Алгебра 2

Igor Engel

1 Определения

(a, b) - НОД(a, b).

2 Линейные диофантовы уравнения

$$ax + by = c.$$

Определение 2.1. a и b - взаимно простые, если $(a, b) = 1$

Лемма 2.1.1. Если n и m - взаимно простые, то $\forall aam \vdots n \implies a \vdots n$

Доказательство.

$$nx + ny = 1.$$

$$anx + any = a.$$

$$anx \vdots n \wedge amy \vdots n \implies a \vdots n.$$

□

Теорема 2.1. $ax + by = c$ имеет решения только если $c \vdots (d = (a, b))$

Доказательство.

$$d = ax' + by'.$$

$$c = \frac{c}{d}\left(ax' + by'\right) \implies x = \frac{c}{d}x' \wedge y = \frac{c}{d}y'.$$

□

$$ax + by = c = ax' + by'.$$

$$a(x - x') + b(y - y') = 0.$$

$$a(x - x') = -b(y - y').$$

$$\frac{a}{d}(x - x') = -\frac{b}{d}(y - y').$$

a и b - взаимно простые. Значит

$$\frac{a}{d}t = y - y'.$$

$$\frac{a}{d}(x - x') = -\frac{b}{d}t\frac{a}{d}.$$

$$x - x' = -\frac{b}{d}t.$$

$$x' = x + \frac{b}{d}t.$$

$$y' = y - \frac{a}{d}t.$$

3 Алгоритм Евкилда

$$a = r_{-1} = bq_1 + r_1.$$

$$b = r_0 = r_1q_2 + r_2.$$

$$(a, b) = (b, r_1) = (r_1, r_2) = \dots$$

$$r_i \geq 0.$$

$$r_i > r_{i+1}.$$

Бесконечно убываяющая последовательность неотрицательных чисел приходит к нулю. Значит, при определённом i, $r_i = 0$, тогда $r_{i-2} = qr_{i-1} + r_i = qr_{i-1}$. $r_{i-1} = (a, b)$. Множество $(a, b) \cdot \mathbb{Z} = (b, r_1) \cdot \mathbb{Z} = \dots$ Значит, любое $r_i \in (a, b) \cdot \mathbb{Z}$.

$$r_{-1} = 1a + 0b.$$

$$r_0 = 0a + 1b.$$

Пусть $r_i = ax + by$, $r_{i+1} = ax' + by'$, тогда

$$r_{i+2} = r_i - q_{i+2}r_{i+2} = a(x - x'q_{i+2}) + b(y - y'q_{i+2}.$$

Больше всего итераций если $q_i = 1$.

$$f_0 = r_{k+1} = 0.$$

$$f_1 = r_k = 1.$$

$$f_2 = r_{k-1} = r_k + r_{k+1}.$$

$$f_i = f_{i-1} + f_{i-2}.$$

Теорема 3.1. $f_n \geq \varphi^{n-2}$. $n > 1$. φ - золотое сечением, больший корень $x^2 = x + 1$. $\varphi > 1$.

Доказательство.

$$f_1 = 1 \geq \frac{1}{\varphi} < 1.$$

$$f_2 = 1 \geq \varphi^0 = 1.$$

$$f_i = f_{i-1} + f_{i-2} \geq \varphi^{n-3} + \varphi^{n-4} = \varphi^{n-4}(\varphi + 1) = \varphi^{n-4} \cdot \varphi^2 = \varphi^{n-2}.$$

□

$$a = bq_1 + r_1.$$

$$b = r_1 q_2 + r_2.$$

$$N \geq a > b \geq 0.$$

Количество делений с остатком в алгоритме евклида $\leq 1 + FLOOR \log_\varphi N$

Теорема 3.2.

$$r_{k+1-i} \geq f_i.$$

Доказательство.

$$r_{k+1} = 0 \geq f_0 = 0.$$

$$r_k \geq f_1 = 1.$$

$$r_{k+1-i} = r_{k+2-i}q_{k+2-i} + r_{k+3-i} \geq r_{k+2-i} + r_{k+3-i} \geq f_{i-1} + f_{i-2} = f_i.$$

□

Три последовательности: $\varphi^{k-2} \leq f_k \leq r_{k+1-i}$. Последовательность r достигнет a раньше чем f или φ.

$$a = r_{-1} \geq f_{k+2} \geq \varphi^k.$$

$k+1$ - количество делений с остатком. Значит, $\log_\varphi N \geq k \implies 1 + \log_\varphi N \geq k + 1$.

4 Сравнение целых чисел

$$x^2 + 1213x + 5321 = 0.$$

Есть-ли целый решения?
Если x - чётное, то x^2 - чётное, $1213x$ - чётное, 5321 - нечётное. Значит решений нет.
Если x - нечётное, то все три числа нечётных, и решений нет.
Чётность - остаток от делений на два. Будем приплетать другие остатки. Это теория сравнений.

Определение 4.1.

$$n, a, b \in \mathbb{Z}.$$

$$(a \equiv b \mod n) = (a \equiv b(n)) = ab \vdots n.$$

Замечание: $a \equiv b \mod n$ эквивалетно тому, что остатки от деления на n равны.

Доказательство.

$$a \equiv b \mod n \implies (a-b) = nk \implies a = nk + b.$$

$$a = nq_1 + r_1.$$

$$b = nq_2 + r_2.$$

$$0 \leq r_1, r_2 < n.$$

$$a = nq_2 + r_2 + nk = n(q_2 + k) + r_2 \implies r_2 = r_1. \qquad \square$$

4.1 Свойства

$$a \equiv a \mod n.$$

$$a \equiv b \mod n \implies b \equiv a \mod n.$$

$$a \equiv b \mod n \wedge b \equiv c \mod n \implies a \equiv c \mod n.$$

$$a \equiv b \mod 0 \implies a = b.$$

$$\forall a, b \quad a \equiv b \mod 1.$$

$$a \equiv b \mod n \implies a \equiv b \mod -n.$$

$$a \equiv b \mod n \wedge c \equiv d \mod n \implies a + c \equiv b + d \mod n \wedge ac \equiv bd \mod n.$$