§ 5. Функция на Ойлер. Редуцирана система остатъци

**Определение.** Ако *n* е естествено число, с  бележим броя на естествените числа, ненадминаващи *n* и взаимно прости с *n*. Така получаваме една функция, дефинирана в множеството на естествените числа, чиито стойности също са естествени числа. Тази функция се нарича *функция на Ойлер*.

Числата  образуват една пълна система остатъци по модул *n* и по определение  на брой от тях са взаимно прости с *n*. При това едно число *a* е взаимно просто с *n* точно когато всички числа от класа  от остатъци по модул *n* са взаимно прости с *n*. Тогава всяка пълна система остатъци по модул *n* съдържа точно  на брой взаимно прости с *n* числа.

**Упражнение 5.1.** *Да се пресметнат стойностите на  при *

**Упражнение 5.2.** *Да се докаже, че  точно когато p е просто число.*

**Твърдение 5.3.** *Нека p е просто число и . Тогава*

*.*

*Доказателство.* Едно число **не е**  взаимно просто с  точно когато е кратно на *p*. Измежду числата  кратни на *p* са числата  и техният брой е равен на . Тогава останалите  на брой числа **са** взаимно прости с . Следователно .

**Теорема 5.4.** *Ако , то . По-общо, ако числата  са две по две взаимно прости, то  (мултипликативност на функцията на Ойлер).*

*Доказателство.* Да запишем числата  в следната правоъгълна таблица с *b* реда и *a* стълба:

.

**Първа стъпка.** Числата, стоящи в един стълб на таблицата, са сравними помежду си по модул *a*. Тогава или всички числа в даден стълб са взаимно прости с *a*, или всички числа в този стълб не са взаимно прости с *a*. Но в първия ред на таблицата стоят числата  и точно  на брой от тях са взаимно прости с *a*. Тогава техните стълбове (и само те) се състоят от числа, взаимно прости с *a*. Така установихме, че *таблицата съдържа*  *на брой стълба, състоящи се от числа, взаимно прости с a и това са всички числа от таблицата, които са взаимно прости с a.*

**Втора стъпка.** За всяко число *c*, , числата в таблицата, стоящи в стълб с номер *c* са: . Според твърдение 4.5 тези числа образуват пълна система остатъци по модул *b*. Тогава *всеки стълб на таблицата съдържа точно  на брой числа, взаимно прости с b.*

**Трета стъпка.** В първа стъпка видяхме, че таблицата съдържа  на брой стълба, състоящи се от числа, взаимно прости с *a* и това са всички числа от таблицата, които са взаимно прости с *a*. От втора стъпка следва, че всеки един от тези стълбове съдържа точно ** на брой числа, взаимно прости с *b*. Тогава *таблицата съдържа точно  на брой числа, които са взаимно прости както с a, така и с b.*

**Четвърта (финална) стъпка.** И така, доказахме, че таблицата съдържа ** на брой числа, които са взаимно прости както с *a*, така и с *b*. От друга страна (по определение на функцията на Ойлер) таблицата съдържа  на брой числа, които са взаимно прости с *ab*. Но очевидно едно число е взаимно просто с *ab* точно когато е взаимно просто както с *a*, така и с *b*. Следователно **.

Обобщението се получава с индукция по *r*.

**Теорема 5.5.** *Нека  е каноничното разлагане на естественото число  в произведение на прости множители. Тогава*

*= *

*Доказателство.* Тъй като  са различни прости числа, то  при . Тогава от теорема 5.4 получаваме

.

Накрая прилагаме твърдение 5.3, за да получим окончателната формула за .

**Твърдение 5.6.** *В сила е равенството*

*.*

*(сумирането се извършва по всички естествени делители на n).*

*Доказателство.* Да разгледаме всички правилни дроби със знаменател *n*: . Техният брой очевидно е равен на *n*. След като запишем тези дроби като несъкратими, техните знаменатели са всевъзможните делители на числото *n*. Колко са дробите, чийто знаменател е фиксиран делител *d* на *n*? Тъй като те са правилни и несъкратими, числителите им са естествени числа, ненадминаващи *d* и взаимно прости с *d*, при това всевъзможните такива числа. Следователно броят на несъкратимите дроби със знаменател *d* е точно . Сега броят на всички дроби е .

\*\*\*

**Определение.** Под *редуцирана система остатъци по модул n* ще разбираме всяка система от  на брой числа, които са несравними по модул *n* и са взаимно прости с *n*.

Всички естествени числа, ненадминаващи *n* и взаимно прости с *n* образуват една редуцирана система остатъци по модул *n*. При това всяко взаимно просто с *n* число е сравнимо с някое от тези числа по модул *n* (с остатъка си при деление на *n*). Така (изразявайки се малко по-свободно) можем да кажем, че множеството от числата от коя да е редуцирана система остатъци "съвпада по модул *n*" с множеството от естествените числа, ненадминаващи *n* и взаимно прости с *n*. В частност, ако имаме две редуцирани системи остатъци, всяко число от едната система е сравнимо по модул *n* с точно едно число от другата система.

**Твърдение 5.7.** *Ако числата  образуват редуцирана система остатъци по модул n и , то числата  също образуват редуцирана система остатъци по модул n.*

*Доказателство.* Щом числата *a* и  са взаимно прости с *n*, то и  е взаимно просто с *n*. Освен това, ако допуснем, че (например) , то от  следва , което е противоречие. Така числата ** са несравними по модул *n* и са взаимно прости с *n*, следователно действително образуват редуцирана система остатъци по модул *n*.

**Определение.** Ще казваме, че *числото a е обратимо по модул n*, ако съществува число , такова че . Числото  ще наричаме *обратно на a по модул n*.

**Твърдение 5.8.** *Числото a е обратимо по модул n точно когато е взаимно просто с n.*

*В частност, ако p е просто число, то всички числа  са обратими по модул p.*

*Доказателство.* Ако , съществуват числа *u* и *v*, за които  и тогава . Следователно *a* е обратимо по модул *n*. Обратно, ако съществува число , такова че , то всеки общ делител на *a* и *n* дели и числото 1. Следователно .