n = 0$
$a_np^n \vdots q => a_n \vdots q$
$a_0p^n \vdots p => a_0 \vdots q$

12.8 Критерий Эзерштейна

$P(x) \in \mathbb{Z}[x]$
$P(x) = a_nx^n + ... + a_0$
$a_{n-1} \vdots P, a_{n-2} \vdots P, ..., a_0 \vdots P$ и a_nне$\vdots P =>$ неприводима над Q
Доказательство:
Пусть $P(x) = f(x)g(x)$
$f(x) = b_mx^m + ... + b_0$
$g(x) = C_{n-m}x^{n-m} + ... + C_0$
$P(x) = a_nx^n + ... + a_0 = (b_mx^n + ... + b_0)(C_{n-m}x^{n-m} + ... + C_0)$
$a_0 = b_0C_0 \qquad b_0 \vdots P$
. $\qquad C_0$ не$\vdots P$
$a_1 = b_0C_2 + b_1C_1 + b_2C_0 => b_2 \vdots P$
$a_m = b_nC_m + ... + b_mC_0 => b_{n-1} \vdots P$

13 Неприводимые многочлены. Поля Галуа

13.1 Неприводимые многочлены

13.1.1 Определение

Пусть K — поле. Тогда $P(x) \in K[x]$ неприводим, если не существует нетривиальный делитель $Q(x) \in K[x]$, такой, что его степень больше 0, меньше степени многочлена P и $P(x)$ делится на $Q(x)$:

$$\nexists Q(x) \in K[x] : 0 < \deg Q < \deg P \text{ и } P(x) \vdots Q(x)$$

13.1.2 Определение

$P(x)$ свободный от квадратов, если не существует $Q(x)$, такой, что $\deg Q >$ и $P(x) \vdots Q^2(x)$.

13.1.3 Утверждение

$P(x) = Q^k(x)M(x)$
НОД$(Q(x), M(X)) = 1$ и $Q(x)$ неприводим $\Rightarrow P'(x) = Q^{k-1}(x)N(x)$
НОД$(Q(x), N(x)) = 1$

13.1.4 Доказательство

$P'(x) = kQ^{k-1}(x)Q'(x)M(x) + Q^k(x)M'(x)$
$P'(x) = Q^{k-1}(x)(kQ'(x)M(x) + Q(x)M'(x))$, где $kQ'(x)M(x) + Q(x)M'(x) = N(x)$

$kQ'(x)M(x) = N(x) - Q(x)M'(x) \vdots Q(x)$

$kQ'(x) \vdots Q(x)$ — противоречие
$\deg Q' = \deg Q - 1$

Это работает при $\mathbb{Z}_k$ ($k \not\vdots$ характериситку поля).

13.1.5 Следствие

$P(x) = Q_1^{k_1}(x)...Q_m^{k_m}(x)$, Q_i — неприводимы $\Rightarrow$ $P'(x) = Q_1^{k_1-1}(x)...Q_m^{k_m-1}Q(x)$, Q взаимно прост с Q_i

13.1.6 Критерий Эйзенштейн

$P(x) \in \mathbb{Z}[x]$
$P(x) = a_nx^n + ... + a_0$

$a_{n-1} \vdots p,\ a_{n-2} \vdots p,\ ..., a_0 \vdots p,\ a_n \not\vdots p \Rightarrow$ неприводима над Q

13.1.7 Доказательство

Рассмотрим $P(x) = f(x)g(x)$.

$f(x) = b_mx^m + ... + b_0$
$g(x) = c_{n-m}x^{n-m} + ... + c_0$
$p(x) = a_nx^n + ... + a_0 = (b_mx^m + ... + b_0) \cdot (c_{n-m}x^{n-m} + ... + c_0)$

$a_0 = b_0c_0 \vdots p \qquad b_0 \vdots p \qquad c_0 \not\vdots p$

$a_1 = b_0c_2 + b_1c_1 + b_2c_0 \vdots p \Rightarrow b_2 \vdots p$

$\vdots$

$a_m = b_0c_m + ... + b_mc_0 \vdots p \Rightarrow b_{m-1} \vdots p$

$a_n = b_nc_{n-m} \vdots p$ — противоречие

13.2 Поля Галуа

13.2.1 Определение

Конечное поле, или поле Галуа в общей алгебре — поле, состоящее из конечного числа элементов. Обозначается $\mathbb{F}_q$ или $\mathbf{GF}(q)$ или $< \mathbf{GF}(q), +, * >$, где $q = |\mathbf{GF}(q)|$ — порядок поля. Порядком поля называется количество входящих в него элементов. Пример: $\mathbb{Z}_p,\ p \in \mathbb{P}$.

13.2.2 Определение

Характериситка поля F — наименьшее n, такое, что $\forall a \in F$ выполняется следующее равенство:

$$\underbrace{a + a + ... + a}_{n \text{ раз}} = 0$$

Если такого n не существует, то n считается равным 0.

13.2.3 Лемма

Характериситка поля — простое или 0.

