Софийски Университет "Св. Климент Охридски"
Факултет по Математика и Информатика
катедра Алгебра

РЪКОВОДСТВО

ПО

ВИСША АЛГЕБРА

АВТОР

МАЯ СТОЯНОВА

София, 2013 г.

Съдържание

Предговор

Настоящото ръководство съдържа факти и задачи необходими за усвояването на материала по Висша алгебра. Предназначено е за работа със студентите от Факултета по Математика и Информатика при Софийски Университет "Св. Климент Охридски". Съдържанието следва курса по Висша алгебра, който се чете през втория семестър от колегите от катедра Алгебра и мен. В него са събрани задачи от дългогодишния опит на целия колектив.

Книгата се състои от ? глави. В първа глава са представени основни понятия и методи от Теория на числата. Описани са свойствата на делимостта на целите числа, на сравненията и на някои аритметични функции. Подбрани са факти и техники, които се прилагат по-нататък в материала по Висша алгебра. Специално искам да отбележа, че в памет на акад. Стефан Додунеков и проф. Керопе Чакърян в главата са цитирани някои теоретични факти и задачи както са в тяхното ръководство "Задачи по теория на числата".

Във втора глава е разгледано множеството $\mathbb{Z}_n$ на класовете остатъци по модул n. Въведени са операциите събиране и умножение на елементите му и са показани редица свойства на така въведените действия. Авторът се надява, че по този начин студентите по-лесно ще усвоят работата и пресмятанията в крайни пръстени и полета и в пръстена на полиномите с коефициенти от крайно поле, представени в следващи глави на това ръководство.

.....

Глава 1

Елементи от Теория на числата

В тази глава са включени някои понятия, факти и техни приложения от Теория на числата, които са необходими и се използват в курса по Висша алгебра. Ще напомним основните свойства на целите числа (множеството $\mathbb{Z}$), като под число a ще разбираме цяло число.

Да отбележим, че поради големия обем на материала по Висша алгебра (в курса за студентите на ФМИ) на материала от тази глава се отделя минималния възможен брой учебни часове в началото на курса. Поради това критерият за избор на задачите тук не е била тяхната сложност, а напротив - подбрани са само теоретични задачи и лесни практически задачи, които илюстрират свойства и техники от Теория на числата, използващи се в решенията на задачите по Висша алгебра.

1.1 Делимост на цели числа

Нека $a \neq 0$ и b са две цели числа.

Дефиниция 1.1.1. *Ще казваме, че a дели b (или b се дели на a) и ще означаваме $a \mid b$, ако съществува цяло число c, такова че $b = ac$.*

Числата a и c ще наричаме делители на числото b. Ясно е, че ако a дели b, то и $(-a) \mid b$. Ако a не дели b, ще пишем $a \nmid b$.

В сила са следните свойства на делимостта:

1. За всяко ненулево цяло число a е изпълнено $a \mid a$.

2. Ако $a \mid b$ и $b \neq 0$, то $|a| \leq |b|$.

3. Ако $a \mid b$ и $b \mid a$, то $|a| = |b|$, т.е. $a = \pm b$.

4. Ако $a \mid b$ и $b \mid c$, то $a \mid c$.

5. Ако $a \mid b$ и $a \mid c$, то $a \mid (b \pm c)$.

6. Ако $a \mid b$ и $c \in \mathbb{Z}$, то $a \mid bc$.

7. Ако $a \mid b_1, \ldots, a \mid b_n$ и $c_1, \ldots, c_n$ са произволни цели числа, то $a \mid (b_1c_1 + \ldots + b_nc_n)$.

8. Ако $a \mid (b + c)$ и $a \mid b$, то $a \mid c$. В частност, ако $b + c = 0$ и $a \mid b$, то $a \mid c$.

Твърдение 1.1.2. *Всяко ненулево цяло число има краен брой делители.*

Теорема 1.1.3. ***(Теорема за деление с остатък).*** *За всеки две цели числа a и b, $b \neq 0$, съществуват еднозначно определени цели числа q (частно) и r (остатък), такива че $a = bq + r$ и $0 \leq r < |b|$.*

Ясно е, че $a \mid b$ точно когато остатъкът при делението на b с a е равен на 0. За три числа a, b и c имаме, че $c \mid (a - b)$ точно тогава, когато a и b дават един и същи остатък при деление с c.

Следствие 1.1.4. *Нека n е естествено число. От n последователни цели числа (точно) едно се дели на n.*

Следствие 1.1.5. *За всеки две естествени числа a и $p \geq 2$ съществува единствено представяне на a във вида*

$$a = c_n p^n + c_{n-1} p^{n-1} + \ldots + c_1 p + c_0,$$

където $0 \leq c_i < p$ за всяко $i = 0, 1, 2, \ldots, n-1$ и $0 < c_n < p$.

Представянето на числото a в Следствие 1.1.5 се нарича представяне на a в бройна система с основа p (накратко p-ичен запис на a), а c_0, c_1, …, c_n са p-ичните цифри на числото a.

Пример 1.1.6. *За да представим числото $37_{(10)}$ в двоична бройна система делим числото на 2 докато частното стане 0, т.е.*

$$37 = 2.18 + 1;\ 18 = 2.9 + 0;\ 9 = 2.4 + 1;\ 4 = 2.2. + 0;\ 2 = 2.1 + 0;\ 1 = 2.0 + 1.$$

Тогава двоичният запис се образува от получените остатъци записани в обратен ред, т.е. $37_{(10)} = 100101_{(2)}$.

