Глава 3

Сравнения.

3.1 Елементарни свойства на сравненията.

Дефиниция 3.1.1 *Нека $n \neq 0$ е цяло число. Казваме, че целите числа a и b са* ***сравними (конгруентни) по модул*** *n и бележим с*

$$a \equiv b\,(mod\ n),$$

когато разликата $a - b$ се дели на n.

Теорема 3.1.2 *В сила са следните свойства:*

(1) *$a \equiv b\,(mod\ n)$ е релация на еквивалентност;*

(2) *Ако $a \equiv b\,(mod\ n)$ и $c \equiv d\,(mod\ n)$, то $(a \pm c) \equiv (b \pm d)\,(mod\ n)$;*

(3) *Ако $a \equiv b\,(mod\ n)$ и $c \equiv d\,(mod\ n)$, то $ac \equiv bd\,(mod\ n)$;*

(4) *Ако $f(x) \in \mathbb{Z}[x]$ и $a \equiv b\,(mod\ n)$, то $f(a) \equiv f(b)\,(mod\ n)$;*

(5) *Ако $ma \equiv mb\,(mod\ n)$ и $d = (m, n))$, то $a \equiv b\,(mod\ \frac{n}{d})$;*

(6) *Ако $a \equiv b\,(mod\ n)$ и d е общ делител на a и n (в частност $d = (a, n)$), то $d \,|\, b$.*

Доказателство. (3): От условието $a - b = kn$ и $c - d = ln$. Тогава $ac - bd = ac - bc + bc - bd = kcn + lbn = (kc + lb)n$.
(5): Съгласно условието имаме $ma - mb = kn$. Делейки на d получаваме $m_1(a - b) = kn_1$, където $m_1 = m/d$, $n_1 = n/d$. Но $(m_1, n_1) = 1$ и следователно $n_1 \,|\, (a - b)$.

Съгласно свойство (1) целите числа се разбиват на n непресичащи се класове сравними помежду числа. Всеки елемент от даден клас ще наричаме представител на класа.

Забележка 3.1 *Дадената дефиниция се базира само на понятието делимост, така че може да се даде във всяка област на цялост. В частност, понятието сравнимост и свойствата му остават в сила за пръстени от полиноми над поле, както и в $\mathbb{Z}[x]$. В алгебрата понятието се обобщава до сравнение по модул идеал в пръстен.*

От тук нататък ще считаме, че модулът е положителен.

Дефиниция 3.1.3 *Всяка съвкупност от n цели числа $a_1, a_2, \ldots, a_n$, явяващи се представители на различни класове (т.е. несравними две по две) по модул n се нарича* ***пълна система от остатъци*** *по модул n.*

Една пълна система остатъци по модул n образуват числата $0, 1, 2, \ldots, n-1$. Тя се нарича система от най-малките неотрицателни остатъци.

Забележка 3.2 *Свойствата на сравненията показват, че множеството*

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

е комутативен пръстен относно операциите събиране и умножение по модул n, т.е. под произведение на два елемента в $\mathbb{Z}_n$ разбираме остатъка на произведението им като цели числа след делението му на n (аналогично и за сумата). Пръстенът $\mathbb{Z}_n$ е с единица, но в общия случай не е област на цялост. Например $3 \cdot 4 \equiv 12\,(mod\ 12)$, т.е. равно на нула в $\mathbb{Z}_{12}$.

Теорема 3.1.4 *Ако n и m са две взаимнопрости естествени числа, а $r \in \mathbb{Z}$, то числата*

$$r,\ m+r,\ 2m+r,\ \ldots,\ (n-1)m+r$$

образуват пълна система остатъци по модул n.

> ***Доказателство.*** Достатъчно е да покажем, че горните числа две по две не са сравними. Наистина да предположим, че $km + r \equiv lm + r \pmod{n}$. Тогава $(k-l)m \equiv 0 \pmod{n}$. Но $(n, m) = 1$. Следователно $n \mid (k-l)$, което влече $k = l$.

Теорема 3.1.5 *Нека n и m са две взаимнопрости естествени числа. Ако x пробягва пълна система остатъци по модул n, а y пълна система остатъци по модул m, множеството от mn-те числа*

$$mx + ny$$

образуват пълна система остатъци по модул mn.

> ***Доказателство.*** Достатъчно е да покажем, че горните числа две по две не са конгруентни. Наистина да предположим, че $mx+ny \equiv mx_1+ny_1 \pmod{mn}$. Тогава $mx - mx_1 + \equiv ny_1 - ny \pmod{mn}$ и съгласно (6) на Теорема 3.1.2 $mx \equiv mx_1 \pmod{n}$ и $ny \equiv ny_1 \pmod{m}$. Използвайки, че $(n, m) = 1$ получаваме, че $x \equiv x_1 \pmod{n}$ и $y \equiv y_1 \pmod{m}$.

Дефиниция 3.1.6 *Всяка съвкупност от $\varphi(n)$ взаимнопрости с n цели числа, които са две по две неконгруентни по модул n се нарича* ***редуцирана система от остатъци*** *по модул n.*

Теорема 3.1.7 *Нека n и m са две взаимнопрости естествени числа. Ако x пробягва редуцирана система остатъци по модул n, а y редуцирана система остатъци по модул m, целите числа*

$$mx + ny$$

са $\varphi(n)\varphi(n)$ на брой и образуват редуцирана система остатъци по модул mn.

Доказателство. От $(m, n) = (x, n) = (y, m) = 1$ следва, че

$$(mx + ny, m) = (ny, m) = 1 \text{ и } (mx + ny, n) = (nx, n) = 1.$$

Следователно $(mx+ny, mn) = 1$. Обратно , ако $mx+ny$ е взаимнопросто с mn, то $(x, n) = 1$ и $(y, m) = 1$, тъй като противното води до противоречие. От друга страна, съгласно Теорема 3.1.4, когато оставим x и y да приемат произволни стойности разглежданото множество образува пълна система, Следователно с ограничението $(x, n) = (y, m) = 1$ числата $mx + ny$ ще опишат редуцирана система от остатъци. В часност получаваме, че при $(m, n) = 1$

$$\varphi(mn) = \varphi(n)\varphi(n).$$

Теорема 3.1.8 ***(Малка теорема на Ферма)*** *Нека p е просто число. За всяко $a \in \mathbb{Z}$ е в сила*

$$a^p \equiv a\,(mod\ p).$$

Доказателство. Съгласно свойствата на сравненията достатъчно е да покажем, че твърдението е вярно за $0, 1, 2, \dots, p-1$. Разсъждаваме индуктивно по a. При $a = 0$ и $a = 1$ твърдението е очевидно вярно. Да предположим, че $a^p \equiv a \pmod{p}$ за $a < p$. Ще го докажем и за $a + 1$.

$$(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} + 1.$$

Но

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!} \equiv 0 \pmod{p}.$$

Следователно

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

Да отбележим, че твърдението на теоремата е еквивалентно с $a^{p-1} \equiv 1 \pmod{p}$ за всяко $(a, p) = 1$.

В 1760 г. Ойлер доказва следното обобщение на горната теорема, известно като **Теорема на Ойлер**.

Теорема 3.1.9 *Нека n е естествено число. Ако $a \in \mathbb{Z}$ е взаимнопросто с n, то*

$$a^{\varphi(n)} \equiv 1\,(mod\ n).$$

Доказателство. Нека $k = \varphi(n)$ и $a_1, a_2, \dots, a_k$ е една редуцирана система от остатъци по модул n. Тогава числата

$$aa_1, aa_2, \dots, aa_k$$

очевидно са взаимнопрости с n и са несравними две по две по модул n. Следователно образуват редуцирана система от остатъци по модул n. Но тогава е в сила

$$a_1a.a_2a \dots a_ka \equiv a_1a_2 \dots a_k \pmod{n}.$$

Като разделим двете страни на горното сравнение на $\prod a_i$, което е възможно съгласно (5) на Теорема 3.1.2, получаваме

$$a^k \equiv 1 \pmod{n}.$$

При $n = p$ просто число получаваме друго доказателство на Малката теорема на Ферма.

