Задачи по алгебраическим структурам (SE)

Во всех задачах используется материал вопроса “Китайская теорема об остатках и функция Эйлера”; этот вопрос курса подробно изложен в файле `http://mit.spbau.ru/files/numbertheory.pdf`.

Задачи необходимо сдать до 15:55 11-го ноября (то есть в перерыве перед четвертой парой). Студенты подгруппы №1 должны решать задачи для подгруппы №1 и сдать их Е.Е. Горячко. Студенты подгруппы №2 должны решать задачи для подгруппы №2 и сдать их С.С. Афанасьевой. Решение задач для противоположной подгруппы не засчитывается. Будьте внимательны! (Разбиение на подгруппы указано на странице курса на сайте `http://mit.spbau.ru/sewiki/index.php/SE_Wiki`.) Слева от номера каждой задачи указано максимальное количество баллов, которое можно получить за решение данной задачи.

Задачи для подгруппы №1

(**2**) 1. Найдите $11^{17^{19}}$ в кольце $\mathbb{Z}/232$.

(**3**) 2. а) Пусть $a \in \mathbb{N} \setminus \{1\}$ и $m \in \mathbb{N}$; докажите, что m делит $\phi(a^m - 1)$.

б) Пусть $n \in \mathbb{N} \setminus \{1\}$; выразите сумму $\sum\limits_{\substack{a \in \{1,\ldots,n\},\\ \gcd(a,n)=1}} a$ через числа n и $\phi(n)$.

(**3**) 3. а) Пусть $p \in \mathbb{P} \setminus \{2\}$ и $\omega \in \mathbb{N}$, или $p = 2$ и $\omega = 2$; докажите, что $\{a \in \mathbb{Z}/p^\omega \mid a^2 = 1\} = \{1, -1\}$.

б) Пусть $\omega \in \mathbb{N} \setminus \{1, 2\}$; докажите, что $\{a \in \mathbb{Z}/2^\omega \mid a^2 = 1\} = \{1, -1, 2^{\omega-1} + 1, 2^{\omega-1} - 1\}$.

в) Пусть $n \in \mathbb{N}$; обозначим через t число $|\{p \in \mathbb{P} \mid p \mid n\}|$; докажите, что

$$|\{a \in \mathbb{Z}/n \mid a^2 = 1\}| = \begin{cases} 2^t, \text{ если } 2 \nmid n \vee (4 \mid n \wedge 8 \nmid n), \\ 2^{t-1}, \text{ если } 2 \mid n \wedge 4 \nmid n, \\ 2^{t+1}, \text{ если } 8 \mid n. \end{cases}$$

Комментарий к условию: равенство “$a^2 = 1$”, где a — элемент кольца $\mathbb{Z}/p^\omega$, или $\mathbb{Z}/2^\omega$, или $\mathbb{Z}/n$, нужно понимать как равенство в соответствующем кольце; при переходе к кольцу $\mathbb{Z}$ указанное равенство превращается в сравнение “$a^2 \equiv 1$” по соответствующему модулю.

(**4**) 4. Пусть $n \in \mathbb{N}$; докажите, что следующие свойства эквивалентны:

- $\forall\, p \in \mathbb{P}\ (p^2 \nmid n)$;
- $\forall\, k, l \in \mathbb{N}\ \big(k \equiv l \pmod{\phi(n)} \Rightarrow \forall\, a \in \mathbb{Z}/n\ (a^k = a^l)\big)$.

Задачи для подгруппы №2

(**2**) 1. Найдите $11^{17^{19}}$ в кольце $\mathbb{Z}/208$.

(**3**) 2. а) Пусть G — циклическая группа и $m \in \mathbb{N}$; докажите, что $|\{g \in G \mid \operatorname{ord}(g) = m\}| \in \{0, \phi(m)\}$.

б) Пусть $n \in \mathbb{N}$; используя пункт а, докажите, что $\sum\limits_{m \in \mathbb{N},\, m \mid n} \phi(m) = n$.

(**3**) 3. а) Пусть $p \in \mathbb{P}$ и $\omega \in \mathbb{N}$; докажите, что $\{a \in \mathbb{Z}/p^\omega \mid a^2 = a\} = \{0, 1\}$.

б) Пусть $n \in \mathbb{N}$; обозначим через t число $|\{p \in \mathbb{P} \mid p \mid n\}|$; выразите число $|\{a \in \mathbb{Z}/n \mid a^2 = a\}|$ через t.

Комментарий к условию: равенство “$a^2 = a$”, где a — элемент кольца $\mathbb{Z}/p^\omega$ или $\mathbb{Z}/n$, нужно понимать как равенство в соответствующем кольце; при переходе к кольцу $\mathbb{Z}$ указанное равенство превращается в сравнение “$a^2 \equiv a$” по соответствующему модулю.

(**4**) 4. а) Пусть G, J — группы и $f \in \operatorname{Hom}(G, J)$; обозначим через $\operatorname{Ker} f$ подмножество $f^{-1}(1)$ группы G; докажите, что $\operatorname{Ker} f \leq G$. Пусть дополнительно $j \in J$ и $g \in f^{-1}(j)$; докажите, что $f^{-1}(j) = g \operatorname{Ker} f$.

б) Пусть G — циклическая группа, $d \in G$, $G = \langle d \rangle$, $|G| < \infty$, $k \in \mathbb{Z}$, а также $y \in \mathbb{Z}$ и $\gcd(k, |G|)$ делит y. Обозначим через H подгруппу $\{g \in G \mid g^k = 1\}$ группы G и, используя соотношение Безу, представим число $\gcd(k, |G|)$ в виде $uk + v|G|$, где $u, v \in \mathbb{Z}$; докажите, что $\{g \in G \mid g^k = d^y\} = d^{\frac{uy}{\gcd(k,|G|)}} H$.

Комментарий к условию: $\operatorname{Hom}(G, J)$ — множество гомоморфизмов, действующих из G в J; $g \operatorname{Ker} f$ — класс смежности элемента g по подгруппе $\operatorname{Ker} f$ ($g \operatorname{Ker} f = \{gh \mid h \in \operatorname{Ker} f\}$).

Указания к задачам

1. Смотрите пример, разобранный в файле `http://mit.spbau.ru/files/numbertheory.pdf`.

2. а) Указание для подгруппы №1: используйте то, что для любого $n \in \mathbb{N}$ верно $|(\mathbb{Z}/n)^\times| = \phi(n)$, а также лемму о порядке элемента. Указание для подгруппы №2: используйте то, что для любого $n \in \mathbb{N}$ верно $|\{a \in (\mathbb{Z}/n)^+ \mid \mathrm{ord}(a) = n\}| = \phi(n)$, а также теоремы о подгруппах циклической группы.

   б) Указание для подгруппы №1: используйте определение функции Эйлера; пункты а и б независимы.

3. В последнем пункте задачи используйте китайскую теорему об остатках и предыдущие пункты.

   Предостережение для подгруппы №1: теоремы, которые еще не были доказаны на лекциях (например, теорему о группах обратимых остатков), использовать нельзя!

4. Указание для подгруппы №1: используйте китайскую теорему об остатках и теорему Эйлера. Указание для подгруппы №2: используйте элементарные знания о группах, гомоморфизмах групп и подгруппах; в решении пункта б используйте пункт а.