13.2.4 Доказательство

Рассмотрим $n = \alpha\beta$.

$$\underbrace{1 + 1 + ... + 1}_{n \text{ раз}} = 0$$

$$\underbrace{\underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}} + \underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}} + ... + \underbrace{1 + 1 + ... + 1}_{\alpha \text{ раз}}}_{\beta \text{ раз}} = 0$$

$$\underbrace{\alpha + \alpha + ... + \alpha}_{\beta \text{ раз}} = 0 \qquad \Rightarrow \text{ характеристика — } \mathbb{P}$$

13.2.5 Свойства

$f(x) \in \mathbb{Z}_p[x]$ ($f(x)$ принадлежит множеству многочленов с целыми коэффициентами по модулю p) $\mathbb{Z}_p[x]/f(x)$ (кольцо вычетов многочленов с целыми коэффициентами по модулю $f(x)$)

$$\left.\begin{array}{l} g_1(x) \equiv_{f(x)} h_1(x) \\ g_2(x) \equiv_{f(x)} h_2(x) \end{array}\right| \Rightarrow \begin{array}{l} g_1 + g_2 \equiv_{f(x)} h_1 + h_2 \\ g_1 g_2 \equiv_{f(x)} h_1 h_2 \end{array}$$

13.2.6 Теорема

$\mathbb{Z}_p[x]/f(x) \ \Leftrightarrow\ f(x)$ неприводим над $\mathbb{Z}_p$.
$\deg f = m\ \mathbf{GF}(p^m)$

13.2.7 Доказательство

Прямое. Рассмотрим $f(x) = g(x)h(x)$
$g(x)h(x) \equiv_{f(x)} 0 \qquad | \cdot g^{-1}(x)$
$h(x) \equiv_{f(x)} 0| \Rightarrow f(x) = 0$
От обратного. $\forall g(x) \neq 0 \deg g < \deg p$
НОД$(g(x), f(x)) = 1\ \Rightarrow$ по расширенному алгоритму Евклида:
$a(x)g(x) + b(x)f(x) = 1$
$a(x)g(x) \equiv_{f(x)} 1\ \Rightarrow\ a = g^{-1}\ \Rightarrow\ \mathbb{Z}_p$ — поле

13.2.8 Связь с линейным пространством

Поле Галуа образует линейное (векторное) пространство. Его аксиомы:

- $(a+b)+c = a+(b+c)$
- $\exists 0 : a+0 = a$
- $\forall a\ \exists(-a) : a+(-a) = 0$
- $a+b = b+a$
- $\alpha(a+b) = \alpha a + \alpha b$
- $(\alpha+\beta)a = \alpha a + \beta a$
- $\alpha(\beta a) = (\alpha\beta)a$
- $\exists 1 : 1 \cdot a = a$

$\alpha, \beta \in \mathbb{Z}_p$, F — линейное пространство. $m = \dim F$.

13.2.9 Определение

α — примитивный элемент, если $\forall b \neq 0 \in F \qquad b = \alpha^i$.

14 Кодирование с исправлением ошибок. Граница Хэмминга. Полиномиальное кодирование

14.1 Кодирование с исправлением ошибок. Граница Хэмминга

$d : MxM \to \mathbb{R}$ - функция расстояния

1. $d(a,b) \geq 0; \quad d(a,b) = 0 \Leftrightarrow a = b$
2. $d(a,b) = d(b,a)$
3. $d(a,b) + d(b,c) \geq d(a,c)$

$M = \mathbb{Z}_2^m$
$a \in M,\ a = (a_0, a_1, ..., a_{m-1})$
$d(a,b) = \sum\limits_{i=0}^{m-1} |a_i - b_i|$ - кодовое расстояние Хэмминга (КХР)
$a \bigoplus b = (a_0 \bigoplus b_0, ..., a_{m-1} \bigoplus b_{m-1})$

Теорема КРХ - формула расстояния на $\mathbb{Z}_2^m$
$d(a,b) + d(b,c) = \sum\limits_{i=0}^{n-1} |a_i - b_i| + \sum\limits_{i=0}^{n-1} |b_i - c_i| = \sum\limits_{i=0}^{n-1} (|a_i - b_i| + |b_i - c_i|) \geq \sum\limits_{i=0}^{n-1} |a_i - b_i + b_i - c_i| =$
$= \sum\limits_{i=0}^{n-1} |a_i - c_i| = d(a,c)$
$A = \{a^{(0)}, a^{(1)}, ..., a^{(k)}\} \leq \mathbb{Z}_2^m$
$\uparrow$
кодовое слово

Теорема. Если $\forall i \neq j$
$d(a^{(i)}, a^{(j)} \geq 2r+1 \Rightarrow$ можно исправить $\leq r$ ошибок

Доказательство: $a \in \mathbb{Z}_2^m$
$A_i = \{b / d(a^{(i)}, b) \leq r\}$
$\exists \mid A_i \cap A_j = \{c\}$
$$\left.\begin{array}{l} c \subset A_i \\ \\ c \subset A_j \end{array}\right| \begin{array}{l} \quad d(c, a^{(i)}) \leq r \\ \Rightarrow \\ \quad d(c, a^{(j)}) \leq r \end{array}$$
$d(a^{(i)}, a^{(j)}) \leq d(a^{(j)}, c) + d(c, a^{(i)}) \leq 2r \quad ?!$
A_i - область декодирвоания $a^{(i)}$
$a^{(i)} + e \quad d(a^{(i)} + e, a^{(j)}) \leq r \mid \Rightarrow a^{(i)} + e \in A_i \mid \Rightarrow$ декодирование однознач.
$|A_i| = 1 + C_m^1 + C_m^2 + ... + C_m^r \qquad |\mathbb{Z}_2^m| = 2^m$
$\sum\limits_{i=0}^{n-1} |A_i| \leq |\mathbb{Z}_2^m|; \qquad k = |A| \qquad k|A_i| \leq |\mathbb{Z}_2^m| \mid \Rightarrow k = \frac{2^m}{\sum\limits_{i=0}^{r} C_m^i}$ - граница Хэмминга
$M = \{0, 1\} \mid \rightarrow A = \{000, ..., 111\}$
$m = 3 \Rightarrow r = 1 \qquad d(a^0, a^1) = 3 \geq 2r + 1 \qquad k \leq \frac{2^3}{C_3^0 + C_3^1} = \frac{8}{1+3} = 2$

