Задачи по алгебраическим структурам (SE). 2

Задача 22

(**5**) 22. а) Пусть K — поле и $f \in K[x] \setminus \{0\}$; докажите, что $|\{c \in K \mid f(c) = 0\}| \leq \deg f$.

б) Постройте такое кольцо R и такой многочлен $f \in R[x]$, что $\deg f = 1$ и $|\{r \in R \mid f(r) = 0\}| = \infty$.

в) Пусть K — поле, $G \leq K^\times$ и $|G| < \infty$; докажите, что группа G циклическая.

Выведите из этого факта существование первообразного корня по любому простому модулю.

Указание к задаче 22

22. а) Для любого коммутативного кольца R имеет место следующий факт: $\forall\, f \in R[x],\ r \in R\ \big(f(r) = 0 \Leftrightarrow$ $\Leftrightarrow$ (многочлен $x - r$ делит многочлен f)$\big)$ (доказательство такое же, как и в случае поля: нужно поделить f на $x - r$ с остатком). Докажите утверждение пункта а, используя данный факт (из доказательства должно быть видно, где используется то, что рассматриваются корни многочлена f в поле).

б) Пример, который нужно построить в пункте б, показывает, что над кольцами утверждение пункта а может быть бесконечно далеко от истины. Для того, чтобы построить нужный пример, вспомните изученные в вопросе 6 курса конструкции, которые можно применять к кольцам.

в) Обозначим через m число $\operatorname{lcm}(\{\operatorname{ord}(g) \mid g \in G\})$ и через f многочлен $x^m - 1$. Сначала докажите, что $G \subseteq \{c \in K \mid f(c) = 0\}$; затем используйте пункт а задачи 22 и пункт в задачи 21.

Задачи по алгебраическим структурам (SE). 3

Задачи

(**2**) 23. а) Выпишите явно изоморфизм колец, действующий из кольца $\mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/11$ в кольцо $\mathbb{Z}/165$ и являющийся обратным к изоморфизму, рассматриваемому в китайской теореме об остатках.

б) Решите уравнение $a^{82} = 1$ в кольце $\mathbb{Z}/165$.

(**3**) 26. Пусть $n \in \mathbb{N} \setminus \{1\}$; обозначим через p число $\min\{p \in \mathbb{P} \mid p \mid n\}$.

а) Пусть также $a \in \mathbb{Z}$ и $a^n \equiv 1 \pmod{n}$; докажите, что $a \equiv 1 \pmod{p}$.

б) Докажите, что $2^n \not\equiv 1 \pmod{n}$, а также что, если $3^n \equiv 1 \pmod{n}$, то $2 \mid n$.

(**3**) 27. Пусть $p \in \mathbb{P}$; обозначим через G группу $(\mathbb{F}_p^+)^2$ (то есть $\mathbb{F}_p^+ \times \mathbb{F}_p^+$); будем называть *прямыми, проходящими через* 0*, в плоскости над полем* $\mathbb{F}_p$ подгруппы группы G, отличные от $\{(0,0)\}$ и G.

Опишите явно все прямые, проходящие через 0, в плоскости над полем $\mathbb{F}_p$ и найдите их количество.

(**5**) 33. а) Пусть G — группа, $g \in G$ и $m \in \mathbb{N}_0$; докажите, что следующие свойства эквивалентны:

- $\operatorname{ord}(g) = m$;
- $g^m = 1 \,\wedge\, \forall p \in \mathbb{P}\ (p \mid m \Rightarrow g^{\frac{m}{p}} \neq 1)$.

б) Пусть $n \in \mathbb{N}$; докажите, что следующие свойства эквивалентны:

- $n \in \mathbb{P}$;
- $\exists\, d \in \mathbb{Z}/n\ \big(d^{n-1} = 1 \,\wedge\, \forall p \in \mathbb{P}\ (p \mid (n-1) \Rightarrow d^{\frac{n-1}{p}} \neq 1)\big)$.

Существует ли алгоритм, позволяющий для любого простого числа n найти какое-либо число d, обладающее по модулю n свойствами $d^{n-1} = 1$ и $\forall p \in \mathbb{P}\ (p \mid (n-1) \Rightarrow d^{\frac{n-1}{p}} \neq 1)$, за полиномиальное время от длины двоичной записи числа n?

в) Для каждого числа n из множества $\{15791, 1579, 263, 131, 13\}$ найдите минимальный элемент множества $\{d \in \{0, \ldots, n-1\} \mid d^{n-1} = 1 \,\wedge\, \forall p \in \mathbb{P}\ (p \mid (n-1) \Rightarrow d^{\frac{n-1}{p}} \neq 1)$ в кольце $\mathbb{Z}/n\}$.

Комментарий к пункту в: для того, чтобы найти требуемые в пункте в числа, используйте компьютер; доказывать ничего не надо; пункт в засчитывается только студентам, решившим пункты а и б.

Указания к задачам

23. Используйте китайскую теорему об остатках, малую теорему Ферма и тот факт, что для любых $p \in \mathbb{P}$ и $k \in \mathbb{Z}$ выполнено $|\{a \in \mathbb{F}_p^\times \mid a^k = 1\}| = \gcd(k, p-1)$. Пример решения аналогичной задачи был изучен на занятиях; решения, полученные перебором с помощью компьютера, не принимаются.

26. а) Используя то, что $a^n \equiv 1 \pmod{n}$, и лемму о порядке элемента, найдите $\mathrm{ord}(a)$ в группе $\mathbb{F}_p^\times$.

    б) Используйте пункт а.

27. Сначала докажите, что каждая из рассматриваемых прямых является циклической группой. Затем докажите, что для каждой, кроме ровно одной, прямой H, проходящей через 0, в плоскости над полем $\mathbb{F}_p$ существует единственный такой элемент c поля $\mathbb{F}_p$, что $H = \{(x, cx) \mid x \in \mathbb{F}_p\}$.

    Предупреждение для тех, кто знаком с линейной алгеброй над произвольными полями: задачу нужно решать, используя только материал курса (то есть элементарные знания о группах и полях).

33. а) Используйте элементарные знания о порядке элемента группы.

    б) Используйте пункт а и теорему о группах обратимых остатков (точнее, пункт в задачи 22). При ответе на вопрос о существовании алгоритма используйте информацию, о которой шла речь на занятиях.

    в) Ищите требуемые числа перебором с помощью компьютера.