Дефиниция 3.1.10 *Едно цяло число наричаме **обратимо по модул n**, когато съществува $x \in \mathbb{Z}$, такова че $ax \equiv 1\,(mod\ n)$. Числото x се нарича **обратно на** a **по модул n**.*

Ясно е, че всяко x_1, което удовлетворява горната дефиниция е сравнимо с x. По-общо, ако $a_1 \equiv a$ и $x_1 \equiv x$, то x_1 е обратно на a_1 по модул n. Затова казваме, че обратното число е определено еднозначно с точност до сравнимост по модул n и можем да говорим за обратни един на друг класове остатъци.
Числото x, което е обратно на a и $1 \leq x \leq n-1$ ще бележим с $a^{-1} \pmod{n}$ или просто с a^{-1}, когато е ясен модулът.

Теорема 3.1.11 *Нека n е естествено число. Цялото число a е обратимо по модул n тогава и само тогава, когато $(a, n) = 1$.*

Доказателство. $a \in \mathbb{Z}$ е обратимо по модул n число $\iff$ съществува x цяло, така че $ax \equiv 1 \pmod{n}$. Последното е изпълнено тогава и само тогава, когато съществува $y \in \mathbb{Z}$, така че

$$ax + yn = 1.$$

Горното равенство е възможно $\iff$ $(a, n) = 1$ и числата x и y се намират чрез алгоритъма на Евклид. Ясно е, че $b \in \mathbb{Z}_n : \quad b \equiv x \pmod{n}$ е търсения обратен на a елемент. Той може да се изрази и чрез a. Съгласно Теоремата на Ойлер $b = a^{\varphi(n)-1}$ удовлетворява сравнението $ab \equiv 1 \pmod{n}$.

Забележка 3.3 *Горната теорема показва, че броят на обратимите елементи в $\mathbb{Z}_n$, т.е редът на мултипликативната група $|\mathbb{Z}_n^*| = \varphi(n)$. Следователно $\mathbb{Z}_n$ е поле тогава и само тогава, когато $\varphi(n) = n - 1$, т.е. когато n е просто число. Обратният на a в $\mathbb{Z}_n$ се дава с формулата $a^{-1} = a^{\varphi(n)-1}\,(mod\ n)$, но намирането му чрез алгоритъма на Евклид изисква по-малко операции, дори когато стойността $\varphi(n)$ е известна.*

Теорема 3.1.12 (Теорема на Уилсон) *Необходимото и достатъчно условие естественото число n да е просто число е*

$$(n-1)! + 1 \equiv 0\,(mod\ n)$$

.

Доказателство. *Необходимост.* Нека $n = p$ е просто число. Тъй като $x^2 \equiv 1 \pmod{p}$ тогава и само тогава, когато p дели $x - 1$ или $x + 1$, то единствените числа, които съвпадат със своите обратни по модул p са 1 и $p - 1$. Останалите числа от 2 до $p-2$ се разбиват на двойки от обратни един на друг елементи. Следователно

$$2.3\dots(p-2) \equiv 1 \,(\mathrm{mod}\ p).$$

Но тогава

$$(p-1)! \equiv p-1 \equiv -1 \,(\mathrm{mod}\ p),$$

откъдето получаваме

$$(p-1)!+1 \equiv 0 \,(\mathrm{mod}\ p).$$

Достатъчност. Нека естественото число $n = ab$ удовлетворява сравнението и $1 \leq a < n$. Тъй като $a \,|\, (n-1)!$, то от свойство (6) на Теорема 3.1.2 следва, че $a \,|\, 1$, т.е. $a = 1$ и n е просто.

3.2 Линейни сравненията. Китайска теорема за остатъците.

Да разгледаме линейното сравнение $ax + b \equiv 0 \,(\mathrm{mod}\ n)$. По дефиниция n не дели a, т.е. $a \not\equiv 0 \,(\mathrm{mod}\ n)$.

Теорема 3.2.1 *Сравнението*

$$ax + b \equiv 0 \,(mod\ n) \tag{3.1}$$

има решение тогава и само тогава, когато $d = (a,n)$ дели b. В този случай сравнението има точно d решения

$$x_0,\, x_0 + \frac{n}{d},\, x_0 + 2\frac{n}{d},\, \dots,\, x_0 + (d-1)\frac{n}{d}, \tag{3.2}$$

където

$$x_0 \equiv -b_1 a_1^{\varphi(n_1)-1} \,(mod\ n_1)$$

и $a_1 = a/d,\ b_1 = b/d$ и $n_1 = n/d$.

Доказателство. Съгласно свойство (6) на Теорема 3.1.2, ако сравнението има решение, то $d = (a,n)$ трябва да дели b. Обратно, нека последното е изпълнено. Тогава (5) на Теорема 3.1.2 ни дава, че сравнението (3.1) има решение тогава и само тогава, когато има решение

$$a_1 x + b_1 \equiv 0 \,(\mathrm{mod}\ n_1), \tag{3.3}$$

където $a_1 = a/d,\ b_1 = b/d$ и $n_1 = n/d$. Тъй като $(a_1, n_1) = 1$, то съгласно Теорема 3.1.11 съществува единствено по модул n_1 естествено число x_1, така че $a_1 x_1 \equiv 1 \,(\mathrm{mod}\ n_1)$. Следователно $x_0 = -b_1 x_1$ удовлетворява (3.3) и е единственото му по модул n_1 решение. Числата дадени с (3.2) съвпадат като решения (по модул n_1) на (3.3), но са различни решения на (3.1). От друга страна всяко решение на (3.1) трябва да е сравнимо с x_0 по модул n_1. Следователно трябва да е сравнимо с $x_0 + kn_1$, т.е. с някое от (3.2), по модул n. С това теоремата е доказана.

Упражнение 3.2.1 *Докажете, че ако* $(a_1, a_2, \dots a_k, b, n) = d$, *то решенията на*

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b\,(mod\ n)$$

се дават с формулите

$$\mathbf{x}_0 + \mathbf{y} + \frac{n}{d}\mathbf{v},$$

където $\mathbf{x}_0 = (x_{01}, \dots, x_{0k})$ *е решение на*

$$a_1'x_1 + a_2'x_2 + \cdots + a_k'x_k \equiv b'\,(mod\ n_1),$$

$\mathbf{y} = (y_1, \dots, y_k)$ *е решение на*

$$a_1'x_1 + a_2'x_2 + \cdots + a_k'x_k \equiv 0\,(mod\ n_1),$$

$a_i' = a_i/d$, $b' = b/d$ *и* $n_1 = n/d$, *а* $\mathbf{v} = (v_1, v_2, \dots, v_k)$ *удовлетворява* $v_i \in \{0, 1, \dots, d-1\}$.

Следващата теорема е популярна под името ***Китайска теорема за остатъците***. Формулирана е в книга на китайския математик Сун Тзу (около 250 г.), но вероятно и била известна на китайските математици още преди новата ера. В края на първи век от новата ера Никомахус, математик от Палестина дава решение на конкретен пример следвайки стъпките в даденото по-долу доказателство.

