Примеры полей и коммутативных колец

А2◇1. В поле $\mathbb{C}$ явно вычислите $\operatorname{Re} z$, $\operatorname{Im} z$, $|z|$, $\operatorname{Arg} z$, если **а)** $z = (5+i)(7-6i)/(3+i)$
б) $z = (1+i)^5/(1-i)^3$ **в)** $\left((\sqrt{3}+i)/(1-i)\right)^{30}$ **г)** $z^2 = a + ib$, где $a, b \in \mathbb{R}$ даны.

А2◇2. Выразите $\sin 5\varphi$ через $\sin\varphi$ и получите для $\sin(4\pi/5)$ и $\cos(2\pi/5)$ явные выражения в радикалах от рациональных чисел.

А2◇3. В поле $\mathbb{C}$ вычислите **а)** $z^m + z^{-m}$, если $z + z^{-1} = 2\cos\vartheta$, где $\vartheta \in \mathbb{R}$ дано
б) сумму **в)** произведение s-тых степеней всех корней степени n из 1 (для всех $n, s \in \mathbb{N}$).

А2◇4. Вычислите суммы: **а)** $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$ **б)** $\binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots$ **в)** $\sin x + \sin 2x + \cdots + \sin nx$.

А2◇5 (Гауссовы целые числа). Найдите все обратимые элементы *Гауссовых колец*
а) $\mathbb{Z}[i] \overset{\text{def}}{=} \{\, a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z},\ i^2 = -1 \}$ **б)** $\mathbb{Z}[\omega] \overset{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\,\}$.

А2◇6 (кольца вычетов). Составьте таблицы умножения для колец $\mathbb{Z}/(m)$ с $4 \leqslant m \leqslant 8$. В каждом из них найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

А2◇7. Пусть $f : A \to B$ — ненулевой гомоморфизм коммутативных колец с единицами. Верно ли, что $f(1) = 1$? А если в B нет делителей нуля?

А2◇8 (взаимная простота). Пусть $ax + by = 1$ в некотором коммутативном кольце A. Справедливы ли для произвольного $m \in A$ импликации: **а)** $a|mb \Rightarrow a|m$ **б)** $a|m \;\&\; b|m \Rightarrow ab|m$.

А2◇9. Является ли кольцо $\mathbb{R}[x]/(f)$ полем для **а)** $f = x^4 + 1$ **б)** $f = x^3 + 1$ **в)** $f = x^2 + 3$?

А2◇10 (функция Эйлера). Обозначим через $\varphi(n)$ число обратимых элементов кольца $\mathbb{Z}/(n)$. Покажите, что **а)** $k \pmod n$ обратим в $\mathbb{Z}/(n) \iff$ нод$(n,k) = 1$ в $\mathbb{Z}$
б) φ является *мультипликативным характером*[1]
в) $\varphi(m) = m \cdot \left(1 - p_1^{-1}\right) \cdots \left(1 - p_n^{-1}\right)$ для $m = p_1^{k_1} \cdots p_n^{k_n}$, где все p_i просты и различны.

А2◇11. Найдите все $m \in \mathbb{N}$ с $\varphi(m) = 10$.

А2◇12 (теорема Эйлера). Вычислите $a^{\varphi(n)}$ для произвольного обратимого $a \in \mathbb{Z}/(n)$.

А2◇13 (поле $\mathbb{F}_p$). Пусть $\mathbb{F}_p \overset{\text{def}}{=} \mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое. **а)** Покажите, что $\mathbb{F}_p$ — поле.
б) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов $\mathbb{F}_p$ и докажите *теорему Вильсона*: натуральное $m \geqslant 2$ просто $\iff m \mid ((m-1)!+1)$.
в) Какие значения принимают многочлены $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на $\mathbb{F}_p$ и на квадратах из $\mathbb{F}_p$?
г) Сколько в $\mathbb{F}_p$ ненулевых квадратов? Всегда ли в $\mathbb{F}_p$ разрешимо уравнение $x^2 + y^2 = -1$?
д*) Выпишем $\mathbb{F}_p$ в виде: $-(p-1)/2\,,\ \ldots\,,\ -1\,,\ 0\,,\ 1\,,\ \ldots\,,\ (p-1)/2$. Докажите *лемму Гаусса*: $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» при умножении на a, чётно.

А2◇14. При каких p в $\mathbb{F}_p$ разрешимы уравнения[2] **а)** $x^2 = -1$ **б)** $x^2 = 2$

А2◇15*. Есть ли среди фактор колец кольца $\mathbb{Z}[i]$ поле характеристики **а)** 2 **б)** 3, и если да, то сколько в нём может быть элементов?

А2◇16*. При каком простом p существует ненулевой гомоморфизм $\mathbb{Z}[i] \to \mathbb{Z}/(p)$?

А2◇17*. Разложите 5 на неприводимые[3] множители в кольце $\mathbb{Z}[i]$. Какие неприводимые $p \in \mathbb{Z}$ остаются таковыми и в $\mathbb{Z}[i]$?

---

[1] функция $f : \mathbb{Z} \to \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)\ \forall\, m, n$ с нод$(m,n) = 1$

[2] ответы: в (а) — $p = 2$ и $p \equiv 1 \pmod 4$; в (б) — когда $(p^2-1)/8$ чётно

[3] элемент коммутативного кольца с единицей называется *приводимым*, если он является произведением двух необратимых элементов

Персональный табель ______________________________________ . Листок № 2 (4 сентября 2013)
(напишите свои фамилию, имя и отчество)

№	дата сдачи	имя и фамилия принявшего	подпись принявшего
1а			
б			
в			
г			
2			
3а			
б			
в			
4а			
б			
в			
5а			
б			
6			
7			
8а			
б			
9			
10			
11			
12			
13			
14			
15			
16			
17			