МАТЕМАТИКА

Многочлены с целыми коэффициентами

Шарич Владимир Златкович

Высшая школа экономики

Национальный исследовательский университет

Факультет математики

2018/2019

Лемма о делимости

Если $P(x) \in \mathbb{Z}[x]$ и $b, c \in \mathbb{Z}$,

Лемма о делимости

Если $P(x) \in \mathbb{Z}[x]$ и $b, c \in \mathbb{Z}$,

то $P(b) - P(c) \,\vdots\, b - c$.

Лемма о делимости

Если $P(x) \in \mathbb{Z}[x]$ и $b, c \in \mathbb{Z}$,
то $P(b) - P(c) \vdots b - c$.

$\square$

$$b^k - c^k = (b-c)(b^{k-1} + b^{k-2}c + \ldots + bc^{k-2} + c^{k-1}).$$

$\blacksquare$

Пусть $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, где $a_n, a_{n-1}, ..., a_1, a_0 \in \mathbb{Z}$.

Определим *содержание* как $\mathrm{cont} P = \text{НОД}(a_n, a_{n-1}, ..., a_1, a_0)$.

Лемма Гаусса $\mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \,\vdots\, p$.

Докажем, что $\mathrm{cont}\,Q \,\vdots\, p$ или $\mathrm{cont}\,R \,\vdots\, p$.

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \,\vdots\, p$.

Докажем, что $\mathrm{cont}\,Q \,\vdots\, p$ или $\mathrm{cont}\,R \,\vdots\, p$.

Пусть $Q(x) = b_k x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$.

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Докажем, что $\mathrm{cont}\, Q \vdots p$ или $\mathrm{cont}\, R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_1 x + c_0$.

Лемма Гаусса $\operatorname{cont}(QR) = \operatorname{cont}(Q)\operatorname{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\operatorname{cont}(QR) \vdots p$.

Докажем, что $\operatorname{cont} Q \vdots p$ или $\operatorname{cont} R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_1 x + c_0$.

Пусть $Q(x)R(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$.

Лемма Гаусса $\mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Докажем, что $\mathrm{cont}\,Q \vdots p$ или $\mathrm{cont}\,R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_1 x + c_0$.

Пусть $Q(x)R(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$.

Допустим, что $b_0, b_1, \ldots, b_{s-1} \vdots p$, но $b_s \not\vdots p$.

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Докажем, что $\mathrm{cont} Q \vdots p$ или $\mathrm{cont} R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1} x^{m-1} + \ldots + c_1 x + c_0$.

Пусть $Q(x)R(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$.

Допустим, что $b_0, b_1, \ldots, b_{s-1} \vdots p$, но $b_s \not\vdots p$.

Допустим, что $c_0, c_1, \ldots, c_{t-1} \vdots p$, но $c_t \not\vdots p$.

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

$\square$ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Докажем, что $\mathrm{cont}Q \vdots p$ или $\mathrm{cont}R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$.

Пусть $Q(x)R(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

Допустим, что $b_0, b_1, \ldots, b_{s-1} \vdots p$, но $b_s \not\vdots p$.

Допустим, что $c_0, c_1, \ldots, c_{t-1} \vdots p$, но $c_t \not\vdots p$.

$a_{s+t} = b_{s+t}c_0 + b_{s+t-1}c_1 + \ldots + b_s c_t + \ldots + b_1 c_{s+t-1} + b_0 c_{s+t}$

Лемма Гаусса $\quad \mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$

□ Пусть $p \in \mathbb{P}$, $\mathrm{cont}(QR) \vdots p$.

Докажем, что $\mathrm{cont}\,Q \vdots p$ или $\mathrm{cont}\,R \vdots p$.

Пусть $Q(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$.

Пусть $R(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$.

Пусть $Q(x)R(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

Допустим, что $b_0, b_1, \ldots, b_{s-1} \vdots p$, но $b_s \not\vdots p$.

Допустим, что $c_0, c_1, \ldots, c_{t-1} \vdots p$, но $c_t \not\vdots p$.

$$a_{s+t} = b_{s+t}c_0 + b_{s+t-1}c_1 + \ldots + b_s c_t + \ldots + b_1 c_{s+t-1} + b_0 c_{s+t}$$

Тогда $a_{s+t} \not\vdots p$ ↯ ■

Лемма о рациональных корнях

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Если $P(b/c) = 0$, где $b, c \in \mathbb{Z}$, $b \perp c$,

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Если $P(b/c) = 0$, где $b, c \in \mathbb{Z}$, $b \perp c$,
то $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Z}[x]$.