По-този начин можем да получим и следните представяния:

$$\begin{aligned} 11111011101_{(2)} &= 1.2^{10} + 1.2^9 + 1.2^8 + 1.2^7 + 1.2^6 + 0.2^5 + 1.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 1 = 2013_{(10)}, \\ 2202120_{(3)} &= 2.3^6 + 2.3^5 + 0.3^4 + 2.3^3 + 1.3^2 + 2.3^1 + 0 = 2013_{(10)}, \\ 2013_{(10)} &= 2.10^3 + 0.10^2 + 1.10^1 + 3. \end{aligned}$$ ◇

Числото b се нарича *общ делител* на числата $a_1, a_2, \ldots, a_n$, ако то дели всяко от тях. Всеки две цели числа имат общ делител, например $d = 1$.

Дефиниция 1.1.7. *Нека поне едно от целите числа a и b е ненулево. Под най-голям общ делител (НОД) на a и b ще разбираме цялото число d, притежаващо следните свойства:*

1. $d \mid a$, $d \mid b$.

2. Ако $d_1 \mid a$, $d_1 \mid b$, то $d_1 \mid d$.

Ще използваме означението $d = (a, b)$.

Ако d е общ делител, то и $-d$ е такъв. Ще считаме, че (a, b) е естествено число и тогава най-големият общ делител на целите числа a и b е определен еднозначно.

Аналогично се определя най-голям общ делител $(a_1, a_2, \ldots, a_n)$ на произволен краен брой цели числа $a_1, a_2, \ldots, a_n$. В сила е равенството

$$(a_1, a_2, \ldots, a_n, a_{n+1}) = ((a_1, a_2, \ldots, a_n), a_{n+1}).$$

Ако $(a, b) = 1$, ще казваме, че целите числа a и b са *взаимно прости*. По-общо числата $a_1, a_2, \ldots, a_n$ са взаимно прости, ако $(a_1, a_2, \ldots, a_n) = 1$. За всеки две цели числа съществува най-голям общ делител и той може да се пресметне с известния *Алгоритъм на Евклид*.

– Ако едно от числата a и b, например a, е нула, то $b \neq 0$ и тогава $(0, b) = |b|$.

– Ако и двете са различни от нула, то понеже $(a, b) = (\pm a, \pm b)$ при произволно разположение на знаците можем да предполагаме, че $a > 0, b > 0$. Нека $a \geq b$. Чрез последователно прилагане на теоремата за деление с остатък (Теорема 1.1.3) имаме равенствата

$$\begin{array}{ll} a = bq_1 + r_1, & 0 \leq r_1 < b, \\ b = r_1 q_2 + r_2, & 0 \leq r_2 < r_1, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ r_{k-1} = r_k q_{k+1} + r_{k+1}, & 0 \leq r_{k+1} < r_k, \\ r_k = r_{k+1} q_{k+2}, & r_{k+2} = 0. \end{array}$$

Получаването на нулев остатък r_{k+2} е сигурно, защото редицата $b > r_1 > r_2 > \ldots$ не може да съдържа повече от b на брой естествени числа. Ще покажем, че $(a, b) = r_{k+1}$. От $a = bq_1 + r_1$ следва, че всеки общ делител на a и b дели r_1 и всеки общ делител на b и r_1 дели a. В частност $(a, b) = (b, r_1)$. С аналогични разсъждения стигаме до равенствата

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_k, r_{k+1}) = (r_{k+1}, 0) = r_{k+1},$$

т.е. последният ненулев остатък r_{k+1} е търсеният най-голям общ делител.

Да отбележим, че алгоритъмът на Евклид освен правило за намиране е и доказателство за съществуване на НОД на две цели числа.

Твърдение 1.1.8. ***(тъждество на Безу)***. *За всеки две цели числа a и b съществуват цели числа u и v, такива че $(a, b) = d = ua + vb$. При това $(u, v) = 1$. В частност, a и b са взаимно прости числа тогава и само тогава, когато съществуват цели числа u и v, за които $ua + vb = 1$.*

За всеки n на брой цели числа $a_1, a_2, \ldots, a_n$ с НОД $d = (a_1, a_2, \ldots, a_n)$ е сила равенството

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1.$$

Пример 1.1.9. *Покажете с помощта на алгоритъма на Евклид, че НОД на числата $a = 183183$ и $b = 130845$ е равен на $(a, b) = 26169$ и е в сила равенството $(a, b) = ua + vb$ за $u = -2$ и $v = 3$.* ♢

Твърдение 1.1.10. *Нека $a, b, c \in \mathbb{Z}$. В сила са следните твърдения:*

а) $(ac, bc) = c(a, b)$;

б) Ако $a = (a,b)a_1$, $b = (a,b)b_1$, *то* $(a_1, b_1) = 1$.

в) Ако $(a,b) = 1$, *то* $(ac, b) = (c, b)$;

г) Ако $(a,b) = 1$ *и* $a \mid bc$, *то* $a \mid c$;

д) Ако $a \mid c$, $b \mid c$ *и* $(a,b) = 1$, *то* $ab \mid c$;

е) Ако $(a,b) = 1$ *и* $(a,c) = 1$, *то* $(a, bc) = 1$.

