Теория чисел – продолжение

Шифрование

– Симметричное

key

$enc(m, key) = x$

$dec(x, key) = m$

– Асимметрич.

Ключи: public
– private

public$_A$ – знают все

$enc(m, pub_A) = x$

$dec(x, private_A) = m$

RSA Ривест Шамир Адлеман 1977

p, q — случ. простые числа (большие)

e — случ.: $1 \le e < \varphi(n)$

$\Rightarrow n = pq$

d: $ed \equiv 1 \pmod{\varphi(n)}$

$ed = k \cdot \varphi(n) + 1$

public = $\langle n, e \rangle$

private = $\langle n, d \rangle$

$enc(m, \langle n, e \rangle) = m^e \bmod n = x$

$dec(x, \langle n, d \rangle) = x^d \bmod n$

$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n =$

$= m^{k\varphi(n)+1} \bmod n =$

$= m \cdot (m^{\varphi(n)})^k \bmod n =$

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

$= m \bmod n = m$

$m < n$

$(m, n) = 1$

Противник не знает $\varphi(n)$

$= (p-1)(q-1)$

$\sqrt[4]{n}$ gcd $l = 2048$ бит

$n \sim 2^{2048}$

$Time = l \times ($ умнож. + деление по модулю $)$

данных l

$- l^2$

$- l^2 / w^2$

$- l \log^2 l$

$- l \log l$

$Time = - l^3$

$- l^2 \log l$

Схема Диффи – Хеллмана (– Меркля)

$g, p \in \mathbb{P}$

A

Ген. случ. a

B

Ген. случ. b

$A = g^a \bmod p$ ⟶ $K = A^b_{\bmod p} = g^{ab} \bmod p$

$K = B^a = g^{ab} \bmod p$ ⟵ $B = g^b \bmod p$

$\uparrow \bmod p$

Противник: $g, p, g^a \bmod p, g^b \bmod p$

$g^{ab} \bmod p$

Дискретное логарифм!

СЛАУ

$Ax = b$

A – $n \times n$

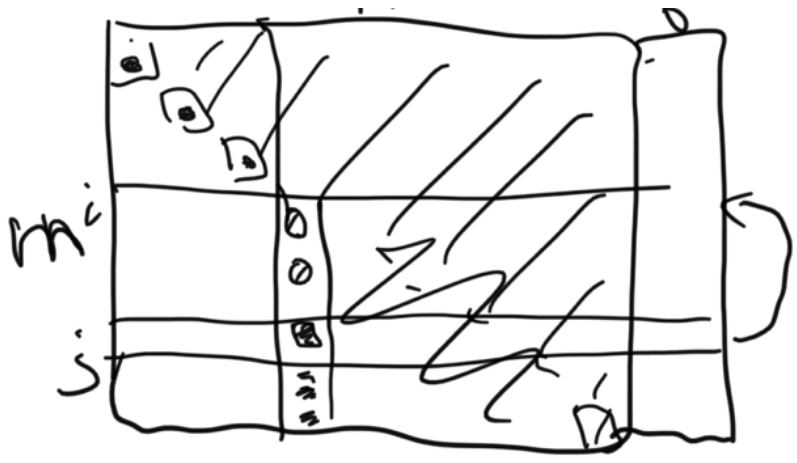
x – n

b – n

Алг. Гаусса (I)

