Определение 1. *Алгеброй* (более точно, алгеброй над $\mathbb{R}$) называется множество A, содержащее в себе множество $\mathbb{R}$, на котором заданы операции сложения и умножения, удовлетворяющие следйющим свойствам:

- A является абелевой группой по сложению, в которой $0 \in \mathbb{R} \subseteq A$ выступает нулём.
- Умножение дистрибутивно относительно сложения, а элемент $1 \in \mathbb{R} \subseteq A$ выступает единицей.
- Операции над вещественными числами в A такие же, как обычно, и $at = ta$ для всех $a \in A$, $t \in \mathbb{R}$.

Алгебра называется ассоциативной (коммутативной), если умножение в ней ассоциативно (коммутативно). Алгебра называется алгеброй с делением, если для любых $a, b \in A, a \neq 0$ существуют и единственны левые и правые частные, то есть такие элементы b/a и $a \setminus b$, что $(b/a)a = b$ и $a(a \setminus b) = b$.

Задача 1. **а)** Докажите, что всякая алгебра является векторным пространством над $\mathbb{R}$, если задать умножение на число с помощью умножения в алгебре. **б)** Придумайте какую-нибудь двумерную алгебру, кроме $\mathbb{C}$. **в)** Придумайте алгебру произвольной конечной размерности.

Определение 2. *Кватернионы* – это выражения вида $a+bi+cj+dk$, $a, b, c, d \in \mathbb{R}$ которые складываются покоординатно, а умножаются по следующей таблице:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Запомнить её можно, например, так: расположите мнимые единицы $i \to j \to k \to i$ по кругу, тогда произведение каждой мнимой единицы на следующую равно третьей, а произведение мнимой единицы на предыдущую равно третьей со знаком минус. Множество всех кватернионоы обозначается $\mathbb{H}$. Число a называется *скалярной частью* кватерниона, а выражение $bi+cj+dk$ – *векторной частью*. Кватернион с нулевой вещественной частью называется *чисто мнимым*. Если выбрать в трёмхерном пространстве базис, состоящий из трёх единичных взаимно перпендикулярных векторов i, j, k, то векторную часть кватерниона можно рассматривать как вектор в трёхмерном пространстве.

Задача 2. **а)** Докажите, что кватернионы образуют ассоциативную, но не коммутативную алгебру. **б)** Дадим альтернативное определение кватернионов: кватернионы – это формальные записи от двух переменных i, j (например, $\sqrt{2\pi} - 7ijiji + j^{17}$), которые можно преобразовывать по правилам $i^2 = j^2 = -1, ij = -ji$. Докажите, что если положить $k = ij$, то любой кватернион приводится к виду $a + bi + cj + dk$, и что это определение эквивалентно предыдущему.

Определение 3. *Векторным произведением* двух векторов u и v в $\mathbb{R}^3$ называется вектор $[u, v]$, перпендикулярный плоскости векторов u и v и имеющий длину $|u| \cdot |v| \cdot \sin\varphi$.

Задача 3. **а)** Вычислите $(a + bi + cj + dk)^2$ и убедитесь, что квадрат кватерниона вещественный тогда и только тогда, когда сам кватернион чисто мнимый. **б)** Пусть u и v – два чисто мнимых кватерниона. Докажите, что $uv = -(u, v) + [u, v]$, где $(-,-)$ — скалярное произведение, а $[-,-]$ — векторное произведение.

Задача 4. Выясните, в какие тождества для скалярного и векторного произведения превращается ассоциативность кватернионного умножения $(uv)w = u(vw)$ и докажите тождество Якоби, $[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0$.

Задача 5. Найдите все такие $z \in \mathbb{H}$, что $zq = qz$ для любого $q \in \mathbb{H}$.

Задача 6. Может ли многочлен с вещественными коэффициентами иметь бесконечно много корней в $\mathbb{H}$?

1 а	1 б	1 в	2 а	2 б	3 а	3 б	4	5	6

Определение 4. Пусть $q \in \mathbb{H}$, $q = a + bi + cj + dk$. Кватернион $a - bi - cj - dk$ называется *сопряжённым* к q, и обозначается $\overline{q}$. Число $\sqrt{a^2 + b^2 + c^2 + d^2}$ называется *модулем* кватерниона q и обозначается $|q|$.

Задача 7. Докажите, что: **а)** $\overline{(q_1 + q_2)} = \overline{q_1} + \overline{q_2}$, $\overline{q_1 q_2} = \overline{q_2 q_1}$. **б)** $q\overline{q} = \overline{q}q = |q|^2$, $|q_1 q_2| = |q_1||q_2|$, **в)** $\mathbb{H}$ является алгеброй с делением.