Определение. Код называется совершенным (или плотно упакованным), если $\bigcup\limits_{i=0}^{n-1} A_i = \mathbb{Z}_2^m$

14.2 Полиномиальное кодирование

$M \Rightarrow \widetilde{M}$
$M \rightarrow C \Rightarrow \widetilde{C} \rightarrow M$
$\uparrow \qquad \uparrow$
сообщ. код. слово
Код линейный if $\forall a, b \in A$
Вес Хэмминга $W(a)$
$a \in A \leq \mathbb{Z}_2^m$
$a = (a_0, ..., a_{m-1})$
$W(a) =$ количество ненулевых a_i
Минимальное кодовое расстояние $d^* = \min\limits_{i \neq j} d(a^{(i)}, a^{(j)})$
Лемма. $d^* = \min\limits_{a \neq 0} W(a)$
Доказательство: $W(a) = d(a, 0) \geq d^*$
$d(a, b) = d(a + b, b + b) = d(a + b, 0) = W(a + b)$
$d^* = \min\limits_{a \neq b} d(a, b) = \min\limits_{a \neq b} W(a + b) = \min\limits_{a \neq 0} W(a)$
$a = (a_0, a_1, ..., a_{m-1}) \mid \rightarrow a_0 + a_1 k + ... + a_{m-1} x^{m-1}$

Код циклический
$if (a_0, a_1, ..., a_{m-1}) \in A \Rightarrow (a_{m-1}, ..., a_{m-2}) \in A$
$$\begin{array}{lc} a \rightarrow A(x) & \\ & a + b \rightarrow A(x) + B(x) \\ b \rightarrow B(x) & \end{array}$$

$$\begin{array}{rr} a \rightarrow a_0 + a_1 x + ... + a_{m-1} x^{m-1} & xA(x) \, mod(x^m + 1) \\ a_2 \rightarrow a_{m-1} + a_0 x + ... + a_{m-2} x^{m-1} & x^m \equiv 1 \, mod(x^m + 1) \end{array}$$

$A(x)$ - количество кодов $\Rightarrow P(x)A(x)$ - кодов
Порождающий многочлен - ненулевое приведение мн. наименьшей степени в коде.
$A = \{...\}$

Теорема. $G(x)$ - порождающий многочлен

минимальный цикл кода $\Leftrightarrow x^m + 1 \vdots G(x)$

Доказательство:

$\Leftarrow\ x^m + 1 \vdots G(x)$

$A(x), B(x)$

$A = \{P(x)G(x)\, mod(x^m + 1)\}$

$A(x) = P_A(x)G(x) \qquad A(x) + B(x) = (P_A(x) + P_B(x))G(x)$

$B(x) = P_B(x)G(x) \qquad \alpha A(x) = (\alpha P_A(x))G(x)$

$xA(x)\, mod(x^m + 1)$

$xA(x) = xP_A(x)G(x)$

$r(x) = xA(x) \equiv_{x^m+1} Q(x)G(x) + R(x)$

$xA(x) = S(x)(x^m + 1) + r(x) = S(x)(x^n + 1) + Q(x)G(x) + R(x)$

$P(x)G(x) = Q(x)(x^m + 1) + R(x)$

$P(x)G(x)\, mod(x^m + 1) \qquad 0 \equiv_{(x^m+1)} Q(x)G(x) + R(x)$

$x^m + 1 \vdots G(x) \qquad degR < degG\, ?! \Rightarrow$

$x^m + 1 = Q(x)G(x) + R(x)$ *обязательно делится*

$x^m + 1$

$G(x)$

$d^* = \min\limits_{P(x) \neq 0} W(P(x)G(x)\, mod x^m + 1)$

$d^* > 2r + 1 \qquad r < \frac{d^*}{2}$

$M \to C$

$M(x) \to C(x)$

$C(x) = M(x)G(x)$

$C(x) + E(x)$

$\widetilde{C}(x) = C(x) + E(x)$ - многочлен ошибок

$W(E(x)) \leq r$

$\widetilde{C}(x)\, mod(G(x)) = S(x)$ - синдром

Теорема. $E_1(x) \neq E_2(x) \Rightarrow E_1(x)\, modG(x) \neq E_2(x)\, modG(x)$

$W(E_1(x)) \leq r$

$W(E_2(x)) \leq r$

Доказательство:

$E_1(x) + E_2(x) \neq 0$

$W(E_1(x) + E_2(x)) \leq 2r$

$\sqsupset E_1(x) \equiv E_2(x)\, modG(x)$

$E_1(x) + E_2(x) \vdots G(x),\ W(E_1 + E_2) \geq d^* \geq 2r + 1$

$\widetilde{C}(x) = C(x) + E(x) = M(x)G(x) + E(x)$

$modG(x):$

$S(x) \equiv E(x),\ C(x) = \widetilde{C} + E(x)$

$M(x) = \frac{C}{G}$

Если все ошибки в $degG$ послед. разр.