Теорема 3.2.2 *Нека* $m_1, m_2, \dots, m_n$ *са две по две взаимнопрости естествени числа. За всяка съвкупност от цели числа* $a_1, a_2, \dots, a_n$ *съществува и то единствено по модул* $m = m_1m_2\dots m_n$ *цяло число* x, *което е едновременно решение на конгруенциите*

$$x \equiv a_1\,(mod\ m_1),\ x \equiv a_2\,(mod\ m_2),\ \dots,\ x \equiv a_n\,(mod\ m_n). \tag{3.4}$$

Доказателство. Да означим с $M_i = m/m_i$. Условието за модулите m_i влече $(M_1, M_2, \dots, M_n) = 1$. Следователно съществуват цели числа $u_1, u_2, \dots, u_n$, такива че

$$u_1M_1 + u_2M_2 + \cdots + u_nM_n = 1.$$

Тогава за всяко $i = 1, 2, \dots, n$ е изпълнено $e_i = u_iM_i \equiv 1\,(\mathrm{mod}\ m_i)$, което заедно с очевидните сравнения $e_j = u_jM_j \equiv 0\,(\mathrm{mod}\ m_i)$, за всяко $j \neq i$, показват, че

$$x = a_1u_1M_1 + a_2u_2M_2 + \cdots + a_nu_nM_n$$

е решение на системата (3.4).
Ако y е произволно решение на (3.4), то разликата $y - x$ трябва да се дели на всеки от модулите m_i. Тъй като те са две по две взаимнопрости, то тя се дели и на произведението им $m = m_1m_2\dots m_n$.

Забележка 3.4 *Сравнението* $u_iM_i \equiv 1\,(mod\ m_i)$ *показва, че* $u_i = M_i^{-1}\,(mod\ m_i)$. *Следователно числата* $u_1, \dots, u_n$ *могат да се намерят независимо едно от друго прилагайки алгоритъма на Евклид за* M_i *и* m_i, $i = 1, \dots, n$.

Пример 3.2.1 Да решим системата следните три сравнения:

$$x \equiv 1 \,(\mathrm{mod}\ 3), \quad x \equiv 4 \,(\mathrm{mod}\ 5), \quad x \equiv 4 \,(\mathrm{mod}\ 7).$$

Трите модула са два по два взаимно прости и съгласно Китайската теорема за остатъците системата има единствено решение по модул $3.5.7 = 105$. Следвайки доказателството ѝ намираме $M_1 = 35$, $M_2 = 21$ и $M_3 = 15$. Тогава $u_1 = 35^{-1} = 2^{-1} = 2 = -1 \,(\mathrm{mod}\ 3)$, $u_2 = 21^{-1} = 1^{-1} = 1 \,(\mathrm{mod}\ 5)$ и $u_3 = 15^{-1} = 1^{-1} = 1 \,(\mathrm{mod}\ 7)$. Тогава търсеното решение е

$$x = 1 \cdot (-1) \cdot 35 + 4 \cdot 1 \cdot 21 + 4 \cdot 1 \cdot 15 = 109$$

Следователно всяко

$$x \equiv 4 \,(\mathrm{mod}\ 105)$$

е решение на системата.

Теорема 3.2.3 *Нека $m_1, m_2, \ldots, m_k$ са две по две взаимнопрости естествени числа и $m = m_1 m_2 \ldots m_k$. Тогава*

$$\mathbb{Z}_m = I_1 \oplus I_2 \oplus \cdots \oplus I_k \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k},$$

където $I_j \cong \mathbb{Z}_{m_i}$ са идеали на $\mathbb{Z}_m$.

Доказателство. Изоморфизмът може да се докаже директно като се разгледа изображението

$$\varphi: \begin{cases} \mathbb{Z}_m \longrightarrow \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k} \\ \varphi(x) = (x_1, x_2, \ldots, x_k), \end{cases}$$

където $x_i \equiv x \,(\mathrm{mod}\ m_i)$, $i = 1, \ldots, k$. От китайската теорема следва, че това изображение е сюрективно и тъй като очевидно е инективно получаваме, че φ е биекция. Свойствата на сравненията ни дават, че то запазва операциите, т.е. явявя се и хомоморфизъм. Следователно φ е търсеният изоморфизъм.

По-интерестное е, обаче, как $\mathbb{Z}_m$ се представя като директна сума на свои подпръстени (идеали). Следвайки означенията от доказателството на китайската теорема за остатъците нека $M_i = m/m_i$ и $e_i = u_i M_i$. Тогава в $\mathbb{Z}_m$

$$e_1 + e_2 + \cdots + e_k = 1 \ \text{ и } \ e_i e_j = 0,$$

откъдето получаваме и

$$e_i^2 = e_i(1 - \sum_{j \neq i} e_j) = e_i.$$

Следователно $I_i = e_i \mathbb{Z}_{m_i} = \{0, e_i, 2e_i, \ldots, (m_i - 1)e_i\}$ са идеали в $\mathbb{Z}_m$, а e_i изпълняват ролята на единици в I_i. Съгласно китайската теорема за всяко $x \in \mathbb{Z}_m$ е в сила единственото представяне

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_k e_k,$$

където $x_i \equiv x \,(\mathrm{mod}\ m_i)$. Това доказва, че $\mathbb{Z}_m$ е директна сума от идеалите I_i.

Следствие 3.2.4 *Ако $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ е разлагането на n на прости множители, то*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_1^{e_2}} \oplus \dots \oplus \mathbb{Z}_{p_1^{e_k}}$$

Упражнение 3.2.2 *Докажете, че необходимото и достатъчно условие системата сравнения*

$$x \equiv a_1 \,(mod\ m_1),\ x \equiv a_2 \,(mod\ m_2),\ \dots,\ x \equiv a_t \,(mod\ m_t)$$

да има решение е за всяко $i \neq j$ да е изпълнено $(m_i, m_j) \,|\, (a_i - a_j)$. Решението е единствено по модул най-малкото общо кратно $[m_1, \dots, m_t]$ на модулите.

3.3 Сравненията от втора и по-висока степен.

Дефиниция 3.3.1 *Нека $f(x) = a_0 + a_1 x + \dots + a_k x^k$ и $g(x) = b_0 + b_1 x + \dots + b_l x^l$ са два полинома с цели коефициенти. Казваме, че те са* ***тъждествено конгруентни*** *и записваме*

$$f(x) \equiv g(x) \,(mod\ n),$$

когато $a_i \equiv b_i \,(mod\ n)$ за $i = 0, 1, \dots, \max\{k, l\}$.

Забележка 3.5 *От алгебрата е известно, че пръстенът $\mathbb{Z}[x]$ е област на цялост с еднозначно разлагане на неразложими множители (макар да не е пръстен от главни идеали) и всеки два полинома имат НОД (който не е задължително със старши коефициент 1). Затова свойствата на сравненията дадени с Теорема 3.1.2 остават в сила - при това по модул проиволен полином, не само по цяло число.*

Ако $f(x) \equiv g(x) \,(\mathrm{mod}\ n)$, то за всяко цяло число a е в сила

$$f(a) \equiv g(a) \,(\mathrm{mod}\ n).$$

Но обратното не е вярно дори последното сравнение да е в сила за безброй много a.

Пример 3.3.1 Например, сравнението

$$(x+1)(x+2)\dots(x+n) \equiv 2x(x-1)(x-2)\dots(x-n+1) \,(\mathrm{mod}\ n)$$

е вярно за всяко цяло x, но двете му страни като полиноми не са сравними по модул n.

Дефиниция 3.3.2 *Казваме, че $g(x)$ дели $f(x)$ по модул n, когато е изпълнено*

$$f(x) \equiv g(x)h(x) \,(mod\ n),$$

за $h(x) \in \mathbb{Z}[x]$.

Пример 3.3.2 Полиномът $x^2 + 5$ се дели на $x - 1$ по модул 6, тъй като е изпълнено $x^2 + 5 \equiv x^2 - 1 \,(\mathrm{mod}\ 6)$.

Дефиниция 3.3.3 *Нека $f(x) = a_0 + a_1x + \cdots + a_kx^k \in \mathbb{Z}[x]$.* ***Алгебрична конгруенция*** *наричаме сравнението*

$$f(x) \equiv 0\,(mod\ n), \tag{3.5}$$

чиито решение x се търси по модул n. Ако $a_k \equiv \cdots \equiv a_{t+1} \equiv 0$, но $a_t \not\equiv 0$ по модул n, то казваме, че сравнението е от степен t.

