11.03.19

**Алгоритм Евклида (задача для компьютера)**

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

Найти: (a, b).

Алгоритм решения:

повторять пока а > 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 (а, 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 а ≠ 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 = 22 = 6\*(-2) + 14\*1 | 1. a = 22, b = 19

d = 12 = 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>.

a1, b1 — первая пара чисел АЕ

a2, b2 — первая пара чисел АЕ и т.д.

a1 = a = <1, 0>

b1 = b = <0, 1>

ai, bi — (шаг АЕ) -> ai, mod bi, bi

где ai = < $\hat{x\_{i}}$, $\hat{y\_{i}}$>, bi = <$\overbar{x\_{i}}$, $\overbar{y\_{i}}$>

Делим с остатком: ai = qbi + r

ai+1 = r = ai – qbi = < $\hat{x\_{i}}$, $\hat{y\_{i}}$ > - q< $\overbar{x\_{i}}$, $\overbar{y\_{i}}$ > = < $\hat{x\_{i}}$ – q$\overbar{x\_{i}}$, $\hat{y\_{i}}$ - q$\overbar{y\_{i}}$>

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:

a1 = 22 = <1, 0>, b1 = <0, 1>

a2 = 3 = <1, 0> - <0, 1> = <1, -1>, b2 = <0, 1>

a3 = 3 = <1, -1>, b3 = 1 = <0, 1> - 6<1, -1> = <-6, 7>

a4 = 0, b4 = 1 = <-6, 7>

Ответ: 1 = <-6, 7> = 22\*(-6) + 19\*7

**Решение линейных Диофантовых уравнений**

Диофантово уравнение (ДУ) — уравнение в целых числах.

Например, x2 + y2 = z2 (x, y, z ϵ Z) — ДУ, частным решением которого является x = 3, y = 4, z = 5.

Общее решение:

u, v ϵ Z

x = u2 – v2

y = 2uv

z = u2 + v2 (u = 5, v = 1 → z = 5)

x3 + y3 = z3. 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 $\vdots $ d имеет решение.

Доказательство:

→

Пусть ax + by = c для каких-то x0, y0.

a $\vdots $ d

b $\vdots $ d —> ax0 + by0 $\vdots $ d —> c $\vdots $ d

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

←

Найдём линейное разложение НОДа и b:

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

c $\vdots $ d —> c / d — целое число. Домножим

a\*($\overbar{x}\frac{c}{d}$) + b\*($\overbar{y}\frac{c}{d}$) = d$\frac{c}{d}$ = c, где $\overbar{x}\frac{c}{d}$ — x0, $\overbar{y}\frac{c}{d}$ — y0

x0, y0 — решение ДУ, ч.т.д

Что если решений несколько?

Пусть ax1 + by1 = c, ax2 + by2 = c.

Вычтем из 1-ого 2-ое:

a(x1 – x2) + b(y1 – y2) = 0

 (x1 – x2)a = -(y1 – y2)b

(x1 – x2)$ \frac{a}{d}$ = -(y1 – y2)$ \frac{b}{d}$ , где $ \frac{a}{d}$ и $\frac{b}{d}$ — взаимно простые числа.

(x1 – x2)$ \frac{a}{d}$ $\vdots $ $\frac{b}{d}$ ↔ (x1 – x2)$ \vdots $ $\frac{b}{d}$ . Аналогично (y1 – y2) $\vdots \frac{a}{d}$ .

***Теорема:*** Если x0, y0 — решение ax + by = c, то x= x0 - $\frac{b}{d} $k

 — всё множество решений.

(где k ϵ Z) y= y0 + $\frac{a}{d} $k

Доказательство:

Проверим, что все решения имеют нужный вид.

Продолжим вывод:

x0 – x1 $\vdots $ $\frac{b}{d}$ —> x0 – x1 = k$ \frac{b}{d}$

y0 – y1 $\vdots $ $\frac{a}{d}$ —> y0 – y1 = l$ \frac{a}{d}$

—> x1 = x0 – k$ \frac{b}{d}$ , y1 = y0 - l$ \frac{a}{d}$

Подставим в уравнение:

c = ax1 + by1 = a\*( x0 – k$ \frac{b}{d}$) + b\*( y0 - l$ \frac{a}{d}$) = ax0 + by0 - $\frac{ab}{d}$ k - $\frac{ab}{d}$ l

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

Итого:

 x1 = x0 - $\frac{b}{d} $k

 ч.т.д.

 y1 = y0 + $\frac{a}{d} $k