$x^i S(x) \equiv_{G(x)} T(x)$

$i \in [0; m-1]$

$W(T(x)) \leq r$

$x^m S(x) \equiv_{G(x)} x^{m-i} T(x)$

$|||$
$x^m + 1 \equiv_{G(x)} 0$

Теорема. $G(x) \vdots x+1 \geq W(P(x)G(x)) \vdots 2$

Доказательство: $G(x) = (x+1)A(x)$
$P(x)G(x) \vdots x+1$
$P(1)G(1) = 0$
$W(P(x)G(x)) \vdots 2$

Следствие. $G(x) \vdots x+1 \geq$ детект. $\forall$ на ошиб.
$C(x) + E(x)$

15 15. Префиксные коды.Неравенство Крафта.Алгоритм Хаффмана.

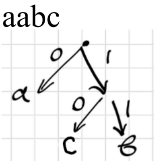
15.1 Префиксные коды

$A = a_1, \dots, a_n$ - алфавит $n \leq 2^k \to \begin{cases} a_1 \sim \underbrace{0\dots0}_{\text{k}} - c_1 \\ a_2 \sim \underbrace{0\dots0}_{\text{k}} 1 - c_2 \\ \dots \end{cases}$

$l_1 = l_2 = l_k$; $M : a_{i_1}, a_{i_2}, \dots, a_{i_s}$; $\alpha = ks \geq s \log n$

Шеннон-Фано

aabc



$\underbrace{0}_{\text{a}} \underbrace{0}_{\text{a}} \underbrace{11}_{\text{b}} \underbrace{01}_{\text{c}}$

$\begin{cases} a \sim 0 \\ b \sim 11 \\ c \sim 01 \end{cases}$

15.1.1 Определение

Код называется *префиксным*, если ни одно кодовое слово не является началом другого кодового слова.

15.2 Неравенство Крафта

Для префиксного кода с длинами $l_1, \dots, l_s$
$\sum_{i=1}^{s} 2^{-l_i} \leq 1$

15.2.1 Доказательство

$l_1 \leq l_2 \leq \dots \leq l_s = q$
$A_i = \{ \underbrace{(\dots)}_{\text{q двоичных чисел}})|\text{нач. с } l_i\}$

$A_i \cap A_j = \emptyset$

15.2.2 Замечание

$\cup A_i \leq \{\underbrace{(\ldots)}_{\text{q раз p}}\}$

$\sum\limits_{i=1}^{s} 2^{q-l_i} \leq 2^q$

15.2.3 Теорема

$p_1, \ldots, p_n$ - вер, с которой встречаются $a_1, \ldots, a_n$

Сред. длин. код. слова $L = \sum\limits_{i=1}^{n} l_i p_i$; $L \geq H(p_1, \ldots, p_s)$

15.2.4 Доказательство

$\sqsupset q_i = \frac{2^{-l_i}}{\sum\limits_{i=1}^{n} 2^{l_i}}$; $L - H(p_1, \ldots, p_n) = \sum\limits_{i=1}^{n} l_i p_i + \sum\limits_{i=1}^{n} p_i \log_2 p_i = \sum\limits_{i=1}^{n} p_i \log_2 (p_i 2^{l_i}) =$

$= \sum\limits_{i=1}^{n} p_i log \frac{p_i}{2^{-l_i}} \geq \sum\limits_{i=1}^{n} p_i \log_2 \frac{p_i \sum\limits_{j=1}^{n} 2^{-l_j}}{2^{-l_i}} = \sum\limits_{i=1}^{n} p_i \log_2 \frac{p_i}{q_i} = D(p||q) \geq 0$

$\to L \geq H(p_1, \ldots, p_n) + D(p||q)$

15.3 Алгоритм Хаффмана

$a_1, \ldots, a_n$ с $p_1, \ldots, p_n$

$p_i = \frac{N(a_i)}{N}$

$p_1, p_2, \ldots, p_s$

$p_i \geq p_j \to l_i \leq l_j$

$\sum\limits_{i=1}^{s} 2^{-l_i} \leq 1 (*)$

p_{n-1}, p_n - наим.вер $\to l_{n-1} = l_n$

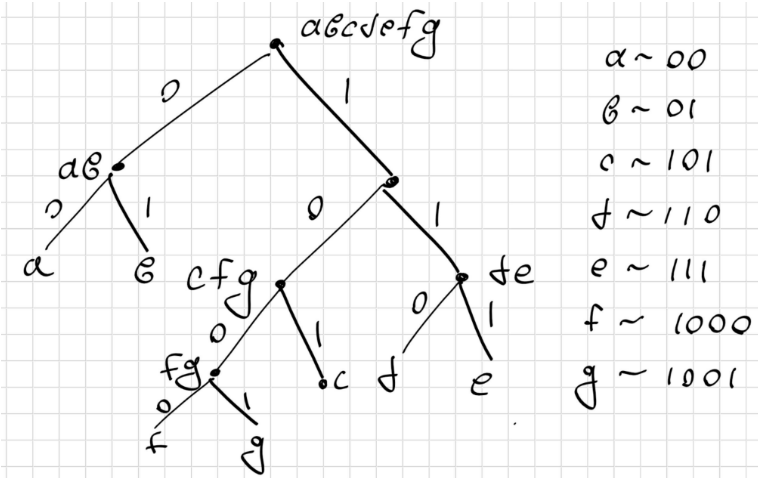
[чтобы знам $(*)$ сокращался]