Коефициентите a_i на $f(x)$ в (3.5) могат да се заместват с произволни, конгруентни на a_i по модул n цели числа, т.е. те са представители на съответните класове по модул n. Следователно $f(x)$ можем да разглеждаме като полином над $\mathbb{Z}_n$ и да намерим решенията в цели числа на (3.5) означава да решим в $\mathbb{Z}_n$ уравнението $f(x) = 0$. Ако изрично не е уговорено друго ще считаме, че $f(x)$ е записан с истинската си степен, т.е. старшият коефициент не е сравним с нула по модул n.

Лема 3.3.4 *Необходимото и достатъчно условие a да е корен на (3.5) е*

$$f(x) \equiv (x-a)g(x)\,(mod\ n), \tag{3.6}$$

където $g(x) \in \mathbb{Z}[x]$.

> ***Доказателство.*** Достатъчността е очевидна. За да докажем необходимостта нека да разделим $f(x)$ на $x - a$. Получаваме $f(x) = (x-a)g(x) + r$, където $g(x) \in \mathbb{Z}[x]$, а $r \in \mathbb{Z}$. Замествайки x с a получаваме $r = f(a)$. следователно, ако $f(a) \equiv 0\,(\mathrm{mod}\ n)$, то (3.6) е изпълнено.

Теорема 3.3.5 *Ако p е просто число и*

$$f(x) \equiv 0\,(mod\ p),$$

е конгруенция от степен $t \geq 1$, то тя има най-много t корена.

> ***Доказателство.*** Ако $t = 1$ твърдението е вярно. Да предположим, че е вярно за $t - 1$. Нека a е корен, т.е. $f(a) \equiv 0\,(\mathrm{mod}\ p)$. Съгласно Лема 3.3.4 съществува полином $g(x)$ от степен $t-1$, такъв че $f(x) \equiv (x-a)g(x)\,(\mathrm{mod}\ p)$. Нека c е друго решение, т.е. $c \not\equiv a\,(\mathrm{mod}\ p)$. Тогава $(c-a)g(c) \equiv 0\,(\mathrm{mod}\ p)$, откъдето следва, че $g(c) \equiv 0\,(\mathrm{mod}\ p)$. По индукционното предположение $g(x) \equiv 0\,(\mathrm{mod}\ p)$ има най-много $t-1$ решения. Следователно $f(x) \equiv 0\,(\mathrm{mod}\ p)$ има най-много t решения. В частност от доказателствота следва, че ако $a_1, \ldots, a_s$ са неконгруентни решения, то
>
> $$f(x) \equiv (x-a_1)(x-a_2)\ldots(x-a_s)g(x)\,(\mathrm{mod}\ p),$$
>
> където $\deg g(x) = t - s$.

Горната теорема всъщност твърде, че в $\mathbb{Z}_p$ уравнение от степен t има най-много t корена. Но $\mathbb{Z}_p$ е поле, а за полиноми над полета този резултат е добре известен и горното доказателство съвпада с разсъжденията в общия случай. Както се вижда, то се основава на факта, че в поле няма делители на нулата. Не е така, обаче, в $\mathbb{Z}_n$, когато n е съставно. Сравнението

$$x^2 \equiv 1\,(\mathrm{mod}\ 12)$$

има за решения $x = \pm 1,\ \pm 5$. В този случай в $x^2 - 1 \equiv (x-1)g(x) \,(\mathrm{mod}\ 12)$ полагайки $x = 5$ не може да заключим, че $g(5) \equiv 0 \,(\mathrm{mod}\ 12)$, тъй като в $\mathbb{Z}_{12}$ числото 4 е делител на нулата. В пръстена $\mathbb{Z}_{12}[x]$ няма и еднозначно разлагане на неразложими множители:

$$x^2 - 1 = (x-1)(x+1) = (x-5)(x+5)$$

.

Теорема 3.3.6 *Нека* $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ *е разлагането на* n *на прости множители и* $f(x) \in \mathbb{Z}[x]$. *Алгебричната конгруенция*

$$f(x) \equiv 0 \,(mod\ n) \tag{3.7}$$

е еквивалентна на системата

$$f(x) \equiv 0 \,(mod\ p_1^{e_1}),\ f(x) \equiv 0 \,(mod\ p_2^{e_2}),\ \dots,\ f(x) \equiv 0 \,(mod\ p_k^{e_k}). \tag{3.8}$$

При това, ако $f(x) \equiv 0 \,(mod\ p_i^{e_i})$, $i = 1, \dots, k$, *има* t_i *неконгруентни по модул* $p_i^{e_i}$ *решения, то (3.7) има точно* $t_1 t_2 \dots t_k$ *неконгруентни по модул* n *решения.*

Доказателство. Ако x_0 е решение на (3.7), то очевидно е решение и на (3.8). Обратно, нека x_0 е решение на (3.8). Тогава $p_i^{e_i} \mid f(x_0)$ за всяко i. Но $p_i^{e_i}$ са две по две взаимнопрости числа. Следователно тяхното произведение n също дели $f(x_0)$.

Сега да преброим решенията на (3.7). Нека $a_i \in \mathbb{Z}$, $i = 1, \dots, k$, е решение на $f(x) \equiv 0 \,(\mathrm{mod}\ p_i^{e_i})$. Съгласно китайската теорема за остатъците съществува $x \in \mathbb{Z}$, такова че

$$x \equiv a_1 \,(\mathrm{mod}\ p_1^{e_1}),\ x \equiv a_2 \,(\mathrm{mod}\ p_2^{e_2}),\ \dots,\ x \equiv a_n \,(\mathrm{mod}\ p_k^{e_k}) \tag{3.9}$$

и x е еднозначно определено по модул n. Оставяйки a_i да пробягва всички различни t_i решения получаваме $t_1 t_2 \dots t_k$ различни системи (3.9) и съответно толкова решения на (3.7).

Дефиниция 3.3.7 *Казваме, че* $a \in \mathbb{Z}$ *е* k*-кратен корен по модул* n *на* $f(x) \not\equiv 0$, *ако*

$$f(x) \equiv (x-a)^k g(x) \,(mod\ n), \tag{3.10}$$

но $f(x)$ *не се дели на* $(x-a)^{k+1}$ *по модул* n.

Съгласно Лема 3.3.4 числото a е k-кратен корен по модул n точно тогава, когато е в сила (3.10), но $g(a) \not\equiv 0 \,(\mathrm{mod}\ n)$.

Дефиниция 3.3.8 *Нека* $f(x) = a_0 + a_1 x + \dots + a_m x^m \in \mathbb{Z}[x]$. *Под* ***производна*** *на* $f(x)$ *разбираме полинома*

$$f'(x) = a_1 + 2a_2 x + \dots + m a_m x^{m-1}.$$

Упражнение 3.3.1 *Проверете, че така дефинираната производна притежава свойствата:*

(1) $[f(x) \pm g(x)]' = f'(x) \pm g'(x)$, $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$ *и* $[cf(x)]' = cf'(x)$;

(2) $f^{(k)}(x) = k! \left[a_k + \binom{k+1}{k} a_{k+1} x + \cdots + \binom{m}{k} a_m x^{m-k} \right]$;

(3) $f(x) = f(a) + (x-a)f'(a) + \cdots + \frac{1}{k!}(x-a)^k f^{(k)}(a) + \cdots + \frac{1}{m!}(x-a)^m f^{(m)}(a)$ *(Формула на Тейлор).*

Твърдение 3.3.9 *Ако $a \in \mathbb{Z}$ е k-кратен корен по модул n на $f(x) \in \mathbb{Z}[x]$, то a е поне $k-1$-кратен корен по модул n на $f'(x)$ и*

$$f(a) \equiv f'(a) \equiv \frac{f''(a)}{2} \equiv \cdots \equiv \frac{f^{(k-1)}(a)}{(k-1)!} \equiv 0 \, (mod\ n). \tag{3.11}$$

Обратно, ако (3.11) е изпълнено, то a е поне k-кратен корен по модул n на $f(x)$.