Пример 1.1.11. *За числата от Пример 1.1.9 имаме* $a = 183183 = 7.13.2013$ *и* $b = 130845 = 5.13.2013$. *От Твърдение 1.1.10 а) получаваме НОД* $(a,b) = 13.2013.(7,5) = 13.2013 = 26169$. ♢

Нека $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$. Числото $c \in \mathbb{Z}$ се нарича *общо кратно* на a и b, ако $a \mid c$, $b \mid c$. Всеки две ненулеви цели числа a и b имат общо кратно, например ab.

Дефиниция 1.1.12. *Нека* $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$. *Под най-малко общо кратно (НОК) на* a *и* b *ще разбираме цялото число* m, *притежаващо следните свойства:*

1. $a \mid m$, $b \mid m$.

2. Ако $a \mid m_1$, $b \mid m_1$, *то* $m \mid m_1$.

Ще използваме означението $m = [a, b]$.

Да отбележим, че всяко общо кратно на числата a и b е от вида $\dfrac{ab}{(a,b)}t$, $t \in \mathbb{Z}$. Тогава съществуването на НОК е ясно от факта, че има краен брой естесвени числа, ненадминаващи $|ab|$ (очевидно $[a,b] \leq |ab|$). Най-малкото общо кратно на две цели числа е определено еднозначно, ако считаме, че то е положително число. Аналогично се определя НОК $[a_1, a_2, \ldots, a_n]$ на произволен краен брой различни от нула цели числа $a_1, a_2, \ldots, a_n$. В сила е равенството

$$[a_1, a_2, \ldots, a_n, a_{n+1}] = [[a_1, a_2, \ldots, a_n], a_{n+1}].$$

За всеки две ненулеви цели числа е изпълнено равенството $(a,b)[a,b] = ab$. В частност, ако $(a,b) = 1$, то $[a,b] = ab$.

Пример 1.1.13. *За числата от Пример 1.1.9 имаме* $a = 183183 = 7.13.2013$ *и* $b = 130845 = 5.13.2013$. *Тогава НОК* $[a,b] = 5.7.13.2013 = 915915$. ♢

Дефиниция 1.1.14. *За едно естествено число* $p > 1$ *ще казваме, че е просто, ако единствените му делители са числата* ± 1 *и* $\pm p$. *Едно число* $n > 1$ *се нарича съставно, ако не е просто. Числото 1 не е нито просто, нито съставно.*

Ясно е, че ако p е просто число и a е цяло, то $(p,a) = 1$ е еквивалентно на $p \nmid a$.

Едно съставно число n се дели на 1, на себе си и на поне още едно цяло число.

Твърдение 1.1.15. *Всяко естествено число* $a > 1$ *притежава поне един прост делител.*

Твърдение 1.1.16. *Всяко съставно естествено число* $a > 1$ *притежава поне един прост делител* p *такъв, че* $p \leq \sqrt{a}$.

Твърдение 1.1.17. ***(Евклид)****. Съществуват безбройно много прости числа.*

Твърдение 1.1.18. *Едно естествено число $p > 1$ е просто тогава и само тогава, когато удовлетворява условието: за всеки две цели числа a и b, за които $p \mid ab$, е изпълнено $p \mid a$ или $p \mid b$.*

Един начин за намиране на всички прости числа, които не са по-големи от дадено естествено число n, е така нареченото решето на Ератостен. Методът е изключително популярен и разпространен в интернет.

Теорема 1.1.19. ***(Основна теорема на аритметиката)****. Всяко естествено число $n > 1$ се представя по единствен начин (с точност до реда на множителите) като произведение на краен брой прости числа.*

Дефиниция 1.1.20. *Нека за естественото число n имаме*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \tag{1.1.1}$$

като $p_1, \dots, p_k$ са две по две различни прости числа и $\alpha_i \geq 1$ $(i = 1, \dots, k)$, Представянето (1.1.1) се нарича канонично разлагане на n на прости множители.

Забележка 1.1.21. *Всеки естествен делител d на числото n с каноничнo разлагане (1.1.1) има вида*

$$d = {q_1}^{\beta_1} {q_2}^{\beta_2} \dots {q_k}^{\beta_k},$$

където $0 \leq \beta_i \leq \alpha_i$ $(i = 1, 2, \dots, k)$ и обратно, всяко число от горния вид очевидно е делител на n.

Забележка 1.1.22. *Нека a и b са две естествени числа и нека $q_1, q_2, \dots, q_t$ са всички прости числа, участващи в каноничното разлагане на ab на прости множители. Числата a и b могат да се запишат по следния начин:*

$$a = {q_1}^{\alpha_1} {q_2}^{\alpha_2} \dots {q_t}^{\alpha_t}, \quad b = {q_1}^{\beta_1} {q_2}^{\beta_2} \dots {q_t}^{\beta_t},$$

където $\alpha_i \geq 0$, $\beta_i \geq 0$ $(i = 1, 2, \dots, t)$ са цели числа. Тогава

$$(a, b) = {q_1}^{\min(\alpha_1, \beta_1)} {q_2}^{\min(\alpha_2, \beta_2)} \dots {q_t}^{\min(\alpha_t, \beta_t)}$$

($\min(\alpha_i, \beta_i)$ означава по-малкото от числата α_i и β_i),

$$[a, b] = {q_1}^{\max(\alpha_1, \beta_1)} {q_2}^{\max(\alpha_2, \beta_2)} \dots {q_t}^{\max(\alpha_t, \beta_t)}$$

($\max(\alpha_i, \beta_i)$ означава по-голямото от числата α_i и β_i).

