Задача 1. $(a+bi)+(c+di)=(a+c)+(b+d)i$
$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$.

Упражнение 1. Делители единицы имеют норму 1 и находятся перебором.

Задача 2. Докажем деление с остатком по норме $N(a+bi)=(a+bi)(a-bi)=a^2+b^2$ в целых гауссовых числах: если $x,y\in\mathbb{Z}[i]$ и $y\neq 0$, то существуют $r,t\in\mathbb{Z}[i]$, такие что $x=yr+t$ и $N(t)<N(y)$.

Доказательство в алгебраической интерпретации: пусть $x=a+bi$ и $y=c+di$, тогда $x/y=(a+bi)/(c+di)=(a+bi)(c-di)/(c^2+d^2)=((ac+bd)+(bc-ad)i)/(c^2+d^2)=n+mi+(k+li)/(c^2+d^2)$, где n,m,k,l — целые, и $|k|,|l|\leq(c^2+d^2)/2$ (обычное деление с остатком $ac+bd$ и $bc-ad$ на c^2+d^2). Значит, $a+bi=(c+di)(n+mi)+(k+li)(c+di)/(c^2+d^2)$, причем $(k+li)(c+di)/(c^2+d^2)\in\mathbb{Z}[i]$ и $N(k+li)=k^2+l^2\leq(c^2+d^2)^2/2$, поэтому $N((k+li)(c+di)/(c^2+d^2))=N(k+li)N(c+di)/N(c^2+d^2)\leq N(c+di)/2$. Значит, $r=n+mi$ и $t=(k+li)(c+di)/(c^2+d^2)$ — подходят.

В геометрической интерпретации это доказательство выглядит так: множество целых гауссовых чисел, кратных y, выглядит на плоскости комплексных чисел как квадратная решетка, натянутая на векторы y и yi, которые имеют равную длину и ортогональны друг другу. Это решетка естественным образом разбивает плоскость на квадраты со стороной, равной длине вектора y, то есть $\sqrt{c^2+d^2}=\sqrt{N(y)}$. В частности, вектор x лежит в каком-то из этих квадратов, и мы можем выбрать его вершину $z=rb$ такую, что расстояние от неё до x — минимальное. Тогда расстояния e и f от z до проекций x на стороны квадрата, прилежащие к z, не больше половины стороны квадрата, и квадрат расстояния $|x-z|^2=e^2+f^2\leq(c^2+d^2)/2=N(y)/2$, поэтому $r=z/b$ и $t=x-z$ — подходят.

Из деления с остатком теперь легко доказать основную теорему арифметики. Заметим, что если p — простое и x не делится на p, то применяя к x и p алгоритм Евклида, мы получим $ax+bp=1$ для каких-то a и b. Далее, если xy делится на p, то x или y делятся на p — действительно, иначе $ax+bp=1$ и $cy+dp=1$ для каких-то a,b,c,d, поэтому $acxy=(1-bp)(1-dp)=1+p(bd-b-d)$ делится на p, противоречие.

Для любого z существует можно построить какое-то разложение на простые, просто раскладывая его на сомножители, отличны от делителей единицы (норма уменьшается, поэтому процесс когда-нибудь закончится). Если есть два различных разложения на простые, то сначала сократим на одинаковые простые, а потом для произвольного оставшегося простого p получим, что он делит произведение отличных от него простых, что невозможно (достаточно несколько раз применить то, что если xy делится на p, то x или y делятся на p).

Задача 3. Заметим, что если n делится на 2, то $x = 0$, т.к. разность квадратов натуральных чисел делится на их сумму, которая больше 1. Значит, если n делится на 2, то $x = 0$ и $y = \pm 1$.

Если n не делится на 2, то разложим в целых гауссовых числах $x^2+1 = (x+i)(x-i) = y^n$. Заметим, что $2|x$, т.к. иначе $x^2+1 \equiv 2 \mod 4$, а $y^n \not\equiv 2 \mod 4$ при $n > 1$. Значит, $\gcd(x+i, x-i) = \gcd(2i, x-i) = \gcd(2i, -i) = 1$, то есть $x+i$ и $x-i$ взаимно просты. Значит, из единственности разложения на множители, $x+i = \varepsilon z^n$, где $z \in \mathbb{Z}[i]$, а ε — делитель единицы в $\mathbb{Z}$, то есть $\varepsilon \in \{1, -1, i, -i\}$. Но n не делится на 2, так что после умножения z на делитель единицы можно считать, что $x + i = z^n$. Пусть $z = a + bi$, тогда $i = \operatorname{Im} z^n = i(na^{n-1}b - \binom{n}{3}a^{n-3}b^3 + \ldots + (-1)^{\frac{n-1}{2}}b^n)$. Значит, 1 делится на b, то есть $b = \pm 1$. Заметим, что a делится на 2, т.к. иначе $z = a + bi \equiv 1 + i \mod 2$, поэтому $z^2 \equiv (1+i)^2 \equiv 0 \mod 2$ и $x^2 + 1 = z^n \equiv 0 \mod 2$, но x делится на 2, противоречие. Если $a = 0$, то $x + i = \pm i$, поэтому $x = 0$ и $y = 1$.

Если $a \neq 0$, то $1 \equiv (-1)^{\frac{n-1}{2}}b^n \mod 4$, поэтому $1 = (-1)^{\frac{n-1}{2}}b^n$ и $0 = \binom{n}{n-2} + \ldots + (-1)^{\frac{n-5}{2}}\binom{n}{3}a^{n-5} + (-1)^{\frac{n-3}{2}}na^{n-3} = \binom{n}{2} + \ldots + (-1)^{\frac{n-5}{2}}\binom{n}{n-3}a^{n-5} + (-1)^{\frac{n-3}{2}}\binom{n}{n-1}a^{n-3}$. Докажем, что все слагаемые в этой сумме, кроме $\binom{n}{2}$, делятся на степень 2, большую, чем $\binom{n}{2}$ — из этого очевидно следует, что равенство невозможно. Для этого заметим, что

$$\binom{n}{2k}a^{2k-2} = \binom{n}{2}\binom{n-2}{2k-2}\frac{2a^{2k-2}}{(2k-1)2k} = \binom{n}{2}\binom{n-2}{2k-2}\frac{(a/2)^{2k-2}}{2k-1}\frac{2^{2k-2}}{k}$$

и $2^{2k-2} > k$ при $k \geq 2$, из чего следует предыдущее утверждение. Значит, уравнение не имеет других решений, кроме $x = 0, y = 1$ при любом $n \geq 2$, и $x = 0, y = -1$ при четном n.

Задача 4. а) Если $p = 2$, то $p = (1+i)(1-i)$, поэтому p не простое в гауссовых целых числах.

Если $p = 4k+3$, то предположим противное, т.е. p не простое гауссово число. Тогда пусть $p = q_1 q_2 \ldots q_n$ — разложение на простые. Заметим, что $\bar{p} = p = \bar{q}_1 \ldots \bar{q}_n$, поэтому p делится на сопряженные к своим простым делителям. Заметим, что сопряженное к простому также простое (иначе его разложение можно снова сопрячь), и в нашем случае оно отличается от исходного (с точностью до домножения на делитель единицы). Действительно, иначе при $q = a + bi$ число $q/\bar{q} = (a+bi)/(a-bi) = ((a^2-b^2)+2abi)/(a^2+b^2)$ должно быть целым гауссовым, что возможно только в случаях $a = \pm b$ и $ab = 0$ (т.к. $|2ab| \leq a^2 + b^2$). В первом случае q делится на $1+i$, поэтому $p\bar{p} = p^2$ делится на $(1+i)(1-i) = 2$, противоречие. Во втором случае можно считать, что q — натуральное (с точностью до домножения на делитель единицы), но p простое в целых

числах, поэтому $q = p$ и p — простое в целых гауссовых, противоречие.

Значит, q и $\bar{q}$ — различные простые (q — простой делитель p в целых гауссовых), и p делится на оба. Значит, p делится на $q\bar{q} = a^2 + b^2$, и т.к. p — простое в целых числах, то $p = a^2 + b^2$. Но как известно, простое p вида $4k + 3$ нельзя представить в виде суммы двух квадратов (посмотрим на остатки по модулю 4), противоречие.

Если $p = 4k + 1$, то (как известно) -1 является вычетом по модулю p, поэтому существует натуральное n такое, что $n^2 + 1 = (n + i)(n - i)$ делится на p. Если бы p было простым гауссовым, то $n + i$ или $n - i$ делилось бы на p, что очевидно не верно. Значит, p не простое гауссово.

б) Пусть $n = a^2 + b^2 = (a + bi)(a - bi)$ и $m = c^2 + d^2 = (c + di)(c - di)$, тогда $nm = ((a+bi)(c+di))((a-bi)(c-di)) = ((ac-bd)+(ad+bc)i)((ac-bd)-(ad+bc)i)) = (ac - bd)^2 + (ad + bc)^2$.

в) Рассмотрим минимальное такое n, что $n = x^2 + y^2$ для целых x и y, и при этом не удовлетворяет условию теоремы 2. Тогда n делится на какое-то простое $p = 4k + 3$ в нечетной степени. Но т.к. -1 невычет по модулю p, то из того, что $x^2 + y^2$ делится на p, следует, что x и y делятся на p. Значит, n делится на p^2 и $n/p^2 = (x/p)^2 + (y/p)^2$, причем n/p^2 делится на p в нечетной степени, что противоречит минимальности n. Значит, если натуральное $n = x^2 + y^2$, то оно удовлетворяет условию теоремы 2.

Обратно, если n удовлетворяет условию теоремы 2, то из пункта б) достаточно показать, что 2, простое $p = 4k+1$ и p^2 для простого $p = 4k+3$ — представимы в виде суммы двух квадратов. Действительно, $2 = 1^2+1^2$, $p^2 = p^2 + 0^2$ для любого p, а $p = 4k + 1$ — составное в целых гауссовых, поэтому делится на гауссово простое $q = a + bi$, причем (аналогично пункту а)) $q \neq \pm 1 \pm i$ и $ab \neq 0$, поэтому p делится на $q\bar{q} = a^2 + b^2$. Значит, $p = a^2 + b^2$ из простоты p в целых числах.

Задача 5. Будем считать, что n удовлетворяет условию теоремы 2 (т.е. представляется хотя бы одним способом). Тогда, как видно из решения задачи 4, для любого представления n в виде суммы $x^2 + y^2$ — мы можем сократить на все простые вида $4k + 3$, поэтому можно считать, что n не делится на простые вида $4k + 3$ (число представлений от этого не изменится). Пусть $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_m^{\alpha_m}$ – разложение на простые в целых числах, тогда, как видно из решения задачи 4, его разложения в целых гауссовых будет иметь вид $n = (1 + i)^{\alpha_0}(1 - i)^{\alpha_0} q_1^{\alpha_1}(\bar{q}_1)^{\alpha_1} \dots q_m^{\alpha_m}(\bar{q}_m)^{\alpha_m}$, где q_i — простой делитель p_i. Каждому представлению n в виде суммы двух квадратов соответствует разложение $n = (x + yi)(x - yi) = z\bar{z}$, где $z = x + yi$ определено с точность до домножения на делители единицы и сопряжения. Количество способов составить z с точностью до делителей единицы, как видно из разложения n на простые гауссовы, равно

$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ (т.к. $1+i$ и $1-i$ — одинаковые простые). При сопряжении z совпадает с собой (с точностью до делителя единицы) тогда и только тогда, когда z делится на каждое простое в степени, в 2 раза меньшей степени вхождения в n. Такое возможно только в том случае, когда все $\alpha_1,\dots,\alpha_m$ — четные, т.е. $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ — нечетное. Значит, окончательная формула количества представлений n в виде суммы двух квадратов — $\lfloor((\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)+1)/2\rfloor$.