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Если $P(b/c) = 0$, где $b, c \in \mathbb{Z}$, $b \perp c$,
то $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Z}[x]$.

$\square$ $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Q}[x]$

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Если $P(b/c) = 0$, где $b, c \in \mathbb{Z}$, $b \perp c$,
то $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Z}[x]$.

$\square$ $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Q}[x]$
Домножим P и Q на НОК знаменателей коэффициентов Q.

Лемма о рациональных корнях

Пусть $P(x) \in \mathbb{Z}[x]$.

Если $P(b/c) = 0$, где $b, c \in \mathbb{Z}$, $b \perp c$,

то $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Z}[x]$.

$\square$ $P(x) = (cx - b)Q(x)$, где $Q(x) \in \mathbb{Q}[x]$

Домножим P и Q на НОК знаменателей коэффициентов Q.

Воспользуемся леммой Гаусса. $\blacksquare$

Неприводимые многочлены

Неприводимые многочлены

$P(x) \in \mathbb{Z}[x]$ неприводим,

если из $\begin{array}{c} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x] \end{array}$

Неприводимые многочлены

$P(x) \in \mathbb{Z}[x]$ неприводим,

если из $\begin{array}{c} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x] \end{array}$

следует $\left[\begin{array}{l} Q(x) \equiv \pm 1 \\ R(x) \equiv \pm 1 \end{array} \right.$

P неприводим над $\mathbb{Z} \Rightarrow P$ неприводим над $\mathbb{Q}$

P неприводим над $\mathbb{Z} \Rightarrow P$ неприводим над $\mathbb{Q}$

$\square$ Из леммы Гаусса! $\blacksquare$

Признак Эйзенштейна

Признак Эйзенштейна

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$,
где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.

Признак Эйзенштейна

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$,
где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.

Если $\exists p \in \mathbb{P}$: $a_n \not\vdots\, p$, $a_{n-1}, \ldots, a_1, a_0 \vdots\, p$, $a_0 \not\vdots\, p^2$

Признак Эйзенштейна

Пусть $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.
Если $\exists p \in \mathbb{P}$: $a_n \not\vdots\, p$, $a_{n-1}, \ldots, a_1, a_0 \vdots\, p$, $a_0 \not\vdots\, p^2$
то P неприводим

Признак Эйзенштейна

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$,
где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.

Если $\exists p \in \mathbb{P}$: $a_n \not\vdots\, p$, $a_{n-1}, \ldots, a_1, a_0 \,\vdots\, p$, $a_0 \not\vdots\, p^2$

то P неприводим

$\square$ Рассмотрим всё $\mod p$. $\blacksquare$

Теорема Дюма

Теорема Дюма

$P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$.

Теорема Дюма

$P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$.

Диаграмма Ньютона для $P(x)$.

Теорема Дюма

$P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$.

Диаграмма Ньютона для $P(x)$.

Система векторов $\mathcal{V}(P(x))$.

Теорема Дюма

$P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$.

Диаграмма Ньютона для $P(x)$.

Система векторов $\mathcal{V}(P(x))$.

Если $\begin{cases} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x], \end{cases}$

Теорема Дюма

$P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$.

Диаграмма Ньютона для $P(x)$.

Система векторов $\mathcal{V}(P(x))$.

Если $\begin{array}{l} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x], \end{array}$

то $\mathcal{V}(P(x)) = \mathcal{V}(Q(x)) \cup \mathcal{V}(R(x))$.

Кто все эти люди?

Кто все эти люди?

Эйзенштейн

Кто все эти люди?

Эйзенштейн Фердинанд Готтхольд Макс

Кто все эти люди?

Эйзенштейн Фердинанд Готтхольд Макс (Германия, 1823–1852)

Кто все эти люди?

Эйзенштейн Фердинанд Готтхольд Макс (Германия, 1823–1852)

Дюма

Кто все эти люди?

Эйзенштейн Фердинанд Готтхольд Макс (Германия, 1823–1852)

Дюма Густав

Кто все эти люди?

Эйзенштейн Фердинанд Готтхольд Макс
(Германия, 1823–1852)

Дюма Густав
(Швейцария, 1872–1955)

Удачных занятий математикой!

Шарич В.З.
mathschool.ru/sharich

Фоксфорд

Высшая школа экономики
Национальный исследовательский университет

Математическая школа

Центр Педагогического Мастерства