

Reszty Kwadratowe

Filip Maniak

Poręba Wielka, 11.2023

1 Czym jest reszta kwadratowa?

Reszta kwadratowa $a \pmod{p}$ to taka liczba, że istnieje x taki że $x^2 \equiv a \pmod{p}$. Przykładowo dla 4 resztami kwadratowymi są 0 i 1, dla 5 są 0, 1 i 4, dla 7 są 0, 1, 2, 4.

2 Symbol Legendre'a

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{dla } a \text{ będącego resztą kwadratową} \\ 0 & \text{dla } p \mid a \\ -1 & \text{dla } a \text{ nie będącego resztą kwadratową} \end{cases}$$

Twierdzenie 1 (Kryterium Eulera) Niech p będzie nieparzystą liczbą pierwszą:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

Faktem wynikającym bezpośrednio z kryterium Eulera, jest że (-1) jest resztą kwadratową tylko dla liczb pierwszych $p = 4k + 1$

Twierdzenie 2 (Multiplikatywność symbolu Legendre'a) Niech p będzie nieparzystą liczbą pierwszą:

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

Twierdzenie 3 (Prawo wzajemności reszt kwadratowych) Jeśli p i q to różne nieparzyste liczby pierwsze to:

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

Jeśli p to nieparzysta liczba pierwsza to:

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

3 Zadania

1. *Dana jest nieparzysta liczba pierwsza p , oraz jej generator g . Udowodnij że

$$\left(\frac{g^k}{p}\right) = 1 \iff k \equiv 0 \pmod{2}$$

2. *Udowodnij że wyrażenie $\frac{x^2+1}{y^2-5}$ nie jest całkowite dla żadnych liczb całkowitych x, y .
3. **Dana jest liczba pierwsza p i takie liczby całkowite a, b że p dzieli $a + 1 - b^2$ i $a - 1$. Udowodnić że istnieje takie c że $p \mid a^3 + 1 - c^2$.
4. **Udowodnij że 3 jest resztą kwadratową tylko dla $p \equiv 1, -1 \pmod{12}$
5. Dane są parami względnie pierwsze liczby całkowite a, b, c spełniające zależność

$$a^2 - ab + b^2 = c^2. \tag{1}$$

Wykazać, że każda liczba pierwsza p taka, że $p \mid c$ jest postaci $p = 6k + 1$.

6. **Udowodnij że liczba postaci $2^n + 1$ nie ma dzielników pierwszych postaci $8k + 7$.

7. **Rozstrzygnąć czy istnieje taka liczba pierwsza $p = 4k + 1$, że liczby:

$$1^3 + 1, 2^3 + 2, \dots, p^3 + p$$

dają parami różne reszty modulo p .

8. ***Udowodnij że każdy dzielnik liczby $n^4 - n^2 + 1$ jest w formie $12k+1$.
9. ***Udowodnij że dla każdej liczby pierwszej p istnieją a i b takie że: $p \mid a^2 + b^2 + 1$
10. ****Udowodnij że jeśli $2^n - 1 \mid 3^n - 1$, to $n = 1$ *Prop. Antoni Łuczak*
11. ****Udowodnij że nie istnieją liczby całkowite takie że $3(ab + bc + ca) \mid a^2 + b^2 + c^2$
12. ****Udowodnij że jeśli p jest liczbą pierwszą postaci $4k + 3$ to istnieją różne liczby $a, b \in 0, 1, 2, \dots, p-1$ takie że $p \mid a^2 + ab + b^2 + 1$
13. ****Zbiór S to zbiór wszystkich liczb postaci:

$$\frac{(a_1^2 + a_1 - 1) \dots (a_n^2 + a_n - 1)}{(b_1^2 + b_1 - 1) \dots (b_n^2 + b_n - 1)}$$

Dla a_i, b_i, n będących liczbami całkowitymi dodatnimi. Udowodnij że w S jest nieskończenie wiele liczb pierwszych.

4 Solvy

1. Zauważmy że $g^{p-1} \equiv 1 \pmod{p}$, czyli g^{p-1} to reszta kwadratowa. Zauważmy że g^{p-1-2i} jest resztą kwadratową ponieważ $\left(\frac{g^{p-1-2i}}{p}\right) \left(\frac{g^{2i}}{p}\right) = \left(\frac{g^{p-1}}{p}\right)$ C. K. D.
2. Zauważmy że jeśli y jest nieparzyste, to $y^2 - 5$ jest podzielne przez 4, a $x^2 \equiv 1, 2 \pmod{4}$, więc nie istnieje taki x . Jeśli y jest parzysty to $y^2 - 5 = 4k + 3$, czyli ma jakiś dzielnik $p = 4m + 3$. Zauważmy że $x^2 \equiv -1 \pmod{p}$, co jest sprzeczne z kryterium Eulera, czyli również nie istnieje taki x .
3. Zauważmy że teza jest równoważna temu że $a^3 + 1$ to reszta kwadratowa. jednak:

$$\left(\frac{a^3 + 1}{p}\right) = \left(\frac{a + 1}{p}\right) \left(\frac{a^2 - a + 1}{p}\right)$$

Wiemy że $a+1$ to reszta kwadratowa, oraz że $a^2 - a + 1 \equiv a^2 \pmod{p}$, czyli oba symbole po prawej są równe 1, czyli ten po lewej też jest równy 1, C. K. D.

