§ 9. Сравнения от произволна степен

Нека *m* е естествено число. Ако  и  са полиноми с цели коефициенти, ще пишем , когато коефициентите пред еднаквите степени на *x* в двата полинома са сравними по модул *m*. В този случай за всяко цяло число *c* е изпълнено .

**Лема 9.1.** *Нека  е полином с цели коефициенти от степен n. Ако числото c е решение на сравнението*

*,*

*то съществува полином с цели коефициенти*  *от степен , такъв че*

*.*

*Доказателство.* Разделяме полинома ** на  с частно и остатък: . Тъй като старшият коефициент на делителя  е равен на 1, то частното  е полином също с цели коефициенти и остатъкът *r* е цяло число. Сега от  и от  следва . Следователно

**.

По-нататък ще разглеждаме сравнения само по прост модул.

**Теорема 9.2.** *Нека p е просто число,  е полином с цели коефициенти и . Тогава сравнението*

**

*има най-много n различни решения.*

*Доказателство.* Да допуснем противното и нека  са  на брой различни решения на сравнението (напомняме, че "различни" означава "несравними по модул *p*"). От лема 9.1 следва

,

където  е полином от степен . Тогава

.

Тъй като *p* е просто число и , то Прилагайки отново лема 9.1, получаваме

,

където  е полином вече от степен .Тогава

.

Продължавайки по същия начин, след *n* стъпки получаваме

.

Сега имаме

.

Но това е противоречие, защото *p* не дели нито един от множителите . Теоремата е доказана.

Ще отбележим, че ако *p* не е просто число, теоремата престава да бъде вярна. Проверете, че сравнението  има 4 на брой различни решения.

Като приложение ще докажем още веднъж теоремата на Уилсън: *ако p е просто число, в сила е сравнението .* Ще разгледаме само случая .

Според теоремата на Ферма числата  са решения на сравнението  и както в доказателството на теорема 9.2 заключаваме, че

.

Като положим  и вземем предвид, че  е четно число, получаваме .

**Теорема 9.3.** *Нека p е просто число,  е полином с цели коефициенти и . Тогава сравнението*

**

*е еквивалентно на сравнението*

*,*

*където  е остатъкът, получен при делението на полинома  с полинома . Така всяко сравнение по модул p е еквивалентно на сравнение, чиято степен не надминава .*

*Доказателство.* Нека  и . Според теоремата на Ферма за всяко цяло число *c* е в сила  и значи . Сега е ясно, че сравненията  и  са еквивалентни.