7. Redukcja.

Mówimy, że $(\alpha,\gamma),(\beta,\delta)\in\mathbf{Z}^2$ tworzą bazę $\mathbf{Z}^2$, jeśli każdy wektor $(x,y)\in\mathbf{Z}^2$ zapisuje się jako $m(\alpha,\gamma)+n(\beta,\delta)$ dla pewnych całkowitych m,n.

1. Udowodnij, że $(\alpha,\gamma),(\beta,\delta)\in\mathbf{Z}^2$ tworzą bazę $\mathbf{Z}^2 \iff \alpha\delta-\beta\gamma=\pm1$.
2. Udowodnij, że pole równoległoboku rozpiętego przez wektory $(\alpha,\gamma),(\beta,\delta)$ jest równe $|\alpha\delta-\beta\gamma|$.
3. Udowodnij, że przekształcenie $F\colon\mathbf{Z}^2\to\mathbf{Z}^2$ dane wzorem $F(x,y)=(\alpha x+\beta y,\gamma x+\delta y)$ jest bijekcją $\iff$ $\alpha\delta-\beta\gamma=\pm1$. Napisz wzorem przekształcenie odwrotne.
4. Udowodnij, że równoważność form kwadratowych jest przechodnia: $P\sim Q\sim R\Rightarrow P\sim R$.
5. Udowodnij, że formy równoważne mają równe wyróżniki.
6. Znajdź wszystkie zredukowane formy o wyróżniku -23.
7. Dla każdego z następujących ujemnych wyróżników istnieje jedyna forma zredukowana:

   $$-3,-4,-7,-8,-11,-19,-43,-67,-163.$$

   Sprawdź to dla kilku liczb z tej listy. Wyciągnij wnioski dotyczące reprezentowania liczb pierwszych przez znalezioną formę.
   (Gauss przypuszczał, że lista jest kompletna; Heegner pokazał to w latach 50-tych XX wieku.)
8. Żadne dwie zredukowane formy nie są równoważne. Uzasadnij to w przypadku, gdy jedna z nich – $Q(x,y)=ax^2+bxy+cy^2$ – spełnia $|b|<a<c$. (Ogólny przypadek jest nieznacznie trudniejszy.) Wskazówki:
   a) Uzasadnij, że $Q(x,y)\geq(a-|b|+c)\min(x^2,y^2)$.
   b) Uzasadnij, że $a<c<a-|b|+c$ to trzy najmniejsze niezerowe liczby reprezentawane przez Q, przy czym wartość a jest przyjmowana jedynie na $(\pm1,0)$, zaś c jedynie na $(0,\pm1)$.
9. Rozstrzygnij, które liczby pierwsze są postaci x^2+5y^2, a które postaci $2x^2+2xy+3y^2$.

Książki:
Gauss, Disquisitiones Arithmeticae
Cox, Primes of the form x^2+ny^2
Edwards, Fermat's Last Theorem