Na tej liście $d \neq 1$ jest bezkwadratową liczbą całkowitą (nie podzielną przez kwadrat żadnej liczby pierwszej). Przez $\mathbb{Q}[\sqrt{d}]$ oznaczmy zbiór wszystkich liczb zespolonych postaci $a + b\sqrt{d}$, gdzie $a, b \in \mathbb{Q}$.

Przez $\mathbb{Z}[\sqrt{d}]$ oznaczamy zbiór liczb postaci $a + b\sqrt{d}$ dla pewnych $a, b \in \mathbb{Z}$. Łatwo sprawdzić, że jest on zamknięty na dodawanie i mnożenie.

Zadanie 0. Przekonaj się że $\mathbb{Q}[\sqrt{d}]$ i $\mathbb{Z}[\sqrt{d}]$ są zamknięte na dodawanie i mnożenie.

Zadanie 1. Pokaż że w $\mathbb{Q}[\sqrt{d}]$ można dzielić przez niezerowe elementy (tzn. wynik dzielenia jest w $\mathbb{Q}[\sqrt{d}]$).

Normą elementu $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ nazywamy liczbę $N(z) = a^2 - db^2$. W szczególności gdy $d < 0$, to $N(z) = |z|^2$ jako liczby zespolonej.

Zadanie 2. Udowodnij że:

a) norma jest multiplikatywna, tzn. $N(z_1 z_2) = N(z_1)N(z_2)$,

b) jeżeli $z \in \mathbb{Q}[\sqrt{d}]$, $z \neq 0$, to $N(z) \neq 0$,

c) jeżeli $z \in \mathbb{Z}[\sqrt{d}]$, to $z^{-1} \in \mathbb{Z}[\sqrt{d}] \iff N(z) = \pm 1$,

d) jeżeli $z \in \mathbb{Z}[\sqrt{d}]$ i $\pm N(z)$ jest liczbą pierwszą, to z jest nierozkładalny w $\mathbb{Z}[\sqrt{d}]$, tzn. nie jest odwracalny i nie zapisuje się w postaci $z = z_1 z_2$ dla żadnych nieodwracalnych $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$,

e) każdy niezerowy element $\mathbb{Z}[\sqrt{d}]$ przedstawia się jako iloczyn elementów nierozkładalnych.

Zadanie 3. Przedstaw w postaci iloczynu elementów nierozkładalnych:

a) $2 \in \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$,

b) $7 \in \mathbb{Z}[\sqrt{-6}]$,

c) $5 \in \mathbb{Z}[\sqrt{3}]$,

d) $13 \in \mathbb{Z}[\sqrt{-3}]$

Zadanie 4. Wyliczając normy sprawdź że $1 + \sqrt{-5}, 1 - \sqrt{-5}$, 2 i 3 są nierozkładalne w $\mathbb{Z}[\sqrt{-5}]$, ale

$$6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 2 \cdot 3,$$

więc w $\mathbb{Z}[\sqrt{-5}]$ rozkład z ostatniego podpunktu zadania 2. jest bardzo niejednoznaczny.

Zadanie 5. Uzasadnij że jeżeli $d > 0$ i $x \in \mathbb{Z}[\sqrt{d}]$ i $x \neq 0, 1, -1$, to $x, x^2, x^3, x^4, x^5, \ldots$ są parami różne.

Zadanie 6. Wylicz $N(1+\sqrt{2})$ w $\mathbb{Z}[\sqrt{2}]$. Rozważając normy potęg $x=(1+\sqrt{2})$, udowodnij że równanie $a^2-2b^2=1$ ma nieskończenie wiele rozwiązań całkowitych.

Zadanie 7. Udowodnij że równanie ma nieskończenie wiele rozwiązań całkowitych:

a) $a^2=5b^2+1$ b) $a^2=5b^2+11$ c) $a^2=11b^2+23$ d) $a^2=7b^2+8$

Zadanie 8. Weźmy $d=-1$, tak że $\sqrt{d}=\mathbb{Z}[i]$. Uzasadnij że:

a) Dla każdej $z\in\mathbb{Q}[i]$ (a nawet każdej liczby zespolonej z!) istnieje takie $z'\in\mathbb{Z}[i]$, że $N(z-z')=|z-z'|^2\leq\frac{1}{2}$.

b) Weźmy $x,y\in\mathbb{Z}[i]$, $y\neq 0$. Dla $z=\frac{x}{y}$ uzasadnij, że $N(x-yz')<N(y)$.

c) Wywnioskuj że możemy podzielić x przez y z resztą, tzn. $x=yq+r$ dla pewnych $q,r\in\mathbb{Z}[i]$, przy czym $N(r)<N(y)$.

d) Wywnioskuj że jeżeli x,y są względnie pierwsze, to istnieją $a,b\in\mathbb{Z}[i]$ takie że $ax+by$ jest największym wspólnym dzielnikiem x i y (tzn. jest podzielne przez każdy inny ich wspólny dzielnik). W tym celu rozważ niezerowy element postaci $ax+by$ o najmniejszej możliwej normie.

e) Wywnioskuj że jeżeli x jest nierozkładalny i dzieli iloczyn zw, to x dzieli z lub x dzieli w (wskazówka: gdyby tak nie było, to $1=ax+bz=a'y+b'z$ i $1\cdot 1=?$).

f) Załóżmy że $x=a+bi\in\mathbb{Z}[d]$ jest nierozkładalny i p dzieli $a^2+b^2=N(x)$. Uzasadnij że wtedy $a^2+b^2=p$ lub $a+bi\in\{p,-p,ip,-ip\}$. W tym celu rozłóż p na czynniki nierozkładalne (może ich być 1 lub 2) i zauważ, że dzielą one $a^2+b^2=(a+bi)(a-bi)$, więc któryś z nich musi dzielić $a+bi$.

g) Uzasadnij że jeżeli $N(x)$ dzieli się przez p, to x dzieli się przez p lub ma dzielnik o normie p.

h) Załóżmy że $p\equiv 1 \pmod 4$. Korzystając z faktu, że istnieje $x\in\mathbb{Z}$ spełniający $x^2\equiv -1 \pmod p$, pokaż, że można wybrać $x<p/2$ i wtedy $x^2+1=N(x+i)=kp<p^2$. Korzystając z poprzedniego podpunktu wywnioskuj, że $x+i$ ma dzielnik o normie p, więc p jest rozkładalna.

i) Uzasadnij, że jeżeli p jest liczbą pierwszą i $p\equiv 3 \pmod 4$, to p jest nierozkładalna w $\mathbb{Z}[i]$.

j) Wywnioskuj że (nieodwracalne) elementy nierozkładalne w $\mathbb{Z}[i]$ to dokładnie:

- liczby postaci $p,-p,ip,-ip$, gdzie $p\equiv 3 \pmod 4$ jest pierwsze,
- liczby postaci $a+bi$, gdzie $a^2+b^2=p$ jest liczbą pierwszą dającą resztę 1 z dzielenia przez 4.

Zadanie 9. Zauważ że sumy dwóch kwadratów liczb całkowitych to dokładnie normy elementów $\mathrm{Z}[i]$. Wywnioskuj stąd, że $k \in \mathrm{N}$ jest sumą dwóch kwadratów dokładnie wtedy gdy w rozkładzie k na czynniki pierwsze liczby pierwsze dające resztę 1 z dzielenia przez 4 występują parzystą liczbę razy. (Wskazówka: załóżmy że k jest sumą dwóch kwadratów. Znajdź $x \in \mathrm{Z}[i]$ i rozłóż go na czynniki nierozkładalne.)