§ 4. Числови сравнения. Пълна система остатъци

**Определение.** Нека *n* е естествено число и . Ще казваме, че *числото a е сравнимо с b по модул n*, ако *n* дели разликата .

В това определение числата *a* и *b* са "равноправни" (ясно е, че щом , то ), ето защо можем да се изразяваме, че *a и b са сравними по модул n.*

Ако *a* и *b* са сравними по модул *n*, ще използваме означението . В противен случай ще пишем .

Сравнението  означава, че .

**Твърдение 4.1**. *Две числа a и b са сравними по модул n точно когато дават един и същи остатък при деление на n.*

*Доказателство.* Нека ,  и   Тогава  Сега е ясно, че  точно когато . Но това е възможно единствено когато , т.е. когато .

**Основни свойства на сравненията**. Ще формулираме основните свойства на сравненията без доказателство, тъй като повечето от тях следват непосредствено от определенията.

**1)** За всяко число *a* е в сила .

**2)** Ако , то .

**3)** Ако  и , то .

**4)** Ако  и , то .

**5)** Ако  и , то .

**6)** Ако  и , то 

**7)** Ако  и , то .

**8)** Ако  и , то .

**9)** Ако и , то .

**10)** Ако  и  е полином с цели коефициенти то .

Изброените свойства показват, че относно операциите събиране, изваждане и умножение, със сравненията можем да работим така, както се работи с равенства.

Последното свойство ще отделим като самостоятелно твърдение.

**Твърдение 4.2**. *Нека  и . Тогава . В частност, ако  и , то .*

*Доказателство.* Нека ; тогава . По условие , т.е. . Но тогава  и тъй като , то . Това означава, че , което и трябваше да се докаже.

Особено важен е частният случай, когато **. В този случай можем да разделим двете страни на сравнението на общия множител *k*, без да променяме модула *n*.

**Твърдение 4.3.** *Нека . Тогава ; в частност  точно когато .*

*Доказателство.* Щом **, числата *a* и *b* дават един и същи остатък *r* при деление на *n*. Тогава  и аналогично . Следователно **.

**Твърдение 4.4.** *Ако p е просто число, то  По-общо, .*

*Доказателство.* Като използваме формулата за нютоновия бином и факта, че  за , получаваме



Обобщението се получава с индукция по *n*.

\*\*\*

**Пълна система остатъци.** Първите три свойства на сравненията означават, че релацията сравнимост по модул *n* е релация на еквивалентност. Тогава множеството ***Z*** на всички цели числа се разбива на непресичащи се класове на еквивалентност: две числа *a* и *b* принадлежат на един и същи клас, ако **. т.е. ако *a* и *b* дават един и същи остатък при деление на *n*. Тези класове се наричат *класове остатъци по модул n.* Броят им е равен на *n*, колкото са различните остатъци при деление на *n*.

Ако , с  ще бележим класа от остатъци по модул *n*, на който принадлежи числото *a*. Равенството  е изпълнено точно когато **.

Всички класове остатъци по модул *n* се изчерпват с класовете . Класът  се състои от всички числа, кратни на *n*; класът  се състои от всички числа, даващи остатък 1 при деление на *n* и т.н.

**Определение.** Под *пълна система остатъци по модул n* ще разбираме всяка система от *n* числа, които принадлежат на различни класове остатъци по модул *n* (т.е. несравними са по модул *n*).

При деление на *n* числата от една пълна система остатъци по модул *n* дават остатъци , взети в някакъв ред. Най-често използваната пълна система остатъци по модул *n* е именно системата от числа . Всеки *n* последователни цели числа образуват пълна система остатъци по модул *n*. Например числата  са пълна система остатъци по модул 5.

**Твърдение 4.5.** *Нека ,  и числата  образуват пълна система остатъци по модул n. Тогава числата  също образуват пълна система остатъци по модул n.*

*Доказателство.* Трябва само да покажем, че числата ** ** са несравними по модул *n*. Да допуснем, че (например) . Тогава  и тъй като **, следва, че , което е противоречие с условието. Следователно числата ** действително образуват пълна система остатъци по модул *n*.