Задача 6. Докажем, что уравнение $x^3+y^3+z^3=0$ с $xyz\neq 0$ не имеет решений в целых числах. Предположим противное, тогда после сокращения на $\gcd(x,y,z)$ можем считать, что x,y,z взаимно просты в совокупности (а значит, и попарно). Если xyz не делится на 3, то $x^3,y^3,z^3\equiv\pm1 \mod 9$, поэтому $x^3+y^3+z^3\not\equiv 0 \mod 9$. Значит, одно из x,y,z делится на 3 (из взаимной простоты — ровно одно) – без ограничения общности z делится на 3. Заменяя z на $-z$, получаем уравнение $x^3+y^3=z^3$, где z делится на 3. Далее будем работать в $\mathbb{Z}[\xi]$, где $\xi=\frac{-1+\sqrt{-3}}{2}$, и обозначим $\pi=1-\xi$ – простое число, такое что $\pi\bar{\pi}=-\xi^2\pi^2=3$.

Докажем, что если для взаимно простых $x,y,z\in\mathbb{Z}[\xi]$ выполнено $x^3+y^3=uz^3$, где u — делитель единицы, и z делится π, то z делится на π^2. Действительно, $x^3+y^3=(x+y)(x+\xi y)(x+\xi^2y)=(x+y)(x+y-\pi y)(x+y+\pi y-\xi^2\pi^2y)$, поэтому из того, что $x^3+y^3=uz^3$ делится на π, следует, что $x+y$ делится на π, значит, все 3 множителя в разложении делятся на π, причем $x+y\not\equiv x+y-\pi y\not\equiv x+y+\pi y \mod \pi^2$ (т.к. y не делится на π), и каждое число в $\mathbb{Z}[\xi]$ очевидно сравнимо с $0,1$ или 2 по модулю $\pi=1-\xi$. Значит, один из этих множителей делится на π^2, поэтому uz^3 делится на π^4. Значит, z делится на π^2.

Теперь докажем, что если для взаимно простых $x,y,z\in\mathbb{Z}[\xi]$ выполнено $x^3+y^3=uz^3$, где u – делитель единицы, z делится π^k и не делится на π^{k+1} с $k\geq 2$, то существуют взаимно простые $x_1,y_1,z_1\in\mathbb{Z}[\xi]$ с $x_1^3+y_1^3=u_1z_1^3$, где u_1 — делитель единицы, z делится π^{k-1} и не делится на π^k. Разложением $x^3+y^3=(x+y)(x+\xi y)(x+\xi^2y)=(x+y)(x+y-\pi y)(x+y+\pi y-\xi^2\pi^2y)=uz^3$ мы снова получаем, что все 3 множителя в разложении делятся на π, причем ровно один из них делится на π^2 (а значит, на π^{3k-2}). После домножения y на ξ или ξ^2 можно считать, что $x+y$ делится на π^{3k-2}.

Из единственности разложения получаем, что $x+y=u_1\pi^{3k-2}a^3$, $x+\xi y=u_2\pi b^3$, $x+\xi^2y=u_3\pi c^3$, где u_i — делители единицы, и a,b,c не делятся на π. Из равенства $0=(x+y)+\xi(x+\xi y)+\xi^2(x+\xi^2y)$ получаем $u_1\pi^{3k-2}a^3+\xi u_2\pi b^3+\xi^2u_3\pi c^3=0$. После сокращения уравнение можно привести к виду $b^3+u_4c^3=u_5(a\pi^{k-1})^3$, где u_4 и u_5 — делители единицы. Докажем, что $u_4=\pm1$. Действительно, заметим, что если $b=n+m\xi$,

где n, m целые числа, то $b^3 = (n + m\xi)^3 \equiv n^3 + m^3 \equiv \pm 1 \mod 3$, т.к. b не делится на π. Аналогично $c^3 \equiv \pm 1 \mod 3$, и $(\pi^{k-1})^3$ делится на 3 из $k \geq 2$. Значит, $\pm 1 \pm u_4$ делится на 3, поэтому $u_4 = \pm 1$. После замены c на $u_4 c$ получаем $b^3 + c^3 = u_5(a\pi^{k-1})^3$, откуда мы получаем нужные x_1, y_1, z_1.

Теперь можно рассмотреть целочисленное решение $x^3 + y^3 = z^3$ с z, делящимся на 3, и спуском по степени вхождения π в z получить противоречие, т.к. z делится на π^2.

Упражнение 2. Имеем $x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$ и решаем квадратное уравнение.

Задача 7. Заметим, что для $a = x + yi \in \mathbb{Z}[\xi]$ стандартная норма $N(a) = x^2 + y^2$ будет целой, т.к. $a = (z + \sqrt{-3}t)/2$, где z и t — одной четности. Для ненулевого $a \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ числа, кратные a, образуют решетку в плоскости комплексных чисел, разбивающую её на правильные треугольники со стороной $|a|$. Для любой точки в таком треугольнике квадрат расстояния от неё до любой вершины (кроме остальных в том случае, когда точка совпадает с вершиной) меньше $|a|^2 = N(a)$, откуда следует деление с остатком по норме комплексных чисел (чтобы поделить b на a с остатком, надо вычесть из b ближайшее к нему на комплексной плоскости число вида ac). Аналогично задаче 2, отсюда мы получаем основную теорему арифметики для $\mathbb{Z}[\xi]$.

Задача 8. Для делителей единицы в $\mathbb{Z}[\xi]$ норма должна быть 1 (т.к. у обратного норма должна быть целой). Для $a = (x + \sqrt{-3}y)/2 \in \mathbb{Z}[\xi]$ – $N(a) = (x^2 + 3y^2)/4$, поэтому если a — делитель единицы, то $-2 \leq x \leq 2$ и $-1 \leq y \leq 1$. Перебором получаем, что все делители единицы в $\mathbb{Z}[\xi]$ – это $\pm 1, \pm\xi$ и $\pm\xi^2$.

Упражнение 3. а) Замкнутость относительно умножения следует из равенства $(x + y\sqrt{d})(z + t\sqrt{d}) = (xz + dyt) + (xt + yz)\sqrt{d}$.
б) $\frac{x+y\sqrt{d}}{z+t\sqrt{d}} = \frac{(xz-dyt)+(yz-xt)\sqrt{d}}{z^2-dt^2}$.

Упражнение 4. ξ является целым в $\mathbb{Q}[\sqrt{-3}]$. $\frac{1+i}{2}$ не является целым в $Z[i]$.

Упражнение 5. Очевидно.

Упражнение 6. а) $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha) = (x - \alpha)(x - \bar{\alpha})$. Подставляя в $x = \alpha$, получаем ноль.
б) Вычисление.

Задача 9. По предыдущему упражнению $x + y\sqrt{d}$ цело в $\mathbb{Q}[\sqrt{d}]$ тогда и только тогда, когда числа $2x$ и $x^2 - dy^2$ целы. Легко проверить, что для элементов $Z[\omega]$ это условие выполнено.
Пусть числа $2x$ и $x^2 - dy^2$ целы. Если x целое, то dy^2 целое, откуда y целое и $x + y\sqrt{d} \in Z[\omega]$. Если $x = n/2$, где n нечетно, то $4dy^2$ целое,

откуда $y = m/2$, где m целое. При этом $dm^2 \equiv n^2 \equiv 1 \bmod 4$, откуда m нечетно и $d \equiv 1 \bmod 4$. Тогда $x + y\sqrt{d} = m\omega + (n-m)/2 \in \mathbb{Z}[\omega]$.

Упражнение 7. Если $N(\gamma) = \pm 1$, то $\frac{1}{\gamma} = \pm\bar{\gamma} \in \mathbb{Z}[\omega]$.
Если $\frac{1}{\gamma} \in \mathbb{Z}[\omega]$, то $1 = N(1) = N(\gamma\frac{1}{\gamma}) = N(\gamma)N(\frac{1}{\gamma})$, откуда $N(\gamma) = \pm 1$, поскольку $N(\frac{1}{\gamma}) \in \mathbb{Z}$.

Упражнение 8. Предположим, что γ не просто: $\gamma = ab$, $a, b \in \mathbb{Z}[\omega]$, $N(a) \neq \pm 1$, $N(b) \neq \pm 1$. Тогда $|N(\gamma)| = |N(a)||N(b)|$, откуда одно из (натуральных) чисел $|N(a)|$ и $|N(b)|$ равно 1. Противоречие.
Покажем, что $5 \in Z[\sqrt{3}]$ простое, хотя $N(5) = 25$ – составное число. Пусть $5 = ab$, где $a, b \in \mathbb{Z}[\sqrt{3}]$, $N(a) \neq \pm 1$, $N(b) \neq \pm 1$. Тогда $N(a)N(b) = 25$, откуда $N(a) = \pm 5$. Если $a = x + y\sqrt{3}$, то $x^2 - 3y^2 = \pm 5$. Это уравнение не имеет решений по модулю 3.

Упражнение 9. Индукция по $|N(\gamma)|$.

Задача 10. Поскольку $N(3) = 9$, $N(5) = 25$, $N(1 + \sqrt{-14}) = N(1 - \sqrt{-14}) = 15$, норма неотрицательна, и норма произведения равна произведению норм, то достаточно показать, что не существует числа $\alpha \in \mathbb{Z}[\sqrt{-14}]$ с $N(\alpha) = 3$ или $N(\alpha) = 5$. Пусть $\alpha = x + y\sqrt{-14}$, где x, y — целые. А уравнения $x^2 + 14y^2 = 3$ и $x^2 + 14y^2 = 5$ не имеют решений в целых числах, поскольку $x^2 + 14y^2 > 5 > 3$ при $y \neq 0$.

Задача 11. а) Для ненулевого $b \in \mathbb{Z}[\sqrt{-2}]$ числа, кратные b, образуют решетку в плоскости комплексных чисел, разбивающую её на прямоугольники со сторонами $|b|$ и $\sqrt{2}|b|$. Для любой точки внутри такого прямоугольника существует вершина, для которой квадрат расстояния от неё точки не больше $(\frac{1}{2}|b|)^2 + (\frac{1}{2}\sqrt{2}|b|)^2 = \frac{3}{4}|b|^2 < N(b)$. Из этого, аналогично случаю гауссовых чисел, мы получаем деление с остатком, алгоритм Евклида и единственность разложения на множители.

б) Для ненулевого $b \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ числа, кратные b, образуют решетку в плоскости комплексных чисел, разбивающую её на равнобедренные треугольники с основанием $|b|$ и боковыми сторонами $\sqrt{\frac{1+7}{4}}|b| = \sqrt{2}|b|$. Для равнобедренного треугольника с основанием y и боковыми сторонами x легко получить формулу радиуса описанной окружности $R = x^2/\sqrt{4x^2 - y^2}$, и для любой точки внутри треугольника существует вершина, расстояние до которой не больше R (т.к. в равнобедренном треугольнике с боковыми сторонами R расстояние до одной из двух боковых вершин не больше R). Значит, для доказательства деления с остатком достаточно проверить, что в нашем равнобедренном треугольнике $R < |b|$. Действительно, $x = \sqrt{2}|b|$, $y = |b|$, $R = 2|b|^2/(\sqrt{7})|b| = (2/\sqrt{7})|b| < |b|$. Далее аналогично получаем основную теорему арифметики.

Задача 12. а,б) Заметим, что норма $N(a + \sqrt{-d}b) = a^2 + db^2$ для делителя единицы должна быть равна 1, поэтому при $d > 1$ получаем

$b = 0$, значит $a = \pm 1$, т.е. все делители единицы — это ± 1. Если же $d = 1$, то $-1 \le a, b \le 1$, откуда перебором получаем, что все делители единицы — это ± 1 и $\pm i$.

в) Задача 8.

