11.03.19

Алгоритм Евклида (задача для компьютера)

Дано: a, b ≥ 0, a или b не 0, (a, b) = (±a, ±b).

Найти: (a, b).

Алгоритм решения:

повторять пока a > 0 и b > 0

{

если a < b

a, b —> a, b mod a

иначе

a, b —> a mod b, b

}

a + b ϵ N (сумма постоянно уменьшается)

Ответ: a + b (a, если b = 0; b, если a = 0)

Пример:

a= 5, b = 7

5, 7 —> 5, 2 —> 1, 2 —> 1,0 → НОД = 1

Бинарный алгоритм Евклида (задача для компьютера)

Алгоритм решения:

ответ = 1 (инициализация переменной, в которую записывается результат)

повторять пока a ≠ 0 и b ≠ 0

{

если a и b — чётные

{

ответ = 2*ответ

a, b —> a / 2, b /2

}

если a — чётное, b — нечётное

a —> a / 2

если a — нечётное, b — чётное

b —> b / 2

если a и b — нечётные

{

a, b —> a – b, b (или a, b —> a, b – a)

ответ = a*ответ (если b = 0) (или ответ = в*ответ (если a = 0))

}

}

Пример:

a = 13, b = 19

13, 19 —> 13, 6 —> 13, 3 —> 10, 3 —> 5, 3 —> 2, 3 —> 1,3 —> 1, 2 —> 1,0 → НОД = 1

***Определение*:** Пусть a, b ϵ Z, d = (a, b), тогда равенство d = ax +by (где x, y ϵ Z) называется линейным представлением НОД.

Примеры:

1) a = 6, b = 14
d = 2
2 = 6*(-2) + 14*1

2) a = 22, b = 19
d = 1
2 = 22*(-6) + 19*1

***Теорема*:** Для любых a, b ϵ Z существует x, y такие, что ax + by = (a, b), т.е. всегда если линейное представление НОД.

Доказательство:

Дано: a, b ϵ Z.
Обозначим за <x, y> значения ax + by. (Например, <1, 0> = a*1 + b*0 = a)
Выполняем алгоритм Евклида (АЕ):
Дано: a = <1, 0>, b = <0, 1>.
a_1, b_1 — первая пара чисел АЕ
a_2, b_2 — первая пара чисел АЕ и т.д.
a_1 = a = <1, 0>
b_1 = b = <0, 1>
a_i, b_i — (шаг АЕ) -> a_i, mod b_i, b_i
где a_i = < $\hat{x}_i$, $\hat{y}_i$>, b_i = <$\acute{x}_i$, $\acute{y}_i$>
Делим с остатком: ai = qbi + r
a_{i+1} = r = a_i – qb_i = < $\hat{x}_i$, $\hat{y}_i$ > - q< $\acute{x}_i$, $\acute{y}_i$ > = < $\hat{x}_i$ – q$\acute{x}_i$, $\hat{y}_i$ - q$\acute{y}_i$>
В конце АЕ получается пара a = d и b = 0, значит d = <$\hat{x}_n$, $\hat{y}_n$> = a$\hat{x}_n$ + b$\hat{y}_n$.

Пример:

a_1 = 22 = <1, 0>, b_1 = <0, 1>
a_2 = 3 = <1, 0> - <0, 1> = <1, -1>, b_2 = <0, 1>
a_3 = 3 = <1, -1>, b_3 = 1 = <0, 1> - 6<1, -1> = <-6, 7>
a_4 = 0, b_4 = 1 = <-6, 7>
Ответ: 1 = <-6, 7> = 22*(-6) + 19*7

Решение линейных Диофантовых уравнений

Диофантово уравнение (ДУ) — уравнение в целых числах.
Например, $x^2 + y^2 = z^2$ (x, y, z ϵ Z) — ДУ, частным решением которого является x = 3, y = 4, z = 5.

Общее решение:

u, v ϵ Z
$x = u^2 – v^2$
y = 2uv
$z = u^2 + v^2$ (u = 5, v = 1 → z = 5)

$x^3 + y^3 = z^3$. Если x, y, z ϵ N, то для всех степеней больше 2, решений нет (по теореме Ферма).

Решение уравнения ax + by = c, где a, b, c даны. Например, для уравнения 2x + 7y = 3 частными решениями являются x = -2, y = 1; x = 5, y = -2 и др.

Как же устроено множество решений уравнения ax + by = c?

Теорема: a, b ϵ Z, d = (a, b), a ≠ 0 или b ≠ 0, тогда уравнение ax + by = c ↔ c ⋮ d имеет решение.

Доказательство:

→

Пусть ax + by = c для каких-то x_0, y_0.

a ⋮ d

b ⋮ d —> ax0 + by0 ⋮ d —> c ⋮ d

Пример: 6x + 4y = 1001 — нет решений, т.к. 1001 не делится нацело на 2.

←

Найдём линейное разложение НОДа и b:

$a\acute{x} + b\acute{y} = d$

c ⋮ d —> c / d — целое число. Домножим

$a*(\acute{x}\frac{c}{d}) + b*(\acute{y}\frac{c}{d}) = d\frac{c}{d} = c$, где $\acute{x}\frac{c}{d}$ — x_0, $\acute{y}\frac{c}{d}$ — y_0

x_0, y_0 — решение ДУ, ч.т.д

Что если решений несколько?

Пусть $ax_1 + by_1 = c$, $ax_2 + by_2 = c$.

Вычтем из 1-ого 2-ое:

$a(x_1 – x_2) + b(y_1 – y_2) = 0$

$(x_1 – x_2)a = -(y_1 – y_2)b$

$(x_1 – x_2)\frac{a}{d} = -(y_1 – y_2)\frac{b}{d}$, где $\frac{a}{d}$ и $\frac{b}{d}$ — взаимно простые числа.

$(x_1 – x_2)\frac{a}{d} \vdots \frac{b}{d} \leftrightarrow (x_1 – x_2) \vdots \frac{b}{d}$. Аналогично $(y_1 – y_2) \vdots \frac{a}{d}$.

Теорема: Если x_0, y_0 — решение ax + by = c, то $\begin{cases} x = x_0 - \frac{b}{d}k \\ y = y_0 + \frac{a}{d}k \end{cases}$ — всё множество решений.

(где k ϵ Z)

Доказательство:

Проверим, что все решения имеют нужный вид.

Продолжим вывод:

$x_0 – x_1 \vdots \frac{b}{d}$ —> $x_0 – x_1 = k\frac{b}{d}$

$y_0 – y_1 \vdots \frac{a}{d}$ —> $y_0 – y_1 = l\frac{a}{d}$

—> $x_1 = x_0 – k\frac{b}{d}$, $y_1 = y_0 - l\frac{a}{d}$

Подставим в уравнение:

$c = ax_1 + by_1 = a*(x_0 – k\frac{b}{d}) + b*(y_0 - l\frac{a}{d}) = ax_0 + by_0 - \frac{ab}{d} k - \frac{ab}{d} l$

—>$\frac{ab}{d} k + \frac{ab}{d} l = 0$ —> k = -l

Итого:

$$\begin{cases} x_1 = x_0 - \frac{b}{d}k \\ y_1 = y_0 + \frac{a}{d}k \end{cases}$$ ч.т.д.