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

Załóżmy, że $d \in \mathbf{Z}$ jest bezkwadratowa (tzn. nie dzieli się przez kwadrat żadnej liczby pierwszej). Interesować nas będzie równanie

$$n = a^2 - db^2. \tag{1}$$

Chcemy wiedzieć, dla jakich całkowitych n równanie to ma całkowite rozwiązania. Niech $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbf{Z}\}$ (dla $d < 0$ przyjmijmy $\sqrt{d} = i\sqrt{-d}$). Dla $z = a + b\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$ określamy $\overline{z} = a - b\sqrt{d}$ i $N(z) = z\overline{z} = a^2 - db^2$. Dla $d < 0$ 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 $z \in \mathbf{Z}[\sqrt{d}]$ takiego, że $N(z) = n$.

1. Wylicz, że $N(zw) = N(z)N(w)$. Wywnioskuj stąd, że 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. Kwestia jednoznaczności rozwiązań wiąże się z pojęciem elementu odwracalnego. Element $z \in \mathbf{Z}[\sqrt{d}]$ nazywamy *odwracalnym,* jeżeli istnieje $w \in \mathbf{Z}[\sqrt{d}]$, takie że $zw = 1$.

2. Udowodnij, że $z \in \mathbf{Z}[\sqrt{d}]$ jest odwracalny wtedy i tylko wtedy, gdy $N(z) = \pm 1$. Wyjaśnij, jak – mając element $z \in \mathbf{Z}[\sqrt{d}]$, $z \neq 1$, spełniający $N(z) = 1$ – przerobić rozwiązanie równania (1) na inne rozwiązanie równania (1).

d=-2

Elementy odwracalne.

3. Wyznacz elementy odwracalne w $\mathbf{Z}[\sqrt{-2}]$.

Algorytm Euklidesa.

Podzielność w $\mathbf{Z}[\sqrt{d}]$ definiujemy jak w $\mathbf{Z}$: liczba w jest dzielnikiem z (piszemy: $w|z$), jeśli istnieje $q \in \mathbf{Z}[\sqrt{d}]$, takie że $z = qw$.

4. Zauważ, że jeśli $w|z$ w $\mathbf{Z}[\sqrt{d}]$, to $N(w)|N(z)$ w $\mathbf{Z}$.

5. Uzasadnij, że dla dowolnej liczby zespolonej c istnieje liczba $z \in \mathbf{Z}[\sqrt{-2}]$, taka że $|z - c| \leq \frac{\sqrt{3}}{2}$.

Przybliżając w ten sposób dokładny zespolony iloraz $\frac{z}{w}$ dwóch liczb $z, w \in \mathbf{Z}[\sqrt{-2}]$ dostajemy:

6. 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 $N(r) \leq \frac{3}{4}N(w)$.

Liczby q i r nie są wyznaczone jednoznacznie, więc i "algorytm" Euklidesa w $\mathbf{Z}[\sqrt{-2}]$ zbudowany w oparciu o zadanie 6 nie będzie algorytmem w ścisłym sensie. Mimo to: dzielimy – jak w zadaniu 6 – z przez w, potem w przez r i tak dalej. Normy kolejnych reszt ściśle maleją, a są całkowite – w końcu musimy więc dostać resztę 0.

7. Udowodnij, że ostatnia niezerowa reszta w powyższym algorytmie Euklidesa to największy wspólny dzielnik liczb z i w, tzn. (1) jest ona ich dzielnikiem i (2) jest podzielna przez każdy ich wspólny dzielnik.

W szczególności pokazaliśmy, że każde dwie (niezerowe) liczby w $\mathbf{Z}[\sqrt{-2}]$ w ogóle mają największy wspólny dzielnik. Jest on też jedyny:

8. W $\mathbf{Z}[\sqrt{d}]$ iloraz dwóch największych wspólnych dzielników (zdefiniowanych jak w poprzednim zadaniu) jest zawsze elmentem odwracalnym. W $\mathbf{Z}[\sqrt{-2}]$ największy wspólny dzielnik jest więc – z dokładnością do znaku – jednoznaczny.

