Алгебра

1. Теория чисел и алгебраические структуры

<u>Th</u>: (теорема о делении с остатком)

$\forall a, b \in \mathbb{Z} : b \neq 0 \quad \exists!\, q, r \in \mathbb{Z} : a = b \cdot q + r$ и $0 \le r < |b|$

<u>Док-во</u>:

1. Существование q и r

1) $a = 0$: $q = 0$, $r = 0$

2) $a > 0$, $b > 0$. Доказываем индукцией по a

2.1) База индукции $a < b$: $a = b \cdot 0 + a$

2.2) Переход: пусть $a \ge b$. Посмотрим на $a - b \ge 0$ и $a - b < a$. По пре индукции найдутся $\tilde{q}$ и $\tilde{r}$ такие, что $a - b = b \cdot \tilde{q} + \tilde{r}$ и $0 \le \tilde{r} \le b$. Тогда $a = b(\tilde{q} + 1) + \tilde{r}$.

3) $a < 0$, $b > 0$: $-a > 0$, значит, $-a = b \cdot \tilde{q} + \tilde{r}$, $0 \le \tilde{r} < b$. Получаем $a = -b \cdot \tilde{q} - \tilde{r}$

3.1) $\tilde{r} = 0$: $a = b(-\tilde{q}) + 0$

3.2) $1 \le \tilde{r} < b$: $a = b(-\tilde{q}) - b + b - \tilde{r} = b(-\tilde{q} - 1) + (b - \tilde{r})$.

Т.к. $-b + 1 \le -\tilde{r} \le -b - 1$, то $1 \le b - \tilde{r} < b$, п. 3.2 доказан

4) $a < 0$, $b < 0$: $-b > 0$, значит $a = (-b) \cdot \tilde{q} + \tilde{r}$ и $0 \le r < -b$. Тогда $a = b(-\tilde{q}) + \tilde{r}$ и $0 \le \tilde{r} < |b|$.

2. Единственность q и r

Пусть $a = b \cdot q + r = b \cdot \tilde{q} + \tilde{r}$. Тогда $b(q - \tilde{q}) = (\tilde{r} - r)$. Если $q = \tilde{q}$, то $r = \tilde{r}$. Если $q \neq \tilde{q}$, то $|b| \cdot |q - \tilde{q}| = |\tilde{r} - \tilde{r}|$ и $|b| \cdot |q - \tilde{q}| \ge |b|$. С другой стороны $0 \le r$, $\tilde{r} < |b|$, поэтому $|r - \tilde{r}| < |b|$ Противоречие.

<u>Def</u>: $a, b \in \mathbb{Z}$; a делится на b, если $\exists c \in \mathbb{Z}$, что $a = b \cdot c$

Обозначается как $a \vdots b$ или $b \mid a$.

Свойства делимости:

1) если $a \vdots c$ и $b \vdots c$, то $(a+b) \vdots c$
2) если $a \vdots c$, то $(a \cdot k) \vdots c$
3) если $ka \vdots kb$ и $k \neq 0$, то $a \vdots b$
4) $\forall a \in \mathbb{Z}$: $0 \vdots a$
5) $\forall a \in \mathbb{Z}$: $a \vdots 1$
6) если $a \vdots b$ и $|a| < |b|$, то $a = 0$

Линейные диофантовы уравнения

$ax + by = c$, где $a, b, c \in \mathbb{Z}$

Def: идеал $\mathbb{Z}$ — A (подмножество $\mathbb{Z}$), такое что

1) для любых a и $b \in A$ $a+b \in A$
2) $\forall a_1 \in A$ и $\forall k \in A$ $a \cdot k \in A$
3) $A \neq \varnothing$

Def: числа, кратные a — главный идеал, порождённый A ($\langle a \rangle$)

Th: в $\mathbb{Z}$ все идеалы главные.

