Ждем слушателей

Докажем, что:

Утв $a, b \in \mathbb{Z}$ $a \neq 0$ или $b \neq 0$

$d = (a, b)$ – НОД a и b

$\forall \bar{d}: a \vdots \bar{d}$ и $b \vdots \bar{d}$, $d \vdots \bar{d}$

НОД делится на любой общий делитель

Д-во рассмотрим все общие делители a, b

Пусть $a = 6$, $b = 4$ $\pm 1, \pm 2$

$d_1\, d_2 \dots d_k$ – все ОД.

$M = [d_1\, d_2\, d_3 \dots d_k]$ – НОК$(d_1 \dots d_k)$

В примере НОК$(\pm 1, \pm 2) = 2$

$a \vdots d_i$ $\forall i$ $\Rightarrow$ a – общее кратное d_i

Знаем, что общее кратное $\vdots$ НОК (было, но 2 чисел)

т.е. $\boxed{a \vdots M}$ аналогично $b \vdots M$

Итого M – общий делитель a и b

Ясно, что M наибольший из ОД, т.к. $M \vdots d_i$ $\forall i$

Итого $\underline{M = (a, b) \text{ и } M \vdots d_i}$ ∎

Утв. Если $ac \vdots b$ и $(c, b) = 1$

Тогда $a \vdots b$

Д-во $cb = [c, b]$ т.к. $[c, b] = \dfrac{cb}{\underbrace{(c,b)}_{=1}}$.

$$\left.\begin{aligned} &ac \vdots c \leftarrow \text{очевидно} \\ &ac \vdots b \leftarrow \text{усл} \end{aligned}\right\} \Rightarrow ac \text{ – общее кратное } c \text{ и } b.$$

$\Rightarrow ac \vdots [c, b] \Rightarrow ac \vdots cb \Rightarrow a \vdots b$ ∎

В прошлый раз:

$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ $\qquad (a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\min(\alpha_n, \beta_n)}$

$b = p_1^{\beta_1} p_2^{\beta_1} \dots p_n^{\beta_n}$ $\qquad [a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\max(\alpha_n, \beta_n)}$

почему $(a,b) \vdots$ ОД

ОД $= p_1^{\gamma_1} \ldots p_k^{\gamma_k}$

$\gamma_i \leq \alpha_i \quad \gamma_i \leq \beta_i$

$\Rightarrow \gamma_i \leq \min(\alpha_i, \beta_i)$

$\Rightarrow$ НОД $\vdots\ p_i^{\gamma_i}$

$ac \vdots b = p_1^{\beta_1} \ldots p_k^{\beta_k} \qquad (c,b)=1$

b c все простые множители не из b

$c \not\vdots p_i$

$\Rightarrow$ все p_i находятся в a.

$\Rightarrow a \vdots b$

Поиск НОД

Метод 1 Использовать утв $(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)}$

но для этого надо знать разложение a и b на простые.

Это вычислительно сложная задача. Для нее не известно эфф. на практике алгоритма.

На практике нужно раскладывать числа порядка 2^{2048}

≈ 600 цифр.

Метод 2 Алгоритм Евклида.

Утв. $(a,b) = (a, b-a)$, где $a, b \in \mathbb{Z}$

$a \neq 0$ или $b \neq 0$.

Д-во. Покажем, что ОД a и b и ОД a и b-a совпадают. Тогда и наибольшие из них совпадут.

] d - ОД a и b : $a \vdots d$, $b \vdots d$ $\Rightarrow$ $b-a \vdots d$

$\Rightarrow$ d - ОД a и $b-a$

] d - ОД a и $b-a$, $a \vdots d$ $b-a \vdots d \Rightarrow$

$\Rightarrow$ $a+(b-a) \vdots d = b \vdots d$ $\Rightarrow$ d - ОД a и b ■

Пример $\underbrace{(10,25)}_{=5} = \underbrace{(10,15)}_{=5} = \underbrace{(10,5)}_{=5}$

Утв. $(a,b) = (a, b \bmod a)$

Д-во $r = b \bmod a$ $b = aq + r$ ← деление b с остатком на a.

$\Rightarrow r = b - aq$

$(a,b) = (a, b-a) = (a, b-2a) = \ldots = (a, \underbrace{b-qa}_{=r})$ ■

Алгоритм Евклида поиска (a,b), если даны a и b.

a, b - два числа на первом шаге.