$n \times n$

$\det A \neq 0$



$\mathbb{F}_p$ $(\mathbb{Z}_p)$

$\mathbb{R}$ $\mathbb{C}$

$m = n$

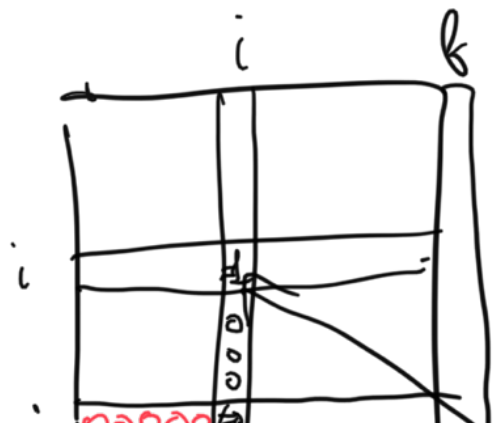
```
vector<vector<F>> a(m, vector<F>(n));
for (i=0; i<n; ++i){
    int j=i;
    while(a[j][i]==0)
        ++j;
    swap(a[i],a[j]); // O(1)
    for(j=i+1; j<m; ++j)
    if a[j][i] ≠ 0:
        c = a[j][i]/a[i][i]
        for(k=i; k<n; ++k)
            a[j][k] -= a[i][k]*c;
```

for $j = 0 \ldots m-1$, skip $j = i$

}

$O(n^3)$

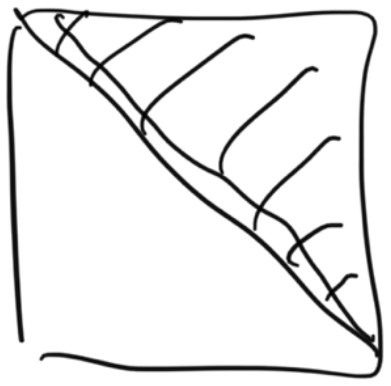
$\Lambda: \sum (n-i)^2 \approx \frac{n^3}{\_}$



$\sum_{i=1}^{n} \frac{n(n-i)}{3}$

$a[j][i]$ $a[i][i]$

diag: $\sum_{i=1}^{n} n(n-i) \approx \frac{n^3}{2}$



diag: $x_i = a[i][n] / a[i][i]$

$O(n)$

Δ: for $i = n-1 \ldots 0$

$x_i = \left(a[i][n] - \sum_{j=i+1}^{n-1} a[i][j] * x[j]\right) / a[i][i]$

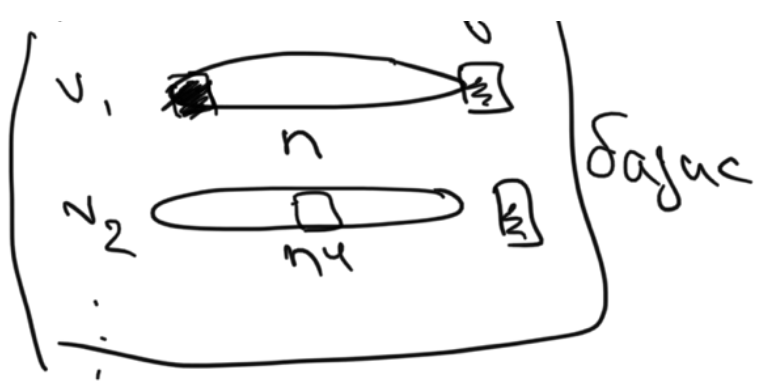
$O(n^2)$

$\Delta: c\frac{n^3}{3} + O(n^2)$

diag: $c \cdot \frac{n^3}{2} + O(n)$

Гаусс

Глава II



$\langle v_1, v_2, \dots, v_m \rangle$

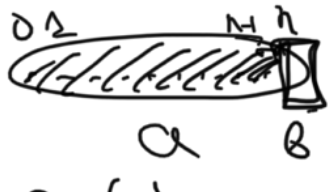
$u_1, u_2, \dots, u_k$ $k \le m$


```
vector<vector<F>> U; // базис с 0-шками
vector<int> col; // координ. ответств.
                 // векторов у базиса
```

```
bool add(vector<F> a){
    for (int i=0; i<U.size(); ++i){
        if a[col[i]]!=0:
            c = a[col[i]]/U[i][col[i]] *0
            for k=0..n                  // в том же
                a[k] -= U[i][k]*c
}
```

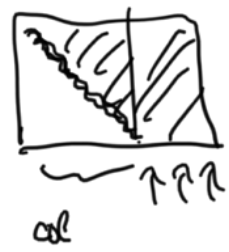
```
int i = 0;
while (i<=n && a[i]==0)
    ++i;
```

```
if i==n+1: // a - л.к. старших вект.
    return true
```




```
if i==n: // противоречие 0=(!0)
    return false
```

```
U.push(a);
col.push(i);
return true;
}
```



