Algebra ISIM 2. Lista 5

Na tej liście p i q oznaczają nieparzyste liczby pierwsze. Przez $(\mathbf{Z}/n)^\times$ oznaczamy multyplikatywną grupę reszt odwracalnych modulo n. Homomorfizm z grupy G w multyplikatywną grupę $\mathbf{T}$ liczb zespolonych o module 1 nazywamy charakterem grupy G.

Ćwiczenia

1. Przedyskutuj kwestię jednoznaczności rozkładu skończonej grupy abelowej w produkt czynników postaci $\mathbf{Z}/p^k$.
2. Udowodnij, że jeśli p nie dzieli a, to $a^{p-1} \equiv 1 \bmod p$. (Użyj grupy $(\mathbf{Z}/p)^\times$.)
3. Udowodnij, że $(p-1)! \equiv -1 \bmod p$. (Użyj grupy $(\mathbf{Z}/p)^\times$.)
4. Uzasadnij, że jeśli $x^2 \equiv 1 \bmod p$, to $x \equiv \pm 1 \bmod p$.
5. Uzasadnij, że $\mathbf{Z}/n$ ma n różnych charakterów.
6. Niech ϕ będzie nietrywialnym charakterem $\mathbf{Z}/n$. Uzasadnij, że $\sum_{g\in\mathbf{Z}/n} \phi(g) = 0$.
7. Niech $\phi, \psi\colon \mathbf{Z}/n \to \mathbf{T}$ będą dwoma różnymi charakterami. Uzasadnij, że $\sum_{g\in\mathbf{Z}/n} \phi(g)\overline{\psi(g)} = 0$.

Zadania

W kolejnych pięciu zadaniach zakładamy, że G jest skończoną grupą abelową.

8. Niech $\phi, \psi\colon G \to \mathbf{T}$ będą dwoma różnymi charakterami. Uzasadnij, że $\sum_{g\in G} \phi(g)\overline{\psi(g)} = 0$.
9. Udowodnij, że G ma $|G|$ różnych charakterów.
10. Niech $\widehat{G}$ oznacza zbiór charakterów grupy G. Tworzy on grupę (tzw. *grupę dualną* do G) z działaniem mnożenia: $(\phi\psi)(g) = \phi(g) \cdot \psi(g)$. Udowodnij, że $\widehat{\widehat{G}} \simeq G$ (w sposób naturalny: wyjaśnij, w jaki sposób elementy G zadają charaktery grupy $\widehat{G}$), i że $\widehat{G} \simeq G$ (w sposób nienaturalny).
11. Przestrzeń $L^2(G)$ zespolonych funkcji na grupie G ma naturalny iloczyn skalarny: $\langle f, s\rangle = \sum_{g\in G} f(g)\overline{s(g)}$. Uzasadnij, że charaktery G tworzą bazę ortogonalną tej przestrzeni.
12. *Transformata Fouriera* $L^2(G) \ni f \mapsto \widehat{f} \in L^2(\widehat{G})$ jest określona wzorem $\widehat{f}(\chi) = \langle f, \chi\rangle = \sum_{g\in G} f(g)\overline{\chi(g)}$. Uzasadnij, że:
$$f = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi \quad \text{(równość w } L^2(G)\text{)}; \qquad \widehat{\widehat{f}}(g) = |G| f(g^{-1}).$$

Dla liczby całkowitej a niepodzielnej przez p określamy symbol Legendre'a $\left(\frac{a}{p}\right)$ jako $+1$, jeśli a jest kwadratem modulo p, zaś jako -1, jeśli a nie jest kwadratem modulo p.

13.

a) Udowodnij, że element grupy cyklicznej rzędu $2n$ jest w niej kwadratem pewnego elementu $\iff$ jego n-ta potęga jest elementem neutralnym.

b) Udowodnij, że $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

c) Udowodnij, że $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

14. Udowodnij, że $(\mathbf{Z}/pq)^\times \simeq (\mathbf{Z}/p)^\times \times (\mathbf{Z}/q)^\times$:

a) Sprawdź, że $\phi\colon x \bmod pq \mapsto (x \bmod p, x \bmod q)$ jest monomorfizmem.

b) Wywnioskuj, że ϕ jest izomorfizmem.

c) Sprawdź, że obrazem przez ϕ podgrupy $\{\pm 1\}$ jest podgrupa $\{(1,1), (-1,-1)\}$.