Największy wspólny dzielnik liczb z, w (którykolwiek z dwóch) będziemy oznaczać (z, w).

9. Uzasadnij, że $(z, w) = uz + vw$ dla pewnych $u, v \in \mathbf{Z}[\sqrt{-2}]$.

Dla nieparzystej liczby pierwszej p i niepodzielnej przez nią liczby całkowitej a określamy *symbol Legendre'a* $(\frac{a}{p})$ jako $+1$, jeśli kongruencja $x^2 \equiv a \bmod p$ ma rozwiązanie, a jako -1, jeśli nie ma ona rozwiązania.

Rozkład na czynniki pierwsze.

Nieodwracalny element $z \in \mathbf{Z}[\sqrt{d}]$ nazywamy *nierozkładalnym,* jeśli w każdym jego rozkładzie $z = uw$ na czynniki z $\mathbf{Z}[\sqrt{d}]$ jeden czynnik jest odwracalny. (W $\mathbf{Z}[\sqrt{-2}]$, podobnie jak w $\mathbf{Z}$, znaczy to, że jeden czynnik jest równy ± 1.)

Nieodwracalny element $z \in \mathbf{Z}[\sqrt{d}]$ nazywamy *pierwszym,* jeśli dla dowolnych $u, w \in \mathbf{Z}[\sqrt{d}]$ zachodzi implikacja: $z|uw \Rightarrow z|u \vee z|w$.

10. Uzasadnij, że jeśli $N(z)$ jest liczbą pierwszą w $\mathbf{Z}$, to z jest nierozkładalny w $\mathbf{Z}[\sqrt{d}]$. Podaj przykłady takich elementów z w $\mathbf{Z}[\sqrt{-2}]$. Podaj przykłady liczb pierwszych w $\mathbf{Z}$, które są rozkładalne w $\mathbf{Z}[\sqrt{-2}]$.
11. Wywnioskuj z zadania 9, że w $\mathbf{Z}[\sqrt{-2}]$ każdy element nierozkładalny jest pierwszy. Sprawdź też, że w $\mathbf{Z}[\sqrt{d}]$ każdy element pierwszy jest nierozkładalny.
12. Udowodnij, że każdy element $\mathbf{Z}[\sqrt{d}]$ daje się rozłożyć w skończony iloczyn elementów nierozkładalnych.
13. Używając zadania 11 wykaż, że w $\mathbf{Z}[\sqrt{-2}]$ rozkład na czynniki pierwsze jest jednoznaczny – z dokładnością do znaku czynników i ich kolejności.

Równanie $p = a^2 + 2b^2$**.**(Zakładamy, że p jest nieparzystą liczbą pierwszą.)