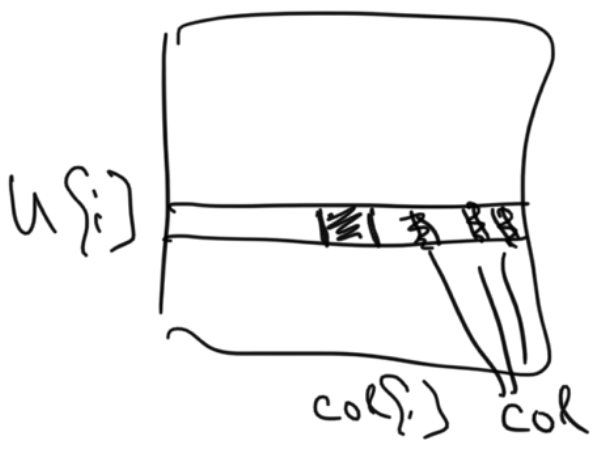
Свободные перем: ∉ col

$$m \times k \times n = O(n^3)$$

↑ разр. лин. об.

```
vector<F> getX(){
    vector<F> x(n,0); // св.перем.=0
    for i = U.size()-1 .. 0 {
        x[col[i]] = U[i][n] - Σ_{j=i+1}^{U.size()-1} U[i][col[j]] * x[col[j]]
                              ---------------------------------------------
                                          U[i][col[i]]
```

$$-\sum_{j=i+1}^{U.size()-1} U[i][col[j]] * x[col[j]]$$




```
    return x
}
```

$O(n \cdot k^2)$

$O(n+k)$

0). $S = 0$ Начальное решение с св. перем. $= 0$

$(n-k)$ своб. перем.

1). x_{i_1} – первая св. перем.

$x_{i_1} := 1$, все ост. $= 0$

↓

решение V_1

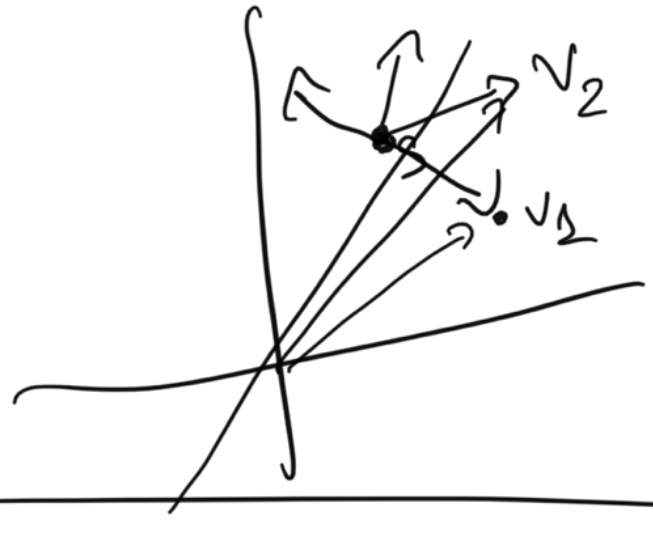
2). x_{i_2} – вторая св. перем.

$x_{i_2} := 1$, все ост. $= 0$

↓

реш. V_2

$S \quad V_1, V_2, \dots, V_{n-k}$



Решение: $S + \langle V_1 - S, V_2 - S, \dots, V_{n-k} - S \rangle$

$$O((n-k)(n+k^2)) = O(n^3)$$

Случаи полей

- F_p
- F_2 $O(n^3/w)$
- R (C)