г) Докажем, что все делители единицы имеют вид $\pm(1+\sqrt{2})^n$ для всех целых n. Т.к. $(1+\sqrt{2})(1-\sqrt{2}) = -1$, то все такие числа — делители единицы. Предположим, что существует какой-то другой делитель единицы $a + b\sqrt{2}$. После домножения на -1 и сопряжения можно считать, что $a, b > 0$ (если $ab = 0$, то $a = \pm 1$ и $b = 0$ из $a^2 - 2b^2 = \pm 1$). Рассмотрим минимальный такой делитель единицы $a + b\sqrt{2}$ (с $a, b \ge 0$ и $a + b\sqrt{2} \ne \pm(1+\sqrt{2})^n$). Тогда $(a + b\sqrt{2})(\sqrt{2} - 1) = (2b - a) + (a - b)\sqrt{2}$. Докажем, что $a > b$ и $2b > a$. Действительно, заметим, что если $b = 1$, то $a^2 = 2 \pm 1$, откуда $a = 1$ и $a + b\sqrt{2} = 1 + \sqrt{2}$, противоречие. Значит, $b > 1$, поэтому $a^2 = 2b^2 \pm 1 > b^2$, откуда $a > b$. Если $a = 1$, то $2b^2 = 1 \pm 1$, откуда $b = 1$ и $a + b\sqrt{2} = 1 + \sqrt{2}$, противоречие. Значит, $a > 1$, поэтому $(2b)^2 = 2(a^2 \pm 1) > a^2$, откуда $2b > a$.

Отсюда получаем $0 < 2b - a < a$ и $0 < a - b < b$, поэтому $(2b - a) + (a - b)\sqrt{2} < a + b\sqrt{2}$, что противоречит минимальности $a + b\sqrt{2}$. Значит, все делители единицы имеют вид $\pm(1+\sqrt{2})^n$.

Задача 13. а,в) Будем доказывать деление с остатком по норме $N(a + b\sqrt{D}) = |a^2 - Db^2|$, где $D = 2$ или 3. Пусть $x = a + b\sqrt{D}$ и $y = c + d\sqrt{D}$, тогда $x/y = (a + b\sqrt{D})/(c + d\sqrt{D}) = (a + b\sqrt{D})(c - d\sqrt{D})/(c^2 - Dd^2) = ((ac - Dbd) + (bc - ad)\sqrt{D})/(c^2 - Dd^2) = n + m\sqrt{D} + (k + l\sqrt{D})/(c^2 - Dd^2)$, где n, m, k, l – целые, и $|k|, |l| \le |(c^2 - Dd^2)|/2$ (обычное деление с остатком $ac - Dbd$ и $bc - ad$ на $c^2 - Dd^2$). Значит, $a + b\sqrt{D} = (c + d\sqrt{D})(n + m\sqrt{D}) + (k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2)$, причем $(k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2) \in \mathbb{Z}[\sqrt{D}]$ и $N(k + l\sqrt{D}) = |k^2 - Dl^2| \le (3/4)(c^2 - Dd^2)^2$, поэтому $N((k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2)) = N(k + l\sqrt{D})N(c + d\sqrt{D})/N(c^2 - Dd^2) \le (3/4)N(c + d\sqrt{D}) < N(c + d\sqrt{D})$, из чего следует деление с остатком. Отсюда аналогично предыдущим случаям следует основная теорема арифметики.

б) Заметим, что $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, причем $N(2) = N(1 + \sqrt{-3}) = N(1 - \sqrt{-3}) = 4$. Докажем, что $2, 1 + \sqrt{-3}$ и $1 - \sqrt{-3}$ — простые в $\mathbb{Z}[\sqrt{-3}]$. Для этого достаточно заметить, что $N(a + b\sqrt{-3}) = a^2 + 3b^2 \ne 2$ при целых a и b. Значит, $2, 1 + \sqrt{-3}$ и $1 - \sqrt{-3}$ не представимы в виде произведения двух чисел с неединичной нормой, поэтому они простые. Значит, разложение 4 на простые в $\mathbb{Z}[\sqrt{-3}]$ — не единственно.

г) Заметим, что $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, причем $N(3) = N(2 + \sqrt{-5}) = N(2 - \sqrt{-5}) = 9$. Аналогично получаем, что $3 \ne N(a + b\sqrt{-5}) = a^2 + 5b^2$, все числа в разложении 9 — простые, поэтому разложение не единственно.

д) Заметим, что $4 = 2 \cdot 2 = (\sqrt{5}+1)(\sqrt{5}-1)$, причем $N(2) = N(\sqrt{5}+1) = N(\sqrt{5}-1) = 4$. Так как $N(a+b\sqrt{5}) = a^2 - 5b^2 \equiv \pm 1 \mod 5$, то $\pm 2 \neq N(a+b\sqrt{5})$. Значит, все числа в разложении 4 — простые, поэтому разложение не единственно.

е) Заметим, что $9 = 3 \cdot 3 = (\sqrt{10}+1)(\sqrt{10}-1)$, причем $N(3) = N(\sqrt{10}+1) = N(\sqrt{10}-1) = 9$. Так как $N(a+b\sqrt{10}) = a^2 - 10b^2 \equiv \pm 1 \mod 5$, то $\pm 3 \neq N(a+b\sqrt{10})$. Значит, все числа в разложении 9 — простые, поэтому разложение не единственно.

ж) Аналогично пунктам а,в) нам достаточно показать, что если $|a|, |b| \leq 1/2$, то $|N(a+b\omega)| < 1$, где $\omega = \frac{1+\sqrt{5}}{2}$. Действительно, $a+b\omega = ((2a+b)+b\sqrt{5})/2$, поэтому $|N(a+b\omega)| = |((2a+b)^2-5b^2)/4| = |a^2+ab-b^2| \leq 3/4 < 1$.

з) Задача 11б.

и) Абсолютно аналогично случаю $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ получаем $R = \frac{3}{\sqrt{11}}|b| < |b|$, из чего следует деление с остатком и основная теорема арифметики.

к) Для $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ деление с остатком не выполняется, причем не только по стандартной норме, но и по любой (можете попробовать строго доказать это, рассмотрев число, не являющееся делителем единицы, с наименьшей нормой). Будем доказывать более слабое утверждение — что в $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ все идеалы главные (см. следующую часть). Для ненулевого идеала I рассмотрим его элемент y с наименьшей (стандартной) нормой. Докажем, что для любого $x \in I$ мы можем поделить с остатком x или $2x$ на y. Аналогично с пунктами а,в,ж) $\omega = \frac{1+\sqrt{-19}}{2}$, $x = a+b\omega$ и $y = c+d\omega$, тогда $x/y = (a+b\omega)/(c+d\omega) = n_1 + m_1\omega + (z_1+t_1\omega))$, где n, m — целые, а $|z_1|, |t_1| \leq 1/2$; аналогично $2x/y = n_2 + m_2\omega + (z_2+t_2\omega))$ с $|z_2|, |t_2| \leq 1/2$. Заметим, что одно из $|t_1|$ и $|t_2|$ не больше $1/3$ (будем считать, что $|t_i| \leq 1/3$). Тогда $|N(z_i+t_i\omega)| = |z_i^2 + z_it_i + 5t_i^2| \leq 1/4 + 1/6 + 5/9 = 35/36 < 1$, откуда следует деление с остатком (попробуйте доказать это утверждение в геометрической интерпретации).

Предположим, что $I \neq (y)$, т.е. существует $x \in I$, не делящееся на y. Тогда $2x$ делится на y, поэтому $2x = (a+b\omega)y$ для целых a и b. Значит, существует $z \in I$, не делящееся на y, для которого $2z = (c+d\omega)y$, где $c = 0$ или -1, а d равно 0 или 1 (поделим на $2y$). Заметим, что $d \neq 0$, т.к. иначе $N(z) = N(-y/2) < N(y)$. Значит, $2z = \frac{\pm 1+\sqrt{-19}}{2}y$, поэтому $\frac{\mp 1+\sqrt{-19}}{2}z + 3y = y/2 \in I$, но $N(y/2) < N(y)$, противоречие. Значит, $I = (y)$, т.е. все идеалы главные.

Теперь для доказательства основной теоремы арифметики достаточно доказать, что если x не делится на простое p, то $ax + bp = 1$ для каких-то a и b. Действительно, рассмотрим идеал (x, p), который равен (z) для какого-то z. Значит, p делится на z, поэтому z равен $p\xi$ или ξ, где ξ — делитель единицы. В первом случае получаем, что x делится на p,

противоречие. Во втором случае получаем, что $1 \in (z) = (x, p)$, поэтому $1 = ax + bp$ для каких-то a и b. Далее доказательство основной теоремы арифметики повторяет задачу 2.

Задача 14. Для этого необходимо и достаточно, чтобы $\xi^2 = a\xi + b$ для целых a и b, то есть ξ является корнем приведенного квадратного многочлена с целыми коэффициентами.

Задача 15. а) Если n четно, то $2 = (3^{n/2} + k)(3^{n/2} - k)$, где $3^{n/2} + k$ и $3^{n/2} - k$ имеют одинаковую четность, противоречие. Значит, n не делится на 2.

Разложив обе части на множители в $\mathbb{Z}[\sqrt{-2}]$, получим $(1+\sqrt{-2})^n(1-\sqrt{-2})^n = (k+\sqrt{-2})(k-\sqrt{-2})$. Легко проверить, что $k+\sqrt{-2}$ и $k-\sqrt{-2}$ взаимно просты (т.к. 3^n не делится на 2), и $1 \pm \sqrt{-2}$ — различные простые. Отсюда из выполнения основной теоремы арифметики для $\mathbb{Z}[\sqrt{-2}]$ получаем, что $(1 + \sqrt{-2})^n = \pm k \pm \sqrt{-2}$. Если $(1 + \sqrt{-2})^n = \pm k - \sqrt{-2}$, то по модулю $1 - \sqrt{-2}$ получаем $(1 + \sqrt{-2})^n \equiv 2^n \equiv \pm k - \sqrt{-2} \equiv \pm k - 1$, поэтому $2^n + 1 \equiv \pm k$. Но n нечетно, поэтому $2^n + 1$ делится на $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, поэтому и k делится на 3, что очевидно неверно.

Значит, $(1 + \sqrt{-2})^n = \pm k + \sqrt{-2}$, и приравнивая коэффициент при $\sqrt{-2}$, получаем

$$1 = \binom{n}{1} - 2\binom{n}{3} + 4\binom{n}{5} - \ldots \pm 2^{(n-1)/2}.$$

При $n = 1$ – $k = \pm 1$, при $n = 3$ — $k = \pm 5$. Докажем, что при $n \geq 5$ решений нет. Перепишем последнюю формулу:

$$0 = -\frac{(n+1)(n-1)(n-3)}{3} + 4\binom{n}{5} - 8\binom{n}{7} + \ldots \pm 2^{(n-1)/2}.$$

Теперь, аналогично задаче 3, докажем, $\frac{(n+1)(n-1)(n-3)}{3}$ и $2^k\binom{n}{2k+1}$ при $k > 2$ делятся на степень двойки большую, чем $4\binom{n}{5}$, из чего будет следовать противоречие. Для $\frac{(n+1)(n-1)(n-3)}{3}$ это очевидно, т.к. n на делится на 2 и $4\binom{n}{5} = \frac{n(n-1)(n-2)(n-3)(n-4)}{30}$. Перепишем второй тип слагаемых:

$$2^k\binom{n}{2k+1} = 4\binom{n}{5}\binom{n-5}{2k-4}\frac{15 * 2^{k-1}}{(2k-3)(2k-1)(2k+1)(k-1)k}.$$

Осталось заметить, что $2^{k-1} > k > k-1$ при $k > 2$, поэтому $2^{k-1}/(k(k-1))$ делится на 2, из чего следует наше утверждение.

б) Если n четно, то $7 = (2^{n/2}+k)(2^{n/2}-k)$, поэтому $2^{n/2} = 4$ и $k = \pm 3$, т.е. $n = 4, k = \pm 3$ – единственное решение при четном n. Далее считаем n нечетным.