Задачи

Задача 1.1.23. *Да се докаже, че за всяко цяло число a:*

а) a^2 е от вида $3k$ или $3k + 1$;

б) $(a-1)a(a+1)$ *се дели на* 6*;*

в) (a^5-a) *се дели на* 30*;*

г) (a^5-5a^3+4a) *се дели на* 120*;*

д) $(a^6-5a^4+4a^2)$ *се дели на* 360*;*

е) $n!$ *дели произведението на* n *последователни цели числа,* $n \in \mathbb{N}$.

Решение. г) Числото a^5-5a^3+4a можем да запишем във вида

$$a^5-5a^3+4a = a(a^2-1)(a^2-4) = (a-2)(a-1)a(a+1)(a+2),$$

т.е. имаме произведение на 5 последователни цели числа. Числото $(a-1)a(a+1)(a+2)$ като произведение на четири последователни цели числа се дели на 24 (обосновете този факт), а $5 \mid (a-2)(a-1)a(a+1)(a+2)$ (Следствие 1.1.4). Тъй като $(5,24)=1$ по Твърдение 1.1.10 а) следва, че $120 \mid (a-2)(a-1)a(a+1)(a+2)$. □

Задача 1.1.24. *Да се намерят всички цели числа* a*, за които:*

а) $a+2$ *дели* a^2+3*;* *б)* $a-2$ *дели* a^3-2*;*

в) числото $\dfrac{a+6}{a-5}$ *е цяло;* *г) числото* $b=\dfrac{11a+5}{5a+7}$ *е цяло;*

д) числото $b=\dfrac{10a+12}{3a+5}$ *е цяло;* *е) числото* $b=\dfrac{13a+25}{3a+7}$ *е цяло.*

Решение. б) От равенството $a^3-2 = a^3-2^3+6 = (a-2)(a^2+2a+4)+6$ следва, че $(a-2) \mid 6$ и значи $a-2 = \pm1, \pm2, \pm3, \pm6$. Окончателно за a получаваме, че $a \in \{-4,-1,0,1,3,4,5,8\}$.

г) Имаме $b = \dfrac{11a+5}{5a+7} = 2+\dfrac{a-9}{5a+7}$ и числото b е цяло само когато числото $\dfrac{a-9}{5a+7}$ е цяло. Лесно се забелязва, че за $a<-4$ и $9<a$ имаме $0<\dfrac{a-9}{5a+7}<1$ и значи за такива стойности на a числото b не е цяло. За оставащите цели стойности на a с непосредстена проверка се показва, че единствено за $a=-1$ числото $b=-5$ е цяло, т.е. само $a=-1$ е решение. □

Отг. а) $a \in \{-9,-3,-1,5\}$; в) $a \in \{-6,4,6,16\}$;
д) $a \in \{-2,-1\}$; е) $a \in \{-3,-2,-1\}$.

Задача 1.1.25. *Да се докаже, че за всяко естествено число* n*:*

а) числото $a_n = n^3+17n$ *се дели на 6;*

б) ако b *е цяло число, такова, че* $6 \mid (b+1)$*, то* $6 \mid a_n = n^3+bn$*;*

в) числото $a_n = 7^{n+1}-6n-7$ *се дели на 36;*

г) ако b *е цяло число, то* $a_n = b^{n+1}-(b-1)n-b$ *се дели на* $(b-1)^2$*;*

д) числото $a_n = 3^{3n+3}-26n-27$ *се дели на* 676*;*

е) числото $a_n = (n+1)(n+2)\dots(n+n)$ *се дели на* 2^n*, но не се дели на* 2^{n+1}*;*

ж) числото $a_n = 2^{3^n}+1$ *се дели на* 3^{n+1}*, но не се дели на* 3^{n+2}.

з) числото $a_n = 2^{2^{n+1}}+2^{2^n}+1$ *се дели на* 21*;*

Решение. Използва се принципа на математическата индукция.

ж) При $n = 1$ имаме $a_1 = 9$ и $3^2 \mid a_1$, но $3^3 \nmid a_1$. Нека $3^{k+1} \mid a_k$, но $3^{k+2} \nmid a_k$. Тъй като

$$a_{k+1} = a_k({a_k}^2 - 3.2^{3^k})$$

и очевидно $9 \nmid ({a_k}^2 - 3.2^{3^k})$, то $3^{k+2} \mid a_{k+1}$, но $3^{k+3} \nmid a_{k+1}$. Съгласно принципа на математическата индукция твърдението е изпълнено за всяко естествено число n.

