Задачи по алгебраическим структурам (SE). 3

• 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.

• В задаче 34 используется следующее обозначение: для любого числа $k \in \mathbb{Z}$ и любой группы G обозначим через $\mathrm{pow}_{k,G}$ отображение, действующее из G в G по правилу $g \mapsto g^k$ для любых $g \in G$; свойства этого отображения изучались в задачах 5 и 20.

Задачи

(**2**) 24. Пусть $p \in \mathbb{P}$; докажите, что $\mathrm{MRT}(p) = \mathbb{F}_p^{\times}$.

(**3**) 28. а) Найдите такое нечетное число n в диапазоне от 3 до 4999, что $\frac{|\mathrm{ET}(n)|}{\phi(n)} = \frac{1}{8}$ и $\frac{|\mathrm{ET}(2n+3)|}{\phi(2n+3)} = \frac{1}{15}$.

б) Пусть n есть число, найденное в пункте а; докажите, что $25 \in \mathrm{FT}(n)$ и $25 \notin \mathrm{ET}(n)$.

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

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

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.

Все пункты задачи 33 могут сдавать на занятии 26.11 следующие студенты: Ю. Александров, А. Веслогузова, С. Кривохатский, А. Лазаревич, Ф. Муратов, Д. Павлюченко, С. Прошев, П. Сергеев, С. Целовальников, П. Юргин и И. Гайдай. Только пункты б и в задачи 33 могут сдавать на занятии 26.11 следующие студенты: А. Крамар, М. Москвитин и Д. Мелешко.

(**5**) 34. а) Пусть $p \in \mathbb{P} \setminus \{2\}$; докажите, что $|\operatorname{Im} \mathrm{pow}_{2,\mathbb{F}_p^{\times}}| = \frac{p-1}{2}$ и $\operatorname{Im} \mathrm{pow}_{2,\mathbb{F}_p^{\times}} = \operatorname{Ker} \mathrm{pow}_{\frac{p-1}{2},\mathbb{F}_p^{\times}}$.

б) Придумайте алгоритм, позволяющий для любого простого числа p и любого элемента a поля $\mathbb{F}_p$ выяснить, верно ли, что $a \in \operatorname{Im} \mathrm{pow}_{2,\mathbb{F}_p^{\times}}$, за полиномиальное время от длины двоичной записи числа p.

в) Пусть $p \in \mathbb{P}$; докажите, что следующие свойства эквиваленты:

• $p \bmod 4 = 3$; • $-1 \notin \operatorname{Im} \mathrm{pow}_{2,\mathbb{F}_p^{\times}}$; • $(x^2+1) \in \mathrm{Irr}(\mathbb{F}_p[x])$; • $\mathbb{F}_p[x]/(x^2+1)$ — поле.

Указания к задачам

24. Используйте то, что $\{c \in \mathbb{F}_p \mid c^2 = 1\} = \{1, -1\}$.

28. Для поиска требуемого числа n используйте компьютер. Затем докажите, что число n обладает свойствами $\frac{|\mathrm{ET}(n)|}{\phi(n)} = \frac{1}{8}$, $\frac{|\mathrm{ET}(2n+3)|}{\phi(2n+3)} = \frac{1}{15}$ и $25 \in \mathrm{FT}(n) \setminus \mathrm{ET}(n)$, используя комментарий к задаче 20.

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.

34. а) Используйте комментарий к задаче 20 и вторую теорему о подгруппах циклической группы.

   б) Используйте пункт а.

   в) В доказательстве того, что $p \bmod 4 = 3 \Leftrightarrow -1 \notin \operatorname{Im} \operatorname{pow}_{2,\mathbb{F}_p^\times}$, используйте пункт а. В доказательстве того, что $-1 \notin \operatorname{Im} \operatorname{pow}_{2,\mathbb{F}_p^\times} \Leftrightarrow (x^2+1) \in \operatorname{Irr}(\mathbb{F}_p[x])$, используйте элементарные знания о неприводимых многочленах. В доказательстве того, что $(x^2+1) \in \operatorname{Irr}(\mathbb{F}_p[x]) \Leftrightarrow (\mathbb{F}_p[x]/(x^2+1)$ — поле), используйте элементарные знания о кольцах остатков по модулю многочлена.