Kongruencje kwadratowe

Notacja i podstawowe fakty:

Przez p oznaczamy nieparzystą liczbę pierwszą, a przez $\equiv$ przystawanie modulo p ($a \equiv b \iff p|a-b$). Oznaczamy też: $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$, $\mathbf{Z}_p^\times = \{1, \ldots, p-1\}$. Liczbę całkowitą zwykle utożsamiamy z jej resztą modulo p, i działania arytmetyczne wykonujemy zwykle modulo p. Wiemy że $p|ab \Rightarrow (p|a \vee p|b)$, oraz że $a^{p-1} \equiv 1$ dla $a \in \mathbf{Z}_p^\times$. W zbiorze $\mathbf{Z}_p^\times$ istnieje *pierwiastek pierwotny* u, tzn. element spełniający $\{1, u, u^2, \ldots, u^{p-2}\} = \mathbf{Z}_p^\times$ (potęgowanie modulo p).

Ile jest $x \in \mathbf{Z}_p$ spełniających $x^2 \equiv 1$? Dla takiego x zachodzi $p|x^2-1 = (x-1)(x+1)$, stąd $x = \pm 1$.

1.a) Uzasadnij, że w $\mathbf{Z}_p$ kongruencja $x^2 \equiv 0$ ma jedyne rozwiązanie: $x = 0$.

b) Udowodnij, że dla $a \in \mathbf{Z}_p^\times$ kongruencja $x^2 \equiv a$ albo nie ma rozwiązań w $\mathbf{Z}_p$, albo ma dokładnie dwa rozwiązania w $\mathbf{Z}_p$.

c) Dla $p = 7$ znajdź wszystkie $a \in \mathbf{Z}_p$ dla których kongruencja $x^2 \equiv a$ ma rozwiązanie.

Definicja. Dla $a \in \mathbf{Z}_p^\times$ określamy *symbol Legendre'a* następująco: $\left(\frac{a}{p}\right) = +1$ jeśli kongruencja $x^2 \equiv a$ ma rozwiązanie, zaś $\left(\frac{a}{p}\right) = -1$ jeśli ta kongruencja nie ma rozwiązania. (Przyjmuje się też czasem $\left(\frac{0}{p}\right) = 0$; nie będziemy tego używać.)

2. Udowodnij, że $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$. [Wsk. rozważ $a = u^{2k}$ i $a = u^{2k+1}$, gdzie u to pierwiastek pierwotny.]

3. Wywnioskuj z poprzedniego zadania:

a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

b) jeśli $x^2 \equiv a$ nie ma rozwiązania i $x^2 \equiv b$ też nie ma rozwiązania, to $x^2 \equiv ab$ ma rozwiązanie.

4. Uzasadnij, że -1 jest kwadratem modulo $p \iff p$ jest postaci $4k+1$.

5. Przypomnij sobie wzór na rozwiązania równania kwadratowego i jego wyprowadzenie. Przepisz je na przypadek kongruencji kwadratowej modulo p: udowodnij, że $\alpha x^2 + \beta x + \gamma \equiv 0$ ma rozwiązanie w $\mathbf{Z}_p$ wtedy i tylko wtedy, gdy: $\left(\frac{\beta^2 - 4\alpha\gamma}{p}\right) = +1$ (i wtedy są dwa rozwiązania), lub $\beta^2 - 4\alpha\gamma = 0$ (i wtedy jest jedno rozwiązanie).

6. Rozwiąż kongruencję $x^2 + x + 1 \equiv 0$ modulo 11, a także modulo 13.

Obliczenie $\left(\frac{2}{p}\right)$.

7. Niech $L = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}$, i niech $R = 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)$. Uzasadnij, że

a) $R \equiv 2^{\frac{p-1}{2}} L$;

b) nieparzyste czynniki iloczynu L przystają – z minusem – do czynników iloczynu R większych od $\frac{p}{2}$;

c) czynników iloczynu R większych od $\frac{p}{2}$ jest $\lfloor \frac{p}{2} \rfloor - \lfloor \frac{p}{4} \rfloor$;

d) czynników iloczynu R większych od $\frac{p}{2}$ jest $k+1$ (jeśli $p = 4k+3$) lub k (jeśli $p = 4k+1$).

e) $\left(\frac{2}{p}\right) = +1$ gdy $p \equiv \pm 1 \bmod 8$, zaś $\left(\frac{2}{p}\right) = -1$ gdy $p \equiv \pm 3 \bmod 8$; jednym zgrabnym wzorem:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

8. Oblicz $\left(\frac{-2}{p}\right)$.

9. O liczbach postaci $a^2 + 2b^2$.

a) Uzasadnij, że jeśli $p = a^2 + 2b^2$, to $\left(\frac{-2}{p}\right) = +1$, i w konsekwencji $p \equiv 1, 3 \bmod 8$.

b) Uzasadnij, że jeśli $p|a^2 + 2b^2$, to $p \equiv 1, 3 \bmod 8$ – chyba że $p|a$ i $p|b$.

c) Uzasadnij, że jeśli $p|a^2 + 2b^2$, to w rozkładzie $a^2 + 2b^2$ na czynniki pierwsze czynnik p występuje z wykładnikiem parzystym, chyba że $p \equiv 1, 3 \bmod 8$.

d) Uzasadnij, że w rozładzie $a^2 + 2b^2$ na czynniki pierwsze czynniki postaci $8k-1$ i czynniki postaci $8k-3$ występują z wykładnikami parzystymi.

e) Uzasadnij, że jeśli $p \equiv 1, 3 \bmod 8$, to $\left(\frac{-2}{p}\right) = +1$, i wtedy istnieją $a, b \in \mathbf{Z}_p^\times$ spełniające $p|a^2 + 2b^2$.

---

10. Imitując zadanie 7 oblicz $\left(\frac{5}{p}\right)$. Iloczyn L pozostanie taki sam; napisz odpowiednią wersję iloczynu R.
    a) Uzasadnij, że liczba czynników iloczynu R które przystają modulo p do ujemnych elementów zbioru $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$ jest równa $\lfloor 0{,}4\,p \rfloor - \lfloor 0{,}3\,p \rfloor + \lfloor 0{,}2\,p \rfloor - \lfloor 0{,}1\,p \rfloor$.
    b) Przyjmij $p = 10k + r$ i dla każdej możliwej wartości r oblicz wyrażenie z poprzedniego podpunktu.
    c) Zauważ, że $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$.

Obserwacja kończąca ostatnie zadanie jest szczególnym przypadkiem *prawa wzajemności reszt kwadratowych* udowodnionego przez Gaussa. Prawo to mówi, że dla nieparzystych liczb pierwszych p, q zachodzi $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ – chyba że $p \equiv q \equiv 3 \bmod 4$, kiedy to $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Jednym zgrabnym wzorem pisze się to tak:

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

11.* Udowodnij prawo wzajemności dla $q = 3$. Zastosuj je do następującego zadania:
" Dane są takie liczby całkowite a i b, że $a \neq 0$ oraz liczba $3 + a + b^2$ jest podzielna przez $6a$. Wykazać, że liczba a jest ujemna."