15. Celem tego zadania jest dowód prawa wzajemności reszt kwadratowych przez policzenie (na dwa sposoby) iloczynu wszystkich elementów grupy $(\mathbf{Z}/pq)^\times/\{\pm 1\}$, izomorficznej przez ϕ (patrz poprzednie zadanie) z $((\mathbf{Z}/p)^\times \times (\mathbf{Z}/q)^\times)/\{\pm(1,1)\}$. Niech $p = 2P+1$, $q = 2Q+1$.

a) Wymnóż względnie pierwsze z pq elementy zbioru $\{1, 2, \ldots, \frac{pq-1}{2}\}$. Pokaż, że obraz tego iloczynu przez ϕ to $\pm\left(\frac{(p-1)!^Q}{q^P}, \frac{(q-1)!^P}{p^Q}\right)$

b) Wymnóż elementy zbioru $\{1, 2, \ldots, P\} \times \{1, 2, \ldots, q-1\}$ i otrzymaj $\pm(P!^{q-1}, (q-1)!^P)$.

c) Uzasadnij, że $(p-1)! \equiv (-1)^P P!^2 \bmod p$.

d) Porównaj wyniki z użyciem punktu c); pokaż, że

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

16. Uzasadnij, że jeśli x i y nie dzielą się przez p, ale $p|x^2+5y^2$, to $p \equiv 1, 3, 7, 9 \bmod 20$.
17. Wykaż, że grupa $(\mathbf{Z}/p^n)^\times$ jest cykliczna:
a) Uzasadnij, że jeśli a jest generatorem $(\mathbf{Z}/p)^\times$, to a lub $a+p$ jest generatorem $(\mathbf{Z}/p^2)^\times$.
b) Dla $n \geq 2$ uzasadnij, że jeśli a jest generatorem $(\mathbf{Z}/p^n)^\times$, to a jest też generatorem $(\mathbf{Z}/p^{n+1})^\times$.
18. Niech liczba pierwsza p będzie postaci $1+2^k n$, gdzie n jest nieparzysta. Uzasadnij, że jeśli a jest niepodzielna przez p, to ciąg $(a^n \bmod p, a^{2n} \bmod p, a^{4n} \bmod p, \ldots, a^{2^k n} \bmod p)$ albo składa się z samych jedynek, albo tuż przed pierwszym wystąpieniem jedynki ma wyraz -1.

---

19. Na własności z poprzedniego zadania oparty jest *test pierwszości Millera–Rabina.* Dla podejrzanej o pierwszość liczby p losujemy $a < p$ i sprawdzamy własność z zadania. Jeśli liczba p jest złożona, to wykryjemy to z prawdopodobieństwem $\geq 3/4$. Wielokrotne powtórzenie tego testu z niezależnym losowaniem a pozwala zwiększyć to prawdopodobieństwo.

    Dla nieparzystej liczby naturalnej n o rozkładzie na czynniki pierwsze $n = \prod_i p_i^{\alpha_i}$ oraz niepodzielnej przez n liczby a definiujemy symbol Jacobiego jako $\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$.
20. Udowodnij, że dla dodatnich nieparzystych liczb całkowitych m, n zachodzi

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\left(\frac{n}{m}\right)$$

    Ta zależność pozwala sprawnie wyliczać symbole Legendre'a.
21. Test pierwszości Solovaya–Strassena. Chcemy sprawdzić, czy nieparzysta liczba n jest pierwsza. W tym celu losujemy liczbę $a < n$, upewniamy się, czy $(a, n) = 1$ (np. algorytmem Euklidesa), po czym sprawdzamy, czy $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$. Jeśli n jest pierwsza, to tak będzie. Jeśli n jest złożona, to szansa, że tak będzie jest nie większa niż $1/2$; aby ją zmniejszyć, należy test wykonać kilka razy, niezależnie losując a.