15.3.1 Пример

$\underbrace{a \sim 0,22 \text{ ; } b \sim 0,2}_{ab \sim 0,42}$; $c \sim 0,15$; $\underbrace{d \sim 0,13 \text{ ; } e \sim 0,12}_{de \sim 0,25}$; $\underbrace{f \sim 0,1 \text{ ; } g \sim 0,18}_{fg \sim 0,18}$

$\underbrace{cfg \sim 0,33 \text{ ; } de \sim 0,25}_{cdefg \sim 0,58}$; $ab \sim 0,42$

$\underbrace{ab \sim 0,42 \text{ ; } cdefg \sim 0,58}_{abcdefg \sim 1}$



16 Коды Рида-Соломона:

Рассмотрим алгоритм на примере:
Поле $GF(16)$ порождается присоединением к $GF(2)$ корня a многочлена $P(x)$, $P(x) = x^4 + x^3 + 1$
Пусть порождающий много член имеет вид $G(x) = (x - a)(x - a^2)(x - a^3)(x - a^4)$, тогда количество ошибок многочлена которое исправит код Рида-Соломона $2t = deg(G(x)) \Rightarrow t = 4/2 = 2$.
Принятое сообщение $S(x) = a^9x^14 + a^5x^{13} + a^{12}x^{12} + a^{10}x^{11} + a^7x^9 + a^5x^8 + a^7x^7 + a^{13}x^6 + a^3x^5 +$
$+a^{11}x^4 + a^3x^3 + a^{10}x^2 + a^8x + a$
Вырази все a пока они не зациклятся, т.е. $a_n = a_0$
$a^0 = a^0 = 1$
$a^1 = a$
$a^2 = a^2$
$a^3 = a^3$
$a^4 = a^3 + 1$
$a^5 = a * a^4 = a^4 + a = a^3 + a + 1$
$a^6 = a^3 + a^2 + a + 1$
$a^7 = a^2 + a + 1$
$a^8 = a^3 + a^2 + a$
$a^9 = a^2 + 1$
$a^{10} = a^3 + a$
$a^{11} = a^3 + a^2 + 1$
$a^{12} = a + 1$
$a^{13} = a^2 + a$
$a^{14} = a^3 + a^2$
$a^{15} = a^4 + a^3 = 1$
И так как у нас поле $GF(16)$ то $a^{15} = a^0 = 1$
Из порождающего многочлена выразим корни уравнения и подставим их в принятое сообщение S(x).
$S_1(a) = a^4$
$S_2(a^2) = 0$
$S_3(a^3) = a^2$
$S_4(a^4) = a^2$
Теперь строим систему уравнений вида

$$\begin{pmatrix} S_n & S_{n+1} & \dots & S_{n+t-1} \\ S_{n+1} & S_{n+2} & \dots & S_{n+t} \\ . & . & . & . \\ S_{n+t-1} & S_{n+t} & \dots & S_{n+2t-2} \end{pmatrix} \begin{pmatrix} \lambda_t \\ \lambda_{t-1} \\ . \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} S_{n+t} \\ S_{n+t+1} \\ . \\ S_{n+2t-2} \end{pmatrix} \tag{2}$$

Где $n = 1, t = 2$, подставим значения в матрицу и получим:

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \begin{pmatrix} \lambda_2 \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} S_3 \\ S_4 \end{pmatrix} \tag{3}$$

$$\begin{pmatrix} a^4 & 0 \\ 0 & a^2 \end{pmatrix} \begin{pmatrix} \lambda_2 \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} a^2 \\ a^2 \end{pmatrix} \tag{4}$$

Решив систему мы получим что $\lambda_2 = a^{13}, \lambda_1 = 1$.

$L(x) = 1 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_t x^t$. Подставим значения от 1 до a^{15} и найдем такие значения a что $L(a^n) = 0$. В нашем случае такими значениями являются a^3 и a^{14}. Найдем обратные к этим значениям $\gamma_1 = \frac{a^{15}}{a^3} = a^{12}, \gamma_2 = a$.

$$\begin{pmatrix} {\gamma_1}^s & {\gamma_2}^s & ... & {\gamma_t}^s \\ {\gamma_1}^{s+1} & {\gamma_2}^{s+1} & ... & {\gamma_t}^{s+1} \\ . & . & . & . \\ {\gamma_1}^{s+t-1} & {\gamma_2}^{s+t-1} & ... & {\gamma_t}^{s+t-1} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ . \\ e_t \end{pmatrix} = \begin{pmatrix} S_n \\ S_{n+1} \\ . \\ S_{n+t-1} \end{pmatrix} \tag{5}$$

Подставим значения и получим:

$$\begin{pmatrix} a^{12} & a \\ a^{24} & a^2 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} a^4 \\ 0 \end{pmatrix} \tag{6}$$

Используя метод Крамера найдем e_1 и e_2:

$$e_1 = \frac{\begin{vmatrix} a^4 & a \\ 0 & a^2 \end{vmatrix}}{\begin{vmatrix} a^{12} & a \\ a^{24} & a^2 \end{vmatrix}} = \frac{a^6}{a^{13}} = a^8 \tag{7}$$

$$e_2 = \frac{\begin{vmatrix} a^{12} & a^4 \\ a^{24} & 0 \end{vmatrix}}{\begin{vmatrix} a^{12} & a \\ a^{24} & a^2 \end{vmatrix}} = \frac{-a^{28}}{a^{13}} = a^{15} = 1 \tag{8}$$

Найдем многочлен ошибок $E(x) = e_1 x^{i_1} + e_2 x^{i_2} + e_3 x^{i_3} + ... + e_t x^{i_t}$, $\gamma_1 = a^{i_1}, ...\gamma_t = a^{i_t}$, $E(x) = a^8 x^{12} + x$. Теперь найдем правильный код $V(x) + E(x)$, в нашем случае правильный код $V(x) + E(x) = a^9 x^{14} + a^5 x^{13} + a^{11} x^{12} + a^{10} x^{11} + a^7 x^9 + a^5 x^8 + a^7 x^7 + a^{13} x^6 + a^3 x^5 + a^{11} x^4 + a^3 x^3 + a^{10} x^2 + a^6 x^1 + a$ далее используя схему Горнера находим исходное сообщение $A(x)$.

