Задачи по алгебраическим структурам (SE). 3

Задачи $5'$ и $6'$ предназначаются только следующим студентам: А. Крамар, Ф. Муратов, Д. Павлюченко, Ю. Фетцер и С. Целовальников.

(**2**) $5'$. Пусть G — группа и $|G| \in 2\mathbb{N}$; докажите, что $\exists\, g \in G\ (\mathrm{ord}(g) = 2)$.

(**2**) $6'$. Пусть G — группа и $|G| \in (2\mathbb{N} - 1)$.

Докажите, что отображение, действующее из G в G по правилу $g \mapsto g^2$ для любых $g \in G$, является биекцией (используйте лемму о порядке элемента и принцип Дирихле).

• В связи с тестами на простоту были введены следующие обозначения:
⋆ пусть $n \in \mathbb{N} \setminus \{1\}$; тогда $\mathrm{FT}(n) = \{a \in \mathbb{Z}/n \mid a^{n-1} = 1\}$;
⋆ пусть $n \in (2\mathbb{N}+1)$; тогда $\mathrm{ET}(n) = \{a \in \mathbb{Z}/n \mid a^{\frac{n-1}{2}} \in \{1, -1\}\}$;
⋆ пусть $n \in (2\mathbb{N}+1)$ (можно рассматривать $n \in \mathbb{N} \setminus \{1\}$); представим число $n-1$ в виде $2^{\psi} j$, где $\psi \in \mathbb{N}$ и $j \in (2\mathbb{N}+1)$; тогда $\mathrm{MRT}(n) = \{a \in \mathbb{Z}/n \mid a^j = 1 \ \vee\ \exists\, \chi \in \{0, \ldots, \psi - 1\}\ (a^{2^{\chi} j} = -1)\}$.

• Тестирование числа n на простоту заключается в проверке принадлежности выбранного случайно ненулевого остатка a по модулю n множеству $\mathrm{FT}(n)$ (тест Ферма), или множеству $\mathrm{ET}(n)$ (тест Эйлера), или множеству $\mathrm{MRT}(n)$ (тест Миллера–Рабина). Если остаток a не принадлежит соответствующему множеству, то число n заведомо непростое; если же принадлежит, то число n, возможно, простое.

Задачи

(**2**) 25. Пусть $n \in \mathbb{N}$, Y — линейно упорядоченное множество, $f \in \mathrm{Map}(\{1, \ldots, n\}, Y)$, а также $i \in \{1, \ldots, n-1\}$ и $f(i) \neq f(i+1)$; докажите, что

$$\mathrm{inv}(f\sigma_i) = \begin{cases} \sigma_i \times \sigma_i(\mathrm{inv}(f) \setminus \{(i, i+1)\}), \text{ если } (i, i+1) \in \mathrm{inv}(f); \\ \sigma_i \times \sigma_i(\mathrm{inv}(f)) \cup \{(i, i+1)\}, \text{ если } (i, i+1) \notin \mathrm{inv}(f). \end{cases}$$

(**3**) 28. Обозначим через n число 1649. а) Докажите, что $\frac{|\mathrm{FT}(n)|}{\phi(n)} = \frac{1}{6}$ и $\frac{|\mathrm{ET}(n)|}{\phi(n)} = \frac{1}{12}$ (используйте то, что $n = 17 \cdot 97$ и $n - 1 = 2^4 \cdot 103$, а также устные вычисления). б) Докажите, что $8 \in \mathrm{FT}(n) \setminus \mathrm{ET}(n)$ (используйте то, что $17 \mid (8^8 - 1)$ и $97 \mid (8^8 + 1)$, а также устные вычисления).

Пункт а задачи 28 могут сдавать все студенты, кроме А. Крамар; пункт б задачи 28 могут сдавать все студенты, кроме Д. Павлюченко и Т. Бондарева.

(**3**) 29. а) Пусть $s \in \mathbb{N} \setminus \{1\}$, $i_1, i_2, \ldots, i_s \in \mathbb{N}$ и $i_1 < i_2 < \ldots < i_s$.

Опишите явно все элементы множества $\mathrm{inv}((i_1\ i_2\ \ldots\ i_s))$ и найдите его порядок.

б) Пусть $i, j \in \mathbb{N}$ и $i < j$; запишите перестановку $(i\ j)$ в виде произведения фундаментальных транспозиций в количестве, равном $2(j - i) - 1$.

(**4**) 30. Пусть $n \in \mathbb{N}$; докажите, что следующие свойства эквивалентны:
• $\forall\, p \in \mathbb{P}\ (p^2 \nmid n)$; • $\forall\, k, l \in \mathbb{N}\ \big(k \equiv l \pmod{\phi(n)} \Rightarrow \forall\, a \in \mathbb{Z}/n\ (a^k = a^l)\big)$.

Указания к задачам

25. Указание к этой задаче было дано на лекции о симметрических группах (напоминание смысла обозначения “$\sigma_i \times \sigma_i$”: $\sigma_i \times \sigma_i(j, k) = (\sigma_i(j), \sigma_i(k))$ для любых $(j, k) \in \{1, \ldots, n\}^2$). В решении достаточно рассмотреть только первый случай (когда $(i, i+1) \in \mathrm{inv}(f)$).

28. а) Используйте китайскую теорему об остатках и комментарий к задаче 20.

б) На лекции об элементарной теории чисел были разобраны примеры аналогичных вычислений (2^{340} в кольце $\mathbb{Z}/341$ и 2^{1638} в кольце $\mathbb{Z}/3277$).

29. Для решения этой задачи достаточно понимать, что такое инверсии. В пункте б нужно использовать доказательство теоремы о разложении перестановки в произведение фундаментальных транспозиций.

30. Используйте элементарные знания из теории чисел.