Док-во:

Пусть a — произвольный идеал. Если $a = \langle 0 \rangle$, то это главный идеал. Если в a есть элемент $b \neq 0$, то $|b| \in a$, $-b \in a$. Пусть a' — наименьшее положительное число в идеале a. Если b — произвольное число в идеале a и r — остаток от деления числа b на число a' $(r < a')$, то $b = qa' + r$, где $0 \leq r < a'$. Т.к. a' и $b \in$ идеалу a, то $r = b - qa'$ тоже принадлежит идеалу a. Т.к. $r < a'$, то $r = 0$, значит, $b = qa'$, т.е. все числа идеала a кратны a'. Отсюда следует, что $a' = \langle a \rangle$, т.е. главный идеал.

Def: пусть $a, b \in \mathbb{Z}$, тогда НОД(a,b) – наибольший общий делитель, такой что:

1) d – общий делитель a и b
2) если d' – общий делитель a и b, то $d' | d$

НОД определён с точностью до знака

Линейное представление НОД: $\exists x, y \in \mathbb{Z}: ax + by = \text{НОД}(a,b)$

Док-во: Если $a = b = 0$, то НОД$(a,b) = 0$. Пусть $a \neq 0$. Рассмотрим множество N вида $au + bv$ для $v, u \in \mathbb{Z}$ и обозначим наименьший ненулевой элемент за d: $d = au_0 + bv_0$. Покажем, что d – общий делитель a и b: $a = dq + r = (au_0 + bv_0)q + r$, откуда $r = a(1 - u_0 q) + b(-v_0 q)$. $r < d$ – натуральное число, хотя d было наименьшим натуральным числом, значит, $r = 0$ и $a \vdots d$. Аналогично $b \vdots d$. Пусть d' – общий делитель a и b. Тогда по свойствам делимости $d' | au_0$ и $d' | bv_0$ и $d' | au_0 + bv_0 = d$, ч.т.д.

Th: $ax + by = c$ имеет решение в $\mathbb{Z}$ $\Leftrightarrow$ $c \vdots \text{НОД}(a,b)$

Алгоритм Евклида

$(a,b) = (a - k \cdot b, b)$. Дальнейшими преобразованиями можно получить пару $(d, 0) = d$, где $d = \text{НОД}(a,b)$.

Основная теорема арифметики

Def: пусть a – целое число, $a \neq 0, \pm 1$. Тогда a простое, если

$$(a = bc) \Rightarrow \left[\begin{array}{l} b = \pm 1 \\ c = \pm 1 \end{array}\right., \ b, c \in \mathbb{Z}$$

Th: любое целое число $n \neq 0$ однозначно представляется в виде $n = \pm p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$, где p_i – простое и $0 \leq p_1 \leq p_2 \leq \ldots \leq p_n$

Каноническое разложение: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$, $p_1 < p_2 < \ldots < p_n$

a_i – степень вхождения p_i в n

$V_{p_i}(n) = a_i$

Замечание: $V_{p_i}(n) = a_i$, если $n \vdots p_i^{a_i}$ и $n \not\vdots p_i^{a_{i+1}}$

Свойства степеней вхождения:

1) $V_p(a, b) = V_p(a) + V_p(b)$

2) $\min(V_p(a), V_p(b)) \leq V_p(a+b)$

Факт 1:

$a = \prod_{i=1}^{n} p_i^{a_i}$, $a_i \geq 0$

$b = \prod_{i=1}^{n} p_i^{b_i}$, $b_i \geq 0$

$a \vdots b \Leftrightarrow a_i \geq b_i \ \forall i$

Факт 2:

$\exists c: a = c^k \Rightarrow a \vdots k \ \forall i$

Def: $НОК(a, b) = [a, b] = LCM(a, b) \Rightarrow c \vdots a$ и $c \vdots b$, если $c' \vdots a$ и $c' \vdots b$, то $c' \vdots c$.

Факт 3:

$НОД(a, b) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$

Факт 4:

$\exists\ [a,b] = \prod_{i=1}^{n} p_i^{\max(a_i, b_i)}$

$[a,b] \cdot (a,b) = ab$

Факт 5:

Пусть $\tau(a)$ – количество натуральных делителей a.