Матрица Гильберта

$$A_{ij} = \frac{1}{i+j-1}$$

$$\det A \neq 0$$

$$Ax = 0 \xrightarrow{?} x = 0$$

$n = 11$ → не хватит double

$n = 17$ → не хватит long double

Решения проблем

1). Эвристика max элемента

$|a_{ji}| \to max$

$j \geq i$

$|a_{jk}| \to max$

2). BigDecimal

2.1). точность l

точность 2l

ред сильно отмах. $\to l_* = 2$

2.2). библ. max точность

в TL

3). Метод итераций

а) $x = Ax$ $\|A\| < 1$

$\|A\| = \sup_{x:|x|=1} |Ax|$

$x_0 = random$

$x_i = Ax_{i-1}$

$|A^k x_0 - A^{k-1} x_0| = |A^{k-1}(Ax_0 - x_0)| \leq$

$$\leq \|A^{k-1}\| \cdot \|A\| \leq \underbrace{\|A\|^{t}}_{\to 0} \cdot \dots$$

t шагов за $t \cdot n^2$

$\underbrace{A^{2^k}}_{k \cdot n^3} \cdot x_0 \qquad 2^k = t \qquad O(n^3 \cdot \log t)$

в). $\boxed{x = Ax + b} \qquad \|A\| < 1$

$x_0 = \text{random}$

$x_1 = Ax_0 + b$

$x_2 = A^2 x_0 + Ab + b$

$x_3 = A^3 x_0 + A^2 b + Ab + b$

$x_4 = A^4 x_0 + A^3 b + A^2 b + Ab + b$

$x_8 = \dots$

$$S_{2^k} = A^{2^k - 1} b + A^{2^k - 2} b + \dots + Ab + b$$

$$S_0 = b$$

$$S_{2^{k+1}} = A^{2^k} \cdot S_{2^k} + S_{2^k} = \left(A^{2^k} + E\right) \cdot S_{2^k}$$

