10 июля

Поле $\mathbb{Z}_p$ и многочлены над ним

Определение. *Полем* называется множество, в котором определены операции сложения и умножения, причем выполняются следующие свойства:
а) сложение ассоциативно, коммутативно, существует нейтральный по сложению элемент (он обозначается 0) и у каждого элемента есть обратный по сложению.
б) умножение ассоциативно, коммутативно, существует нейтральный по умножению элемент (он обозначается 1) и у каждого ненулевого элемента есть обратный по умножению.
в) сложение и умножение связаны законом дистрибутивности: $x \cdot (y + z) = x \cdot y + x \cdot z$.
г) при этом $0 \neq 1$.

Примеры полей. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{Z}_2$ – поля. $\mathbb{Z}, \mathbb{R}[x]$ – не поля.

1. а) Докажите, что если в поле выполнено $a \cdot b = 0$, то $a = 0$ или $b = 0$.
б) При каких n множество $\mathbb{Z}_n$ является полем?

Вывод. Существуют поля как конечные, так и бесконечные.

2. а) Разложите на множители над $\mathbb{Z}_p$ многочлен $x^{p-1} - 1$.
б) Докажите *теорему Вильсона*: $(p-1)! \equiv -1 \pmod p$ при простом p.
в) Найдите сумму $\sum\limits_{0<l<m<s<h<p} lmsh \pmod p$.

3. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ – произвольная функция. Тогда найдется такой многочлен $\hat{f} \in \mathbb{Z}_p[x]$, для которого при любом c выполнено $f(c) = \hat{f}(c)$. (Другими словами, на множестве $\mathbb{Z}_p$ не имеет смысла рассматривать никакие функции помимо многочленов!)

4. Многочлены $f(x)$ и $g(x)$ равны в функциональном смысле тогда и только тогда, когда их разность делитсяна на $x^p - x$.

5. Над $\mathbb{Z}_p$ существует бесконечно много неприводимых многочленов.

Замечание. Если многочлен $f(x)$ имеет целые коэффициенты, то его можно рассмотреть как многочлен над $\mathbb{Z}_p$ (дабы непосвященные понимали как можно меньше, то новый многочлен точно также обозначим $f(x)$).

6. (Критерий Эйзенштейна) Пусть $f(x)$ — многочлен с целыми коэффициентами, у которого старший коэффициент не делится на p, все остальные коэффициенты делятся на p, а свободный член не делится на p^2 для какого-то простого числа p. Тогда $f(x)$ неприводим над $\mathbb{Z}$.

7. Многочлен $x^{n-1} + x^{n-2} + \dots + x + 1$ неприводим над $\mathbb{Z} \iff n$ – простое.
(Тонкий намек: $f(x)$ неприводим $\iff f(x + 2008)$ – неприводим).

8. Пусть для натурального n и простого числа p нашлось $(n+1)$ целое число, n-е степени которых дают одинаковые остатки при делении на p. Докажите, что среди этих чисел найдутся два, дающие одинаковые остатки при делении на p.

9. $f(x) \in \mathbb{Z}[x]$, $f(0) = 0$, $f(1) = 1$. Простое число p таково, что для любого целого n остаток от деления $f(n)$ на p равен 0 или 1. Докажите, что $\deg(f) \geq p-1$. (Степень $p-1$, очевидно, бывает.)