§ 11. Закон за реципрочност на квадратичните остатъци

Ще започнем със следната лема на Гаус.

**Лема 11.1 (Гаус).** *Нека p е нечетно просто число*,  *и*



*където . Нека s е броят на числата от множеството*, *които* *са отрицателни. Тогава*  .

*Доказателство.*Нека  са числата от множеството, които са отрицателни, а  са тези от тях, които са положителни (никое от числата  не е равно на 0). Тогава числата  и  са в интервала  и (както лесно се съобразява) са две по две различни. Така тези числа образуват пермутация на числата . Следователно  или, все едно,  , т.е.

. (1)

От друга страна, от условието имаме

. (2)

От (1) и (2) (след съкращаване на ) получаваме . Това, заедно с критерия на Ойлер (предвид  ), дава .

**Забележка.** Ако в лемата на Гаус бяхме взели числата  да лежат в "стандартния" интервал , то възловото число *s* представлява броя на тези от тях, които лежат в интервала .

Това съображение ще използваме в следващото следствие.

**Следствие 11.2** *Ако p е нечетно просто число, то* ***.***

*Доказателство.*Използваме означенията в лемата на Гаус при  .

Числата  са две по две различни, намират се между 1 и  и значи съвпадат с остатъците си при деление на *p*. Тогава



(с *|X|* означаваме броя на елементите на множеството *X*).

Директно се проверява, че числото  е четно при  и е нечетно при . По същия начин „се държи” и числото  . Следователно

.

**Теорема 11.3 (закон за реципрочност на квадратичните остатъци).** *Ако p и q са различни нечетни прости числа, то*

.

*Доказателство.* Нека *p* и *q* са различни нечетни прости числа. В означенията на лемата на Гаус (при ) имаме .

Нека $x$ е цяло число, , за което  и  . Това означава, че съществува (единствено) цяло число $y$, такова че . При това, от  следва (проверете) .

Да означим

.

Имаме **.

Горните разсъждения показват, че числото $s$ е равно на броя на елементите , за които  или, все едно, .

Разменяйки ролите на $p$ и $q$, по аналогичен начин получаваме, че , където $t$ е броят на елементите , за които .

Да означим

, 

и освен това

, .

Лесно се съобразява, че множествата  са две по две непресичащи се и обединението им е равно на *A*. Тогава

. (3)

По-нататък, ако , да означим

.

Имаме , така че  е инективно изображение. Освен това, директно се проверява, че ако , то  и значи . Аналогично, ако , то  и значи . (Чисто и просто, ограничението на  върху (например) *S* е биекция от *S* към *T*.) Следователно .

Сега от (3) следва

.

Така . Следователно

.

Теоремата е доказана.

**Забележка.** Формалните разсъждения за множествата  могат да се онагледят геометрично по следния начин.

Множеството A представлява множеството от точките в равнината с целочислени координати, лежащи във вътрешността на правоъгълника с върхове . Точките от  са тези точки от *A*, които са заключени между успоредните прави  (диагонала на правоъгълника) и . Аналогично, точките от  са между правите *d* и . Точките от *S* лежат над *l*, а от *T* − под *m*. При това, върху d, *l* и *m* няма точки с цели координати (върху *d* няма, защото *p* и *q* са взаимно прости, а върху *l* и *m* няма, защото  и  не са цели числа). Така действително .

**Коментар.** Да запишем закона за реципрочност на квадратичните остатъци във вида

.

Нечетните прости числа *p* и *q* са от вида  или . Степента  е **нечетно** число единствено когато **и двете числа** *p* и *q* са от вида . В този случай  (т.е. ако *p* е **квадратичен остатък** по модул *q*, то *q* е **квадратичен неостатъ**к по модул *p*). В случая, когато поне едно от числата *p* и *q* е от вида  имаме  (т.е. *p* е квадратичен остатък по модул *q* точно когато и *q* е квадратичен остатък по модул *p*).