Разложив обе части уравнения $2^{n-2} = (k^2+7)/4$ на множители в $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, получаем

$$((1+\sqrt{-7})/2)^{n-2}((1-\sqrt{-7})/2)^{n-2} = ((k+\sqrt{-7})/2)((k-\sqrt{-7})/2),$$

где $(1+\sqrt{-7})/2$ и $(1-\sqrt{-7})/2$ — различные простые, $(k+\sqrt{-7})/2$ и $(k-\sqrt{-7})/2$ – взаимно просты. Обозначим $m = n-2$, тогда из выполнения основной теоремы арифметики для $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ получаем, что $((1+\sqrt{-7})/2)^m = (\pm k \pm \sqrt{-7})/2$. Если $m = 1$, то $n = 3$ и $k = \pm 1$. Докажем, что если $m > 1$, то $((1+\sqrt{-7})/2)^m = (\pm k - \sqrt{-7})/2$. Действительно, иначе $((1+\sqrt{-7})/2)^m - ((1-\sqrt{-7})/2)^m = \sqrt{-7}$, и по модулю $(-3-\sqrt{-7})/2 = ((1-\sqrt{-7})/2)^2$ получаем, что $((1+\sqrt{-7})/2)^m - ((1-\sqrt{-7})/2)^m \equiv (-1)^m \equiv -1 \equiv \sqrt{-7}$, поэтому $1+\sqrt{-7} = ((1+\sqrt{-7})/2)^2(1-\sqrt{-7})/2)$ делится на $((1-\sqrt{-7})/2)^2$, противоречие.

Значит, $((1+\sqrt{-7})/2)^m = (\pm k - \sqrt{-7})/2$, и приравнивая коэффициенты при $\sqrt{-7}$ по модулю 7, получаем $-2^{m-1} \equiv m \mod 7$. Т.к. 2 является вычетом по модулю 7, то $m \equiv 3, 5, 6 \mod 7$, при этом $m \equiv 0, 2, 1 \mod 3$ соответственно. Значит, $m \equiv 3, 5, 13 \mod 21$, при этом $m = 3, 5, 13$ подходят — им соответствуют решения $n = 5, k = \pm 5$; $n = 7, k = \pm 11$; $n = 15, k = \pm 181$. Докажем, что это все решения.

Предположим противное, тогда $m \equiv m_0 \mod 21$, где $m_0 = 3, 5$ или 13, и $m > m_0$. Пусть $r = m - m_0$ делится на 7^α и не делится на $7^{\alpha+1}$. Тогда по модулю $7^{\alpha+1}$ получаем

$$(1+\sqrt{-7})^r = 1 + r\sqrt{-7} + \ldots + (\sqrt{-7})^l \binom{r}{l} + \ldots + (\sqrt{-7})^r \equiv 1 + r\sqrt{-7},$$

т.к. $l!$ делится на 7 в степени, меньшей $l/6 = l/7 + l/49 + \ldots$. Также $2^r \equiv (8)^{r/3} \equiv 1 \mod 7^{\alpha+1}$. Значит,

$$((1+\sqrt{-7})/2)^m = ((1+\sqrt{-7})/2)^{m_0}((1+\sqrt{-7})/2)^r \equiv ((k_0-\sqrt{-7})/2)(1+r\sqrt{-7}) \equiv$$

$$\equiv ((k_0+7r) + (k_0 r - 1)\sqrt{-7})/2 \equiv (k - \sqrt{-7})/2 \mod 7^{\alpha+1},$$

поэтому $k_0 r$ делится на $7^{\alpha+1}$. Но тогда k_0 делится на 7, противоречие (т.к. иначе 2^n делится на 7). Значит, других решений нет.

Задача 16. Мы будем использовать задачи 27 и 28.
а) В $\mathbb{Z}[\sqrt{-5}]$ имеется разложение $(x+\sqrt{-5})(x-\sqrt{-5}) = y^3$. Т.е. произведение идеалов $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ является кубом идеала (y). Если идеалы $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ не взаимно просты, то они имеют общий простой делитель I. Тогда идеал, порожденный $2\sqrt{-5} = (x+\sqrt{-5}) - (x-\sqrt{-5})$ делит I. Разложим $(2\sqrt{-5}) = (2, 1+\sqrt{-5})^2(\sqrt{-5})$. Т.е. $I = (2, 1+\sqrt{-5})$

или $I = (\sqrt{-5})$. В первом случае x нечетно, откуда $x^2+5 = y^3$ делится на 2, но не делится на 4, противоречие. Во втором случае x делится на 5, откуда $x^2+5 = y^3$ делится на 5, но не делится на 25, противоречие. Значит, идеалы $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ взаимно просты и каждый из них является кубом некоторого идеала. Используя задачу 28 нетрудно проверить, что куб неглавного идеала будет неглавным, откуда $(x+\sqrt{-5})$ — куб главного идеала. Т.е. $(x+\sqrt{-5}) = (a+b\sqrt{-5})^3$, поскольку делители единицы в $\mathbb{Z}[\sqrt{-5}]$ имеют вид ± 1 и являются кубами. Раскрывая скобки и приравнивая коэффициенты при $\sqrt{-5}$ получаем $(3a^2 - 5b^2)b = 3a^2b - 5b^3 = 1$. Отсюда $b = \pm 1$. Легко видеть, что оба случая невозможны. Следовательно, уравнение не имеет решений.

б) Заменяя x на $z-1$ получаем уравнение $z^2 + 6 = y^3$. Решений нет, доказательство аналогично пункту а).

в) Разложим $5x^2+1 = (1+x\sqrt{-5})(1-x\sqrt{-5}) = y^3$. Аналогично пункту а) x четно и идеалы $(1+x\sqrt{-5})$ и $(1-x\sqrt{-5})$ взаимно просты. Тогда $(1+x\sqrt{-5}) = (a+b\sqrt{-5})^3$. Раскрывая скобки и приравнивая вещественные части получаем $a(a^2-15b^2) = a^3-15ab^2 = 1$. Если $a = 1$, то $b = 0$, откуда $x = 0$, $y = 1$. Случай $a = -1$ невозможен. Т.е. $x = 0$, $y = 1$.

г) Заменяя x на $z-1$ получаем уравнение $6z^2 + 1 = y^3$. Решение единственно: $x = 0$, $y = 1$, доказательство аналогично пункту в).

д) Приведем решение, не использующее идеалы. Похожие решения есть и для пунктов а,б).

Прибавим 8 и разложим на множители: $x^2 + 2 = (y+2)(y^2-2y+4)$. Рассмотрев остатки по модулю 4 получим, что x нечетно, откуда $x^2 + 2 \equiv 3 \bmod 8$. Используем, что -2 является квадратичным невычетом по модулю простого p тогда и только тогда, когда $p \equiv 1$ или $3 \bmod 8$ (это следует, например, из квадратичного закона взаимности). Тогда все простые делители x^2+2 имеют вид $8k+1$ или $8k+3$, т.е. все делители $x^2+2 = (y+2)(y^2-2y+4)$ дают остатки 1 или 3 при делении на 8. Т.к. $y+2$ дает остаток 1 или 3 по модулю 8, то y дает остаток ± 1. Из этих двух случаев (y^2-2y+4) дает остаток 1 или 3 только если $y \equiv 1 \bmod 8$. Отсюда $x^2+2 = y^3+8 \equiv 1 \bmod 8$. Противоречие.

Упражнение 10. Очевидно.

Упражнение 11. Если $a, b \in I \cap J$, то $a+b \in I$, т.к. $a, b \in I$; аналогично $a+b \in J$. Отсюда $a+b \in I \cap J$.

Если $a \in I \cap J, b \in \mathbb{Z}$, то $ab \in I \cap J$ по аналогичной причине.

Задача 17. а,б) Следует из линейного представления НОД.

в) Пусть d — наименьшее натуральное число в идеале I (если такого нет, то $I = (0)$). Если $I \neq (d)$, то I содержит число a, не делящееся на d. Остаток от деления a на d лежит в I и меньше d. Противоречие.

Упражнение 12. Заметим, что (α) состоит из чисел вида αx, где

$x \in \mathbb{Z}[\omega]$, а также $(\alpha) \subset (\beta) \Leftrightarrow \alpha \in (\beta) \Leftrightarrow \alpha/\beta \in \mathbb{Z}[\omega]$. Имеем

$(\alpha) = (\beta) \Leftrightarrow \alpha \in (\beta)$ и $\beta \in (\alpha) \Leftrightarrow \alpha/\beta \in \mathbb{Z}[\omega]$ и $\beta/\alpha \in \mathbb{Z}[\omega] \Leftrightarrow \alpha/\beta$ – делитель единицы

Упражнение 13. Очевидно.

Задача 18. Заметим, что $(2, \sqrt{-14}) = \{x + y\sqrt{-14} \mid x$ четно, $y \in \mathbb{Z}\}$ (проверьте!) Отсюда имеем, что, $1 \notin (2, \sqrt{-14}))$ и $(2, \sqrt{-14}) \neq (2)$. Предположим, что $(2, \sqrt{-14}) = (\alpha)$. Тогда $2 = \alpha x$, $x \in \mathbb{Z}[\sqrt{-14}]$, откуда $4 = N(2) = N(\alpha)N(x)$.
Если $N(\alpha) = 1$, то $1 = \alpha\bar{\alpha} \in (\alpha)$, т.е. $(1) \in (\alpha) = (2, \sqrt{-14})$, противоречие.
$N(\alpha) \neq 2$, т.к. уравнение $x^2 + 14y^2 = 2$ не имеет решений в целых числах.
Если $N(\alpha) = 4$, то $N(\sqrt{-14}) = 14$ не делится на $N(\alpha)$, т.е. $\sqrt{-14} \notin (\alpha)$.

Задача 19. Пусть α — наименьшее натуральное число в I, $\beta = a + b\omega$ — число с наименьшим положительным коэффициентом b при ω. Несложно проверить, что $I = (\alpha, \beta)$.

Упражнения 14-15. Вычисления, не приводим.

Упражнение 16. Из упражнения 13 достаточно найти ответ в $\mathbb{Z}$: (360), (2), (180).

Упражнение 17. Вычисления, мы приведем доказательство для $I + J$. Если $a, b \in I + J$, то $a = i_1 + j_1$, $b = i_2 + j_2$, где $i_1, i_2 \in I$, $j_1, j_2 \in J$. Тогда $a + b = (i_1 + i_2) + (j_1 + j_2) \in I + J$, т.к. $i_1 + i_2 \in I$, $j_1 + j_2 \in J$.
Для $c \in \mathbb{Z}[\omega]$ имеем $ac = (i_1 + j_1)c = i_1c + j_1c \in I + J$, т.к. $i_1c \in I$, $j_1c \in J$.

Задача 20. Поскольку $N(a_i)$ и $\mathrm{Tr}(a_i\bar{a}_j)$ — целые числа, то имеем $(N(a_i), \mathrm{Tr}(a_i\bar{a}_j))_{1 \leq i,j \leq n} = (a)$, где $a = \text{НОД}(N(a_i), \mathrm{Tr}(a_i\bar{a}_j))$. Заметим, что $N(a_i)$ и $\mathrm{Tr}(a_i\bar{a}_j)$ делятся на a. Т.к. $N(a_i) = a_i\bar{a}_i$ и $\mathrm{Tr}(a_i\bar{a}_j) = a_i\bar{a}_j + a_j\bar{a}_i$, то

$$(a) = (N(a_i), \mathrm{Tr}(a_i\bar{a}_j))_{1 \leq i,j \leq n} \subset (a_1, ..., a_n)(\bar{a}_1, ..., \bar{a}_n)$$

Достаточно доказать, что $a_i\bar{a}_j \in (a)$ для всех $1 \leq i, j \leq n$, т.е. что $a_i\bar{a}_j/a$ — целое алгебраическое. По упражнению 6 достаточно показать, что его норма и след целые. $N(a_i\bar{a}_j/a) = \frac{a_i\bar{a}_j a_j\bar{a}_i}{a^2} = \frac{N(a_i)N(a_j)}{a^2}$ целое, т.к. $N(a_i)$ и $N(a_j)$ делятся на a. $\mathrm{Tr}(a_i\bar{a}_j/a) = \mathrm{Tr}(a_i\bar{a}_j)/a$ целое, т.к. $\mathrm{Tr}(a_i\bar{a}_j)$ делится на a.

