Многочлены с целыми коэффициентами

1. Лемма о делимости **Если** $P(x) \in \mathbb{Z}[x]$ и $b, c \in \mathbb{Z}$, **то** $P(b) - P(c) \vdots b - c$.
   □ $b^k - c^k = (b-c)(b^{k-1} + b^{k-2}c + \ldots + bc^{k-2} + c^{k-1})$. ■
2. Пусть $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, где $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$.
   Определим *содержание* как $\mathrm{cont} P = \text{НОД}(a_n, a_{n-1}, \ldots, a_1, a_0)$.
3. Лемма Гаусса $\mathrm{cont}(QR) = \mathrm{cont}(Q)\mathrm{cont}(R)$
   □ 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 $b_s \nvdots p$. Допустим, что $c_0, c_1, \ldots, c_{t-1} \vdots p$, но $c_t \nvdots p$.
   $a_{s+t} = b_{s+t}c_0 + b_{s+t-1}c_1 + \ldots + b_s c_t + \ldots + b_1 c_{s+t-1} + b_0 c_{s+t}$ Тогда $a_{s+t} \nvdots p$ ↯ ■
4. 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 $Q(x) \in \mathbb{Z}[x]$.
   □ $P(x) = (cx-b)Q(x)$, где $Q(x) \in \mathbb{Q}[x]$
   Домножим P и Q на НОК знаменателей коэффициентов Q.
   Воспользуемся леммой Гаусса. ■
5. Неприводимые многочлены
   $P(x) \in \mathbb{Z}[x]$ неприводим, если из $\begin{matrix} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x] \end{matrix}$ следует $\left[\begin{matrix} Q(x) \equiv \pm 1 \\ R(x) \equiv \pm 1 \end{matrix}\right.$
6. P неприводим над $\mathbb{Z} \Rightarrow P$ неприводим над $\mathbb{Q}$
   □ Из леммы Гаусса! ■
7. 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 $\exists p \in \mathbb{P}$: $a_n \nvdots p$, $a_{n-1}, \ldots, a_1, a_0 \vdots p$, $a_0 \nvdots p^2$ **то** P неприводим
   □ Рассмотрим всё $\bmod p$. ■
8. Теорема Дюма
   $P(x) \in \mathbb{Z}[x]$, $p \in \mathbb{P}$. Диаграмма Ньютона для $P(x)$. Система векторов $\mathcal{V}(P(x))$.
   Если $\begin{matrix} P(x) = Q(x)R(x), \\ Q(x), R(x) \in \mathbb{Z}[x], \end{matrix}$ то $\mathcal{V}(P(x)) = \mathcal{V}(Q(x)) \cup \mathcal{V}(R(x))$.