$\tau(a) = \prod_{i=1}^{n} (a_i + 1)$

Док-во: делители X однозначно соотносятся с $\{(b_1, b_2 \dots b_n) \mid 0 \le b_i \le a_i\}$

Факт 6:

Пусть $\sigma(a)$ – сумма натуральных делителей a.

$$\sigma(a) = \frac{\prod (p_i^{a_i+1} - 1)}{\prod (p_i - 1)}$$

Доказательство основной теоремы арифметики

1. Существование

Докажем от противного. Пусть существуют натуральные числа, не раскладывающиеся на простые сомножители, из которых n — наименьшее.

Случай 1: n — простое: противоречие

Случай 2: n — составное, которое раскладывается на непростые сомножители. Любой из них меньше n, что противоречит тому, что n — наименьшее такое число.

<u>Лемма</u>: пусть $ab \vdots c$, $(a,c)=1$. Тогда $b \vdots c$.

<u>Док-во</u>:

$\exists x,y: ax+cy=1 \quad | \cdot b$

$abx+cby=b$

Т.к. $ab \vdots c$ и $cb \vdots c$, то $b \vdots c$.

<u>Лемма</u>: пусть p — простое, $ab \vdots p$, тогда $\left[\begin{array}{l} a \vdots p \\ b \vdots p \end{array}\right.$

<u>Док-во</u>:

$НОД(a,b)=d$, при этом $p \vdots d$. $\Rightarrow (a,p)=\pm 1$ или $(a,p)=\pm p$

$$\underset{b \vdots p}{\Downarrow} \qquad\qquad \underset{a \vdots p}{\Downarrow}$$

<u>Следствие</u>: пусть $a_1 \cdot \ldots \cdot a_n \vdots p$, тогда $\exists i: a_i \vdots p$.

<u>Док-во</u>:

База: $n=2$

Переход: $n \to n+1$. Пусть $\prod_{i=1}^{n+1} a_i \vdots p \to a_1 \cdot a_2 \cdot \ldots \cdot a_{n+1} \vdots p$, т.е. либо $a_1 \cdot a_2 \cdot \ldots \cdot a_n \vdots p$, либо $a_{n+1} \vdots p$, т.е. по индукции доказано.

2. Единственность

Пусть существуют числа, разнораскладывающиеся на множители. Пусть — n — наименьшее такое число.

$n_1 = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$

$n_2 = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_n$

Значит, $p_1 \cdot p_2 \cdot \ldots \cdot p_n \vdots q_1$. По следствию из леммы $\exists i : p_i \vdots q_1$. Тогда

$n' = \frac{n_2}{q_1} \cdot q_2 \cdot \ldots \cdot q_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Противоречие, т.к. нашлось ~~на~~меньшее число, чем n, хотя n было наименьшим.

Алгебраические структуры

Def: группа — такой набор данных $(G, *)$, где G — множество, а $*$ — бинарная операция : $G \times G \to G$, так что:

1. $a * (b * c) = (a * b) * c$ → ассоциативность
2. $\exists e \in G : \forall a \in G \quad a * e = e * a = a$ → нейтральный элемент
3. $\forall a \in G \; \exists a^{-1} : a * a^{-1} = e$ → обратный элемент

Def: группа G называется абелевой, если $\forall a, b \in G$ $a * b = b * a$ → коммутативность.

Пусть M — множество, $\forall y \in M \; \exists! x \in M$, $f(x) = y$. Найдем $g(y)$: получим отображение $g: M \to M$, где $(g \circ f)(x) = x$ (тождественное ~~вира~~ отображение). Это главный пример группы (группа с операцией композиции).

$f: M \to N$ — инъекция, если $\forall y \in N$ $\exists$ не более 1 $x \in M$, т.ч. $f(x) = y$

$f: M \to N$ — сюръекция, если $\forall y \in N$ $\exists$ не менее 1 $x \in M$, т.ч. $f(x) = y$

$f: M \to N$ — биекция, если каждому $y \in N$ сопоставлен ровно один $x \in M$, т.ч. $f(x) = y$

$X \xrightarrow{f} Y \xrightarrow{g} Z$, тогда $g \circ f : X \to Z$, т.е. $x = g(f(x))$ – композиция

<u>Def:</u> Кольцо – $(R, +, \cdot)$, где R – множество, $+$ и $\cdot$ – бинарные операции на R, такие что:

1. Относительно сложения R – абелева группа
2. $\forall a, b, c \in R$: $a \cdot (b+c) = a \cdot b + a \cdot c$ и $(b+c) \cdot a = b \cdot a + c \cdot a$

Если выполнена аксиома 6 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, то кольцо называется ассоциативным.