14. Pokaż, że jeśli $a^2 + 2b^2 = p$ ma rozwiązanie, to kongruencja $u^2 \equiv -2 \bmod p$ też ma rozwiązanie.
15. Pokażemy, że jeśli kongruencja $u^2 \equiv -2 \bmod p$ ma rozwiązanie, to $p = a^2 + 2b^2$.
    a) Uzasadnij, że jeśli $p|a + b\sqrt{-2}$ w $\mathbf{Z}[\sqrt{-2}]$, to $p|a$ i $p|b$ (w $\mathbf{Z}$).
    b) Niech $p|u^2 + 2$. Używając rozkładu $u^2 + 2 = (u + \sqrt{-2})(u - \sqrt{-2})$ uzasadnij, że p nie jest pierwsza w $\mathbf{Z}[\sqrt{-2}]$. A zatem p jest rozkładalna w $\mathbf{Z}[\sqrt{-2}]$.
    c) Uzasadnij, że w $\mathbf{Z}[\sqrt{-2}]$ liczba p rozkłada się na dwa czynniki, oba o normie p. Wywnioskuj stąd, że $p = a^2 + 2b^2$.
16. Uzasadnij, że jeśli kongruencja $u^2 \equiv -2 \bmod p$ nie ma rozwiązania, to liczba p jest elementem pierwszym w $\mathbf{Z}[\sqrt{-2}]$.
17. Udowodnij, że każdy nierozkładalny element w $\mathbf{Z}[\sqrt{-2}]$ jest dzielnikiem pewnej liczby p pierwszej w $\mathbf{Z}$. Wywnioskuj stąd, że każdy element nierozkładalny jest albo liczbą pierwszą p spełniającą $(\frac{-2}{p}) = -1$, albo jednym z dwóch czynników liczby pierwszej p spełniającej $(\frac{-2}{p}) = 1$. (Z dokładnością do znaku; no i jest jeszcze element $\sqrt{-2}$ pochodzący od parzystej liczby pierwszej 2.)
18. Niech w rozkładzie liczby całkowitej n na czynniki pierwsze występuje w potędze nieparzystej pewna liczba pierwsza p spełniająca $(\frac{-2}{p}) = -1$. Pokażemy, że wtedy $n \neq a^2 + 2b^2$. Załóżmy nie wprost, że $n = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$. Uzasadnij, że liczba p (która jest pierwsza także w $\mathbf{Z}[\sqrt{-2}]$) występuje z takim samym wykładnikiem w rozkładzie $a + b\sqrt{-2}$ i w rozkładzie $a - b\sqrt{-2}$. Zatem p występuje z parzystym wykładnikiem w rozkładzie n, sprzeczność.
19. Sformułuj warunek na przedstawialność liczby całkowitej w postaci $a^2 + 2b^2$.

Pozostaje stwierdzić, kiedy $(\frac{-2}{p}) = 1$, a kiedy $(\frac{-2}{p}) = -1$. To jest już jednak trochę inna bajka.

---

d=2

Równanie $a^2 - 2b^2 = 1$ ma nieskończenie wiele rozwiązań: liczba $\epsilon = 3 - 2\sqrt{2}$ i jej potęgi o całkowitych wykładnikach (też ujemnych!) należą do $\mathbf{Z}[\sqrt{2}]$ i mają normę 1. Potęgi te są parami różne, gdyż $|\epsilon| < 1$.

20. Niech $N(z) = 1$, $z \in \mathbf{Z}[\sqrt{2}]$, $\epsilon = 3 - 2\sqrt{2}$.
    a) Dla pewnego $n \in \mathbf{Z}$ element $w = z\epsilon^n \in \mathbf{Z}[\sqrt{2}]$ spełnia $N(w) = 1$ i $|\epsilon| \leq |w| < 1$.
    b) Można założyć, że $w = a - b\sqrt{2}$, gdzie $a, b \geq 0$ (kosztem ewentualnej zmiany w na $-w$).
    c) $\overline{w} = a + b\sqrt{2}$, $1 < |a + b\sqrt{2}| \leq \frac{1}{|\epsilon|} = 3 + 2\sqrt{2}$.
    d) $0 \leq a < 6$, $0 \leq b < 5$. Przepatrz te 20 możliwości.
    e) Konkluzja: $z = \pm\epsilon^n = \pm(3 - 2\sqrt{2})^n$ dla pewnego $n \in \mathbf{Z}$.
21. Wszystkie całkowite rozwiązania równania $a^2 - 2b^2 = 1$ to ($n \in \mathbf{Z}$, znaki w obu wyrażeniach zgodne):

$$a = \pm\frac{1}{2}(\epsilon^n + \epsilon^{-n}), \qquad b = \pm\frac{1}{2\sqrt{2}}(\epsilon^n - \epsilon^{-n}).$$

Postępując podobnie można pokazać, że wszystkie rozwiązania równania $N(z) = \pm 1$ są postaci $\pm(1 - \sqrt{2})^n$, co daje opis wszystkich odwracalnych elementów w $\mathbf{Z}[\sqrt{2}]$.