

## Алгоритм Евклида, Идеалы и прочее

**Определение 1.** Наибольшим общим делителем набора многочленов  $A_1, A_2, \dots, A_n$  называется такой их общий делитель, который делится на любой другой их общий делитель.

**Замечание.** а) Наибольший общий делитель определен с точностью до умножения на константу. Иногда константу подбирают так, чтобы многочлен был *приведенным*, т.е. его старший коэффициент равнялся 1.

б) Для данного определения не очевидно существование такого многочлена. Мы докажем его двумя способами.

в) Из данного определения следует, что наибольший общий делитель является делителем наибольшей степени.

**Определение 2.** Пусть  $K$  — коммутативное кольцо. Подмножество  $I \subseteq K$  называется идеалом, если  $I$  замкнуто относительно сложения и произведения любого элемента из  $a \in K$  на любой элемент  $b \in I$  принадлежит  $ab \in I$ .

1. Даны два целых числа  $a_1, a_2, \dots, a_n$ . Рассмотрим множество  $I$  — это все числа вида  $a_1k_1 + \dots + a_nk_n$ . Докажите, что

а) если  $c \in I$  и  $d \in I$ , то  $c + d \in I$ ,  $c - d \in I$ ,  $cn \in I$  (иными словами  $I$  — идеал);

б) если  $c \in I$  и  $d \in I$ , то остаток от деления  $c$  на  $d$  принадлежит  $I$ ;

в) пусть  $e$  — самое маленькое положительное число в  $I$ , тогда если  $c \in I$ , то  $c : e$  (в частности покажите отсюда, что  $e$  является общим делителем  $a_1, a_2, \dots, a_n$ );

г) пусть  $m = (a_1, a_2, \dots, a_n)$ , тогда если  $c \in I$ , то  $c : m$ ; д) докажите, что  $e = m$ ;

Иными словами мы доказали, что  $m$  представим в виде  $a_1k_1 + \dots + a_nk_n$ .

2. Для данных многочленов  $A_1, A_2, \dots, A_n$  обозначим через  $I$  множество многочленов представимых в виде  $A_1X_1 + A_2X_2 + \dots + A_nX_n$ , где  $X_i$  — произвольные многочлены. Пусть  $D$  многочлен наименьшей степени в множестве  $I$ . а) Докажите, что  $I$  — идеал.

б) Докажите, что для любого  $M$  из  $I$ ,  $M : D$ .

в) Докажите, что  $D$  является наибольшим общим делителем  $A_1, A_2, \dots, A_n$ .

**Определение 3.** Пусть  $K$  — коммутативное кольцо. Идеал  $I$  называется главным, если существует такой элемент  $a \in I$  такой, что любой элемент из  $I$  делится на  $a$ .

3. Докажите, что в кольце а) целых чисел; б) кольце многочленов над полем  $K[x]$  любой идеал главный. в) Приведите пример идеала в  $K[x, y]$ , который не является главным.

4. Пусть число  $\alpha$  является корнем некоторого многочлена с рациональными коэффициентами (“является алгебраическим числом”). Тогда все многочлены с рациональными коэффициентами, обращающиеся в ноль в точке  $\alpha$  кратны некоторому одному многочлену с рациональными коэффициентами.

**Определение 4.** Алгоритмом Евклида для многочленов  $A$  и  $B$  называется последовательность делений с остатком:

$$\begin{aligned} A &= BQ_1 + R_1, \\ B &= R_1Q_2 + R_2; \\ &\dots \\ R_{n-2} &= R_{n-1}Q_n + R_n; \\ R_{n-1} &= R_nQ_{n+1}. \end{aligned}$$

Последний ненулевой остаток  $R_n$  называется *результатом работы алгоритма Евклида*.

**5.** Докажиет, что результат алгоритма Евклида является НОДом многочленов  $A$  и  $B$ . Докажите, что существуют такие многочлены  $g, h$ , что  $Ag + Bh = R_n$ .

**6 (Китайская теорема об остатках для многочленов).** Пусть  $g_1, \dots, g_n$  попарно взаимнопростые многочлены и  $r_1, \dots, r_n$  произвольный набор многочленов. Тогда существует многочлен  $f$  такой, что

$$\left\{ \begin{array}{l} f \equiv_{g_1} r_1 \\ f \equiv_{g_2} r_2 \\ \dots \\ f \equiv_{g_n} r_n \end{array} \right.$$

Любые такие многочлены  $f$  и  $f'$  сравнимы  $f \equiv_{g_1 \dots g_n} f'$ .

**7. а)** Рассмотрим набор взаимнопростых натуральных чисел  $b_1, b_2, \dots, b_n$  больших 1 и число  $|a| < b_1 b_2 \dots b_n$ . Докажите, что существуют целые числа  $|c_1| < b_1, \dots, |c_n| < b_n$ , что выполнено равенство

$$\frac{a}{b_1 b_2 \dots b_n} = \frac{c_1}{b_1} + \dots + \frac{c_n}{b_n}.$$

**б)** Сформулируйте обобщение этого результата для многочленов и докажите его.

**8.** Напоминание, уравнение прямой, проходящей через точки  $z_1, z_2$  выглядит так

$$\frac{z_1 - z}{z_2 - z} = \frac{\overline{z_1 - z}}{\overline{z_2 - z}}$$

Вспомнив, как доказывается эта формула, напишите уравнение прямой, проходящей через точку  $z_3$  и перпендикулярной вектору  $z_1 - z_2$ .

**9.** Упростите выражение

$$\cos \alpha + \cos 2\alpha + \dots + \cos n\alpha + i \sin \alpha + i \sin 2\alpha + \dots + i \sin n\alpha.$$

И найдите  $\cos \alpha + \cos 2\alpha + \dots + \cos n\alpha$ .