Если выполнена аксиом 7: $a \cdot b = b \cdot a$, то кольцо называется коммутативным.

8. $\exists 1 : a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$
9. $\forall a \neq 0 \quad \exists a^{-1} : a^{-1} \cdot a = a \cdot a^{-1} = 1$, где $a, a^{-1} \in R$

Если выполнены все 9 аксиом, то R называют полем.
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – поля.

Кольца вычетов

<u>Def:</u> $n \in \mathbb{Z}$, говорят, что a сравнимо с b по модулю n, если $(a-b) \vdots n$. Обозначается как $a \equiv b \mod n$.

<u>Замечание:</u>

$a \equiv b \mod n \iff$ у a и b равные остатки при делении на n

<u>Лемма:</u> (свойство сравнений)

1. $\forall a, b$ если $a \equiv b \mod n$, то $b \equiv a \mod n$
2. $\forall a, b, c$ если $a \equiv b \mod n$, $b \equiv c \mod n$, то $a \equiv c \mod n$.
3. $\forall a$ если $a \equiv a \mod n$, то $(a-a) \equiv 0 \mod n$

$\overline{a} = \{ b \mid a \equiv b \mod n \} = \{ b \mid (a-b) \vdots n \} = \{ b \mid a-b = nk \} =$
$= \{ b \mid a = nk+b \} \to$ класс эквивалентности

$\mathbb{Z} = \bar{1} \cup \bar{2} \cup \bar{3} \cup \ldots \cup \overline{(n-1)}$, $\bar{i} \cup \bar{j} = \varnothing \ \forall i,j \in 0,\ldots,n-1$

$\mathbb{Z}_{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} \rightarrow$ фактор-множество по отношению эквивалентности

__Лемма__: Если $a \equiv b \mod n$ и $c \equiv d \mod n$, то $ab \equiv cd \mod n$ и $(a+b) \equiv (b+d) \mod n$.

__Доказательство:__

$a+c-(b+d) = a-b+c-d$. Т.к $a-b \vdots n$ и $c-d \vdots n$, то $(a+c)-(b+d) \vdots n$

$ac-bd = ab-bc+bc-bd = c(a-b)+b(c-d)$. Т.к. $a-b \vdots n$ и $c-d \vdots n$, то $ac-bd \vdots n$.

__Th__: с введенными операциями на классах $\mathbb{Z}/n\mathbb{Z}$ R — кольцо ~~ассоциативно~~ коммутативное с 1.

__Док-во:__ ⑤ пусть $\exists x,y,z$ — классы, тогда $x(y+z) = xy+xz$
Пусть $\bar{x} = a$, $\bar{y} = b$, $\bar{z} = c$, $a,b,c \in \mathbb{Z}$. Тогда

$x(y+z) = \bar{a}(\bar{b}+\bar{c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac} =$
$= \bar{a}\cdot\bar{b} + \bar{a}\cdot\bar{c} = x\cdot y + x\cdot z$.

__Th__: • $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow (a,n) = 1$
• n — простое $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ — поле

__Def__: R — кольцо, $a \in R$ называется обратимым, если $\exists b \in R$: $ab = ba = 1$.

__Док-во__: 1) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \exists \bar{b} : \bar{a}\cdot\bar{b} = \bar{1}$, т.е. $\overline{ab} = \bar{1}$, т.е. $ab-1 \vdots n$, т.е. $ab-1 = nk$. Т.к. $(a,n) = 1$, то $\exists\, ab-nk = 1$.

