2. Arytmetyka w $\mathbf{Z}[\sqrt{-2}]$

Interesować nas będzie równanie

$$n = a^2 + 2b^2. \tag{1}$$

Chcemy wiedzieć, dla jakich całkowitych n równanie to ma całkowite rozwiązania. Niech

$$\mathbf{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbf{Z}\}$$

(przyjmijmy $\sqrt{-2} = i\sqrt{2}$). Dla $z = a + b\sqrt{-2} \in \mathbf{Z}[\sqrt{-2}]$ określamy $\overline{z} = a - b\sqrt{-2}$ i $N(z) = z\overline{z} = a^2 + 2b^2$. Operacja $\overline{\ }$ pokrywa się ze zwyczajnym sprzężeniem zespolonym, a norma N z kwadratem modułu. Pytanie o rozwiązywalność równania (1) można wyrazić jako pytanie o istnienie $z \in \mathbf{Z}[\sqrt{-2}]$ takiego, że $N(z) = n$.

Wiemy, że $\overline{zw} = \overline{z} \cdot \overline{w}$, i że $N(zw) = N(z)N(w)$. Zatem jeśli (1) ma rozwiązania dla $n = n_1$ i $n = n_2$, to ma je także dla $n = n_1 n_2$. Naturalne jest więc pytanie: dla jakich liczb pierwszych n równanie (1) ma rozwiązanie. W dalszym ciągu p oznacza nieparzystą całkowitą liczbę pierwszą.

1. Wyznacz elementy odwracalne w $\mathbf{Z}[\sqrt{-2}]$.
2. Pokaż, że jeśli $a^2 + 2b^2 = p$ ma rozwiązanie, to kongruencja $x^2 \equiv -2 \bmod p$ też ma rozwiązanie.
3. Zbadaj kilka(naście) początkowych liczb pierwszych i postaw hipotezę: dla jakich p kongruencja $x^2 \equiv -2 \bmod p$ ma rozwiązanie?
4. Udowodnij, że dla dowolnego $z \in \mathbf{Z}[\sqrt{-2}]$ i dowolnego niezerowego $w \in \mathbf{Z}[\sqrt{-2}]$ istnieją $q, r \in \mathbf{Z}[\sqrt{-2}]$, takie że $z = qw + r$ i $N(r) \leq \frac{3}{4}N(w)$.

Można więc w $\mathbf{Z}[\sqrt{-2}]$ wykonywać algorytm Euklidesa i wyliczać największy wspólny dzielnik.

5. W $\mathbf{Z}[\sqrt{-2}]$ nie ma porządku. Co to więc właściwie znaczy "największy wspólny dzielnik"? Udowodnij, że jest on określony z dokładnością do znaku.

Największy wspólny dzielnik liczb $z, w \in \mathbf{Z}[\sqrt{-2}]$ (którykolwiek z dwóch) będziemy oznaczać (z, w). Z algorytmu Euklidesa wnioskujemy, że $(z, w) = xz + yw$ dla pewnych $x, y \in \mathbf{Z}[\sqrt{-2}]$. Dalej, wnioskujemy że dla elementu z pierwszego w $\mathbf{Z}[\sqrt{-2}]$ i dowolnych $x, y \in \mathbf{Z}[\sqrt{-2}]$ zachodzi implikacja: $z|xy \Rightarrow z|x \vee z|y$. Stąd wynika istnienie i jednoznaczność (z dokładnością do stowarzyszenia) rozkładu na czynniki pierwsze w $\mathbf{Z}[\sqrt{-2}]$.

6. Uzasadnij, że jeśli $N(z)$ jest liczbą pierwszą w $\mathbf{Z}$, to z jest nierozkładalny w $\mathbf{Z}[\sqrt{-2}]$. Podaj przykłady takich elementów z w $\mathbf{Z}[\sqrt{-2}]$. Podaj przykłady liczb pierwszych w $\mathbf{Z}$, które są rozkładalne w $\mathbf{Z}[\sqrt{-2}]$.
7. Pokaż, że jeśli kongruencja $x^2 \equiv -2 \bmod p$ ma rozwiązanie, to p rozkłada się w $\mathbf{Z}[\sqrt{-2}]$ na dwa czynniki, oba o normie p. W konsekwencji $p = a^2 + 2b^2$.
8. Uzasadnij, że jeśli kongruencja $x^2 \equiv -2 \bmod p$ nie ma rozwiązania, to liczba p jest elementem pierwszym w $\mathbf{Z}[\sqrt{-2}]$.
9. Udowodnij, że każdy element pierwszy w $\mathbf{Z}[\sqrt{-2}]$ jest dzielnikiem pewnej liczby p pierwszej w $\mathbf{Z}$. Wywnioskuj stąd, że każdy taki element jest (z dokładnoscią do znaku):
   - albo liczbą pierwszą p, taką że $x^2 \equiv -2 \bmod p$ nie ma rozwiązania;
   - albo jednym z dwóch niestowarzyszonych czynników liczby pierwszej p, takiej że $x^2 \equiv -2 \bmod p$ ma rozwiązanie;
   - albo czynnikiem $\sqrt{-2}$ pochodzącym od parzystej liczby pierwszej 2.
10. Niech w rozkładzie liczby całkowitej n na czynniki pierwsze występuje z nieparzystym wykładnikiem pewna liczba pierwsza p, taka że $x^2 \equiv -2 \bmod p$ nie ma rozwiązania. Pokaż, że wtedy $n \neq a^2 + 2b^2$.
11. Sformułuj warunek na przedstawialność liczby całkowitej w postaci $a^2 + 2b^2$.

Pozostaje stwierdzić kiedy kongruencja $x^2 \equiv -2 \bmod p$ nie ma rozwiązanie. Bajka o tym będzie jutro.

12. Zrób zadanie 7 używając tw. Minkowskiego.
13. W terminach rozkładu n na czynniki pierwsze w $\mathbf{Z}$ określ ile rozwiązań ma równanie $n = a^2 + 2b^2$.
14. Rozwiąż w $\mathbf{Z}$: $x^3 = y^2 + 2$.