з) При $n = 1$ имаме $21 \mid 21 = a_1$. Нека $21 \mid a_k$. Тъй като

$$a_{k+1} = 2^{2^{k+2}} + 2^{2^{k+1}} + 1 = {a_k}^2 - 2^{2^k+1}a_k,$$

твърдението следва по индукция. □

Задача 1.1.26. *Нека a и b са две взаимно прости естествени числа. Да се докаже, че сумата S от частните на числата a, $2a$, ..., $(b-1)a$, получени при делението им с числото b, е $S = \dfrac{(a-1)(b-1)}{2}$.*

Решение. Тъй като никое от дадените числа не се дели на b, съгласно Теорема 1.1.3 имаме

$$\begin{array}{ll} a = bq_1 + r_1, & 1 \le r_1 \le b-1, \\ 2a = bq_2 + r_2, & 1 \le r_2 \le b-1, \\ 3a = bq_3 + r_3, & 1 \le r_3 \le b-1, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ (b-1)a = bq_{b-1} + r_{b-1}, & 1 \le r_{b-1} \le b-1. \end{array}$$

Да допуснем, че за някои $1 \le k < l \le b-1$ е изпълнено $r_k = r_l$.

Тогава $la - ka = (l-k)a = b(q_l - q_k)$, т.е. $b \mid a(l-k)$ и тъй като $(a,b) = 1$, то $b \mid (l-k)$. Но $0 < l - k < l < b$, т.е. имаме противоречие. Следователно, $r_k \ne r_l$, щом $k \ne l$ и числата $r_1, r_2, \ldots, r_{b-1}$ са в някакъв ред числата $1, 2, \ldots, b-1$. Като сумираме почленно равенствата по-горе, получаваме

$$a(1+2+\ldots+(b-1)) = b(q_1+q_2+\ldots+q_{b-1})+1+2+\ldots+b-1 = bS+1+2+\ldots+b-1,$$

откъдето $S = \dfrac{(a-1)(b-1)}{2}$. □

Задача 1.1.27. *Нека a и b са цели числа. Да се докаже:*

а) $(a,b) = (3a+4b, 8a+11b)$;

б) ако $(a,b) = 1$, то $(13a+36b, 2a+5b) = 1$ или 7;

в) ако $(a,b) = 1$, то $(a \pm b, ab) = 1$;

г) ако $(a,b) = 1$, то $(a+b, a^2+b^2-ab) = 1$ или 3.

Решение. б) Нека $d = (13a+36b, 2a+5b)$. От $d \mid [5(13a+36b) - 36(2a+5b)] = -7a$, $d \mid [2(13a+36b) - 13(2a+5b)] = 7b$ следва, че $d \mid (-7a, 7b) = (7a, 7b) = 7(a,b) = 7$, т.е. $d = 1$ или 7.

г) Тъй като $a^2+b^2-ab = (a+b)^2 - 3ab$, то $d = (a+b, a^2+b^2-ab) = (a+b, 3ab)$. Освен това $(d, ab) = 1$. Наистина от $d \mid (a+b)$ и $(a,b) = 1$ следва, че $(d,a) = (d,b) = 1$

и съгласно Твърдение 1.1.10 е) имаме, че $(d, ab) = 1$. Ето защо от $d \mid 3ab$ получаваме, че $d \mid 3$, т.е. $d = 1$ или 3. □

Задача 1.1.28. *да се докаже, че ако $a > 1$, m и n са естествени числа, то*

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Решение. Нека $n = mq + r$, $0 \leq r < m$. В сила е равенството

$$a^n - 1 = a^{mq}a^r - 1 = a^r(a^{mq} - 1) + a^r - 1 = k(a^m - 1) + a^r - 1,$$

където k е цяло число. Да използваме индукция по m. При $m = 1$ твърдението очевидно е вярно. От горното равенство следва, че $(a^n - 1, a^m - 1) = (a^n - 1, a^r - 1)$ и тъй като $r < m$, по индукционното предположение $(a^n - 1, a^r - 1) = a^{(n,r)} - 1$. Но $(n, r) = (n, m)$, с което твърдението е доказано. □

Задача 1.1.29. *Нека a, b, m и n са естествени числа, за които $(a, b) = 1$, $a > 1$. Да се докаже, че ако $(a^n + b^n) \mid (a^m + b^m)$, то $n \mid m$.*

Задача 1.1.30. *Да се докаже, че ако $n > 2$ е произволно естествено число, то числата $2^n - 1$ и $2^n + 1$ не са едновременно прости.*

Задача 1.1.31. *Да се намерят всички прости числа p, за които:*

а) числата $p + 8$ и $p + 16$ също са прости;

б) числата $p + 14$ и $p + 28$ също са прости;

в) числото $8p^2 + 1$ също е просто;

г) числата $4p^2 + 1$ и $6p^2 + 1$ също са прости.

Решение. г) Непосредствената проверка показва, че $p = 2$ и $p = 3$ не са решения, т.е. $p \geq 5$. Ако $p = 5$, то $4p^2 + 1 = 101$ и $6p^2 + 1 = 151$ са също прости, т.е. $p = 5$ е решение. Ако $p > 5$, ще разгледаме случаите, когато $p = 5k + j$, $j = 1, 2, 3, 4$. Тогава $4p^2 + 1 = 4(5k + j)^2 + 1 = 100k^2 + 40kj + 4j^2 + 1$ и $6p^2 + 1 = 6(5k + j)^2 + 1 = 150k^2 + 60kj + 6j^2 + 1$. При $j = 1$ имаме $5 \mid 4p^2 + 1$, а за $j = 2, 3, 4$ имаме, че $5 \mid 6p^2 + 1$, т.е. не са прости числа. Следователно единственото просто число с търсеното свойство е $p = 5$. □

Отг. $p = 3$ за а), б) и в).