4. Rozważmy dwa przypadki: $p \equiv 1$ i $p \equiv 2 \pmod{3}$, W pierwszym zauważamy że $\left(\frac{3}{p}\right) = \left(\frac{1}{3}\right) = \left(\frac{p}{3}\right)$. Czyli z prawa wzajemności $p \equiv 1 \pmod{4}$, czyli łącząc z założeniem $p \equiv 1 \pmod{12}$. W drugim przypadku z analogicznej równości otrzymujemy $p \equiv -1 \pmod{4}$, czyli łącząc z założeniem $p \equiv -1 \pmod{12}$, C. K. D.
5. Zauważmy że $2 \nmid c$, bo inaczej lewa strona równania jest nieparzysta, a prawa parzysta. Jeśli $3 \mid c$, to $a^2 - ab + b^2 \equiv 0 \pmod{9} \iff (2a - b)^2 + 3b^2 \equiv 4(a^2 - ab + b^2) \equiv 0 \pmod{9}$, czyli $3 \mid 2a - b$, czyli $9 \mid 3b^2$ co jest sprzeczne z założeniem że b i c są względnie pierwsze. Rozważmy zatem dzielnik pierwszy c $p > 3$. Wtedy możemy zauważyć że $(a - b)^2 = -ab + c^2$ i $(a + b)^2 = 3ab + c^2$, czyli $(a - b)^2 \equiv -ab \pmod{p}$ i $(a + b)^2 \equiv 3ab \pmod{p}$. Czyli $3ab$ i $-ab$ są resztami kwadratowymi modulo p , czyli:

$$\left(\frac{-ab}{p}\right) = \left(\frac{3ab}{p}\right) \iff \left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) \iff \left(\frac{-3}{p}\right) = 1.$$

Gdzie $\left(\frac{p}{q}\right)$ oznacza symbol Legendre'a (Patrz referat o resztach kwadratowych). Jednak -3 jest resztą kwadratową tylko dla $p = 12l + 1$ i $p = 12l + 7$, czyli $p = 6k + 1$. C. K. D.

6. Załóżmy nie wprost że istnieje $p \equiv 7 \pmod{8}$ i $p \mid 2^n + 1$. Jeśli n jest parzyste, to -1 jest resztą kwadratową, ale p przystaje do $3 \pmod{4}$, więc sprzeczność (kryt. Eulera). Jeśli n jest nieparzyste, to -2 jest resztą kwadratową. Jednak $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{-1}{p}\right) = -1$ czyli znowu sprzeczność, C. K. D.
7. Zauważmy że z kryterium Eulera dla każdej liczby $p = 4k + 1$, reszta -1 jest resztą kwadratową. Czyli istnieje taka liczba $a < p$ że $a^3 + a \equiv a(a^2 + 1) \equiv 0 \equiv p^3 + p \pmod{p}$ C. K. D.