17 Алгоритм Берлекемпа

$\exists F$ - многочлен, свободный от квадратов. Разложим $F = f_1 * f_2 * f_3, ..., f_s(f_i$ - неприводим над $\mathbb{Z}_p)$

17.1 Алгоритм:

Составить матрицу A, которая имеет вид:

$$A = \begin{array}{c} \begin{array}{ccccc} x^0 & x^{1*p} & x^{2*p} & ... & x^{(deg(f)-1)*p} \end{array} \\ \begin{pmatrix} . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{pmatrix} \end{array} \begin{array}{c} x^0 \\ x^1 \\ x^2 \\ ... \\ x^{deg(f)-1} \end{array}$$

Каждый столбец матрицы соответствует векторному разложению многочленов из множества
$\{x^0, x^{1*p}, x^{2*p}, ..., x^{(deg(f)-1)*p}\}$ (1)
в базисе $\{x^0, x^1, x^2, ..., x^{deg(f)-1}\}$

Для получения векторного представления каждого из многочленов множества (1) необходимо привести их по модулю f.
$x_0 \equiv_{f(x)} x^0$
$x_1 \equiv_{f(x)} ...$
$x_2 \equiv_{f(x)} ...$

Далее необходимо найти собственные векторы матрицы A. Для этого получим матрицу $B = A - E$, где E - единичная матрица. Далее нужно привести матрицу к ступенчатому виду методом Гаусса или же любым другим методом и найти ранг матрицы.

Если $rankB = 1$, то f - неразложим над $\mathbb{Z}_p$.
Если $1 < rankB$ и $< deg(f) - 1$, то f - разложим над $\mathbb{Z}_p$

Далее решим уравнение для нахождения собственных векторов h_i:
$$B * h_i = \begin{pmatrix} 0 \\ 0 \\ ... \\ 0 \end{pmatrix}$$
Количество подходящих векторов h можно найти по формуле:
Кол-во $h_i = degf - rankB$
h_1 всегда имеет вид $h_1 = \begin{pmatrix} 1 \\ 0 \\ ... \\ 0 \end{pmatrix}$
h_2, h_3 и т.д. необходимо найти аналитическим методом либо другим методом для нахождения собственных векторов матрицы.

После нахождения всех векторов h_i приведем их к виду многочлена.
Пример:
$$h_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 1 * x^0 + 0 * x^1 + 0 * x^2 + 1 * x^3 + 0 * x^4 = x^3 + 1$$

Итоговое разложение будет иметь вид:
$$f(x) = \prod_{c \in \mathbb{Z}_p} \text{НОД}\ (f(x), h_i - c)$$

Примечание: h_1 в формуле разложения не рассматривается, т.к. НОД = 1 или $f(x)$ нас не интересует.

17.2 Пример

$f(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ над $\mathbb{Z}_2$

Шаг 1: Проверить, свободен ли f(x) от квадратов
Шаг 2: Составить матрицу A.
Для этого приведем элементы из множества $\{x^0, x^2, x^4, x^6, x^8, x^{10}, x^{12}\}$ по модулю $f(x)$.
$x^0 \equiv_{f(x)} x^0$

$x^2 \equiv_{f(x)} x^2$
$x^4 \equiv_{f(x)} x^4$
$x^6 \equiv_{f(x)} x^6$
$x^8 \equiv_{f(x)} x^7 + x^6 + x^5 + x^4 + x^2 + x \equiv x^3 + x^2 + 1$
$x^{10} \equiv_{f(x)} x^8 * x^2 \equiv x^2 * (x^3 + x^2 + 1) \equiv x^5 + x^4 + x^2$
$x^{12} \equiv_{f(x)} x^{10} * x^2 \equiv x^7 + x^6 + x^4 \equiv x^5 + x^3 + x + 1$
Тогда A имеет вид:

$$A = \begin{array}{c} \begin{array}{ccccccc} x^0 & x^2 & x^4 & x^6 & x^8 & x^{10} & x^{12} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ x^0 \\ x^1 \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \end{array}$$

Шаг 3: Найти собственные векторы матрицы A

$$B = A - E = \begin{array}{c} \begin{array}{ccccccc} x^0 & x^2 & x^4 & x^6 & x^8 & x^{10} & x^{12} \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array} \begin{array}{c} \\ x^0 \\ x^1 \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \end{array}$$

Приведенная матрица B будет иметь вид:

$$B = \begin{array}{c} \begin{array}{ccccccc} x^0 & x^2 & x^4 & x^6 & x^8 & x^{10} & x^{12} \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \\ x^0 \\ x^1 \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \end{array}$$

$rankB = 5$

Решим уравнение: $B * h_i = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Кол-во $h_i = deg(f) - rankB = 7 - 5 = 2$

$$h_1 = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix} \; h_2 = \begin{pmatrix}0\\0\\1\\0\\0\\1\\0\end{pmatrix}$$

