



Полиномы от одной переменной

Нахождение НОД

«Наивный» метод

Пример: Вычислить НОД

ПОЛИНОМОВ $f = x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5$

$$g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$$

$$x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5 \left| \underline{3x^6 + 5x^4 - 4x^2 - 9x + 21} \right.$$

$$x^8 + \frac{5}{3}x^6 - \frac{4}{3}x^4 - 3x^3 + 7x^2 \qquad \frac{x^2}{3} - \frac{2}{9}$$

$$-\frac{2}{3}x^6 - \frac{2}{3}x^4 + x^2 + 2x - 5$$

$$f - \left(\frac{x^2}{3} - \frac{2}{9} \right) \cdot g \qquad \text{т. е.} \qquad \frac{5}{9}x^4 + \frac{1}{9}x^2 - \frac{1}{3}$$

Пример:

$$p_5 = \text{НОД}(f_5, g_5):$$

$$w = x - 3, \quad v = x + 2, \quad \text{НОД} = 1,$$

но $w_5 = v_5 = x + 2$ и, таким образом,
 $\text{НОД}(w_5, v_5) = x + 2.$

Граница для коэффициентов НОД двух полиномов.

Теорема (неравенство Ландау-Миньотта).

$$b = \sum_{i=0}^{\beta} b_i x^i \quad a = \sum_{i=0}^{\alpha} a_i x^i$$

$$\sum_{i=0}^{\beta} |b_i| \leq 2^{\beta} \left| \frac{a_{\alpha}}{b_{\beta}} \right| \sqrt{\sum_{i=0}^{\alpha} a_i^2}$$

Следствие 1.

$$2^{\min(\alpha, \beta)} \text{НОД}(a_\alpha, b_\beta) \min \left[\frac{1}{|a_\alpha|} \sqrt{\sum_{i=0}^{\alpha} a_i^2}, \frac{1}{|b_\beta|} \sqrt{\sum_{i=0}^{\beta} b_i^2} \right]$$

Лемма 1.

Если число p не делит старший коэффициент $\text{НОД}(a, b)$ полиномов a и b , то степень $\text{НОД}(a_p, b_p)$ больше или равна степени $\text{НОД}(f, g)$.

Следствие.

Если число p не делит старшие коэффициенты полиномов a и b (в частности, может делить один из них, но не оба одновременно), то степень $\text{НОД}(a_p, b_p)$ больше или равна степени $\text{НОД}(a, b)$.

Лемма 2. Пусть $c = \text{НОД}(a, b)$. Если число p удовлетворяет условию следствия и если p не делит $\text{Res}_x(a/c, b/c)$, то $\text{НОД}(a_p, b_p) = c_p$.

Отсюда следует, что существует только конечное число значений p , таких, что степень $\text{НОД}(a_p, b_p)$ отличается от степени $\text{НОД}(a, b)$:

- 1) это те p , которые делят НОД старших коэффициентов;
- 2) это те p , которые делят результат, упоминающийся в лемме (почему у него конечное число делителей **!!??**).

Вычисление НОД

$M :=$ граница_Ландау_Миньотта (A, B) ;

цикл до бесконечности

$P :=$ найти_большое_простое $(2M)$

если степень_остатка (p, A) или

степень_остатка (p, B)

то $C :=$ модулярный_НОД (A, B, p) ;

если делит (C, A) и делит (C, B)

то выход C ;



алгоритм **граница_Ландау_Миньотта**
применяет следствие их неравенства;

алгоритм **найти_большое_простое**
возвращает простое число, большее чем
его аргумент (каждый раз новое число);

алгоритм **степень_остатка** проверяет, что
редукция по модулю p не меняет степень,
т.е. p не делит старший коэффициент;

алгоритм **модулярный_НОД** применяет
алгоритм Евклида по модулю p ;

алгоритм **делит** проверяет, что многочлены
делятся над кольцом целых чисел

M := граница_Ландау_Миньотта (A, B);

Кроме := НОД(Ic(A), Ic(B));

E0: p := найти_простое (Кроме);

 C := модулярный_НОД (A, B, p);

E1: если степень (C) = 0 то выход 1;

 Дано := p;

 Результат := C;

Цикл пока Дано $\leq 2M$

 p := найти_простое (Кроме);

 C := модулярный_НОД (A, B, p);

если степень (C) < степень (Результат) то иди на

E1;

если степень (C) = степень (Результат)

то Результат := CRT(Результат, Дано, C, p);

 Дано := Дано · p;

если делит (Результат, A) и делит (Результат, B)

то выход Результат;

иди на E0;

Ic – старший коэффициент полинома;

найти_простое – выдает простое число, не делящее его аргумент (каждый раз новое число);

CRT – применяет китайскую теорему об остатках к каждому коэффициенту двух полиномов – **Результат** (по модулю Дано) и **C** (по модулю p), представляя целые числа по модулю M между $-M/2$ и M

Оценка стоимости алгоритма

Время вычисления ограничивается величиной $O(n^3 \cdot \log_2^3 N)$, где n - такое, что степени полиномов a , b не больше этого числа;

N - величина, удовлетворяющая неравенству

$$\sqrt{\sum_{i=0}^{\alpha} a_i^2} \sqrt{\sum_{i=0}^{\beta} b_i^2} \leq N$$