2) пусть p — простое, тогда $\bar{a}$ обратим $\Leftrightarrow (a,p) = 1$ $\Leftrightarrow a \not\vdots p$, т.е. $a \not\equiv 0 \mod p$, т.е. $\bar{a} \neq \bar{0}$. Все ненулевые классы обратимы, значит, $(\mathbb{Z}/n\mathbb{Z})^*$ — поле.

Замечание: уравнение $ax=1$ может иметь ≥ 1 решений

Def: Множество всех обратимых элементов R^* — группа по умножению — мультипликативная группа кольца R.

1) $a, b \in R^* \Rightarrow a \cdot b \in R^*$ (замкнутость по умножению)

2) ассоциативность: по определению

3) $1 \in R^*$

4) $a \in R^* \Rightarrow \exists\, b \in R^*: ab = ba = 1$

Док-во (п.1):

Заметим, что $a^{-1} \cdot b^{-1} \cdot b \cdot a = a^{-1} \cdot a = 1$ и $b^{-1} \cdot a^{-1} \cdot a \cdot b = b^{-1} \cdot b = 1$, т.е. $\exists\, (ab)^{-1} = a^{-1} \cdot b^{-1}$.

F — поле $\Rightarrow F^* = F \setminus \{0\}$

$(\mathbb{Z}/p\mathbb{Z}, +): 1, 1+1, \ldots, \underbrace{1+1+\ldots+1}_{p \text{ раз}}; \underbrace{1+1+\ldots+1}_{p} = 0$

Def: пусть G — группа. G называется циклической, если $\exists\, g \in G: \{g^k\}$ — вся группа G, где $k \in \mathbb{Z}$.

Замечание: пусть G — группа, $g \in G$, $k \in \mathbb{Z} \Rightarrow \{g^k\}$ — подгруппа.

Def: пусть S — группа/кольцо/поле. Тогда $\tilde{S} \subset S$ — подгруппа/подкольцо/подполе, если $\tilde{S}$ — группа/кольцо/поле относительно тех же операций.

~~[illegible]~~: $\tilde{S}$ — подгруппа:

1) если $a, b \in \tilde{S} \Rightarrow a \cdot b \in \tilde{S}$

2) если $a \in \tilde{S} \Rightarrow a^{-1} \in \tilde{S}$

3)

$\tilde{S}$ — подкольцо:

1) $0 \in \tilde{S}$

2) $1 \in \tilde{S}$, если кольцо с единицей

3)

$\mathfrak{I}$ - подполе:

1) -/- то же самое, что и у подкольца

2)

Обозначается: $\langle g \rangle \leq G$.

Примеры циклических и нециклических групп:

- $(\mathbb{Z}, +)$ - циклическая: $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z} = \langle -1 \rangle$
- $(\mathbb{Z}/n\mathbb{Z}, +)$ - циклическая: $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$

  $\mathbb{Z}/n\mathbb{Z} = \langle a \rangle$, если $(a, n) = 1$

Def: пусть $g \in G$, тогда порядком g является $\mathrm{ord}(g)$.

Th: пусть $\forall g \in G$ верно одно из двух:

1) все степени g попарно различны $\Rightarrow \mathrm{ord}(g) = \infty$
2) $\exists n$ $: \mathrm{ord}(g) = n$, тогда $\ldots g^{-2}, g^{-1}, g^{0}, g^{1}, g^{2} \ldots$ периодична с периодом $= n$

Док-во: пусть $\exists k, l$, $k \neq l$, $g^k = g^l$, $k > l$, тогда $(g^k \cdot g^l)^{-1} = g^{-k}$. Рассм. $\min k: g^k = e$, $k \in \mathbb{N}$.

Тогда $\forall n \in \mathbb{Z}$ $g^{n+k} = g^n \cdot g^k = g^n \cdot e = g^n$, т.е. $\{g^i\}$ периодична с периодом n

Def: а) пусть G_1, G_2 – группы. $f: G_1 \to G_2$ называется гомоморфизмом, если $\forall a, b \in G_1 \quad f(a \cdot b) = f(a) \cdot f(b)$

б) пусть R_1, R_2 – кольца. $f: R_1 \to R_2$ называется гомоморфизмом, если $\forall a, b$

$$f(a+b) = f(a) + f(b)$$
$$f(a \cdot b) = f(a) \cdot f(b)$$
$$f(1_{R_1}) = 1_{R_2}$$

Def: Изоморфизм – биективный гомоморфизм.