$h_1 = 1$
$h_2 = x^5 + x^2$
Шаг 4: Найдем итоговое разложение

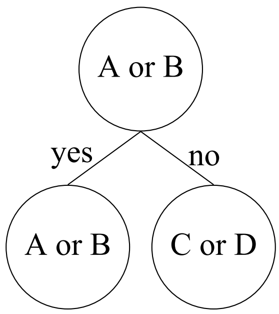
$f(x) = \prod\limits_{c \in \mathbb{Z}_2} \text{НОД}\,(f(x), h_i - c)$
НОД $(f(x), x^5 + x^2 - 0) = x^2 + x + 1$
НОД $(f(x), x^5 + x^2 - 1) = x^5 + x^2 + 1$

Ответ: $f(x) = (x^2 + x + 1)(x^5 + x^2 + 1)$

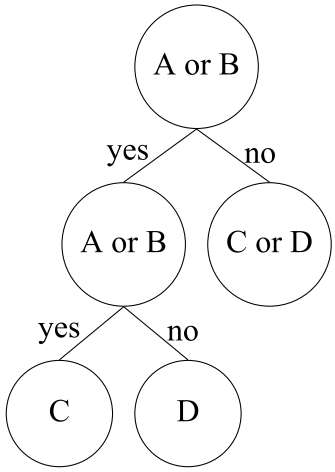
18 Энтропия. Информационное неравенство

18.1 Пример

Рассмотрим две чёрных коробки, одна и вторая может генерировать символы A,B,C и D.
В *первой* вероятности появления символов: $p(A) = 0.25, p(B) = 0.25, p(C) = 0,25, p(D) = 0,25$
Во *второй*: $p(A) = 0.5, p(B) = 0.125, p(C) = 0,125, p(D) = 0,25$ Зададимся вопросом сколько вопросов да или нет нужно задать, чтобы узнать следующий символ, который появится
В первом случае сначала надо можно разделить символы на две равновероятные группы, AB и CD или любые другие по два символа. Мы должны спросить является ли A или B

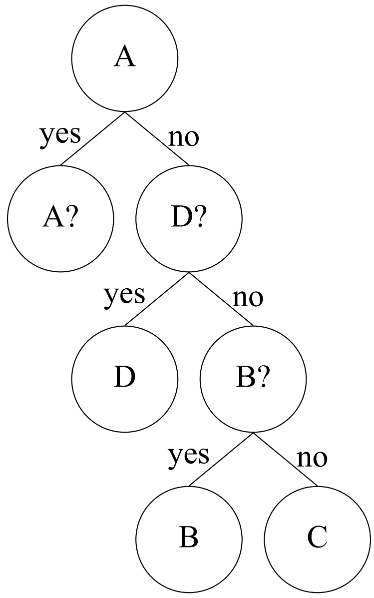


если да,то выбираем из A и B



В среднем количество вопрос для определение - 2

Во втором случае выгоднее сначала спросить является ли это A, т.к. у появление A вероятность 0.5 В случае отрицательного ответа необходимо спросить самое вероятное - D, B и C равновероятны.



Вычислим количество вопросов: $\sum\limits_{i=1}^{4} p_i \cdot amount_i = 1 \cdot p(A) + 2 \cdot p(D) + 3 \cdot p(C) + 3 \cdot p(B) = 1,75$

Вторая коробка генерирует меньше информации, так как генерирует меньше неопределённости, меньше неожиданности. Это и есть энтропия. Обозначается как $H(p_1, p_2, \cdots, p_n)$

За единицу измерения был выбран бит - неопределённость о броске монеты, что эквивалентно одному вопросу

$H = \sum\limits_{i=1}^{n} x_i \cdot amount_i$

Количество вопросов= $\log_2($**количество исходов**$)$

Количество исходов= $\frac{1}{p}$

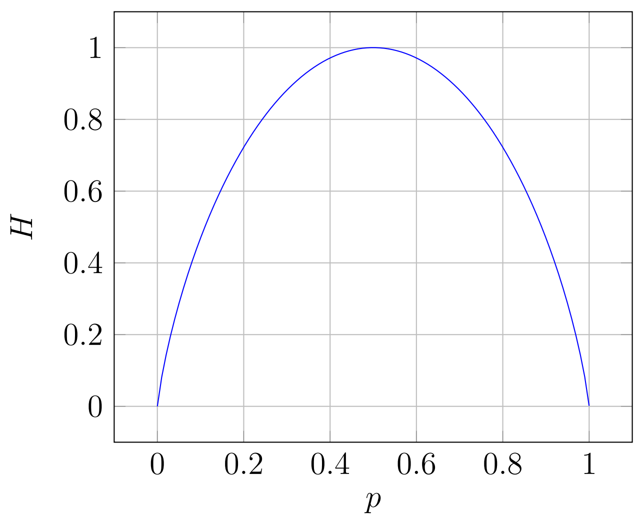
Количество вопросов= $\log_2(\frac{1}{p})$

$H = \sum\limits_{i=1}^{n} \log_2(\frac{1}{p})$ или $H = -\sum\limits_{i=1}^{n} log_2(p_i)$

18.2 Максимум энтропии

Энтропия максимальна когда вероятности вероятности одинаковы.