Задача 8. **а)** Докажите, что не существует такого многочлена P с комплексными коэффициентами, что $P(z) = \overline{z}$ для любого комплексного z. **б)** Найдите такой "некоммутативный многочлен" от q, то есть выражение, использующее только операции сложения и умножения q на фиксированные кватернионы, которое выражает $\overline{q}$ через q.

Задача 9. **а)** Докажите, что если два целых числа представимы в виде суммы четырёх квадратов, то и их произведение тоже. **б)** Для сумм трёх квадратов это неверно.

С помощью кватернионов мы доказали, что существует представление вида $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = P_1^2 + P_2^2 + P_3^2 + P_4^2$, где P_1, P_2, P_3, P_4 – линейные функции от $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$. Аналогичное представление для сумм n квадратов возможно только при $n = 1, 2, 4, 8$. Последнее происходит аналогичным образов из неассоциативной и некоммутативной восьмимерной алгебры с делением $\mathbb{O}$.

Определение 5. Кватернион $a + bi + cj + dk$ называется *рациональным*, если $a, b, c, d \in \mathbb{Q}$, и *целым гурвицевым*, если числа a, b, c, d либо одновременно целые, либо одновременно полуцелые.

Задача 10. **а)** Докажите, что q – целый гурвицев кватернион тогда и только тогда, когда его *след* $q + \overline{q}$ и *норма* $q\overline{q}$ – целые числа. **б)** Проверьте, что аналогичное условия для комплексных чисел задаёт в точности целые гауссовы числа. **в)** Сколько существует целых гурвицевых кватернионов, по модулю равных единице? **г)** Проверьте, что целые гурвицевы кватернионы, по модулю равные единице, образуют группу по умножению. Эта группа называется *бинарной группой тетраэдра* b обозначается T^*. Какие порядки бывают у элементов этой группы? (Напомним, что порядок элемента g – это наименьшее такое число n, что $g^n = 1$.)

Задача 11. **а)** Пусть $\theta = \frac{1+i}{\sqrt{2}}$. Докажите, что $O^* = T^* \cup \{\theta t : t \in T^*\}$ – конечная группа. Она называется *бинарной группой октаэдра*. Какие порядки могут быть у её элементов? **б)** Пусть $\zeta = \frac{1}{2}(\frac{1-\sqrt{5}}{2} + i + \frac{1+\sqrt{5}}{2}j)$. Докажите, что $I^* = \{\zeta^k t : k \in \mathbb{Z}, t \in T^*\}$ – конечная группа. Она называется *бинарной группой икосаэдра*. Найдите количество элементов в I^* и все встречающиеся в ней порядки элементов.

Задача 12. **а)** Докажите, что для любого кватерниона q найдётся такой целый гурвицев кватернион α, что $|q - \alpha| < 1$. **б)** Докажите, что если α, β – целые гурвицевы, то найдётся такое целое гурвицево γ, что $|\beta - \alpha\gamma| < |\alpha|$ (и, вообще говоря, другое γ', такое, что $|\beta - \gamma'\alpha| < |\alpha|$). **в)** Целое гурвицево число π назовём *неприводимым*, если его нельзя представить в виде $\pi = \gamma\delta$, где $|\gamma|, |\delta| > 1$. Докажите *лемму Евклида* для целых гурвицевых чисел: если произведение $\alpha\beta$ делится на π *слева* (*справа*), то есть $\alpha\beta = \pi\varrho$ ($\alpha\beta = \varrho\pi$), то и одно из чисел α или β делится на π слева (справа).

Задача 13. **а)** Пусть p – нечётное простое число. Докажите, что если $a^2 \equiv b^2 (\mathrm{mod}\ p)$, то либо $a \equiv b (\mathrm{mod}\ p)$, либо $a \equiv -b (\mathrm{mod}\ p)$. Сколько элементов в $\mathbb{Z}/p\mathbb{Z}$ являются квадратами? **б)** Докажите, что сравнение $x^2 \equiv 1 - y^2 (\mathrm{mod}\ p)$ имеет решение в целых числах. **в)** Докажите, что p не является простым в целых гурвицевых числах (*указание:* если x, y как выше, то p и $1 - xi - yj$ не взаимно просты). **г)** Докажите, что любое целое число представляется в виде суммы четырёх квадратов.

7 а	7 б	7 в	8 а	8 б	9 а	9 б	10 а	10 б	10 в	10 г	11 а	11 б	12 а	12 б	12 в	13 а	13 б	13 в	13 г