$f: (\mathbb{R}, +) \to (\mathbb{R}, *)$

$f(x) = 2^x$

$f(x+y) = 2^{f(x)+f(y)} = 2^{f(x)} \cdot 2^{f(y)} \Rightarrow$ изоморфизм

Пусть G – циклическая группа, $\operatorname{ord}(g) = \infty$. Тогда любая бесконечная циклическая группа изоморфна ~~$(\mathbb{R}, +)$~~ $(\mathbb{Z}, +)$. Обозначается $\langle g \rangle \cong (\mathbb{Z}, +)$

Док-во: $f: \mathbb{Z} \to \langle g \rangle$, $a \to g^a$

$g^{a+b} = g^a \cdot g^b$ – гомоморфизм. Это инъекция, доказано в теореме; это сюръекция по определению. Значит, $\langle g \rangle \cong (\mathbb{Z}, +)$, ч.т.д.

Пусть G – конечная группа, $\operatorname{ord}(g) = n$. Тогда $\langle g \rangle \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

Док-во:

Если G — циклическая группа, то $\langle g\rangle \cong (\mathbb{Z},+)$ или $\langle g\rangle \cong (\mathbb{Z}/n\mathbb{Z},+)$.

$(\mathbb{Z}/p\mathbb{Z},*)$ циклическая, если $ord = p-1$.

<u>Th</u>: (теорема Лагранжа)
Пусть G — группа, $ord < \infty$. Тогда $\forall g \in G$ $ord(g)$ — делитель $|G|$.

<u>Док-во</u>: рассм. $f: G \to G$, $f(x) = g\cdot x$. Пусть $|G| = n$, $ord(g) = k$.

$x \Rightarrow g\cdot x \Rightarrow g^2\cdot x \Rightarrow g^3\cdot x \Rightarrow \ldots \Rightarrow g^k\cdot x$. 1. В цикле все элементы различны. 2. Периоды цикла совпадают или не пересекаются.

<u>Следствие</u>: $|G| = n$, $\forall g$ $g^n = 1$
<u>Док-во</u>:

$G = (\mathbb{Z}/p\mathbb{Z})^*$, $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$. Тогда

$$\left.\begin{aligned} &\overline{a}^{p-1} = \overline{1} \\ &a^{p-1} \equiv 1 \bmod p \\ &a^{p-1} - 1 \,\vdots\, p \end{aligned}\right\} \text{ малая теорема Ферма}$$

Следствие из т. Лагранжа:

G — группа, $|G| = p$, где p — простое, то G — циклическая.

Док-во: $|G| = p$, $p \geq 2$. Значит, в G есть не только e, но и еще какой-то элемент. Тогда $p \,\vdots\, ord(g) \Rightarrow \left[\begin{array}{l} ord\, g = 1 \\ ord\, g = p \end{array}\right. \Rightarrow \left[\begin{array}{l} g = e \\ ord\, g \neq 1 \end{array}\right.$

$\Rightarrow ord\, g = p \Rightarrow \langle g \rangle = G$

$\mathbb{Z}/n\mathbb{Z}$, где $n = q \cdot p$, где q и p — различные простые

$a \equiv b \mod n$

$a \equiv b \mod pq \Leftrightarrow a \equiv b \mod p$, $a \equiv b \mod q$

Def: пусть G_i — группа / R_i - кольцо $(i = 1 \dots n)$. Прямое произведение набора G_i / R_i — множество $G_1 \times G_2 \times \dots \times G_n / R_1 \times \dots \times R_n$ с определенными операциями:

① $(g_1, g_2, g_3, \dots g_n) \cdot (h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$

② $(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots b_n) = (a_1 + b_1, a_2 + b_2, \dots a_n + b_n)$

Замечание: $G_1 \times G_2 \times \dots \times G_n$ — действительно группа

Доказательство:

1. Ассоциативность — очевидна
2. Нейтральный элемент — набор нейтральных элементов
3. Обратный элемент — набор обратных элементов

Замечание: если R_1 и R_2 — поле, то $R_1 \times R_2$ — не поле.