Доказателство. По условие $f(x) = (x-a)^k g(x) + nh(x)$, откъдето

$$f'(x) = (x-a)^{k-1}[kg(x) + (x-a)g'(x)] + nh'(x)$$

Следователно

$$f'(x) \equiv (x-a)^{k-1}[kg(x) + (x-a)g'(x)] \, (\mathrm{mod}\ n),$$

което доказва първата част от твърдението. От тук непосредствено следва и (3.11). Нека сега е изпълнено (3.11). Замествайки във формулата на Тейлор получаваме, че

$$f(x) \equiv (x-a)^k g(x) \, (\mathrm{mod}\ n)$$

за подходящ полином $g(x) \in \mathbb{Z}[x]$. Да отбележим, че (2) на Упражнение 3.3.1 ни осигурява, че $\frac{1}{k!} f^{(k)}(a)$ са цели числа.

Ще отбележим , че (3.11) не може да го заменим с

$$f(a) \equiv f'(a) \equiv f''(a) \equiv \cdots \equiv f^{(k-1)}(a) \equiv 0 \, (\mathrm{mod}\ n).$$

Следващият пример илюстрира този факт и горното твърдение.

Пример 3.3.3 Нека $f(x) = x^4 - 1$ и $n = 4$. Лесно се проверява, че

$$x^4 - 1 \equiv (x-1)^2(x^2 + 2x - 1) = (x-1)^2 g(x) \, (\mathrm{mod}\ 4)$$

и $g(1) = 1 + 2 - 1 \not\equiv 0 \, (\mathrm{mod}\ 4)$. Следователно 1 е 2-кратен корен по модул 4. Тъй като $f'(x) = 4x^3$, $f''(x) = 12x^2$, то по модул 4 $f(1) = 0 \equiv 0$, $f'(1) = 4.1^3 \equiv 0$ и $\frac{f''(1)}{2} = 6 \not\equiv 0$. Но $f''(1) = 12 \equiv 0 \, (\mathrm{mod}\ 4)$.

Лема 3.3.10 *Нека $0 \le a < p^{r-1}$ е корен на конгруенцията $f(x) \equiv 0 \, (mod\ p^{r-1})$. Тогава*

(1) *ако $p \nmid f'(a)$, то съществува единствено*

$$x = a + tp^{r-1}, \ 0 \le t < p, \tag{3.12}$$

което е решение на

$$f(x) \equiv 0 \, (mod\ p^r); \tag{3.13}$$

(2) *ако* $p \mid f'(a)$ *и* $p^r \mid f(a)$, *то* $f(x) \equiv 0\,(mod\ p^r)$ *има точно* p *решения от вида (3.12);*

(3) *ако* $p \mid f'(a)$, *но* $p^r \nmid f(a)$, *то (3.13) няма решение от вида (3.12).*

Доказателство. Прилагайки формулата на Тейлор за $x = a+tp^{r-1}$, където $0 \le t < p$, получаваме

$$f(a+tp^{r-1}) = f(a)+tp^{r-1}f'(a)+\cdots+\frac{1}{k!}(tp^{r-1})^k f^{(k)}(a)+\cdots+\frac{1}{m!}(tp^{r-1})^m f^{(m)}(a).$$

Следователно за $r \ge 2$

$$f(a+tp^{r-1}) \equiv f(a)+tp^{r-1}f'(a)\,(\mathrm{mod}\ p^r).$$

Но $p^{r-1} \,|\, f(a)$, т.е. $f(a) = c.p^{r-1}$. Следователно

$$f(a+tp^{r-1}) \equiv p^{r-1}(c+tf'(a))\,(\mathrm{mod}\ p^r).$$

(1) Ако $p \nmid f'(a)$, то съгласно Теорема 3.2.1 сравнението

$$c+tf'(a) \equiv 0\,(\mathrm{mod}\ p)$$

има единствено решение t_a. Тогава

$$f(a+t_ap^{r-1}) \equiv p^{r-1}(c+f'(a)t_a) \equiv 0\,(\mathrm{mod}\ p^r),$$

т.е. $a+t_ap^{r-1}$ е единственото решение на (3.13) от вида (3.12).

Нека $p \mid f'(a)$. Тогава

$$f(a+tp^{r-1}) \equiv p^{r-1}c = f(a)\,(\mathrm{mod}\ p^r),\ \text{за всяко}\ \ 0 \le t < p.$$

(2) Ако $p^r \mid f(a)$, т.е. $p \,|\, c$, то

$$f(a+tp^{r-1}) \equiv 0\,(\mathrm{mod}\ p^r),\ \text{за всяко}\ \ t = 0,1,\ldots,p-1.$$

Следователно (3.13) има p решения от вида (3.12).
(3) Ако $p \mid f'(a)$, но $p^r \nmid f(a)$, то $p \nmid c$ и следователно

$$f(a+tp^{r-1}) \not\equiv 0\,(\mathrm{mod}\ p^r),$$

т.е. (3.13) няма нито едно решение от вида (3.12), такова че a да е кратен корен по модул p.

Да напомним очевидния факт, че всяко решение на (3.13) е решение и на $f(x) \equiv 0\,(\mathrm{mod}\ p^i)$ за всяко $i \le r$. При това "спускане", обаче, може да се получи "слепване" на решения, както се вижда от горната лема и Пример 3.3.5. По-интересен е въпросът кога един корен на $f(x)$ по модул p може да се "повдигне" до корен по модул p^r. Следващите теореми дават отговор на този въпрос.

Теорема 3.3.11 *Нека $f(x) \in \mathbb{Z}[x]$ и p е просто число. Ако $x_1 = a$ е прост корен на $f(x) \equiv 0\,(mod\; p)$, то за всяко $r \geq 2$ съществува и то единствено решение x_r на (3.13):*

$$f(x) \equiv 0\,(mod\; p^r), \tag{3.13}$$

такова че $x_r \equiv a\,(mod\; p)$. Търсеното решение има вида

$$x_r = a + t_1 p + t_2 p^2 + \cdots + t_{r-1} p^{r-1}, \;\; 0 \leq t_j < p. \tag{3.14}$$

Доказателство. Очевидно всяко решение $x < p^r$ на (3.13) може да се запише във вида (3.14) (в p-ична бройна система). Това, което ще докажем е, че t_j са еднозначно определени от $x_1 = a$.
Щом a е прост корен по модул p, то $p \nmid f'(a)$. Тогава от $f'(x_j) \equiv f'(a) \not\equiv 0\,(\mathrm{mod}\; p)$ за всяко $j = 1, 2, \ldots, r-1$ следва, че всяко едно от сравненията

$$f'(x_j)z + \frac{f(x_j)}{p^j} \equiv 0\,(\mathrm{mod}\; p) \tag{3.15}$$

има единствено решение $z = t_j$. Прилагаме последователно (1) на Лема 3.3.10 за $j = 1$, след това за $j = 2$ използвайки полученото x_2 и т.н. докато от x_{r-1} получим търсеното решение x_r.