Задача 1.1.32. *Да се докаже, че ако p е просто число, а k е естествено число, за което $1 \leq k \leq p - 1$, то $p \mid \binom{p}{k}$.*

Решение. При даденото условие $(p, k!) = 1$. В частност p не се дели на никое от числата $2, 3, \ldots, k$. От друга страна числото $\binom{p}{k} = \dfrac{p(p-1)\ldots(p-k+1)}{k!}$ е цяло. Така $k! \mid p(p-1)(p-2)\ldots(p-k+1)$ и тъй като $(p, k!) = 1$, то

$$k! \mid (p-1)(p-2)\ldots(p-k+1),$$

откъдето $(p-1)(p-2)\dots(p-k+1) = l.k!$, т.е. $\binom{p}{k} = pl$ за някакво цяло число l. □

Задача 1.1.33. *Да се докаже, че ако p и q са прости числа, по-големи от 3, то числото $p^2 - q^2$ се дели на 24.*

Задача 1.1.34. *Да се докаже, че нечетното число $n > 1$ е просто тогава и само тогава, когато се представя по единствен начин като разлика от квадратите на две цели неотрицателни числа.*

Решение. За всяко нечетно число n е в сила равенството

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2. \tag{1.1.2}$$

Нека n е нечетно просто число и нека $n = a^2 - b^2 = (a-b)(a+b)$, $a > b \geq 0$. Тогава $a - b = 1$, $a + b = n$, откъдето $a = \dfrac{n+1}{2}$, $b = \dfrac{n-1}{2}$, т.е. представянето (1.1.2) е единствено. Обратно, нека n е съставно нечетно число, т.е. $n = ab$, $1 < b \leq a < n$. Тогава равенството

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

е представяне на n като разлика от квадратите на две цели неотрицателни числа, различно от (1.1.2). □

1.2 Сравнения

Нека a и b са цели числа, а n е естествено число, т.е. $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

Дефиниция 1.2.1. *Ще казваме, че a е сравнимо с b по модул n, ако $n \mid (a-b)$. Ще означаваме*

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

В противен случай ще пишем $a \not\equiv b \pmod{n}$. Сравнението $a \equiv b \pmod{n}$ е равносилно с равенство от вида $a = b + nk$ за някое $k \in \mathbb{Z}$. Ясно е, че $a \equiv b \pmod{n}$ тогава и само тогава, когато a и b имат равни остатъци при деление с n. В частност $a \equiv 0 \pmod{n}$ точно когато $n \mid a$. Освен това, ако е в сила сравнението $a \equiv b \pmod{n}$, то $(a, n) = (b, n)$.

В сила са следните свойства на сравненията:

1. За всяко число a е изпълнено $a \equiv a \pmod{n}$ (рефлексивност).
2. Ако $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$ (симетричност).
3. Ако $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$ (транзитивност).
4. Ако $a_1 \equiv b_1 \pmod{n}$ и $a_2 \equiv b_2 \pmod{n}$, то

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n} \quad \text{и} \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

5. Ако $a+b \equiv c \pmod{n}$, то $a \equiv c-b \pmod{n}$.
6. Ако $a \equiv b \pmod{n}$, то $a+c \equiv b+c \pmod{n}$ за всяко $c \in \mathbb{Z}$.
7. Ако $a \equiv b \pmod{n}$, то $ac \equiv bc \pmod{n}$ за всяко $c \in \mathbb{Z}$.
8. Ако $a \equiv b \pmod{n}$, то $a^m \equiv b^m \pmod{n}$ за всяко $m \in \mathbb{N}$.
9. Ако $a \equiv b \pmod{n}$ и $f(x)$ е полином с цели коефициенти, то

$$f(a) \equiv f(b) \pmod{n}.$$

10. Ако $ka \equiv kb \pmod{n}$, то $a \equiv b \pmod{\dfrac{n}{(n,k)}}$. В частност ако $(n,k)=1$, имаме $a \equiv b \pmod{n}$.

Множеството на целите числа $\mathbb{Z}$ се разбива на непресичащи се класове от сравними помежду си числа по модул n, които се наричат *класове остатъци по модул* n. Нека $a \in \mathbb{Z}$ и по Теорема 1.1.3 имаме $a = nk + r$, $0 \leq r < n$. Класът $\overline{a}$ ще се състои от всички цели числа $r + mn$, $m \in \mathbb{Z}$. Ясно е, че числото a принадлежи на класа $\overline{a}$ и ще казваме, че a е (един) представител на класа $\overline{a}$. Очевидно r е друг негов представител, т.е. $\overline{a} = \overline{r}$. Освен това две цели числа a и b принадлежат на един и същи клас $\overline{a}$ тогава и само тогава, когато $a \equiv b \pmod{n}$. Така $\overline{a} = \overline{r} = \{b \in \mathbb{Z} \mid b \equiv r (\mathrm{mod}\ n),\ 0 \leq r < n\}$ и броят n на тези класове е равен на броя от всевъзможните остатъци, получени при деление с модула n.

Множеството от класовете остатъци по модул n ще означаваме с $\mathbb{Z}_n$, т.е.