если $a > b$, то написать вместо $a \to$ $a \bmod b$

если $a < b$, то написать вместо $b \to$ $b \bmod a$

продолжаем, пока a или b не станут 0.

Ответ: ненулевое число.

Утв. Для $a \geq 0$, $b \geq 0$, $a+b > 0$, $a, b \in \mathbb{Z}$

Этот алгоритм даёт НОД a и b (a,b)

Пример

1) 25 40 $40 > 25$

2) 25 15 $40 \to 40 \bmod 25$

3) 10 15 $25 > 15$, $25 \to 25 \bmod 15$

4) 10 5 $5 = 15 \bmod 10$

5) $0 \quad 5$ $\qquad 0 = 10 \bmod 5$

Ответ: $(25, 40) = 5$.

Д-во: На каждом шаге написаны два числа у которых НОД равен исходному.

На каждом шаге a и $b \to a, b \bmod a$

a и $b \to a \bmod b, a$

имеют одинаковый НОД по утверждению выше.

$(a,b) = (b,a) = (b, a \bmod b) = (a \bmod b, a)$

утв

На каждом шаге числа ($a+b$ — сумма) уменьшается

сумма ≥ 0, целая $\Rightarrow$ она не может уменьшаться бесконечно долго, $\Rightarrow$ перестанет уменьшаться. Это значит, что a или $b = 0 \Rightarrow$ на него не поделили.

$(x,0) = x$ или $(0,x) = x$. ∎

Утв. для поиска НОД в общем случае

1) $(\pm a, \pm b) = (a, b)$

Д-во. Проверяем, что множества ОД совпадают ∎

2) $\underbrace{(a_1, a_2 \ldots a_n)}_{\text{НОД } n \text{ чисел}} = \underbrace{((a_1, a_2), a_3 \ldots a_n)}_{\text{НОД } n-1 \text{ числа}}$

Д-во. Вдe? Почему ОД слева и справа одинаковые

$\exists$ d — ОД слева. $a_i \vdots d$

d — ОД a_1 и $a_2 \Rightarrow (a_1, a_2) \vdots d$

$\Rightarrow d$ — ОД чисел справа

$\exists$ d — ОД чисел справа $(a_1, a_2) \vdots d$ $\quad a_i \vdots d$, $i \geq 3$

$\Rightarrow a_1$ и $a_2 \vdots d \Rightarrow a_i \vdots d \; \forall i$ ∎

Утв. (без д-ва). Алг. Евклида для чисел $a, b > 0$ делает не более $C \cdot \log_\varphi \max(a, b)$ шагов $\varphi = \frac{\sqrt{5}+1}{2}$.

Т.е. кол-во шагов $\approx$ кол-во цифр $\cdot\, C$

(Фиб: $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$)

$\to$ самый долгий АЕ.

Линейное разложение НОД

Теорема $\sqsupset a, b \in \mathbb{Z}$. $a \neq 0$ или $b \neq 0$

$\sqsupset d = (a, b)$

Тогда $\exists\, x, y \in \mathbb{Z}$: $ax + by = d$

Примеры. $a = 10$ $b = 7$

$d = (10, 7) = 1$

$\exists\, x, y \in \mathbb{Z}$: $10x + 7y = 1$

$x = 5$, $y = -7$

$x = -2$, $y = 3$

Замечание, интересно, что $x, y \in \mathbb{Z}$ (иначе очевидно $x = 0$ $y = 1/7$)

Или $a = 100$ $b = 31$ $d = 1$

$100x + 31y = 1$ подберете?

Д-во Конструктивное построим x, y

Рассматриваем выражения вида

$ax + by$

Будем пытаться подбирать x y так, чтоб получить d.

Сначала
$$a = a \cdot \underline{\underline{1}} + b \cdot \underline{\underline{0}}$$
$$b = a \cdot \underline{\underline{0}} + b \cdot \underline{\underline{1}}$$

$\sqsupset a > b$, считаем $a \bmod b$ чтоб сделать шаг АЕ

$a \bmod b = a - bq$ ← очередное число АЕ

$$= (a \cdot 1 + b \cdot 0) - (a \cdot 0 + b \cdot 1)q =$$

$$= a(1 - 0q) + b(0 - 1q).$$

Итак, каждое число, которое появляется в АЕ может быть записано в виде $a\bar{x} + b\bar{y}$, где $\bar{x}, \bar{y} \in \mathbb{Z}$.