Пример 3.3.4 Нека p е нечетно просто число и $f(x) = x^2 + p^2 - 1$. Сравнението $f(x) \equiv 0\,(\mathrm{mod}\; p)$ има два прости корена $a = 1$ и $a' = -1$. Същите, $x_2 = 1 + 0.p$, $x_2' = -1 + 0.p$, остават двете единствени решения на $f(x) \equiv 0\,(\mathrm{mod}\; p^2)$. Тъй като $f'(x) = 2x$ и $f(\pm 1)/p^2 = 1$, то решенията по модул p^3 са $1 + tp^2$ и $-1 + sp^2$, където $2t + 1 \equiv 0\,(\mathrm{mod}\; p)$ и $-2s + 1 \equiv 0\,(\mathrm{mod}\; p)$. Следователно решенията на $f(x) \equiv 0\,(\mathrm{mod}\; p^3)$ са

$$1 + \frac{p^2(p-1)}{2} \quad \text{и} \quad -1 + \frac{p^2(p+1)}{2}.$$

Теорема 3.3.12 *Нека $f(x) \in \mathbb{Z}[x]$ и p е просто число. Ако $x_1 = a$ е кратен корен на $f(x) \equiv 0\,(mod\; p)$ и $x_{r-1} \equiv a\,(mod\; p)$ е решение на $f(x) \equiv 0\,(mod\; p^{r-1})$, то (3.13) или няма решение $x \equiv x_{r-1}\,(mod\; p^{r-1})$ или има точно p такива неконгруентни решения:*

$$x_{r-1},\; x_{r-1} + p^{r-1},\; x_{r-1} + 2p^{r-1},\; \ldots,\; x_{r-1} + (p-1)p^{r-1}.$$

Доказателство. Съгласно Лема 3.3.10 $p^{r-1} \mid f(x_{r-1})$. Ако p не дели $f(x_{r-1})/p^{r-1}$ попадаме в случай (3) на Лема 3.3.10 и следователно (3.13) няма решение от вида $x_{r-1} + tp^{r-1}$. Ако $\frac{f(x_{r-1})}{p^{r-1}} \equiv 0\,(\mathrm{mod}\; p)$, то налице е случай (2) на Лема 3.3.10 и $x_{r-1} + tp^{r-1}$ е решение на (3.13) за всяко t, $0 \leq t < p$.

Пример 3.3.5 Нека p е просто число и $f(x) = (x-1)^2 + p^2$. Сравнението $f(x) \equiv 0\,(\mathrm{mod}\; p)$ има един двоен корен $x = 1$, а конгруенцията $f(x) \equiv 0\,(\mathrm{mod}\; p^2)$ има точно p корена:

$$1,\; 1+p,\; 1+2p,\; \ldots,\; 1+(p-1)p.$$

Точно това ни дава и Теорема 3.3.12, тъй като $f'(x) = 2(x-1)$ (при $p = 2$ производната е тъждествено нула) $f(1) = p^2$ се дели на p^2. Сега да разгледаме конгруенцията по модул

p^3. От горните корени по модул p^2 до корен по модул p^3 могат да се "повдигнат" тези и само тези $1+tp$, за които

$$f(1+tp) \equiv 0 \pmod{p^3},$$

т.е.

$$t^2+1 \equiv 0 \pmod{p}.$$

Но това сравнение има решение само, ако $p=2$ или (виж Глава 4) p е просто число от вида $p=4s+1$. В първия случай има единствено решение $t=1$, а във втория - две решения $t=\pm b$. Например при $p=17$ решенията са ± 4. Следователно корените по модул p^3 при $p=4s+1$ са $1+bp+kp^2$ и $1-bp+kp^2$, където $k=0,1,\dots,p-1$. В частност при $p=17$ получаваме $x=69+289k$ и $x=289k-67$, където $k=0,1,\dots,16$.
Ако $p=4s-1$, то $f(x)\equiv 0 \pmod{p^3}$ няма решение.

Теорема 3.3.13 *Нека $n=2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ е разлагането на n на прости множители, където p_i са нечетни прости числа. Тогава броят K на неконгруентните решения на*

$$x^2-1 \equiv 0 \,(mod\ n)$$

се задава с

$$K = \begin{cases} 2^k, & за\ e=0,1 \\ 2^{k+1}, & за\ e=2 \\ 2^{k+2}, & за\ e\geq 3. \end{cases}$$

Твърдението остава в сила и при $k=0$, т.е. когато n е степен на двойката.

Доказателство. Съгласно Китайската теорема за остатъците даденото сравнение е еквивалентно със системата от $k+1$ сравнения:

$$x^2-1 \equiv 0 \pmod{p_1^{e_i}},\quad i=1,2,\dots k \tag{3.16}$$

и

$$x^2-1 \equiv 0 \pmod{2^e}. \tag{3.17}$$

Поради свойствата на простите числа (дори без да използваме Теорема 3.3.11 всяко от сравнинията (3.16) има точно два корена $x=\pm 1$. Следователно приносът на всички тези сравнения в общия брой решения е множител 2^k (съгласно Теорема 3.3.6).
Сега да разгледаме конгруенцията (3.17). При $e=0$ числото 2 не участва в разлагането на n, така че можем да считаме, че приносът на (3.17) в този случай е множител 1. При $e=1$ сравнението има един двоен корен $x=1$ и приносът остава 1. Затова при $e=0$ и 1 общият брой решения е 1.2^k. Нека $e=2$. Тогава (3.17) има две решения $x=\pm 1$, което влече общ брой решения: 2^{k+1}. При $e\geq 3$ (3.17) има четири корена: $x=\pm 1 \quad \pm 1+2^{e-1}$. Следователно общия брой решения на $x^2-1\equiv 0 \pmod{n}$ е 2^{k+2}.

3.4 Примитивни корени и индекси.

Дефиниция 3.4.1 ***Показател (порядък или ред) на цялото число*** *a* ***по модул*** *n наричаме минималното естествено число $\nu = \nu(a)$, такова че*

$$a^\nu \equiv 1\,(mod\ n).$$

Казва се още, че a ***принадлежи на показател*** *ν* ***по модул*** *n.*

Да отбележим, че не всяко a има показател по модул n. Оставяме на читателя да докаже следното НДУ за съществуване на показател.

Упражнение 3.4.1 *Цялото число a има показател по модул n тогава и само тогава, когато $(a, n) = 1$.*

Следващите твърдения дават основните свойства на понятието показател (представляващо всъщност ред на елемент в мултипликативната група $\mathbb{Z}_n^*$), чиито доказателство също оставяме на читателя.

Упражнение 3.4.2 *Ако a има показател ν по модул n, то сравнението $a^m \equiv 1\,(mod\ n)$ е в сила тогава и само тогава, когато $\nu \mid m$.*

Упражнение 3.4.3 *Ако a има показател ν по модул n, то a^k има показател $\frac{\nu}{(\nu, k)}$.*

Упражнение 3.4.4 *Ако $a, b \in \mathbb{Z}$ принадлежат съответно на показатели ν и μ по модул n, то произведението им ab има за показател най-малкото общо кратно $[\nu, \mu]$.*

Следващата теорема показва, че за всяко просто число p съществува цяло число принадлежащо на показател $p - 1$.

Теорема 3.4.2 *Ако p е просто число, то съществува естествено число $g < p$, такова че $g^{p-1} \equiv 1\,(mod\ p)$, но $g^k \not\equiv 1\,(mod\ p)$ за всяко $k = 1, 2, \ldots, p - 2$.*

Доказателство. Ще дадем две доказателства на теоремата.

Доказателство I. Можем и да считаме, че $p > 2$, тъй като случая $p = 2$ е тривиален. Нека с $g(d)$ означим броят на естествените числа $< p$, които имат показател точно d. От Малката теорема на Ферма и Упражнение 3.4.2 следва, че $d \mid (p - 1)$. Но тогава

$$\sum_{d|(p-1)} g(d) = p - 1.$$

От друга страна точно същото равенство удовлетворява и функцията на Ойлер (Теорема 1.4.11), откъдето и Теорема 1.4.15 (формулата за обръщане) получаваме, че

$$g(p - 1) = \varphi(p - 1).$$

Следователно $g(p - 1) > 1$, което показва, че съществува естествено число с показател $p - 1$.