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

със съответни представители (например) $0, 1, \ldots, n-1$.

Дефиниция 1.2.2. *Пълна система от остатъци по модул n ще наричаме всяка система от n на брой несравними помежду си цели числа.*

Очевидно, $0, 1, \ldots, n-1$ е една такава пълна система остатъци по модул n. Ако $r_0, r_1, \ldots, r_{n-1}$ е пълна система остатъци по модул n и a е цяло число, $(a,n)=1$, то

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{\overline{r_0}, \overline{r_1}, \ldots, \overline{r_{n-1}}\}$$

и числата $ar_0 + b, ar_1 + b, \ldots, ar_{n-1} + b$ също образуват пълна система от остатъци по модул n, за произволно $b \in \mathbb{Z}$.

Множеството $\mathbb{Z}_n$ ще е основен обект на разглеждане във втора глава на това ръководство. Тук ще приложим само един пример за илюстрация на понятията по-горе.

Пример 1.2.3. *Нека $n = 7$. Тогава $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \ldots, \overline{6}\}$, като (например) класът $\overline{3}$ се състои от всички цели числа, които при деление на 7 дават остатък 3. Примери за пълни системи остатъци по модул 7 са:*

$$-3, -2, -1, 0, 1, 2, 3; \quad 21, -13, 16, 10, 32, -2, 13; \quad 13, 16, 19, 22, 25, 28, 31.$$

В частност $\overline{3} = \overline{10} = \overline{31}$. ♢

Дефиниция 1.2.4. *Нека $a \not\equiv 0 \pmod n$. За цялото число x_0 ще казваме, че е решение на сравнението от първа степен с едно неизвестно*

$$ax + b \equiv 0 \pmod n, \tag{1.2.1}$$

когато го удовлетворява, т.е. $ax_0 + b \equiv 0 \pmod n$. При това всеки две решения x_1 и x_2 на (1.2.1), такива, че $x_1 \equiv x_2 \pmod n$ ще приемаме за неразлични. Поточно, ще считаме, че $\overline{x_0}$ е едно решение на сравнението (1.2.1), ако числото x_0 го удовлетворява и ще означаваме това решение $\overline{x_0}$ с $x \equiv x_0 \pmod n$.

Така едно сравнение от вида (1.2.1) ще има толкова решения, колкото е броят на числата от една пълна система остатъци, които го удовлетворяват.

Твърдение 1.2.5. *Нека е дадено сравнението (1.2.1) и $(a, n) = d$.*

а) Ако $d = 1$, сравнението (1.2.1) има точно едно решение.

б) Ако $d > 1$ и $d \nmid b$, сравнението (1.2.1) няма решение.

в) Ако $d > 1$ и $d \mid b$, сравнението (1.2.1) има точно d на брой решения. Те са $x_k = x_0 + k\dfrac{n}{d}$, за $k = 0, 1, \ldots, d-1$, където x_0 е единственото решение на редуцираното на (1.2.1) сравнение $\dfrac{a}{d}x + \dfrac{b}{d} \equiv 0 \pmod{\dfrac{n}{d}}$.

За да решим сравнението (1.2.1) е достатъчно да решим неопределеното уравнение $ax + b = ny$ в цели числа x и y. Решаването на това уравнение може да се извърши с метода на Ойлер, който ще илюстрираме в следващия пример.

Пример 1.2.6. *Да решим следното сравнение $3x + 23 \equiv 0 \pmod{44}$. Тъй като $(3, 44) = 1$ по Твърдение 1.2.5 а) то има точно едно решение. За целта трябва да решим неопределеното уравнение $3x + 23 = 44y$. Изразяваме относно неизвестното с по-малък коефициент и получаваме*

$$x = \frac{44y - 23}{3} = 14y - 7 + \frac{2y - 2}{3}.$$

Тъй като x и y са цели числа, то горното равенство ще е изпълнено само ако числото $\dfrac{2y-2}{3}$ също е цяло, т.е. за някое цяло число z имаме $\dfrac{2y-2}{3} = z$. Последното е еквивалентно на $2y - 2 = 3z$. Отново решаваме спрямо неизвестното с по-малък коефициент и получаваме

$$y = \frac{3z + 2}{2} = z + 1 + \frac{z}{2}.$$

Аналогично, числото $\dfrac{z}{2} = t \in \mathbb{Z}$, т.е. $z = 2t$. Тогава $y = 3t + 1$, откъдето $x = 44t + 7$. Следователно решението на даденото сравнение $3x + 23 \equiv 0 \pmod{44}$ е $x \equiv 7 \pmod{44}$. ♢

Пример 1.2.7. *Да решим сравнението $15x + 103 \equiv 0 \pmod{220}$. Тъй като $(15, 220) = 5(3, 44) = 5$, но $5 \nmid 103$ по Твърдение 1.2.5 б) сравнението няма решение.* ♢

Пример 1.2.8. *Да решим сравнението* $15x+115 \equiv 0 \ (mod\ 220)$. *От* $d = (15, 220) = 5$ *и* $5 \mid 115$ *по Твърдение 1.2.5 в) това сравнение ще има 5 решения. За целта първо го разделяме на* $d = 5$ *и получаваме редуцираното на даденото сравнение* $3x + 23 \equiv 0 \ (mod\ 44)$. *Полученото сравнение е това от Пример 1.2.6 и както показахме там има единствено решение* $x \equiv 7 \ (mod\ 44)$. *Тогава петте решения на сравнението* $15x + 115 \equiv 0 \ (mod\ 220)$ *са* $x_k = x_0 + 44k$, *за* $k = 0, 1, 2, 3, 4$. *Окончателно имаме* $x \equiv 7, 51, 95, 139, 183 \ (mod\ 220)$. ♢