Задача 21. Если I делится на J, то $I = JH \subset J$.
Пусть $I \subset J$. По задаче 20 (которая применима, т.к. $J = (\alpha, \beta)$ по задаче 19) имеем $J\bar{J} = (a)$, т.е. $I\bar{J} \subset J\bar{J} = (a)$. Тогда все элементы $I\bar{J}$ делятся на a, откуда $H = I\bar{J}/a = \{x/a \mid x \in I\bar{J}\}$ — идеал. Получаем $JH = (I\bar{J}/a)J = (I\bar{J}J)/a = (I(a))/a = I$, т.е. I делится на J.

Упражнение 18. Доказано в решении задачи 20.

Задача 22. По задаче 21 достаточно доказать, что

$$I \subset H \text{ и } J \subset H \Leftrightarrow I + J \subset H$$

Из левого следует правое, поскольку H замкнут относительно сложения; из правого левое — поскольку $I, J \subset I + J$.

Упражнение 19. $(a)\overline{(a)} = (a\bar{a}) = (N(a)) = (|N(a)|)$ и $|N(a)| \geq 0$, т.е. $N((a)) = |N(a)|$.

Упражнение 20. Т.к. $N(I)N(J) \geq 0$, то достаточно показать, что $(N(I)N(J)) = I\overline{IJ}$. Но $(N(I)N(J)) = (N(I))(N(J)) = I\bar{I}J\bar{J} = I\overline{IJ}$.

Упражнение 21. Если $J = IH$, то $N(J) = N(I)N(H)$ по упражнению 20, откуда $N(I)$ делит $N(J)$.

Упражнение 22. Если $I = (1)$, то $(N(I)) = I\bar{I} = (1)$, т.е. $N(I) = 1$. Если $N(I) = 1$, то $1 \in I\bar{I} \subset I$, т.е. $I = (1)$.

Упражнение 23. Идеал I прост $\Leftrightarrow$ любой идеал, делящий I, совпадает либо с I, либо с (1) $\Leftrightarrow$ (по задаче 21) любой идеал, содержащий I, совпадает либо с I, либо с (1) $\Leftrightarrow$ идеал I максимален.

Упражнение 24. Пусть p_1, p_2 — различные простые идеалы. По упражнению 23 ни один из них не содержится в другом. Тогда $p_1 + p_2$ — идеал, содержащий каждый из них и не совпадающий ни с одним из них. По упражнению 23 получаем $p_1 + p_2 = (1)$.

Задача 23. Заметим, что если $N(I)$ — простое число, то I — простой идеал (по упражнениям 21 и 22) и вычислим нормы: $N(p_1) = N(p_2) = 3$, $N(p_3) = N(p_4) = 5$.

Задача 24. Используем индукцию по $N(I)$ и упражнение 20.

Задача 25. По задаче 21 мы знаем, что $JH \subset I$ и хотим доказать что $H \subset I$. Пусть $h \in H$. Т.к. $I + J = (1)$, то найдутся $i \in I$, $J \in J$, что $i + j = 1$. Тогда $jh \in JH \subset I$ и по определению идеала $ih \in I$. Значит, $h = jh + ih \in I$, что и требовалось.

Задача 26. Пункт а) очевиден.
б) $HI = HJ \Rightarrow (N(H))I = H\bar{H}I = H\bar{H}J = (N(H))J$. Теперь применим пункт а) для $a = N(H)$.

Задача 27. Предположим, что какой-то идеал имеет два различных разложения на простые идеалы. Если какой-то простой идеал встречается в обоих разложениях, то на него по предыдущей задаче можно сократить. Будем сокращать, пока не получим два разложения идеала $p_1...p_n = I = q_1...q_n$ на простые идеалы, такое что все q_i отличны от p_1. Тогда p_1 делит $q_1...q_{n-1}q_n$; p_1 и q_n взаимно просты по упражнению 24. По задаче 25 p_1 делит $q_1...q_{n-1}$. Используем индукцию и получаем противоречие.

Задача 28. а) Пусть $I \subset \mathbb{Z}[\sqrt{-5}]$ — идеал, $x \in I$ — элемент с минимальной ненулевой нормой. Числа, кратные x, образуют на комплексной плоскости решетку из прямоугольников со сторонами 1 и $\sqrt{5}$. Если I не содержит других чисел, то I главный. Пусть $y \in I$, причем y не делится

на x. После параллельного переноса на число, кратное x, можно считать, что y лежит в прямоугольнике с вершинами 0, x, $(1+\sqrt{-5})x$, $\sqrt{-5}x$. Мнимая часть y/x лежит между 0 и $\sqrt{5}$. Если она меньше $\sqrt{3}/2$ или больше $\sqrt{5}-\sqrt{3}/2$, то расстояние от y до одной из вершин прямоугольника меньше $|x|$, что невозможно. Поэтому $\frac{\sqrt{3}}{2} \le \operatorname{Im}\frac{y}{x} \le \sqrt{5}-\frac{\sqrt{3}}{2}$. Значит, $\sqrt{5}-\frac{\sqrt{3}}{2} < \sqrt{3} \le 2\operatorname{Im}\frac{y}{x} \le 2\sqrt{5}-\sqrt{3} < \sqrt{5}+\frac{\sqrt{3}}{2}$. Отсюда следует, что расстояние от $2y$ до одного из чисел $\sqrt{-5}x$, $(1+\sqrt{-5})x$, $(2+\sqrt{-5})x$ меньше $|x|$, т.е. должно равняться нулю. Значит, y равняется $\sqrt{-5}x/2$, $(1+\sqrt{-5})x/2$, либо $(2+\sqrt{-5})x/2$. В первом и третьем случае $-5x/2 \in I$, откуда $x/2 \in I$, что невозможно. То есть $y = (1+\sqrt{-5})x/2$ и $I = ((1+\sqrt{-5})a, 2a)$, где $a = x/2$.

б) Взяв x и y аналогично пункту а) получим, что y равняется $\sqrt{-6}x/2$, $(1+\sqrt{-6})x/2$, либо $(2+\sqrt{-6})x/2$. Во втором случае $\sqrt{-6}(1+\sqrt{-6})x/2 = \sqrt{-6}x/2 - 3x \in I$, откуда $\sqrt{-6}x/2 \in I$, откуда $x/2 = (1+\sqrt{-6})x/2 - \sqrt{-6}x/2 \in I$, что невозможно. В первом и третьем случае получаем $I = (\sqrt{-6}a, 2a)$, где $a = x/2$.

Задача 29. Пусть $0 \ne a \in I$. Тогда $0 \ne a\bar{a} \in I \cap \mathbb{Z}$.

Задача 30. Пусть p — минимальное натуральное число в I, которое существует по предыдущей задаче. Если $p = ab$, где a, b натуральные, то $(a)(b) = (ab)$ содержится в I, т.е. по задаче 21 $(a)(b)$ делится на I, но (a) и (b) не делятся на I. Противоречие.

Задача 31. Возьмем p из предыдущей задачи. $(p) \subset I$, т.е. по задаче 21 (p) делится на I, откуда $N((p)) = p^2$ делится на $N(I)$. По упражнению 22 $N(I) \ne 1$, откуда $N(I)$ равняется p или p^2.

Задача 32. Следует из решения предыдущей задачи.

Задача 33. Если идеал $(p) \subset \mathbb{Z}[\omega]$ не прост, то $(p) = IJ$, где I, J отличны от (1). тогда $N(I)N(J) = N((p)) = p^2$, т.е. $N(I) = p$, откуда $I\bar{I} = (N(I)) = (p)$, что и требовалось.

Задача 34. Предположим, что $0 \le a < p$ является решением уравнения $P_\omega(a) \equiv 0 \bmod p$. Заметим, что $P_\omega(a) = (a-\omega)(a-\bar{\omega})$ делится на p. Тогда $(p, a-\omega)\overline{(p, a-\omega)} = (p^2, p(a-\omega), p(a-\bar{\omega}, (a-\omega)(a-\bar{\omega})) \subset (p)$, откуда $(p) \ne (p, a-\omega) \ne (1)$, при этом $(p, a-\omega)$ содержит (p), т.е. делит (p). Значит, (p) не прост.

В обратную сторону, если (p) не прост, то $(p) = I\bar{I}$, причем $p \in I$. Т.к. $p \in I$, то $p\omega \in I$. Т.к. $I \ne (p)$, то I содежит элемент $x + y\omega$, в котором y не делится на p. Применяя алгоритм Евклида к y и p, получим, что I содержит элемент $b + \omega$ для некоторого $b \in \mathbb{Z}$. Тогда для $a = -b$ имеем $a - \omega \in I$. Из решения задачи 19 следует, что $I = (p, a-\omega)$. Т.к. $(p, a-\omega)\overline{(p, a-\omega)} = (p)$, то $P_\omega(a) = (a-\omega)(a-\bar{\omega})$ делится на p, т.е. a является решением уравнения $P_\omega(a) \equiv 0 \bmod p$.

Задача 35. Предположим противное, то есть существуют рациональное $a = p/q$, где $q > 1$ и $\gcd(p, q) = 1$, и приведённый многочлен $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ с целыми коэффициентами такой, что $P(a) = 0$. Тогда $q^nP(a) = p^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = p^n + q(a_{n-1}p^{n-1} + \ldots + a_1pq^{n-2} + a_0q^{n-1}) = 0$, значит, p^n делится на q. Но $gcd(p, q) = 1$, противоречие.

Задача 36. Пусть $a, b \in \bar{\mathbb{Q}}$, тогда существуют приведённые многочлены $P(x), Q(x)$ с рациональными коэффициентами такие, что $P(a) = Q(b) = 0$. Пусть $P(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$ и $Q(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_m)$, где $\alpha_1, \alpha_2 \ldots \alpha_n$ и $\beta_1, \beta_2 \ldots \beta_m$ – корни $P(x)$ и $Q(x)$ соответственно, причем $a = \alpha_1$ и $b = \beta_1$. Тогда коэффициентами $P(x)$ и $Q(x)$ будут (с точностью до знака) элементарные симметрические многочлены от $\alpha_1, \alpha_2 \ldots \alpha_n$ и $\beta_1, \beta_2 \ldots \beta_m$ соответственно. Докажем, что $a + b \in \bar{\mathbb{Q}}$. Заметим, что $a + b$ является корнем многочлена $R(x) = \prod\limits_{\substack{1\le i\le n\\ 1\le j\le m}} (x - \alpha_i - \beta_j)$, коэффициенты которого есть многочлены от $\alpha_1 \ldots \alpha_n, \beta_1 \ldots \beta_m$ с рациональными коэффициентами. Из того, что для любых $1 \le i, j \le n$ при перестановке α_i и α_j многочлен $R(x, \alpha_1, \ldots, \beta_m)$ сохраняется, следует, что коэффициенты $R(x)$ – многочлены от $\beta_1 \ldots \beta_m$, коэффициенты которых есть симметрические многочлены от $\alpha_1 \ldots \alpha_n$ с рациональными коэффициентами.

Из основной теоремы о симметрических многочленах и того, что элементарные симметрические многочлены от $\alpha_1, \alpha_2 \ldots \alpha_n$ — рациональные коэффициенты $P(x)$, следует, что коэффициенты $R(x)$ — многочлены от $\beta_1 \ldots \beta_m$ с рациональными коэффициентами. Повторяя последнее рассуждение для $\beta_1 \ldots \beta_m$, получаем, что коэффициенты $R(x)$ — симметрические многочлены от $\beta_1 \ldots \beta_m$ с рациональными коэффициентами, и, как следует из теоремы и рациональности элементарных симметрических многочленов от $\beta_1 \ldots \beta_m$, они рациональны. Значит, $R(x)$ имеет рациональные коэффициенты и корень $a + b$, поэтому $a + b \in \bar{\mathbb{Q}}$.

Доказательство $ab \in \bar{\mathbb{Q}}$ дословно повторяет доказательство для $a+b$ с заменой $R(x)$ на $\prod\limits_{\substack{1\le i\le n\\ 1\le j\le m}} (x-\alpha_i\beta_j)$. Осталось заметить, что $-b$ и $1/b$ являются корнями многочленов $Q(-x)$ и $x^mQ(1/x)$ с рациональными коэффициентами соответственно, поэтому $a - b = a + (-b) \in \bar{\mathbb{Q}}$ и $a/b = a(1/b) \in \bar{\mathbb{Q}}$.