Доказателство II. Да означим с m минималното естествено число, такова че $x^m \equiv 1\,(\mathrm{mod}\ p)$ за всяко $x = 1, 2, \ldots, p - 1$. Малката теорема на Ферма ни дава, че такова число съществува и $m \leq p-1$. Но ако $m < p-1$, то ще получим, че сравнението

$$x^m - 1 \equiv 0 \,(\text{mod } p)$$

има повече от m неконгруентни решения, което противоречи на Теорема 3.3.5. Следователно $m = p-1$. Нека $p-1 = q_1^{e_1} q_2^{e_2} \dots q_k^{e_k}$. За всяко i съществува α_i, такова че $\alpha_i^{\frac{m}{q_i}} \not\equiv 1 \,(\text{mod } p)$. Тогава $\gamma_i = \alpha_i^{m/q_i^{e_i}}$ има показател точно $q_i^{e_i}$. Сега Упражнение 3.4.4 ни дава, че числото $g = \gamma_1 \gamma_2 \dots \gamma_k$ принадлежи на показател $q_1^{e_1} q_2^{e_2} \dots q_k^{e_k} = p-1$.

Забележка 3.6 *С горната теорема всъщност доказахме, че мултипликативната група $\mathbb{Z}_p^*$ е циклична. Това е частен случай на по-общия алгебричен резултат: Всяка крайна подгрупа на мултипликативната група на едно поле е циклична. Доказателството в общия случай по същество не се различава от изложеното горе Доказателство II.*

Дефиниция 3.4.3 *Цялото число g се нарича* ***примитивен корен по модул*** *p, ако $g^{p-1} \equiv 0 \,(mod\ p)$, но $g^k \not\equiv 0 \,(mod\ p)$ за всяко естествено $k < p-1$ (т.е., ако g поражда $\mathbb{Z}_p^*$).*

Понятието примитивен корен може да се дефинира и за произволен модул.

Дефиниция 3.4.4 *Цялото число g, $(g,n) = 1$, се нарича* ***примитивен корен по модул*** *n, ако принадлежи на показател $\varphi(n)$. (т.е. ако g поражда $\mathbb{Z}_n^*$). В този случай казваме, че n* ***притежава примитивен корен****.*

Теорема 3.4.2 осигурява, че всяко просто число има примитивен корен, но за различните p различни числа могат да са примитивни корени. Например, числото 2 е примитивен корен по модул $p = 5$, но не е такъв по модул $p = 7$, тъй като $2^3 \equiv 1 \,(\text{mod } 7)$. Примитивен корен по модул 7 е числото 3 - всички степени 3^0, 3, 3^2, 3^3, 3^4, 3^5 са несравними по модул 7.
Ако n не е просто число, то може да няма примитивен корен. Например 6 има за примитивен корен числото 5, докато 12 няма примитивен корен. Наистина $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \,(\text{mod } 12)$. Кога едно число има примитивен корен ще разгледаме в следващия параграф.

Нека n е естествено число, което притежава примитивен корен g. Тогава всички степени

$$1, g, g^2, \dots, g^{\varphi(n)-1}$$

са неконгруентни по модул n, тъй като допускането на противното би означавало, че g има показател по-малък от $\varphi(n)$. Следователно горните числа образуват редуцирана система остатъци по модул n и всяко a, за което $(a,n) = 1$, е сравнимо с някоя от горните степени на g.

Дефиниция 3.4.5 *Нека n е естествено число, което притежава примитивен корен g и $(a,n) = 1$. Единственото естествено число $e \in \{1, 2, \dots, \varphi(n)-1\}$, такова че*

$$a \equiv g^e \,(mod\ n)$$

се нарича ***индекс на*** *a* ***по модул*** *n* ***при основа*** *g. Бележим $e = \text{ind}_g\, a$ или $e = \text{ind}\, a$, когато е ясно, коя е основата (примитивния корен).*

Твърдение 3.4.6 *В сила са следните свойства:*

(1) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \,(mod\ \varphi(n))$;

(2) $\operatorname{ind}(a^k) \equiv k.\operatorname{ind} a \,(mod\ \varphi(n))$ *за всяко естествено* k;

(3) $\operatorname{ind} 1 = 0$ *при всеки избор на основата;*

(4) $\operatorname{ind}_g g = 1$;

(5) $\operatorname{ind}(-1) = \varphi(n)/2$ *за* $n > 2$;

Доказателство. Първите четири твърдения следват непосредствено от дефинициите и доказателството им оставяме за упражнение на читателя. (5): Нека $k = \operatorname{ind}(-1)$. Тогава $g^k \equiv -1 \,(\mathrm{mod}\ n)$, откъдето $g^{2k} \equiv 1 \,(\mathrm{mod}\ n)$. Тъй като g е примитивен корен по модул n, то $\varphi(n) \mid 2k$. Но $k < \varphi(n)$. т.е. $2k < 2\varphi(n)$, което влече $2k = \varphi(n)$. Следователно $k = \frac{\varphi(n)}{2}$.

Твърдение 3.4.7 *Нека* $(a, n) = 1$. *Ако* ν *е показателя на* a *по модул* n, *то*

$$\nu = \frac{\varphi(n)}{(\varphi(n), \operatorname{ind} a)}.$$

Доказателство. Показателят ν е минималното естествено число, такова че $a^\nu \equiv 1 \,(\mathrm{mod}\ n)$. Тогава прилагайки Твърдение 3.4.6-(2) получаваме

$$\nu.\operatorname{ind} a \equiv 0 \,(\mathrm{mod}\ \varphi(n))$$

Ако положим $d = (\varphi(n), \operatorname{ind} a)$, то минималното естествено число, което е решение е точно

$$\nu = \frac{\varphi(n)}{d}.$$

Индексите ни дават възможност да решаваме и показателни сравнения. Нека $(a, n) = (b, n) = 1$ и да разгледаме

$$a^x \equiv b \,(\mathrm{mod}\ n).$$

Прилагайки Твърдение 3.4.6-(2) получаваме

$$x.\operatorname{ind} a \equiv \operatorname{ind} b \,(\mathrm{mod}\ \varphi(n)).$$

Ясно е, че последното сравнение ще има решение тогава и само тогава, когато $d = (\varphi(n), \operatorname{ind} a)$ дели $\operatorname{ind} b$ и в този случай имаме точно d неконгруентни по модул $\varphi(n)$ решения.

3.5 Съществуване на примитивен корен.

Теорема 3.5.1 *Нека k е естествено число. За всяко $k \geq 3$ е в сила*

(1) *Всяко нечетно число a удовлетворява*

$$a^{2^{k-2}} \equiv 1 \,(mod\ 2^k).$$

(2) *Числото 5 има показател 2^{k-2} по модул 2^k.*

(3) *Числата*

$$\pm 5,\ \pm 5^2\ \pm 5^3\ \ldots,\ \pm 5^{2^{k-2}}$$

образуват редуцирана система по модул 2^k.

