§ 6. Теореми на Ойлер и Ферма. Теорема на Уилсън

**Теорема 6.1 (теорема на Ойлер).** *Нека n е естествено число и a е цяло число, взаимно просто с n. Тогава*

.

*Доказателство.* Нека  е редуцирана система остатъци по модул *n*. Според твърдение 5.7 числата  също образуват редуцирана система остатъци по модул *n*. Тогава всяко число от първата система е сравнимо по модул *n* с точно едно число от втората система. Следователно е в сила сравнението

.

Тъй като числата  са взаимно прости с *n*, можем да съкратим на произведението  и получаваме .

**Следствие 6.2 (теорема на Ферма*).*** *Ако p е просто число и pa, то . Еквивалентно: сравнението  е изпълнено за всяко цяло число a.*

*Доказателство.* Тъй като  (щом *pa*) и предвид  сравнението ** следва от теоремата на Ойлер.

По-нататък, като умножим това сравнение с *a*, получаваме сравнението **, което вече се изпълнява за всяко цяло число *a*. Обратно, ако *pa* и **, като разделим това сравнение на *a*, получаваме **.

**Упражнение 6.3.** *Използвайки сравнението*

**

*(твърдение 4.4), докажете още веднъж теоремата на Ферма.*

*Упътване.* При  положете  и , за да получите **.

**Теорема 6.4 (теорема на Уилсън).** *За всяко просто число p е в сила сравнението*

*.*

*Доказателство.* При  сравнението е очевидно, затова нека .

Да означим . Според твърдение 5.8 всяко число  е обратимо по модул *p*, т.е. съществува число , такова че  (числото  можем да изберем също от множеството *P*, защото *P* съдържа всички ненулеви остатъци по модул *p*). За кои числа *a* е изпълнено ? Равенството  означава, че , т.е. *p* дели числото . Но последното е възможно само при  и при .

И така, само числата 1 и  съвпадат със своите обратни по модул *p*, докато всички останали числа от множеството *P* се разбиват на двойки , за които . Произведението на всички такива двойки да означим за краткост с . Очевидно . Сега имаме

.

Теоремата е доказана.

**Упражнение 6.5.** *Докажете, че теоремата на Уилсън може да се обърне: ако p е естествено число, за което е изпълнено сравнението , то p е просто число.*