Задача 37. Будем считать $a_n \neq 0$. Пусть a_i — корень приведённого многочлена рациональными коэффициентами $P_i(x) = \prod\limits_{1\le j\le n_i} (x - \alpha_{ij})$, причем $a_i = \alpha_{i1}$ и все $\alpha_{nj} \neq 0$ (иначе поделим $P_n(x)$ на x в максимальной возможной степени). Рассмотрим все наборы $J = (j_0, j_1, \ldots, j_n)$ из

$n+1$ натурального числа с $1 \le j_k \le n_k$, и многочлен $R(x) = \prod\limits_J (\alpha_{nj_n} x^n + \alpha_{n-1j_{n-1}} x^{n-1} + \dots \alpha_{1j_1} x + \alpha_{0j_0})$. Тогда $R(x)$ делится на $a_n x^n + \dots a_1 x + a_0$, и, следовательно, $R(b) = 0$. Теперь, аналогично решению задачи 36, заметим, что из того, что многочлен $R(x)$ сохраняется при перестановках α_{ki} и α_{kj}, следует, что коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i \le n$, $0 \le j \le n_i$ с рациональными коэффициентами, причем для любого i — они симметрические от α_{ij} , $1 \le j \le n_i$.

Теперь индукцией по $k \le n+1$ покажем, что коэффициенты $R(x)$ — многочлены от α_{ij}, $0 \le i \le n-k$, $0 \le j \le n_i$ с рациональными коэффициентами, причем для $0 \le i \le n-k$ — они симметрические от α_{ij} , $1 \le j \le n_i$. База $k = 0$ — указана выше, переход от k к $k+1$ при $k \le n$ — по предположению индукции коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i < n-k$, $1 \le j \le n_i$ с коэффициентами – симметрическими многочленами с рациональными коэффициентами от α_{n-kj}, $1 \le j \le n_{n-k}$, причем для $0 \le i < n-k$ — они симметрические от α_{ij} , $1 \le j \le n_i$. Из теоремы 1 и рациональности коэффициентов $P_{n-k}(x)$ следует, что коэффициенты коэффициентов $R(x)$ как многочленов от α_{ij}, $0 \le i < n-k$, $1 \le j \le n_i$ — рациональны. Значит, коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i \le n-k-1$, $1 \le j \le n_i$ с рациональными коэффициентами, причем для $0 \le i \le n-k-1$ — они симметрические от α_{ij} , $1 \le j \le n_i$ — переход доказан.

При $k = n+1$ получаем, что коэффициенты $R(x)$ рациональны, и $R(x) \ne 0$, т.к. все $\alpha_{nj} \ne 0$. Значит, b является корнем ненулевого многочлена с рациональными коэффициентами, поэтому $b \in \bar{\mathbb{Q}}$.

Задача 38. а) Для нормы $N(P) = \deg(P)$ делением с остатком будет обычное деление многочленов столбиком.

б) В данном случае делителями единицы будут ненулевые рациональные числа, а простыми — неприводимые непостоянные многочлены. Какое-то разложение на простые можно получить делением многочлена на простые меньшей степени (пока это возможно). Предположим, что у какого-то многочлена R есть два различных (с точностью до домножения на единицы) разложения на простые $R = P_1 P_2 \dots P_n = Q_1 Q_2 \dots Q_m$. Сократив на одинаковые (с точностью до домножения на делители единицы) простые в разложениях, получим, что для какого-то P_i выполнено $P_i | Q'_1 Q'_2 \dots Q'_k$, где $Q'_1 Q'_2 \dots Q'_k$ — оставшиеся простые в правой части. Пусть α — корень P_i, тогда $Q'_1(\alpha) Q'_2(\alpha) \dots Q'_k(\alpha) = 0$, значит $Q'_j(\alpha) = 0$ для какого-то j. Но тогда P_i и Q'_i делятся на минимальный многочлен для α, неприводимы и различны (с точностью до домножения на делители единицы), противоречие. Значит, разложение единственно.

Задача 39. Для многочлена $P(x)$ с рациональными коэффициентами

определим его содержание C_P как положительное рациональное число, такое, что все коэффициенты многочлена $P(x)/C_P$ целые, и их наибольший общий делитель равен 1. Такое число существует, т.к. $P(x)$ можно сначала умножить на наименьшее общее кратное знаменателей всех его коэффициентов, а потом поделить на наибольший общий делитель всех коэффициентов — тогда у получившегося многочлена будут целые коэффициенты с наибольшим общим делителем, равным 1. При этом получившийся многочлен перестает иметь целые коэффициенты при умножении на нецелое рациональное число x/y (т.к. если y делится на простое p, то существует коэффициент a_i, не делящийся на p, поэтому $a_i(x/y)$ не будет целым), и перестает иметь тривиальный наибольший общий делитель всех коэффициентов при умножении на целое число, не равное ± 1. Из этого следует, что такое C_P единственно, поэтому оно корректно определено.

Как видно из определения, достаточно доказать, что если P и Q имеют целые коэффициенты с тривиальным наибольшим общим делителем (то есть $C_P = C_Q = 1$), то их произведение PQ обладает тем же свойством ($C_{PQ} = 1$). Предположим противное, тогда существует простое p, делящее все коэффициенты PQ. Пусть $P(x) = a_n x^n + \dots a_0$ и $Q(x) = b_m x^m + \dots b_0$, и пусть k и r — наименьшие неотрицательные целые числа, такие, что a_k и b_r не делятся на p (такие k и r существуют, иначе p делит все коэффициенты $P(x)$ или $Q(x)$). Тогда коэффициент при x^{k+r} у PQ равен сумме $a_0 b_{k+r} + a_1 b_{k+r-1} + \dots + a_k b_r + \dots + a_{k+r} b_0$, все слагаемые которой, кроме $a_k b_r$, делятся на p из минимальности k и r. Значит, этот коэффициент у PQ не делится на p, противоречие.

Задача 40. Деление с остатком в многочленах с целыми коэффициентами по степени уже не работает (x не делится с остатком на $2x$), но верна единственность разложения — из задачи 38 следует, что любые два разложения на простые в целых числах отличаются домножением на рациональные. Все наибольшие общие делители непостоянных многочленов разложения равны 1, значит по лемме Гаусса многочлены в двух разложениях совпадают с точностью ± 1, поэтому разложения одинаковы.

Как мы видели, из наличия деления с остатком следует, что любой идеал главный. В множестве многочленов от переменной x с целыми коэффициентами имеется не главный идеал $(2, x)$, а в множестве многочленов от двух переменных x, y имеется не главный идеал (x, y).

Задача 41. Поделив с остатком $Q(x)$ на $P_a(x)$, мы получим $Q(x) = R(x)P_a(x) + T(x)$, где $R(x)$ и $T(x)$ — многочлены с рациональными коэффициентами, причем $deg(T) < deg(P_a)$, поэтому $T(a) \neq 0$ при $T(x) \neq 0$. Но подставив $x = a$, получим $Q(a) = 0 = R(a)P_a(a) + T(a) = T(a)$, значит

$T(x) = 0$ и $Q(x) = R(x)P_a(x)$, поэтому $Q(x)$ делится на $P_a(x)$.

Задача 42. Доказательство повторяет доказательство задачи 36 с учетом того, что симметрический многочлен с целыми коэффициентами представляется как многочлен с целыми коэффициентами от элементарных симметрических.

Задача 43. Достаточно доказать, что $\frac{1}{b} \in \mathbb{Q}[a_1, ..., a_n]$. Как следует из задачи 36, b — алгебраическое. Пусть $P(x) = c_n x^n + \ldots + c_1 x + c_0$ — минимальный приведенный многочлен с рациональными коэффициентами для b, тогда $c_0 \neq 0$ минимальности, поэтому $\frac{1}{b} = -\frac{c_n}{c_0} b^{n-1} - \ldots - \frac{c_1}{c_0} \in \mathbb{Q}[a_1, ..., a_n]$.

Задача 44. Пусть a является корнем приведённого многочлена $P(x)$ с целыми коэффициентами, по задаче 41 имеем $P(x) = R(x)Q(x)$, где $R(x)$ — приведённый многочлен с рациональными коэффициентами (т.к. P и Q — приведённые). Заметим, что $C_P = 1$, т.к. он приведённый с целыми коэффициентами, и $1/C_Q$ и $1/C_R$ — натуральные, т.к. они приведённые. По лемме Гаусса $(1/C_Q)(1/C_R) = 1$, поэтому $C_Q = C_R = 1$, значит $Q(x)$ имеет целые коэффициенты.

Также можно было заметить, что коэффициенты $Q(x)$ — многочлены от корней $P(x)$ с целыми коэффициентами, поэтому они целые алгебраические. Но т.к. $Q(x)$ имеет рациональные коэффициенты, то по задаче 35 — они целые.

Задача 45. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена $P(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ с целыми коэффициентами, причем $|\alpha_1| = \ldots = |\alpha_n| = 1$. Тогда заметим, что $P_k(x) = (x-\alpha_1^k)(x-\alpha_2^k)\ldots(x-\alpha_n^k)$ также имеет целые коэффициенты (т.к. они являются симметрическими многочленами от $\alpha_1, \ldots, \alpha_n$ с целыми коэффициентами), и его корни по модулю равны 1. Заметим, что по теореме Виета коэффициент $P_k(x)$ при x^{n-m} не превосходит по модулю $\binom{n}{m}$. Значит, наборы коэффициентов $P_k(x)$ принимают конечное число значений, поэтому какой-то из этих наборов встречается бесконечное число раз при натуральных k. Из единственности разложения многочлена на линейные множители в комплексных числах следует, что для бесконечного числа k набор $\{\alpha_1^k, \ldots, \alpha_n^k\}$ равен какому-то набору $\{\beta_1, \ldots, \beta_n\}$ с точностью до перестановки. Значит, для каких-то различных k_1 и k_2 — $\alpha_i^{k_1} = \alpha_i^{k_2}$ для всех i (из конечности числа перестановок), поэтому $\alpha_i^{k_1-k_2} = 1$ для всех i. Значит, все корни $P(x)$ — корни из 1, ч.т.д.

Задача 46. Достаточно проверить транзитивность — пусть $A \sim B$ и $B \sim C$, тогда $(a)A = (b)B$ и $(d)B = (c)C$, поэтому $(ad)A = (bc)C$ и $A \sim C$.

Задача 47. Если все идеалы главные, то для любых двух идеалов (α) и (β) — $(\beta)(\alpha) = (\alpha)(\beta)$, поэтому $(\alpha) \sim (\beta)$, т.е. все идеалы эквивалентны.

Обратно, если число классов равно 1, то любой идеал I эквивалентен (1), поэтому $(\alpha) = I(\beta)$. Значит, $\alpha = i\beta$ для какого-то $i \in I$, поэтому $I = (\alpha/\beta) = (i)$, т.е. все идеалы главные.

Задача 48. Если $(a)I_1 = (b)I_2$ и $(c)J_1 = (d)J_2$, то $(ac)I_1J_1 = (bd)I_2J_2$, поэтому $I_1J_1 \sim I_2J_2$.

Задача 49. По задаче 28 в обоих случаях есть 2 различных класса — (a) и $((1+\sqrt{-5})a, 2a)$ в $\mathbb{Z}[\sqrt{-5}]$, и (a) и $(\sqrt{-6}a, 2a)$ в $\mathbb{Z}[\sqrt{-6}]$ (для таких a, что это идеал). Обозначим главные идеалы — 0-ым классом, а оставшийся класс — 1-ым. Тогда произведение 0-ых — 0-ой, произведение 0-ого на 1-ого — 1-ый, а произведение 1-ых — 0-ой, т.к. $((1+\sqrt{-5})a, 2a)((1+\sqrt{-5})b, 2b) = ((-4+2\sqrt{-5})ab, (2+2\sqrt{-5})ab, 4ab) = (2ab)$ и $(\sqrt{-6}a, 2a)(\sqrt{-6}b, 2b) = (-6ab, 2\sqrt{-6}ab, 4ab) = (2ab)$. Значит, умножение классов устроено так же, как сложение по модулю 2.

