§ 10. Сравнения от втора степен. Символ на Льожандър. Критерий на Ойлер

Разглеждаме сравнения от вида , където *p* е просто число, *p*. При  сравнението се изследва непосредствено, ето защо *p* ще бъде нечетно просто число. Като умножим това сравнение с и отделим точен квадрат, достигаме до еквивалентното сравнение. Сега е ясно, че е достатъчно да изучаваме сравнения от вида

**. (1)

При това ще считаме, че *p**a* (в противен случай сравнението има единствено решение ). Ясно е, че ако цялото число е решение на сравнението (1), то и е решение. При това  защото . Така сравнението (1) или няма решение, или има точно 2 решения (повече от 2 решения не може да има, защото е от втора степен).

**Определение.** Нека *p* е нечетно просто число,  и *p**a*. Ще казваме, че е *квадратичен остатък по модул p*, ако сравнението ** има решение, т.е. ако съществува цяло число *b*, такова че . Ако това сравнение няма решение, ще казваме, че *a* е *квадратичен неостатък по модул p*.

**Лема 10.1.** *Всяка редуцирана система остатъци по модул p съдържа  на брой квадратични остатъка и също така  на брой квадратични неостатъка.*

*Доказателство.* Всеки квадратичен остатък е сравним по модул *p* с някое от числата . Очевидно е сравнението , така че  и т.н. Следователно само числата от  до  изчерпват всички квадратични остатъци. При това тези числа вече са несравними по модул *p*. Действително, ако допуснем, че  и , следва, че *p* дели разликата . Но това е невъзможно, тъй като и са естествени числа, строго по-малки от *p*. Така квадратичните остатъци по модул *p* действително са  на брой (а значи толкова са и квадратичните неостатъци).

**Определение.** Нека *p* е нечетно просто число,  и *p**a*. Полагаме

, ако *a* е квадратичен остатък по модул *p*,

, ако *a* е квадратичен неостатък по модул *p*.

Символът  се нарича *символ на Льожандър* (чете се "символ на Льожандър на *a* по *p*").

Ясно е, че ако , то . Очевидно е също, че  и .

**Пример.** Квадратичните остатъци по модул 5 са  и . Тогава  и , докато  и .

**Теорема 10.2 (Критерий на Ойлер)**. *Нека p е нечетно просто число,  и p**a. Тогава*

.

*Доказателство.* Първо ще отбележим, че щом числото  е равно на , то сравнението  означава, че , докато  означава  (напомняме, че ).

Теоремата ще бъде доказана, ако покажем, че , ако *a* е квадратичен остатък по модул *p* и , ако *a* е квадратичен неостатък по модул *p*.

Според теоремата на Ферма всяко цяло число, неделящо се на *p* е решение на сравнението , т.е. на сравнението . Тъй като  (и *p* е просто число), то всяко цяло число, неделящо се на *p* е решение на едно от сравненията

, (2)

. (3)

При това не е възможно едно число да е решение и на двете сравнения, защото бихме получили , което е невъзможно при .

Нека *a* е квадратичен остатък по модул *p*, т.е. съществува цяло число *b*, такова че . Тогава

.

Следователно всички квадратични остатъци са решения на сравнението (2). Според лема 10.1 броят на квадратичните остатъци е равен на  колкото е и степента на това сравнение. Следователно квадратичните остатъци по модул *p* изчерпват решенията на сравнението (2). Тогава квадратичните неостатъци по модул *p* са решенията на сравнението (3).

С това теоремата е доказана.

**Примери.** **1. **.

Следователно  и значи 2 е квадратичен остатък по модул 17.

**2.** .

Така , т.е. 3 е квадратичен неостатък по модул 17.

**Следствие 10.3.** *Ако p е нечетно просто число, неделящо целите числа , то*

*.*

*Доказателството* следва от критерия на Ойлер и от равенството

.

В частност, ако , то



(защото ).

**Следствие 10.4.** *Ако p е нечетно просто число, числото  е квадратичен остатък по модул p точно когато p е от вида *

*Доказателство.* От критерия на Ойлер имаме  т.е. . Следователно  точно когато степента  е четно число т.е. когато *p* е от вида (докато  точно когато *p* е от вида ).

**Забележка.** Тъй като всяко цяло число *a* е произведение (с точност до знак) на прости числа, за да можем да пресмятаме символа , трябва да можем да пресмятаме (освен ) символите  и , където *q* е нечетно просто число. С това ще се занимаем в следващия параграф.