k шагов S^{2^k}

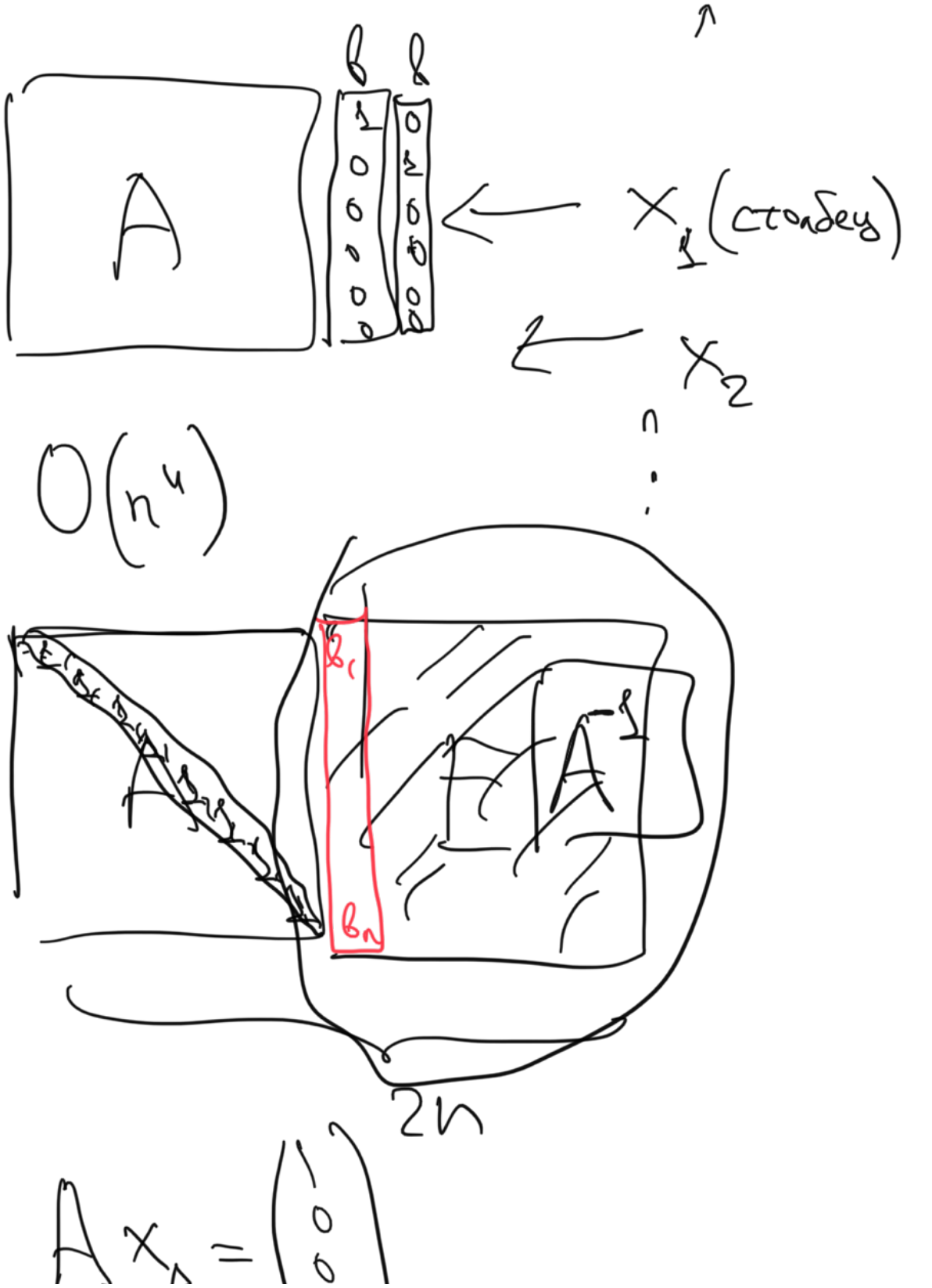
1 шаг за $O(n^3)^{2^k}$

$O(n^3 \log t)$ $A^{t-1} b + A^{t-2} b + \dots + b$

A – квадр., $\det A \neq 0$

A^{-1} ?

$AX = E$



$A x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

$$\begin{cases} x_{11} = b_1 \\ x_{12} = b_2 \\ \vdots \\ x_{1n} = b_n \end{cases}$$

Евклидова кольца

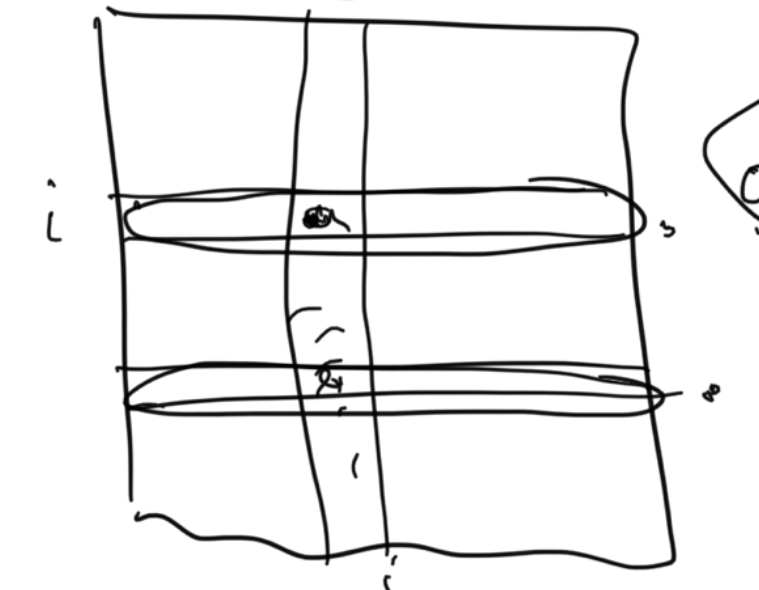
— Область целостности

$$ab = 0 \Rightarrow \begin{cases} a = 0 \\ b = 0 \end{cases}$$

— $\exists d$: $\forall a, b \neq 0$ $\exists q, r$:

$$d: R\setminus\{0\} \to \mathbb{Z}_+ \qquad a = bq + r \qquad \begin{bmatrix} r = 0 \\ d(r) < d(b) \end{bmatrix}$$

