



Серия №32. Многочлены над \mathbb{Z}_p

19 июля

Определение. Множество всех остатков (вычетов) по модулю n обозначим \mathbb{Z}_n . В случае, если n простое, для удобства будем писать \mathbb{Z}_p .

Определим многочлен над \mathbb{Z}_n как формальную запись $P(x) = a_0 + a_1x + \dots + a_mx^m$, где коэффициенты $a_i \in \mathbb{Z}_n, a_m \neq 0$. Множество таких многочленов обозначается $\mathbb{Z}_n[x]$.

Из предыдущего листка:

Если два многочлена $P, Q \in \mathbb{Z}_p[x]$, то $\deg PQ = \deg P + \deg Q$.

Теорема о делении с остатком. Для формальных многочленов $A(x), B(x) \neq 0$ существуют единственные многочлены $Q(x)$ и $R(x)$ такие, что $A(x) = B(x)Q(x) + R(x)$ и $\deg R < \deg B$.

Теорема Безу для многочленов над \mathbb{Z}_p . $P(x) = (x - a)Q(x) + P(a)$

Следствие из теоремы Безу. Количество корней многочлена не превосходит его степени.

Задачи

- Используя теорему Безу, разложите на множители многочлен $x^{p-1} - 1$ и докажите теорему Вильсона: для любого простого p число $(p-1)! + 1$ делится на p .
- а) Приведите пример ненулевого многочлена $P \in \mathbb{Z}_p[x]$ такого, что $P(x) = 0$ во всех точках $x \in \mathbb{Z}_p$.
б) Докажите, для любого многочлена $P \in \mathbb{Z}_p[x]$ существует многочлен $Q \in \mathbb{Z}_p[x]$ степени не выше $p-1$, совпадающий с ним по модулю p во всех точках.
в) Докажите, что если два многочлена $P, Q \in \mathbb{Z}_p[x]$ степени не выше $p-1$ совпадают по модулю p по всех точках, то они равны формально.
- Докажите, что для любого целого m , не кратного $p-1$, существует n , не кратное p , такое, что $n^m \not\equiv 1 \pmod{p}$.
- Дана произвольная функция $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$. Докажите, что существует многочлен $P \in \mathbb{Z}_p[x]$ степени не выше $p-1$, совпадающий с f по модулю p во всех точках.
- Пусть $Q(x)$ – многочлен с целыми коэффициентами, p – простое число. Оказалось, что $Q(0) = 0, Q(1) = 1$, и при любом натуральном k число $Q(k)$ дает остаток 0 или 1 при делении на p . Докажите, что $\deg Q \geq p-1$.