8. Liczbę możemy zapisać jako: $n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2$ i $n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2$. Z pierwszej formy otrzymujemy że $-n^2$ jest resztą kwadratową dla każdego dzielnika p , czyli z kryterium eulera $p = 4k + 1$. Druga równość jest równoważna temu że 3 jest resztą kwadratową dla każdego dzielnika p , czyli z zadania 4, $p = 12 \pm 1$. Łącząc obie formy otrzymujemy tezę.
9. Zauważmy że dla $p = 4k + 1$ istnieje liczba c że $c^2 \equiv -1$. Podstawiając $a = c$ i $b = p$, otrzymujemy tezę. Dla $p = 4k + 3$ zauważamy: $a^2 \equiv -b^2 - 1$, czyli chcemy udowodnić że istnieje jakaś reszta kwadratowa(r) taka że $-r-1$ też jest resztą kwadratową. Załóżmy nie wprost że nie istnieje taka reszta. Wtedy zauważamy że jeśli a jest resztą kwadratową, to $\left(\frac{-a-1}{p}\right) = -1$, czyli $\left(\frac{a+1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{-a-1}{p}\right) = 1$. Indukcyjnie dowodzimy że każda reszta modulo p jest resztą kwadratową co jest oczywistą sprzecznością, czyli istnieje takie k , co kończy dowód.
10. Zauważmy że jeśli n jest parzyste, to $3 \mid 2^n - 1 \mid 3^n - 1$ co jest sprzeczne. Czyli n jest nieparzyste. Zauważmy że $2^n - 1 \mid 3^n - 1 \iff 2^n - 1 \mid 3^n - 2^n$. Czyli $3^n \equiv 2^n \pmod{2^n - 1}$. Podstawmy $n = 2k + 1$, wtedy: $3^{2k+1} \equiv 1 \Rightarrow (3^{k+1})^2 \equiv 3 \pmod{2^{2k+1} - 1}$. Czyli 3 jest resztą kwadratową modulo $2^{2k+1} - 1$. Zauważmy że z zadania 4 3 jest resztą kwadratową tylko dla liczb pierwszych $p \equiv 1, -1 \pmod{12}$. Łatwo zauważyć że liczba $2^{2k+1} - 1$ ma jakiś dzielnik nieprzystający do 1 lub -1, czyli 3 nie może być jego resztą kwadratową, c.k.d.
11. Zauważmy że teza jest równoważna temu że $a^2 + b^2 + c^2 = 3n(ab + bc + ca) \iff (a + b + c)^2 = (3n + 2)(ab + bc + ca)$. Rozważmy $p = 3k + 2$ takie że $p \mid 3n + 2$ w nieparzystej potędze (takie p istnieje, bo z mnożenia 1 i 0 nie otrzymamy 2). Ponieważ p może dzielić lewą stronę tylko w parzystej potędze, to dzieli $ab + bc + ca$. Ponieważ $p \mid a + b + c$ to możemy podstawić $a \equiv -b - c$. Wtedy $p \mid -b^2 - bc - c^2$ czyli mnożąc przez 4 $p \mid (2b + c)^2 + 3c^2$. Oznacza to że -3 to reszta kwadratowa. Załóżmy że jeśli $p = 4k + 1$ to $\left(\frac{-3}{3k+2}\right) = \left(\frac{-1}{3k+2}\right) \left(\frac{3}{3k+2}\right) = \left(\frac{3k+2}{3}\right) = \left(\frac{2}{3}\right) = -1$ czyli sprzeczność. Jeśli $p = 4k + 3$ to analogiczne rozumowanie doprowadza do sprzeczności, c. k. d.
12. Niech c to odwrotność b modulo p . Wtedy: $a^2 + ab + b^2 \equiv -1 \iff a^2 c^2 + ac + 1 \equiv -c^2 \iff x^2 + x + 1 \equiv -c^2 \iff 4x^2 + 4x + 4 \equiv -4c^2 \iff (2c + 1)^2 + 3 \equiv -(2c)^2$. Ponieważ $p = 4k + 3$ to -1 nie jest resztą kwadratową, czyli $-m^2$ też nie jest. Zauważmy że jeśli istnieje liczba t taka że $t = u^2$ i $t + 3 = -v^2$ to możemy tak dobrać x i c a w konsekwencji a i b że teza zachodzi. Ponieważ reszt kwadratowych i niereszt kwadratowych jest tyle samo, i jeśli x jest resztą kwadratową to $-x$ nie jest resztą kwadratową, to w każdej parze y i $-y$ jest dokładnie jedna reszta kwadratowa. Czyli w ciągu:

$$0, 3, 6, 9, \dots, 3 \cdot (p - 1)$$

Występują zarówno reszty i niereszty kwadratowe, przy czym 0 jest resztą kwadratową, czyli po jakiejś reszcie kwadratowej występuje niereszta, czyli możemy wybrać takie t , C. K. D.

13. Udowodnimy że w zbiorze S jest nieskończenie wiele liczb pierwszych z zbioru liczb przystających do 0,1,4 (mod 5). Zauważmy że 5,11 i 19 są w S . teraz załóżmy że wszystkie liczby pierwsze przystające do 0,1,4(mod 5) mniejsze od p_i (będącego liczbą przystającą do 1 lub 4(mod 5)) są w S . Pokażemy że p_i też jest w S . Zauważmy że 5 jest resztą kwadratową mod p_i (z prawa wzajemności reszt kwadratowych), czyli istnieje takie x że $p_i \mid (2x+1)^2 - 5 \Rightarrow p_i \mid x^2 + x - 1$ i $2x + 1 < p_i$. Zauważmy że każda liczba pierwsza dzieląca $x^2 + x - 1$ przystaje do 0,1,4 (mod 5) (bo $\Delta = 5$, a 5 jest resztą kwadratową tylko dla liczb 0,1,4 (mod 5)), i jest mniejsza od p_i , czyli jest w S . Zauważmy że jeśli a jest w S to ab też i $\frac{a}{b}$. Ponieważ wszystkie dzielniki $x^2 + x - 1$ jest iloczynem liczb w S , to też jest w S . A ponieważ p_i dzieli $x^2 + x - 1$, to p_i też jest w S , co kończy dowód.