1). $\mathbb{Z}$ 2). $\mathbb{R}[x]$

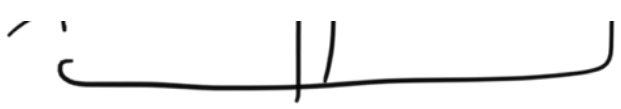


$a, b \to b, a - bk$

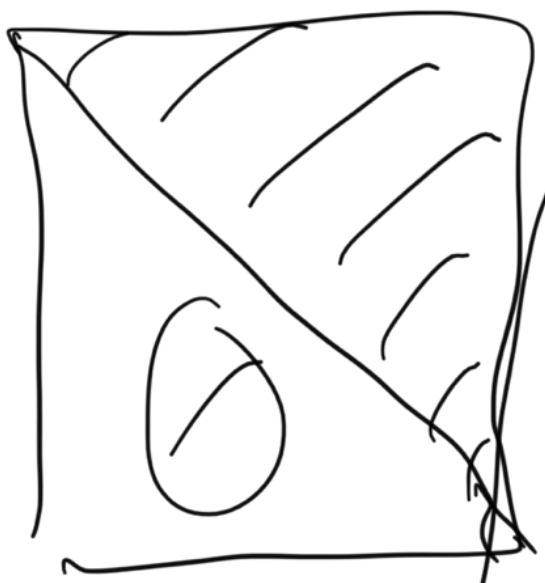
$\vdots$

$0, g$

$A[i]$, $A[j]$



a/b



$0 \neq \det_{\mathbb{Z}} A$

$Ax = b$

$0 \neq \det_{\mathbb{Z}_p} A$

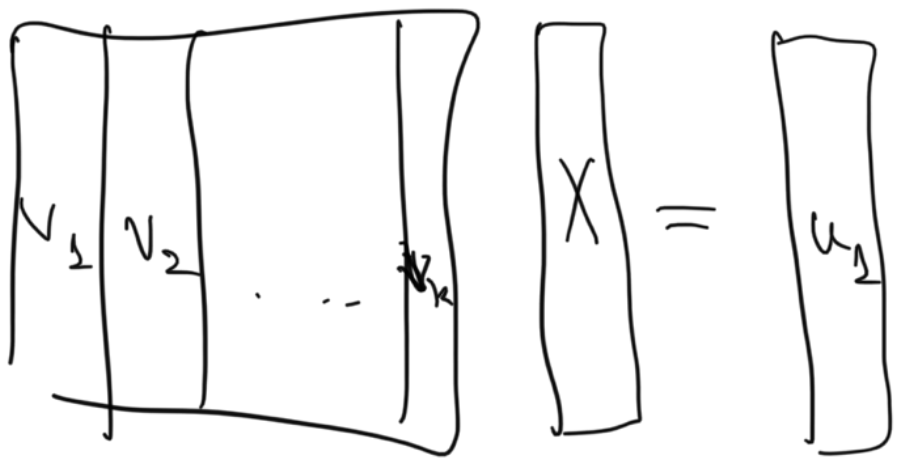
$\Downarrow$

$\det_{\mathbb{Z}} \neq 0$

Разложение вектора по базису

$\{v_1, v_2, \dots, v_k\}$ u_1

$\sum \alpha_i v_i = u_1$



$O(n^3)$

$\sum v_i \cdot x_i = u_1$

① $\{u_1, \dots, u_n\}$ $O(n^3)$

add(v_1)
⋮
add(v_k)

$\forall\, u[i]$
$c_1^{(i)}, \dots, c_k^{(i)}$

$O(n^2)$ → add(u_i)

$u_i = \sum \lambda_i \cdot u[i] =$
$= \sum \lambda_i \cdot \left(\sum_j c_j^{(i)} \cdot v_j\right) =$
$= \sum_j v_j \left(\sum_i \lambda_i \cdot c_j^{(i)}\right)$

② for $i = 0 \dots k-1$
  for $j = 0 \dots i-1$
    $v[i] -= \left(\langle v[i], v[j] \rangle\right) \cdot v[j]$
    (скалярное пр-ие)
  $v[i] /= v[i].\text{len}()$

$O(n^3)$