Задача 50. Это множество лежит в $\widetilde{\mathbb{Z}}$, замкнуто относительно сложения и умножения на $\widetilde{\mathbb{Z}}$ (т.к. I — идеал), поэтому $(1/\alpha)I$ — идеал.

Задача 51. Пусть $P_\alpha(x)$ — минимальный приведенный многочлен для α степени n, тогда набор $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ является базисом в $\mathbb{Q}[\alpha]$, т.к. любой многочлен сравним с многочленом степени меньше n по модулю $P(x)$, и если два различных многочлена от α степени меньше n равны, то $P(x)$ — не минимальный.

Задача 52. Аналогично, пусть $P_i(x)$ — минимальный приведенный многочлен для α_i степени n_i, тогда набор одночленов $\alpha_1^{r_1}\alpha_2^{r_2}\ldots\alpha_k^{r_k}$, где $0 \le r_i < n_i$ — позволяет представить любой элемент $\widetilde{\mathbb{Q}}$ в виде суммы элементов набора с рациональными коэффициентами. Предположим, что какой-то элемент $\widetilde{\mathbb{Q}}$ можно представить таким образом двумя различными способами. Тогда из равенства этих сумм следует, что какой-то элемент набора можно выразить в виде суммы остальных (с рациональными коэффициентами) — выкинем этот элемент из набора. Будем продолжать эту операцию, пока возможно — элементов в наборе конечное число, поэтому этот процесс закончится, и мы получим набор, для которого любой элемент $\widetilde{\mathbb{Q}}$ единственным образом представляется в виде суммы элементов набора с рациональными коэффициентами. Значит, мы получили базис $\widetilde{\mathbb{Q}}$ над $\mathbb{Q}$.

Задача 53. Пусть α является корнем многочлена с целыми коэффициентами $P(x) = a_m x^m + \ldots + a_0$ (возьмем минимальный многочлен и умножим на НОК знаменателей всех коэффициентов). Тогда $a_m^{m-1}P(x) = (a_m x)^m + a_{m-1}(a_m x)^{m-1} + \ldots + a_1 a_m^{m-2}(a_m x) + a_0 a_m^{m-1}$, поэтому число $a_m\alpha$ является корнем многочлена с целыми коэффициентами.

Задача 54. Для начала заметим, что для любого $\alpha \in \widetilde{\mathbb{Q}}$ существует целое ненулевое n, такое что $n\alpha \in I$. Действительно, пусть $\beta \in I$,

$\beta \neq 0$, тогда для β/α существует такое n, что $n\alpha/\beta \in \widetilde{\mathbb{Z}}$, значит $n\alpha = (n\alpha/\beta)\beta \in I$. Отсюда следует, что взяв произвольный базис $\widetilde{\mathbb{Q}}$ над $\mathbb{Q}$ и умножив его элементы на натуральные числа, мы сможем получить базис, элементы которого лежат в I. Возьмем такой базис $\beta_1, \ldots, \beta_n$, тогда каждый элемент $\alpha \in I$ единственным образом записывается в виде $\alpha = x_1\beta_1 + \ldots + x_n\beta_n$, где $x_1, \ldots, x_n$ - рациональные (набор $(x_1, \ldots, x_n)$ будем называть координатами α).

Для каждого $\alpha \in I$ рассмотрим набор его координат по модулю 1, то есть $(\{x_1\}, \{x_2\}, \ldots, \{x_n\})$, являющийся координатами $\alpha - \lfloor x_1 \rfloor \beta_1 - \lfloor x_2 \rfloor \beta_2 - \ldots - \lfloor x_n \rfloor \beta_n \in I$. Как видно из определения, все такие наборы лежат в единичном кубе размерности n. Если таких различных наборов конечное число, то возьмем соответствующие им $\alpha_1, \ldots, \alpha_m \in I$, тогда набор $\beta_1, \ldots, \beta_n, \alpha_1, \ldots, \alpha_m$ — удовлетворяет утверждению задачи.

Предположим, что таких различных наборов бесконечно много. Тогда существует $\alpha \in I$ со сколь угодно маленькими по модулю всеми координатами. Действительно, для любого натурального N разобьем единичный куб на N^n меньших кубов со стороной $1/N$. Из бесконечности числа различных наборов — в каком-то меньшем кубе найдутся 2 различных набора $(x_1, \ldots, x_n)$ и $(y_1, \ldots, y_n)$, тогда $(y_1 - x_1, \ldots, y_n - x_n)$ — координаты какого-то $\alpha \in I$, причем $|y_i - x_i| \leq 1/N$ для всех i. Но N можно выбрать сколь угодно большим (т.е. $1/N$ — сколь угодно маленьким), из чего следует наше утверждение.

Осталось доказать, что у $\alpha \in I$ не могут все координаты быть сколь угодно малыми по модулю. Пусть $P_i(x)$ – минимальный приведенный многочлен с целыми коэффициентами для β_i, и $\beta_{i1}, \beta_{i2}, \ldots, \beta_{in_i}$ – его корни. Рассмотрим все наборы $J = (j_1, \ldots, j_n)$ из $n+1$ натурального числа с $1 \leq j_k \leq n_k$, и многочлен $R(t, x_1, \ldots, x_n) = \prod_J (t - (x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}))$. Этот многочлен сохраняется при перестановках β_{ij} и β_{ik}, поэтому (аналогично с решением задачи 6) он имеет целые коэффициенты. Рассмотрим ненулевое $\alpha \in I$ и подставим в $R(t, x_1, \ldots, x_n)$ его координаты — получим приведенный многочлен $R_\alpha(t)$ с рациональными коэффициентами с корнем α. Значит, $R_\alpha(t)$ делится на минимальный приведенный многочлен $Q_\alpha(t)$ с целыми коэффициентами. В частности, произведение каких-то $x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}$ с точностью до знака совпадает со свободным членом $Q_\alpha(t)$, т.е. равно целому ненулевому числу. Пусть $\epsilon = 1/(n \max_{i,j}(|\beta_{ij}|))$, тогда если $|x_i| < \epsilon$ для всех i, то для всех J — $|x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}| < 1$, поэтому и модуль их произведения < 1. Но он должен быть целым ненулевым, противоречие.

Значит, все координаты α не могут быть по модулю меньше ϵ, поэтому различных наборов конечное число. Как мы уже показали, в этом случае

выполняется утверждение задачи. Задача решена.

Задача 55. Зафиксируем базис $\gamma_1, \ldots, \gamma_n$ в $\mathbb{Q}[\alpha]$, и рассмотрим $\alpha_1, \ldots, \alpha_N$ из предыдущей задачи. Тогда координаты элементов I в нашем базисе порождаются коэффициентами $\alpha_1, \ldots, \alpha_N$ (т.е. их конечными суммами). Рассмотрим первые координаты всех элементов I — они порождаются первыми координатами $\alpha_1, \ldots, \alpha_N$, поэтому они имеют вид $q_1 r$ для фиксированного рационального q_1 и всех целых r (применим алгоритм Евклида к первым координатам $\alpha_1, \ldots, \alpha_N$). Возьмем какой-то $\beta_1 \in I$ с первой координатой q_1 (если $q_1 = 0$, о возьмем $\beta_1 = 0$), и вычтем из элементов I (различные) числа $k\beta_1$ с целым k так, чтобы все первые координаты стали равны 0. Потом применим эту операцию ко второй координате, и так далее. В конце мы получим набор $\beta_1, \ldots, \beta_n$, ненулевые элементы которого удовлетворяют условию задачи: любое $\alpha \in I$ можно представить в нужном виде, т.к. мы можем последовательно вычитать из α числа $k_i\beta_i$ с целыми k_i так, чтобы обнулялись i-ые координаты, и в конце получим 0. При этом такое представление единственно, иначе для каких-то целых k_i – $k_1\beta_1 + \ldots + k_l\beta_l = 0$, причем не все $k_i\beta_i$ равны 0. Пусть $k_r\beta_r$ — ненулевое слагаемое с минимальным r, тогда r-ая координата у $k_r\beta_r$ не равна 0, а у всех остальных слагаемых — нулевая по построению β_i, противоречие.

Задача 56. Это сразу следует из первого утверждения в решении задачи 54 и того, что для элементов целого базиса $\alpha_1, \ldots, \alpha_n$ не существуют целых k_i таких, что $k_1\alpha_1 + \ldots + k_n\alpha = 0$, причем не все k_i равны 0.

Задача 57. Очевидно.

Задача 58. Можно показать, что искомое количество равно $N(I)$.

Задача 59. Применим первое утверждение в решении задачи 54 к $\alpha = 1$.

Задача 60. Пусть целое $m \in I$, и $\alpha_1, \ldots, \alpha_n$ — целый базис $\widetilde{\mathbb{Z}}$. Тогда элементы $\widetilde{\mathbb{Z}}/I$ имеют представителей среди $k_1\alpha_1 + \ldots + k_n\alpha$, где $0 \leq k_i < m$, т.к. $m\alpha_i \in I$. Значит, $\widetilde{\mathbb{Z}}/I$ — конечное множество.

Задача 61. Любой идеал I, содержащий (α), полностью определяется элементами $\widetilde{\mathbb{Z}}/(\alpha)$, которые содержаться в I (если I содержит одного представителя, то он содержит весь класс эквивалентности). Т.к. $\widetilde{\mathbb{Z}}/(\alpha)$ конечно, то и множество его подмножеств конечно, поэтому таких идеалов — конечное число.

Задача 62. Из задачи 56 следует, что вектора элементов целого базиса I являются базисом рационального n-мерного пространства над $\mathbb{Q}$.

Задача 63. Возьмем $M_1 = \max_{i,j}(\|\alpha_i\alpha_j\|) + 1$ и $\beta_i = \alpha_i\beta$. Тогда если $\beta = x_1\alpha_1 + \ldots + x_n\alpha_n$, то $\|\beta_i\| = \|x_1\alpha_1\alpha_i + \ldots + x_n\alpha_n\alpha_i\| \leq \|x_1\alpha_1\alpha_i\| +$

$\ldots + \|x_n\alpha_n\alpha_i\| < M_1(x_1 + \ldots + x_n) = M_1\|\beta\|$, ч.т.д.

Задача 64. Из задачи 56 следует, что для β_i из предыдущей задачи существуют и единственны такие рациональные x_i, что $\alpha = x_1\beta_1 + \ldots + x_n\beta_n$. Возьмем такое $c \in \widetilde{\mathbb{Z}}$, что $c\beta = \lfloor x_1 \rfloor \beta_1 + \ldots + \lfloor x_n \rfloor \beta_n$, тогда $\|\alpha - c\beta\| = \|\{x_1\}\beta_1 + \ldots + \{x_n\}\beta_n\| < \|\beta_1\| + \ldots + \|\beta_n\| < nM_1\|\beta\|$, ч.т.д.

Задача 65. Для каждого натурального $k \leq M_2$ рассмотрим $\alpha'_k = k\alpha - c_k\beta$ такое, что $\|\alpha'_k\| < nM_1\|\beta\|$. Векторы всех α'_k лежат в кубе с центром в 0 и со стороной $2nM_1\|\beta\|$. Разобьем его на $(2n(n+1)M_1)^n$ кубов со стороной $\|\beta\|/(n+1)$, тогда среди $M_2 = (2n(n+1)M_1)^n + 1$ векторов α'_k какие-то α'_k и α'_r, $k \neq r$, лежат в одном кубе со стороной $\|\beta\|/(n+1)$. Значит, $\|\alpha'_k - \alpha'_r\| \leq \|\beta\| n/(n+1) < \|\beta\|$, но $\alpha'_k - \alpha'_r = (k-r)\alpha - c\beta$, где $|k-r| < M_2$. Значит, $m = |k-r|$ подходит.