Док-во: у пары $(0, 0)$ нет обратного элемента.

Китайская теорема об остатках

Th: Пусть m и $n \in \mathbb{Z}$, $(n, m) = 1$. Тогда $\mathbb{Z}_{mn\mathbb{Z}} \cong \mathbb{Z}_{m\mathbb{Z}} \times \mathbb{Z}_{n\mathbb{Z}}$

Док-во: построим $f: \mathbb{Z}_{(m_1, m_2, \ldots, m_k)\mathbb{Z}} \to \mathbb{Z}_{m_1\mathbb{Z}} \times \ldots \times \mathbb{Z}_{m_k\mathbb{Z}}$.

$\overline{a}_{m_1, m_2, \ldots, m_k} \longmapsto (\overline{a}_{m_1}, \overline{a}_{m_2}, \overline{a}_{m_3}, \ldots, \overline{a}_{m_k})$.

Проверим корректность: пусть $\overline{a}_{m_1, m_2, \ldots m_k} = \overline{b}_{m_1, m_2, \ldots, m_k} \Rightarrow$

$\Rightarrow a - b \,\vdots\, m_i \Rightarrow \overline{a}_{m_i} = \overline{b}_{m_i}$.

$f(x+y) = f(x) + f(y) \Rightarrow f(a+b \mod m_1, m_2, \ldots, m_k) = f(\overline{a}_{m_1, \ldots, m_k}) +$
$+ f(\overline{b}_{m_1, m_2, \ldots m_k})$

Проверим, что f — биекция: $f(\overline{a}_{m_1, m_2, \ldots, m_k}) = f(\overline{b}_{m_1, \ldots, m_k})$
$\Leftrightarrow a \equiv b \mod_{m_1, m_2, \ldots, m_k}$. Т.к. все m_i взаимнопростые, то
$\overline{a}_{m_1, m_2, \ldots m_k} = \overline{b}_{m_1, m_2, \ldots, m_k}$.

$$\begin{cases} x \equiv x_1 \mod m_1 \\ x \equiv x_2 \mod m_2 \\ \quad \ldots \\ x \equiv x_i \mod m_i \end{cases} \Leftrightarrow x \equiv x_0 \mod m_1 m_2 m_3 \ldots m_i$$

Заметим: $|\mathbb{Z}_{m_1 m_2 \ldots m_k \mathbb{Z}}| = m_1 m_2 \ldots m_k$, тогда

	$\mathbb{Z}_{5\mathbb{Z}}$				
	0	6	12	3	9
$\mathbb{Z}_{3\mathbb{Z}}$	10	1	7	13	4
	5	11	2	8	14

$$\begin{cases} x \equiv x_1 \mod m_1 \\ \dots \\ x \equiv x_n \mod m_n \end{cases}$$

Утв: пусть A и B – кольцо, тогда $(A \times B^*, \cdot)^* = (A^*, \cdot) \times (B^*)$

Док-во: $(a, b) \in (A \times B)^* \Rightarrow \exists (a', b') : (a, b) \cdot (a^{-1}, b^{-1}) = (1, 1) \Rightarrow$ $a^{-1} a = 1,\ b' b = 1,\ a \in A^*,\ b \in B^* \Rightarrow (a, b) \in (A \times B)^*$

Следствие: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$. Тогда $\mathbb{Z}_{n\mathbb{Z}} \cong \mathbb{Z}_{p_k^{a_k}\mathbb{Z}} \times \mathbb{Z}_{p_1^{a_1}\mathbb{Z}} \ldots$
$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$.