Доказателство. (1): С индукция по k. При $k = 3$ твърдението е вярно тъй като $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \,(\mathrm{mod}\ 8)$. От индукционното допускане $a^{2^{k-2}} \equiv 1 \,(\mathrm{mod}\ 2^k)$ следва, че $a^{2^{k-2}} = 1 + 2^k l$. Повдигайки на квадрат получаваме $a^{2^{k-1}} = (1 + 2^k l)^2 \equiv 1 \,(\mathrm{mod}\ 2^{k+1})$.
(2): От (1) следва, че $5^{2^{k-2}} \equiv 1 \,(\mathrm{mod}\ 2^k)$ за $k \geq 3$, т.е. показателят на 5 по модул 2^k ще е равен на 2^s, за някое $s \leq k-2$. Следователно $2^k \mid (5^{2^s} - 1)$, но $2^k \nmid (5^{2^{s-1}} - 1)$. Тъй като $5^{2^r} \equiv 1 \,(\mathrm{mod}\ 4)$ за всяко $r \geq 0$, то $(5^{2^r} + 1)$ се дели на 2, но не се дели на 4. Следователно $5^{2^{s+1}} - 1 = (5^{2^s} - 1)(5^{2^s} + 1)$ се дели на 2^{k+1}, т.е. $5^{2^{s+1}} \equiv 1 \,(\mathrm{mod}\ 2^{k+1})$. От друга страна, ако допуснем, че $5^{2^s} \equiv 1 \,(\mathrm{mod}\ 2^{k+1})$, ще получим аналогично, че $2^k \mid (5^{2^{s-1}} - 1)$, което противоречи на избора на s. Следователно показателя на 5 по модул 2^{k+1} ще е равен на 2^{s+1}. Сега твърдението следва от факта, че показателят по модул 2^3 е 2.
(3): Тъй като броят на числата е $2 \cdot 2^{k-2} = 2^{k-1} = \varphi(2^k)$, то остава да покажем, че всички числа са несравними две по две по модул 2^k. Ако допуснем, че $5^t \equiv \pm 5^l \,(\mathrm{mod}\ 2^k)$, $t \geq l$, то $5^{t-l} \equiv \pm 1 \,(\mathrm{mod}\ 2^k)$. Но съгласно отбелязаното по-горе $5^{t-l} \not\equiv -1 \,(\mathrm{mod}\ 2^k)$ за $k > 1$, а $5^{t-l} \equiv 1 \,(\mathrm{mod}\ 2^k)$ влече $2^{k-2} \mid (t - l)$, което е невъзможно за $t \neq l$.

От (1) следва, че 2^k има примитивен корен само при $k = 1$ и 2, т.е. в сила е

Следствие 3.5.2 *Групата $\mathbb{Z}^*_{2^k}$ е циклична тогава и само тогава, когато $k = 1$ и 2.*

Теорема 3.5.3 *Ако p е нечетно просто число, то p^k има примитивен корен за всяко k. Един такъв примитивен корен за всяко k е естествено число g, което е примитивен корен по модул p, но $g^{p-1} \not\equiv 1 \,(mod\ p^2)$.*

Доказателство. Ако g е примитивен корен по модул p, то очевидно и $g + p$ също е такъв примитивен корен. Поне единият от тях удовлетворява

$$g^{p-1} \not\equiv 1 \,(\mathrm{mod}\ p^2). \tag{3.18}$$

Наистина, ако $g^{p-1} \equiv 1 \,(\mathrm{mod}\ p^2)$, то

$$(g + p)^{p-1} = g^{p-1} + (p - 1)pg^{p-2} + p^2 A,$$

което не е сравнимо с 1 по модул p^2, тъй като $p^2 \nmid (p-1)pg^{p-2}$. И така можем да предполагаме, че g удовлетворява (3.18).
Директната проверка показва, че от $a = 1+p^l A$ следва, че $a^p = 1+p^{l+1}B$, т.е. $a^p \equiv 1 \pmod{p^{l+1}}$. Следователно $g^{p(p-1)} \equiv 1 \pmod{p^2}$ и поради (3.18) g има показател $p(p-1) = \varphi(p^2)$ по модул p^2, т.е. g е примитивен корен по модул p^2. Тогава $g^{p^2(p-1)} \equiv 1 \pmod{p^3}$ и $p^2(p-1)$ е минималната степен, за която това е изпълнено. Следователно g е примитивен корен по модул p^3. Продължавайки аналогично получаваме, че g е примитивен корен по модул p^k.

Следствие 3.5.4 *Групата $\mathbb{Z}^*_{p^k}$ е циклична за всяко естествено k и всяко просто $p > 2$.*

Теорема 3.5.5 *Естественото число $n > 1$ има примитивен корен тогава и само тогава, когато*

$$n = 2,\ 4,\ p^k \ \text{ или } \ 2p^k,$$

където p е нечетно просто, а k произволно естествено число.

Доказателство. Нека $n = 2^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. От Теорема 3.2.3 следва, че

$$\mathbb{Z}^*_n = I^* \times I^*_1 \times I^*_2 \times \cdots \times I^*_k \cong \mathbb{Z}^*_{2^e} \times \mathbb{Z}^*_{p_1^{e_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{e_k}}.$$

В такъв случай $\mathbb{Z}^*_n$ ще е циклична тогава и само тогава, когато директните ѝ компоненти са циклични и от взаимно прости редове. $\mathbb{Z}^*_{p_i^{e_i}}$ са циклични от четен ред съгласно предходната теорема. Тогава, ако в разлагането на n участват две различни нечетни прости числа, то ще има поне две компоненти, които не са взаимнопрости. Следователно в разлагането участва най-много едно просто число > 2. Групата $\mathbb{Z}^*_{2^e}$ е циклична само за $e = 1, 2$, но при $e = 2$ не може в разлагането да участва нечетно просто число. Обратно, ако n е от посочения вид, то $\mathbb{Z}^*_n$ или е циклична или е директно произведение на две циклични от взаимнопрости редове ($\mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^l}$).

Следствие 3.5.6 *Групата $\mathbb{Z}^*_n$ е циклична тогава и само тогава, когато*

$$n = 2,\ 4,\ p^k \ \text{ или } \ 2p^k,$$

където p е нечетно просто, а k произволно естествено число.

3.6 Допълнителни задачи към Глава 3.

Задача 3.1 *Нека a и b са цели числа. Докажете, че ако n дели $a^n - b^n$, то n дели и $(a^n - b^n)/(a-b)$.*

Задача 3.2 *Докажете, че съществуват безброй много прости числа от вида $4k+1$.*

Задача 3.3 *Да се решат системите сравнения*

а) $\left|\begin{array}{ll} x & \equiv 7 \quad (mod\ 33) \\ x & \equiv 3 \quad (mod\ 63) \end{array}\right.$ *б)* $\left|\begin{array}{ll} 3x & \equiv 5 \quad (mod\ 7) \\ 2x & \equiv 3 \quad (mod\ 5) \\ 3x & \equiv 3 \quad (mod\ 9) \end{array}\right.$ *в)* $\left|\begin{array}{ll} 4x+3y & \equiv 5 \quad (mod\ 12) \\ 6x+5y & \equiv 7 \quad (mod\ 12) \end{array}\right.$

Задача 3.4 *Да се решат уравненията*
а) $x^2 \equiv -1\,(mod\ 85)$; *б)* $x^2 + 3x + 1 \equiv 0\,(mod\ 25)$; *в)* $x^7 + x + 1 \equiv 0\,(mod\ 27)$;
г) $11x^3 \equiv -1\,(mod\ 56)$.

Задача 3.5 *Да се решат системите сравнения*

а) $\left|\begin{array}{rll} 9x^{14} & \equiv 1 & (mod\ 17) \\ 2x & \equiv 3 & (mod\ 9) \end{array}\right.$ *б)* $\left|\begin{array}{lll} x^6 & \equiv 1 & (mod\ 11) \\ 5x & \equiv 2 & (mod\ 31) \end{array}\right.$

Задача 3.6 *Докажете, че ако* $b = 2^\nu B \pm 1$, *където* $\nu \geq 2$ *и* B *нечетно, то* b *има показател* $2^{k-\nu}$ *по модул* 2^k.

Задача 3.7 *Докажете, че*

$$A = \frac{3^n(3^t - 1) - (-1)^n\left((-1)^n - 1\right)}{4}$$

е цяло число и $t = 2^k$ *е минималното* t, *за което* $A \equiv 0(mod\ 2^k)$.

Задача 3.8 *Нека* p *и* q *са прости числа, такива че* $p = 2q + 1$. *Докажете, че поне едно от числата* 2 *или* -2 *е примитивен корен по модул* p.