

Символ на Лъожандър. Квадратичен закон за реципрочност

П. Бойваленков

Институт по математика и информатика, БАН

Семинар по олимпийска математика

Созопол, 3-10 септември 2017

Символ на Лъожандър

Нека $p > 2$ е просто число и a е цяло число, като $(a, p) = 1$.

Дефиниция. Дефинираме символ на Лъожандър по следния начин

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако } a \text{ е квадратичен остатък по модул } p \\ -1, & \text{ако } a \text{ е квадратичен неостатък по модул } p \end{cases}.$$

Например имаме $\left(\frac{1}{p}\right) = 1$ за всяко p и

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ако } p \equiv 1 \pmod{4} \\ -1, & \text{ако } p \equiv 3 \pmod{4} \end{cases}.$$

Символ на Лъожандър

Елементарни свойства на символа на Лъожандър:

Теорема 1. а) Ако $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

б) $\left(\frac{a^2}{p}\right) = 1$.

в) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ (това всъщност е друг запис на критерия на Ойлер).

г) $\left(\frac{a_1 a_2 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \left(\frac{a_2}{p}\right) \dots \left(\frac{a_n}{p}\right)$.

д) Ако $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = 1$ (т.е. произведението на два квадратични остатъка (неостатъка) винаги е квадратичен остатък).

Лема на Айзенщайн

Теорема 2. (Лема на Айзенщайн) Нека p и q са различни нечетни прости числа. Тогава

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

където $k = \sum_{j \leq p-1, j \text{ is even}} \left[\frac{jq}{p}\right].$

Лема на Айзенщайн

Доказателство. Нека x да обхожда четните естествени числа, по-малки от p , и с $r(x)$ да означим остатъка от делението на qx на p (в частност, имаме $r(x) \equiv qx \pmod{p}$).

Да разгледаме числата $(-1)^{r(x)}r(x)$ по модул p . Ясно е, че тези числа са четни (ако $r(x)$ е четно, това е очевидно, а ако $r(x)$ е нечетно, то $(-1)^{r(x)}r(x) \equiv p - r(x) \pmod{p}$).

Освен това те са различни. Действително, ако $(-1)^{r(x)}r(x) \equiv (-1)^{r(y)}r(y) \pmod{p}$, то $x \equiv \pm y \pmod{p}$ и значи $p|x - y$ или $p|(x + y)/2 < p - 1$, противоречие и в двата случая (използвахме, че $2|x$ и $2|y$ и $x \neq y$).

Лема на Айзенщайн

От горното следва, че числата $(-1)^{r(x)}r(x)$ са две по две различни по модул p и всъщност образуват (по модул p) множеството $\{2, 4, \dots, p-1\}$. Това означава, че е изпълнено сравнението

$$(-1)^{r(2)}r(2)(-1)^{r(4)}r(4)\dots(-1)^{r(p-1)}r(p-1) \equiv 2.4\dots(p-1) \pmod{p},$$

откъдето

$$\begin{aligned} & (-1)^{r(2)+r(4)+\dots+r(p-1)}(2q)(4q)\dots((p-1)q) \equiv 2.4\dots(p-1) \pmod{p} \\ \iff & (-1)^{r(2)+r(4)+\dots+r(p-1)}q^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ \iff & (-1)^{r(2)+r(4)+\dots+r(p-1)} \equiv q^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Остава да видим, че числата $r(x)$ и $[qx/p]$ са от еднаква четност, което, заедно с Теорема 1в), ни дава искания резултат. \square

Квадратичен закон за реципрочност

Теорема 3. (Квадратичен закон за реципрочност) Нека p и q са различни нечетни прости числа. Тогава е в сила равенството

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Квадратичен закон за реципрочност

Доказателство. (Айзенщайн) Да разгледаме в правоъгълна координатна система правоъгълника $ABCD$ с върхове съответно $(0, 0)$, $(p, 0)$, $(0, q)$ и (p, q) .

Да забележим, че $\frac{(p-1)(q-1)}{4}$ всъщност е броят точки с цели координати вътре в правоъгълника $AKLM$, където $K = (p/2, 0)$, $L = (p/2, q/2)$ и $M = (0, q/2)$.

Да отбележим още, че във вътрешността на отсечката AC няма целочислени точки.

Квадратичен закон за реципрочност

Частта за $j < p/2$ от степенния показател (сумата) отляво в лемата на Айзенщайн брой целочислените точки с четни абсциси във вътрешността на триъгълника AKL .

За $j > p/2$ същата сума пък брой целочислените точки с четни абсциси в четириъгълника $KBCL$.

Последният брой има същата четност, каквато има броят на целочислените точки с четни абсциси във вътрешността на триъгълника CLN , където $N = (p/2, q)$.

Поради симетрията спрямо L заключаваме, че

$$\sum_{j \leq p-1, j \text{ is even}} \left[\frac{jq}{p} \right] \equiv s \pmod{2},$$

където s е броят на точките с цели координати в AKL .

Квадратичен закон за реципрочност

Размяната на ролите на p и q в лемата на Айзенщайн и аналогично на горното разсъждение ни дава, че

$$\sum_{j \leq q-1, j \text{ is even}} \left[\frac{jp}{q} \right] \equiv t \pmod{2},$$

където t е броят на целочислени точки във вътрешността на ALM .
Получените две сравнения, равенството $s + t = \frac{(p-1)(q-1)}{4}$ и лемата на Айзенщайн ни дават исканото

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{s+t} = (-1)^{\frac{(p-1)(q-1)}{4}},$$

с което доказателството е завършено. □

Задача 1.

Задача 1. За дадени естествено число n и просто число $p > n$ означаваме с $f_p(n)$ броя на числата от множеството $\{1, 2, \dots, n\}$, които са квадратични остатъци по модул p . Естественото число n се нарича спокойно по отношение на квадратичните остатъци (СПОКО), ако за всяко просто число $p > n$ имаме $f_p(n) \geq \frac{n}{2}$.
Да се определи дали 100 е СПОКО.

Задача 1.

Решение. Ще докажем, че 100 не е спокойно по отношение на квадратичните остатъци. За целта е достатъчно да докажем, че $f_p(100) \leq 49$ за някое просто $p > 100$.

Идеята е да изберем просто число p , което е малко по-голямо от 100 и да установим, че квадратичните остатъци в интервала $[101, p-1]$ са повече от половината. Тъй като квадратичните остатъци в $[1, p-1]$ са точно половината, това ще означава, че тези в $[1, 100]$ са по-малко от половината, т.е. $f_p(100) \leq 49$ и значи 100 не е СПОКО.

Числото $p = 109$ има исканите свойства. Директно се проверява, че числата 102, 104, 105, 106 и 108 са квадратични остатъци по модул 109.

Задача 2.

Задача 1. Нека $k = 2^{2^n} + 1$. Да се докаже, че k е просто тогава и само тогава, когато $k | 3^{\frac{k-1}{2}} + 1$.

Задача 2.

Нека $k|3^{\frac{k-1}{2}} + 1$. Тогава показателят на 3 по модул k е $k - 1 = 2^{2^n}$, т.е. $k - 1 | \varphi(k)$ и следователно $\varphi(k) = k - 1$, което означава, че k е просто число.

Обратно, нека k е просто число. От квадратичния закон за реципрочност следва, че

$$\left(\frac{3}{k}\right) = \left(\frac{k}{3}\right) (-1)^{\frac{2^{2^n}}{2}} = \left(\frac{k}{3}\right) = -1,$$

тъй като $k \equiv 2 \pmod{3}$. Сега твърдението следва от критерия на Ойлер.

Задача 1.

Задача 3.