Данный график для двух исходов, из вероятности p и $1 - p$



18.3 Свойства функции энтропии

- $H(p_1, \cdots, p_n)$ определена и непрерывна для всех $p_1, \cdots, p_n$, где $p_i \in [0,\ 1]$ для всех $i = 1, \cdots, n$ **и** $p_1 + \cdots + p_n = 1$
- $H\underbrace{\left(\frac{1}{n},\ \ldots,\ \frac{1}{n}\right)}_{n} < H\underbrace{\left(\frac{1}{n+1},\ \ldots,\ \frac{1}{n+1}\right)}_{n+1}$ для целых, положительных n должно это должно выполняться
- $H\underbrace{\left(\frac{1}{n},\ \ldots,\ \frac{1}{n}\right)}_{n} = H\left(\frac{b_1}{n},\ \ldots,\ \frac{b_k}{n}\right) + \sum\limits_{i=1}^{k} \frac{b_i}{n} H\underbrace{\left(\frac{1}{b_i},\ \ldots,\ \frac{1}{b_i}\right)}_{b_i}.$

  Для целых положительных b_i, Если$\sum\limits_{i=1}^{n} b_i = n$

Шенон показал, что функция выглядит так: $-K\sum\limits_{i=1}^{n} p(i)\log_2 p(i)$
Коэффицент K нужен для перевода в другую систему исчисления, из бит в нат(основание логарифма e), трит(3), хартли

18.4 Th:$H = -K\sum\limits_{i=1}^{n} p(i)\log_2 p(i)$

$$S^m \leq t^n \leq S^{m+1}$$
$$H(\frac{1}{S^m}\cdots) \leq H(\frac{1}{t^n}\cdots) < H(\frac{1}{S^{m+1}}\cdots)$$
$$]A(n) \equiv H(\frac{1}{n}, \cdots, \frac{1}{n})$$
$$A(S^m) \leq A(t^n) < A(S^{m+1})$$
$$A(S^m) = A(S) + \sum_{i=1}^{s} = A(S) + A(S^{m-1}) = 2A(S) + A(S^{m-2}) = \cdots = (m+1)A(S) \qquad |: nA(S)$$
$$\frac{m}{n} \leq \frac{A(t)}{A(S)} \leq \frac{m+1}{n} \qquad | -\frac{m}{n}$$
$$0 \leq \frac{A(t)}{A(S)} - \frac{m}{n} \leq \frac{1}{n}$$

$m \cdot log(s) \leq n \cdot \log(t) < (m+1) \cdot \log(s) \qquad |: n \cdot \log(s)$ - Из начальных условий
$$\frac{m}{n} \leq \frac{\log(t)}{\log(s)} < \frac{m+1}{n} \qquad | -\frac{m}{n}$$
$$0 \leq \frac{\log(t)}{\log(s)} - \frac{m}{n} < \frac{1}{n}$$
Заметим, что $\left|\frac{A(t)}{A(S)} - \frac{\log(t)}{\log(s)}\right| < \frac{1}{n}$
$$\frac{A(t)}{A(S)} = \frac{\log(t)}{\log(s)}; \frac{A(t)}{\log(t)} = \frac{A(S)}{\log(s)} \implies A(s) = k\log(s) \qquad \sum_{i=1}^{s} k = N$$
$$p_1 = \frac{k_1}{N}, \ldots, p_s = \frac{k_s}{N}$$
$$A(N) = H(p_1, \ldots, p_n) + \sum_{i=1}^{s} p_i \cdot\ A(k_i)$$
$$k \cdot \log N = H(p_1, \ldots, p_n) + \sum_{i=1}^{s} p_i \cdot k \cdot \log(k_i)$$

$$H(p_1, \ldots, p_n) = k \cdot \left(\log(N) - \sum_{i=1}^{s} p_i \cdot \log(k_i) \right)$$
$$k \cdot \left(\log(N) - \sum_{i=1}^{s} p_i \cdot \log(p_i) - \sum_{i=1}^{s} p_i \cdot \log(N) \right) = -k \cdot \sum_{i=1}^{s} p_i \cdot \log(p_i)\text{ч.т.д.}$$

18.5 Относительная энтропия

$$D(p \mid\mid q) = \sum_{i=1}^{n} p_i \cdot \log \frac{p_i}{q_i}$$

18.5.1 Th:$D(p \mid\mid q) \geq 0$ и $D(p \mid\mid q) = 0 \Leftrightarrow p \equiv q$ - Информационное неравенство

$f\big(\sum_{i=1}^{k} p_i \cdot x_i\big) \geq \sum_{i=1}^{k} p_i \cdot x_i$ - Неравенство Иенсона

$$-f\big(\sum_{i=1}^{k} p_i \cdot x_i\big) \leq -\sum_{i=1}^{k} p_i \cdot x_i \Leftrightarrow -\sum_{i=1}^{n} p_i \cdot \log \frac{q_i}{p_i} \geq -\log \sum_{i=1}^{n} p_i \cdot \frac{q_i}{p_i} = 0\text{ч.т.д.}$$

18.5.2

$$H(p_1, \ldots, p_n) \qquad q_1 = \ldots = q_n = \frac{1}{n} D(p \mid\mid q) = \sum_{i=1}^{n} p_i \cdot \log \frac{p_i}{q_i} = \sum_{i=1}^{n} p_i \cdot \log(n \cdot p_i) =$$
$$= \sum_{i=1}^{n} p_i \cdot \log n + \sum_{i=1}^{n} p_i \cdot \log(p_i) = \log n + \sum_{i=1}^{n} p_i \cdot \log p_i = A(n) - H(p_1, \ldots, p_n)$$

Так как $A(n) \geq H(p_1, \ldots, p_n) \implies$ максимум достигается при равновероятных событиях