§ 7. Сравнения от първа степен

Нека *m* е естествено число,  е полином с цели коефициенти и . Сравнение от вида



ще наричаме сравнение от степен *n* с едно неизвестно. Да решим това сравнение означава да намерим всички цели числа *c*, за които е изпълнено . При това ясно е, че ако *c* е решение, то всички числа от класа  от остатъци по модул *m* също са решения. Ще считаме, че тези решения не са различни и ще казваме, че  е решение на сравнението. Така броят на различните решения на това сравнение е равен на броя на различните числа от една пълна система остатъци по модул *m*, които го удовлетворяват.

В този параграф ще разгледаме въпроса за броя на решенията на сравнение от първа степен с едно неизвестно. Всяко такова сравнение, след прехвърляне на свободния член в дясната му страна, се записва във вида

. (1)

**Теорема 7.1.** *Ако , сравнението (1) има единствено решение.*

*Доказателство.* **Единственост.** Нека *c* и  са решения на сравнението (1), т.е.  и . Тогава  и от ** следва .

**Съществуване.** Тъй като **, съществуват числа *u* и *v* , такива че . Като умножим това равенство с *b*, получаваме . Тогава , т.е.  е решение на сравнението (1).

*Второ доказателство.* От теоремата на Ойлер имаме . Сега директно се проверява, че  е решение на сравнението (1). Освен това, ако *c* е произволно решение, т.е. , като умножим това сравнение с , получаваме . Следователно сравнението (1) има единствено решение .

**Теорема 7.2.** *Ако , сравнението (1) има решение точно когато . В този случай сравнението има d на брой различни решения.*

*Доказателство.* Нека *c* е решение на сравнението (1), т.е. . Тогава  за някое цяло число *t*. Тъй като  и , следва, че **.

Обратно, нека **. Ще покажем, че в този случай сравнението (1) има *d* на брой различни решения.

Нека ; тогава . Като разделим на *d* двете страни и модула на сравнението (1), получаваме така нареченото редуцирано сравнение . Ясно е, че по обратен път можем "да се върнем" към сравнението (1), така че едно цяло число е решение на редуцираното сравнение точно когато е решение и на сравнението (1).

Тъй като , според теорема 7.1 редуцираното сравнение има единствено решение . Да разгледаме следното множество от числа:

.

Множеството *S* се състои от *d* на брой числа, които са решения на сравнението (1) и са несравними по модул *m*. Действително, разликата на две числа от *S* е число от вида , където  и не се дели на *m*, защото е по-малко от *m*. Ще докажем, че всяко решение на сравнението (1) е сравнимо по модул *m* с някое число от множеството *S*, с което теоремата ще бъде доказана.

Нека *g* е произволно решение на сравнението (1). Тогава *g* е решение и на редуцираното сравнение и значи е от вида  за някое цяло число *t*. Да разделим *t* на *d* с частно и остатък:  Тогава

.

При това , защото . Теоремата е доказана.