Задача 66. Выберем β как ненулевой элемент I с минимальным $\|\beta\|$. Тогда для любого $\alpha \in I$ существует $m \leq M_2$ и $c \in \widetilde{\mathbb{Z}}$ такие, что $\|m\alpha - c\beta\| < \|\beta\|$. Но $m\alpha - c\beta \in I$, поэтому $m\alpha = c\beta$. Значит, для любого $\alpha \in I$ существует $c \in \widetilde{\mathbb{Z}}$ такое, что $M_2!\alpha = c\beta$, поэтому $M_2!I \subseteq (\beta)$. Следовательно, $(1/\beta)M_2!I$ — идеал, и $M_2 = (1/\beta)M_2!\beta \in (1/\beta)M_2!I$.

Задача 67. По задаче 61 — идеалов, содержащих $M_2!$, конечное число, и каждый идеал I по предыдущей задаче эквивалентен одному из них, т.к. $(M!)I = (\beta)((1/\beta)M_2!I)$. Значит, классов эквивалентности идеалов — конечное число.

Задача 68. Пусть $\beta_1, \ldots, \beta_n$ — целый базис I, тогда если $\alpha I \subseteq I$, то $\alpha\beta_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \ldots + a_{in}\beta_n$ для всех i, где все a_{ij} — целые. Перепишем эти уравнения как

$$a_{i1}\beta_1 + a_{i2}\beta_2 + \ldots + a_{i,i-1}\beta_{i-1} + (a_{i,i} - \alpha)\beta_i + a_{i,i+1}\beta_{i+1} \ldots + a_{in}\beta_n = 0,$$

и получим систему однородных линейных уравнений на переменные $\beta_1, \ldots, \beta_n$. Запишем её коэффициенты в виде матрицы

$$\begin{pmatrix} a_{11} - \alpha & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \alpha & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \alpha \end{pmatrix}$$

Те из вас, кто знаком с понятием определителя, могут сразу заметить, что определитель этой матрицы — это приведенный многочлен от α с целыми коэффициентами, и при этом определитель равен 0 ввиду наличия ненулевого решения $(\beta_1, \ldots, \beta_n)$. Из этого мы сразу получаем, что α — целое алгебраическое. Но так как (возможно) не все из вас знакомы

с определителем, то мы проведем несколько более громоздкое рассуждение, использую метод Гаусса решения системы линейных уравнений, или просто метод последовательного исключения переменных. На самом деле, оно будет довольно близко к доказательству одного из основных свойств определителя (что система имеет нетривиальное решение тогда и только тогда, когда определитель равен 0), поэтому принципиально от предыдущего оно ничем не отличается.

Предположим, что α — не целое алгебраическое, т.е. любой ненулевой приведенный многочлен с целыми коэффициентами от α не равен 0. Как известно и очевидно, множество решений системы уравнений не изменится, если мы умножим одно уравнение на ненулевую константу или вычтем из одного уравнения другое, умноженное на константу.

Давайте исключим переменную β_1 из всех уравнений, кроме первого — по предположению $a_{11} - \alpha \neq 0$, поэтому мы можем умножить все остальные уравнения на $a_{11} - \alpha$, а потом вычесть из i-ого уравнения 1-ое, умноженное на a_{i1}. Коэффициенты новой системы будут иметь вид

$$\begin{pmatrix} a_{11}-\alpha & a_{12} & \dots & a_{1n} \\ 0 & (a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12} & \dots & a_{2n}(a_{11}-\alpha) - a_{21}a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}(a_{11}-\alpha) - a_{n1}a_{12} & \dots & (a_{nn}-\alpha)(a_{11}-\alpha) - a_{n1}a_{1n} \end{pmatrix}$$

Теперь можно исключить переменную β_2 из всех уравнений, кроме первого и второго — по предположению коэффициент при β_2 во втором уравнении $(a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12} \neq 0$, поэтому мы можем умножить все уравнения после 2-ого на $(a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12}$, а потом вычесть из i-ого, $i > 2$ уравнения 2-ое, умноженное на старый (до последнего умножения) коэффициент i-ого уравнения при β_2. Покажем по индукции, что мы и дальше сможем по очереди исключать переменные.

Предположим, что для натурального $1 \leq k \leq n$ – при $1 \leq i \leq k$, мы уже исключили i-ую переменную из уравнений с номером, большим i, и коэффициенты уравнений являются многочленами с целыми коэффициентами от α, причем коэффициенты уравнений с номером $i > k$ при β_i – степени 2^k, степени остальных коэффициентов уравнений с номером $i > k$ строго меньше 2^k, и все коэффициенты i-ых уравнений при β_i — с точностью до знака приведенные многочлены:

$$\begin{pmatrix} P_{11}(\alpha) & P_{12}(\alpha) & \dots & & & & & \\ 0 & P_{22}(\alpha) & \dots & & & & & \\ \vdots & \vdots & \ddots & & & & & \\ 0 & 0 & \dots & P_{k,k}(\alpha) & P_{k,k+1}(\alpha) & P_{k,k+2}(\alpha) & \dots & P_{k,n}(\alpha) \\ 0 & 0 & \dots & 0 & P_{k+1,k+1}(\alpha) & P_{k+1,k+2}(\alpha) & \dots & P_{k+1,n}(\alpha) \\ 0 & 0 & \dots & 0 & P_{k+2,k+1}(\alpha) & P_{k+2,k+2}(\alpha) & \dots & P_{k+2,n}(\alpha) \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & P_{n,k+1}(\alpha) & P_{n,k+2}(\alpha) & \dots & P_{n,n}(\alpha) \end{pmatrix},$$

где $\deg(P_{ii}) = 2^k$ при $i > k$, и $\deg(P_{ij}) < 2^k$ при $i, j > k$ и $i \neq j$, причем P_{ii} — приведенный с точностью до знака. Рассмотрим уравнения с номерами $i > k$ от β_i с $i > k$:

$$\begin{pmatrix} P_{k+1,k+1}(\alpha) & P_{k+1,k+2}(\alpha) & \dots & P_{k+1,n}(\alpha) \\ P_{k+2,k+1}(\alpha) & P_{k+2,k+2}(\alpha) & \dots & P_{k+2,n}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ P_{n,k+1}(\alpha) & P_{n,k+2}(\alpha) & \dots & P_{n,n}(\alpha) \end{pmatrix}$$

Для краткости обозначим $Q_{ij} = P_{k+i,k+j}(\alpha)$. По предположению $Q_{11} \neq 0$, поэтому мы можем умножить все уравнения после 1-ого на Q_{11}, а потом вычесть из i-ого, $i > 1$ уравнения 1-ое, умноженное на старый (до последнего умножения) коэффициент i-ого уравнения при β_{k+1}:

$$\begin{pmatrix} Q_{11} & Q_{12} & \dots & Q_{1,n-k} \\ 0 & Q_{22}Q_{11} - Q_{21}Q_{12} & \dots & Q_{2,n-k}Q_{11} - Q_{21}Q_{1,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & Q_{n-k,2}Q_{11} - Q_{n-k,1}Q_{12} & \dots & Q_{n-k,n-k}Q_{11} - Q_{n-k,1}Q_{1,n-k} \end{pmatrix}$$

Тогда $\deg(Q_{ii}Q_{11} - Q_{i,1}Q_{1,i}) = 2^{k+1}$, он приведенный с точностью до знака, и $\deg(Q_{ij}Q_{11} - Q_{i,1}Q_{1,j}) < 2^{k+1}$ при $i \neq j$. Мы исключили β_{k+1} из уравнений с номером $i > k+1$ с сохранением условий на коэффициенты, тем самым переход индукции доказан (база $k = 0$).

Подставляя $k = n$, получим систему уравнений на $\beta_1, \dots, \beta_n$, последнее уравнение которой имеет вид $P_{n,n}(\alpha)\beta_n = 0$, где $P_{n,n}$ – приведенный многочлен с целыми коэффициентами. Значит, $P_{n,n}(\alpha) \neq 0$ и $\beta_n \neq 0$, противоречие. Значит, α — целое алгебраическое, ч.т.д.

Задача 69. Пусть $\alpha_1, \dots, \alpha_n$ — целый базис I, тогда если $JI = I$, то для каждого i существуют такие $\beta_{i1}, \dots, \beta_{in} \in J$, что $\alpha_i = \beta_{i1}\alpha_1 +$

$\ldots + \beta_{in}\alpha_n$. Тем самым мы получаем систему линейных уравнений на $\alpha_1, \ldots, \alpha_n$ с коэффициентами

$$\begin{pmatrix} \beta_{11}-1 & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22}-1 & \ldots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn}-1 \end{pmatrix}$$

Заметим, что ситуация аналогична с предыдущей задачей — целые числа заменены на идеал J, а α — на 1. Аналогично с предыдущей задачей мы можем доказать, что 1 — корень приведенного многочленами с коэффициентами в J, из чего будет следовать, что $1 \in J$, поэтому $J = (1)$.

Задача 70. Очевидно следует из конечности числа классов идеалов.

Задача 71. По предыдущей задаче $(\alpha)I^k = (\beta)I^m$ для каких-то ненулевых α и β. Деля на β, получаем $(\alpha/\beta)I^k = I^m$, и т.к. $I^m \subseteq I^k$, то $(\alpha/\beta)I^k \subseteq I^k$. По задаче 68 получаем, что $\gamma = \alpha/\beta \in \widetilde{\mathbb{Z}}$, т.е. $(\gamma)I^k = I^m = I^k I^{m-k}$. Для любого $\alpha \in I^{m-k}$ получаем $(\alpha)I^k \subseteq (\gamma)I^k$, значит $(\alpha/\gamma)I^k \subseteq I^k$, и по задаче 68 $\alpha/\gamma \in \widetilde{\mathbb{Z}}$, т.е. все элементы I^{m-k} делятся на γ. Поэтому $(1/\gamma)I^{m-k}$ — идеал, и $I^k = (1/\gamma)I^{m-k}I^k$. Значит, по задаче 69 мы получаем $(1/\gamma)I^{m-k} = (1)$, поэтому $I^{m-k} = (\gamma)$.

В частности, для $J = I^{m-k-1}$ — $IJ = (\gamma)$.

Задача 72. Если I делится на J, то $I = JH$ для какого-то идеала H, поэтому $I \subseteq J$.

Обратно, если $I \subseteq J$, то возьмем по предыдущей задаче такой идеал J', что $JJ' = (\alpha)$ для ненулевого α. Тогда $IJ' \subseteq JJ' = (\alpha)$, поэтому $H = (1/\alpha)IJ'$ – идеал, и $I = (1/\alpha)JJ'I = JH$. Значит, I делится на J.

Задача 73. Для ненулевого идеала I обозначим $N(I) = |\widetilde{\mathbb{Z}}/I|$ — количество элементов в $\widetilde{\mathbb{Z}}/I$. Если $I \subset J$, то $N(I) > N(J)$, т.к. классы эквивалентности $\widetilde{\mathbb{Z}}/J$ являются объединением каких-то классов эквивалентности $\widetilde{\mathbb{Z}}/I$, причем класс J содержит больше одного класса $\widetilde{\mathbb{Z}}/I$, т.к. $I \neq J$.

Для ненулевого идеала I найдем какой-то его простой делитель, продолжая по индукции цепочку вложенных собственных идеалов $I \subset I_1 \subset I_2 \subset \ldots$ — т.к. $N(I_k)$ уменьшается, то в какой-то момент мы не сможем её продолжить, тогда последний член в цепочке будет простым идеалом P_1 (т.к. он не содержится в других собственных идеалах). По предыдущей задаче $I = P_1 H$ для какого-то идеала H, причем $N(H) < N(I)$. Аналогично для H получаем $H = P_2 R$, т.е. $I = P_1 P_2 R$ с $N(R) < N(H)$. Продолжая эту операцию, пока можем (т.е. $N > 1$), мы получаем разложение $I = P_1 P_2 \ldots P_n$ на простые идеалы.

Задачи 74 - 78. Аналогично задачам 25 – 27.