§ 13. Примитивни корени

Нека  е естествено число и *a* е цяло число, взаимно просто с *n*. В предния параграф дефинирахме понятието показател на *a* по модул *n* като най-малкото естествено число *r*, за което . В сила е неравенството  (по-точно ). Когато показателят на *a* по модул *n* е равен точно на , *a* се нарича *примитивен корен по модул n*.

В този случай числата  са несравними по модул *n* (твърдение 12.1), взаимно прости са с *n* и броят им е равен на . Следователно тези числа образуват редуцирана система остатъци по модул *n*. Така, ако *a* е примитивен корен по модул *n* , всяко взаимно просто с *n* число е сравнимо (по модул *n*) с някоя степен на числото *a*.

В този параграф ще изследваме за кои естествени числа *n* съществуват примитивни корени по модул *n*.

**Теорема 13.1.** *За всяко нечетно просто число p съществуват примитивни корени по модул p.*

*Доказателство.* От множеството  избираме число *a* с най-голям показател *r* по модул *p*. Ще покажем, че .

Първо имаме . По-нататък, ако *b* е произволно число от множеството *P* и *b* принадлежи на показател *s* по модул *p*, то . Действително, според твърдение 12.6, б), съществува число *c*, чийто показател по модул *p* е равен на . Ако допуснем, че , следва , което противоречи на избора на числото *a*. И така, показателят по модул *p* на всяко число от множеството *P* е делител на числото *r*. От основното свойство на показателя (твърдение 12.2) следва, че всяко число от множеството *P* е решение на сравнението . Тъй като *p* е просто число, това сравнение има най-много *r* различни решения (теорема 9.2). Следователно . Окончателно, , което означава, че *a* е примитивен корен по модул *p*.

**Твърдение 13.2.** *Примитивни корени по модул  съществуват само при  и при .*

*Доказателство.* Числото  е примитивен корен по модул *n* при ** и **. С индукция по *m* ще покажем, че за всяко нечетно число *a* и при  е изпълнено сравнението

. (1)

Числото  се дели на 8, защото е произведение на две последователни четни числа и едното от тях се дели на 4. Така сравнението (1) е изпълнено при . Нека  и да допуснем, че сравнението (1) е изпълнено за . Тогава числото



се дели на , защото според индукционното предположение първият множител се дели на , а вторият е четно число. Следователно сравнението (1) е изпълнено за всяко число .

От доказаното следва, че при  показателят на всяко нечетно число *a* по модул  е равен най-много на . Следователно при  не съществуват примитивни корени по модул .

**Теорема 13.3.** *За всяко нечетно просто число p и за всяко естествено число m съществуват примитивни корени по модул .*

*Доказателство.* Случаят  е разгледан в теорема 13.1, затова нека . Доказателството ще извършим по следната схема.

**Първа стъпка.** Ще покажем, че съществува число *a*, принадлежащо на показател  по модул **.

**Втора стъпка.** Ще покажем, че съществува число *b*, принадлежащо на показател  по модул **.

Тъй като , от твърдение 12.6, а) следва, че числото *ab* принадлежи на показател  по модул **. Но , следователно *ab* е примитивен корен по модул **.

И така, остава да реализираме описаните две стъпки.

**Първа стъпка.** Нека  е примитивен корен по модул *p*. Тогава , но , ако . Имаме последователно

.

Полагаме . Тогава .

От теоремата на Ойлер имаме

, т.е.  или .

Ако допуснем, че  и , то  и тогава от  следва , което е противоречие. Следователно числото *a* принадлежи на показател  по модул **.

**Втора стъпка.** Индуктивно ще покажем, че



Това е очевидно при . По-нататък имаме



за някое цяло число *s*. Тогава

.

От формулата за нютоновия бином лесно се съобразява, че дясната страна е сравнима с  по модул , с което индукционната стъпка е направена.

Сега при  имаме  и тогава . В същото време при  имаме

,

но дясната страна не е сравнима с 1 по модул .

Горните разсъждения показват, че показателят на числото  по модул  е делител на числото , но е по-голям от  и значи е равен точно на . С това доказателството на втората стъпка (и на теоремата) е завършено.

**Следствие 13.4.** *За всяко нечетно просто число p и за всяко естествено число m съществуват примитивни корени по модул .*

*Доказателство.* Ако *g* е примитивен корен по модул , очевидно числото  също е примитивен корен по модул . Нека *h* е нечетното от тези две числа. Като се вземе предвид, че

,

вече лесно се съобразява, че *h* е примитивен корен по модул **.

**Теорема 13.5.** *Примитивни корени по модул n съществуват тогава и само тогава, когато  или , където p е нечетно просто число и m е естествено число.*

*Доказателство.* За всяко естествено число *n* от посочения в условието вид съществуват примитивни корени по модул *n*. Това следва от вече доказаните в този параграф твърдения.

Обратно, нека *n* не е от посочения в условието вид. Ако  и , не съществуват примитивни корени по модул *n* (твърдение 13.2). В останалите случаи лесно се съобразява, че *n* може да се представи във вида , където  и . Нека *a* е произволно цяло число, взаимно просто с *n*. Ще покажем, че *a* не е примитивен корен по модул *n*, с което доказателството ще бъде завършено.

Числата  и  са четни (това следва например от формулата за ) и значи не са взаимно прости. Тогава (използвайки мултипликативност на функцията на Ойлер)

.

От друга страна, щом , то  и от теоремата на Ойлер имаме  и . Тогава  и , откъдето . Тъй като , следва, че *a* не е примитивен корен по модул *n*. Теоремата е доказана.