Многочлены: китайская теорема об остатках, лемма Гаусса, ...

Предварительные сведения

1. $\mathbb{Z}[x]$ — множество многочленов от переменной x с целыми коэффициентами, $\mathbb{R}[x]$ — с действительными коэффициентами, ...
2. Если a, b — целые числа и $f \in \mathbb{Z}[x]$, то $(b-a) \mid (f(b)-f(a))$.
3. *Деление многочленов с остатком.* Если $p(x)$ и $q(x)$ — многочлены, причем $q(x)$ не равен нулю тождественно, то существуют многочлены $t(x)$ и $r(x)$ такие, что $p(x) = q(x)t(x) + r(x)$, и $\deg r(x) < \deg q(x)$; при этом $t(x)$ и $r(x)$ определяются однозначно.
4. *Теорема Безу.* Остаток от деления многочлена $p(x)$ на $(x-c)$ равен $p(c)$.
5. Для двух многочленов $p(x)$, $q(x) \in \mathbb{R}[x]$ всегда определен их *наибольший общий делитель* $d(x) = (p(x), q(x)) \in \mathbb{R}[x]$ (максимальный по делимости многочлен, на который делится каждый из данных).
   При этом существуют $u(x), v(x) \in \mathbb{R}[x]$ такие, что $u(x)p(x) + v(x)q(x) = d(x)$.
   При этом $\mathbb{R}$ можно заменять на $\mathbb{Q}$ или $\mathbb{Z}$.
6. Два многочлена $a(x)$ и $b(x)$ называются *сравнимыми по модулю* $m(x)$, если их разность делится на $m(x)$. Как и для чисел, соотношение сравнимости для двух многочленов записывается в виде $a(x) \equiv b(x) \pmod{m(x)}$.

Задачи

1. Пусть a, b и n — натуральные числа. Известно, что при любом натуральном k $(k \neq b)$ число $a - k^n$ делится без остатка на $b - k$. Докажите, что $a = b^n$.

2. **(a)** Пусть a, m и n — натуральные числа, $a > 1$. Докажите, что если $a^m + 1$ делится на $a^n + 1$, то m делится на n.
(b) Пусть a, b, m, n — натуральные числа, причем $(a, b) = 1$, и $a > 1$. Докажите, что если $a^m + b^m$ делится на $a^n + b^n$, то m делится на n.

3. Пусть $f(x) = x^2 - x + 1$. Докажите, что для любого натурального $m > 1$ числа m, $f(m)$, $f(f(m))$, ... попарно взаимно просты.

4. Пусть f и g — взаимно простые многочлены (т. е. $(f, g) \equiv \text{const}$) с целыми коэффициентами. Докажите, что последовательность чисел $a_n = (f(n), g(n))$ периодическая.

5. **Китайская теорема об остатках для многочленов.** Пусть $m_1(x)$, $\ldots$, $m_n(x)$ — попарно взаимно простые многочлены, то есть $(m_i(x), m_j(x)) = 1$ при $i \neq j$, $a_1(x)$, $\ldots$, $a_n(x)$ — произвольные многочлены. Докажите, что тогда существует ровно один многочлен $p(x)$ такой, что $\deg p(x) < \deg m_1(x) + \ldots + \deg m_n(x)$ и

$$\begin{cases} p(x) \equiv a_1(x) \pmod{m_1(x)} \\ \qquad \ldots \\ p(x) \equiv a_n(x) \pmod{m_n(x)}. \end{cases}$$

6. **Лемма Гаусса I.** Многочлен с целыми коэффициентами называется *примитивным*, если НОД его коэффициентов равен 1. Докажите, что произведение двух примитивных многочленов также является примитивным многочленом.

7. **Лемма Гаусса II.** Если многочлен $f \in \mathbb{Z}[x]$ можно разложить в произведение двух многочленов $g, h \in \mathbb{Q}[x]$, то его можно представить и в виде $f = \widetilde{g}\widetilde{h}$, где $\widetilde{g}, \widetilde{h} \in \mathbb{Z}[x]$.

8. Пусть $p \in \mathbb{Z}[x]$, $\deg p > 1$. Докажите, что существует бесконечная последовательность целых чисел, не являющихся значениями многочлена p.

9. *Лемма Шура.* Пусть $f \in \mathbb{Z}[x]$, $\deg f > 0$. Докажите, что множество простых чисел, делящих хотя бы одно из ненулевых чисел $f(1)$, $f(2)$, $\ldots$, $f(n)$, $\ldots$ бесконечно.

10. Пусть $f, g \in \mathbb{Z}[x]$ — неприводимые многочлены с единичными старшими коэффициентами, и $\deg f, \deg g > 0$. Известно, что для достаточно больших n множества простых делителей чисел $f(n)$ и $g(n)$ совпадают. Докажите, что $f = g$.

11. Пусть $f \in \mathbb{Z}[x]$, $\deg f > 0$ и n, k — натуральные числа. Докажите, что найдется натуральное a такое, что каждое из чисел $f(a)$, $f(a+1)$, $\ldots$, $f(a+n-1)$ имеет по крайней мере k различных простых делителей.