Следствие из т. Лагранжа: $|G| = n$, $a \in G \Rightarrow a^n = e \Rightarrow a^{p-1} = 1 \mod p$

$\exists (a, n) = 1 \Leftrightarrow \bar{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^*$. $\bar{a}^{|(\mathbb{Z}/_{n\mathbb{Z}})^*|} = \bar{1}$, т.е. $a^{|(\mathbb{Z}/_{n\mathbb{Z}})^*|} - 1 \vdots n$

$$|\mathbb{Z}/_{n\mathbb{Z}}^*| = \prod_{i=1}^{k} |(\mathbb{Z}/_{i\mathbb{Z}})^*|$$

$(\mathbb{Z}/_{p^l\mathbb{Z}})^* = \{\bar{a} \in \mathbb{Z}/_{p^l\mathbb{Z}} \mid (a, p^l) = 1\}$, p - простое

$$\{\bar{a} \in \{\bar{0}, \bar{1}, \ldots, \overline{p^l - 1}\} \mid a \not\vdots p\} \Rightarrow |(\mathbb{Z}/_{p^l\mathbb{Z}})^*| = p^l - p^{l-1}$$

$$\Downarrow$$

$$|(\mathbb{Z}/_{n\mathbb{Z}})^*| = \prod_{i=1}^{k} p_i^{a_i}\left(1 - \frac{1}{p_i}\right)$$

$$|(\mathbb{Z}/_{n\mathbb{Z}})^*| = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

<u>Def</u>: Функция Эйлера $\varphi(n) = n\left(n - \frac{1}{p_1}\right)\left(n - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(n - \frac{1}{p_k}\right)$

$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \to$ вероятность того, что случайное число взаимно просто с n.

<u>Th</u>: (теорема Эйлера)

$$(a, n) = 1 \Leftrightarrow a^{\varphi(n)} \equiv 1 \mod n$$

<u>Замечание</u>: $(a, n) \neq 1 \Rightarrow \begin{matrix} a \vdots p \\ n \vdots p \end{matrix} \Rightarrow a^k \not\equiv 1 \mod \forall k$

<u>Замечание</u>! $n \neq p^k$, $n \neq 2 \cdot p^k \Rightarrow \varphi(n)$ - неоптимальная оценка периода

<u>Lm</u>: $f_k : (\mathbb{Z}/_{n\mathbb{Z}})^* \to (\mathbb{Z}/_{n\mathbb{Z}})^* : f_k(x) = x^k$. Тогда f_k - биекция, т.е $\forall x \; \exists! \; x^{\frac{1}{k}} \Leftrightarrow (k, \varphi(n))$ - взаимно простые.

<u>Док-во</u>: $\Leftarrow$: $(k, \varphi(n)) = 1 \Rightarrow \exists x, y : x \cdot k + y \cdot \varphi(n) = 1$.

Тогда $\forall a \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ $(a^k)^x = a^{x \cdot k} = a^{xk} \cdot 1^y = a^{kx} \cdot (a^{\varphi(n)})^y =$

$= a^{xk + \varphi(n) \cdot y} = a^1 = a$.

Алгоритм RSA

A – Алиса

B – Боб

1) A придумывает простые p и q, $x \in (1, \dots p \cdot q - 1)$, $(x, \varphi(n)) = 1$
$n = p \cdot q$. Находим y такой, что $xy \equiv 1 \mod n$.

Число pq, y сообщает Бобу → открытый ключ

x – закрытый ключ, $(p-1) \cdot (q-1)$ – закрытый ключ.

2) Общение происходит так:

B: кодирует сообщение числом $a \in 1 \dots pq$, $(a, pq) = 1$

$a^y \to$ Алисе

A: $(a^y)^x \equiv a^1 \equiv a \mod pq$

N – большое число. Как понять, что оно простое?

1) $a^{N-1} \mod N$, $a \in \{1 \dots n-1\}$

Пусть $a^{N-1} \equiv 1 \mod N$. Тогда проверим другие числа из $\{1, \dots, n-1\}$. Тогда N – псевдопростое со свидетелем a.

N – абсолютно псевдопростое, если $\forall a$ $(a, n) = 1 \to a$ – свидетель.

Числа Кармайкла — абсолютно псевдопростые, но не простые.

<u>Замечание:</u>