От Твердение 1.2.5 а) следва, че всяко сравнение (1.2.1), за което $(a, n) = 1$ може да се приведе във вида $x \equiv c \pmod{n}$. Тогава ако целите числа a_i и естествените числа n_i, $i = 1, 2, \ldots, k$, са такива че $(a_i, n_i) = 1$, то системата от сравнения

$$\left|\begin{array}{lcl} a_1x + b_1 & \equiv & 0 \pmod{n_1} \\ a_2x + b_2 & \equiv & 0 \pmod{n_2} \\ \ldots\ \ldots & \ldots & \ldots\ \ldots \\ a_kx + b_k & \equiv & 0 \pmod{n_k} \end{array}\right.$$

е еквивалентна на системата

$$\left|\begin{array}{lcl} x & \equiv & c_1 \pmod{n_1} \\ x & \equiv & c_2 \pmod{n_2} \\ \ldots & \ldots & \ldots\ \ldots \\ x & \equiv & c_k \pmod{n_k}. \end{array}\right. \tag{1.2.2}$$

Решаването на системата (1.2.2) е равносилно на намирането на целите числа x, които при деление на n_1, n_2, ..., n_k дават съответно остатъци c_1, c_2, ..., c_n, т.е. на китайската задача за остатъците.

Теорема 1.2.9. ***(Китайска теорема за остатъците)***. *Нека* n_1, n_2, ..., n_k *са две по две взаимно прости естествени числа и* c_1, c_2, ..., c_k *са произволни цели числа. Тогава съществува цяло число* x_0, *което е решение на системата (1.2.2), т.е.* $x_0 \equiv c_i \ (mod\ n_i)$ *за всяко* $i = 1, 2, \ldots, k$. *При това решението* $x \equiv x_0 \ (mod\ n)$, *където* $n = n_1n_2 \ldots n_k$.

Пример 1.2.10. *Да решим следната система от сравнения:*

$$\left|\begin{array}{lcl} x & \equiv & 3 \ (mod\ 7) \\ x & \equiv & 5 \ (mod\ 8) \\ x & \equiv & 7 \ (mod\ 11). \end{array}\right.$$

По Китайската теорема за остатъците системата има решение. От първото сравнение на системата имаме $x = 3 + 7y$. *Заместваме го във второто сравнение и получаваме* $3 + 7y \equiv 5 \ (mod\ 8)$. *Оттук* $y \equiv 6 \ (mod\ 8)$, *т.е.* $y = 6 + 8z$. *Откъдето за* x *ще имаме* $x = 3 + 7y = 3 + 7(6 + 8z) = 45 + 56z$ *и го заместваме в третото сравнение на системата. Получаваме* $45 + 56z \equiv 7 \ (mod\ 11)$, *откъдето намираме* $z \equiv 6 \ (mod\ 11)$, *т.е.* $z = 6+11t$. *Тогава за* x *ще имаме* $x = 45+56z = 45+56(6+11t) = 381 + 616z$, *т.е. решението на системата е* $x \equiv 381 \ (mod\ 616)$. ♢

Задачи

Задача 1.2.11. *Да се съставят по три различни пълни системи от остатъци (съответно) по модул 5 и по модул 15.*

Задача 1.2.12. *Да се намери остатъкът r от делението на числото a на числото b, ако:*

а) $a = 3^{73},\ b = 13.$ *б)* $a = 2^{373},\ b = 7.$

в) $a = 7^{44},\ b = 43.$ *г)* $a = 44^{2n+5},\ b = 5,\ n \in \mathbb{N}.$

Решение. а) Търсим цяло число r, такова че $0 \leq r < 13$ и $a = 3^{73} \equiv r \pmod{13}$. Имаме сравнението $3 \equiv 3 \pmod{13}$. След като го повдигнем на трета степен получаваме $3^3 \equiv 1 \pmod{13}$. Откъдето $3^{72} = (3^3)^{24} \equiv 1 \pmod{13}$ и $3^{73} \equiv 3 \pmod{13}$, т.е. $r = 3$.

г) Търсим цяло число r, такова че $0 \leq r < 5$ и $a = 44^{2n+5} \equiv r \pmod{5}$. Но $44 \equiv 4 \pmod{5}$ и значи $44^2 \equiv 4^2 \equiv 1 \pmod{5}$. Откъдето $44^{2n+5} \equiv 44.(44^2)^{(n+2)} \equiv 44.1 \equiv 4 \pmod{5}$. Следователно $r = 4$. □

Отг. б) $r = 2$; в) $r = 6$.

Задача 1.2.13. *Да се намерят последните две цифри от десетичния запис на числото:*

а) $A = (143^{2013} - 141)^{11}.$ *б)* $B = (207^{19} - 41)^{10}.$

Решение. а) Всъщност се търси остатък от делението на даденото число на 100 или все едно такова цяло число r, че $0 \leq r < 100$ и $A = (143^{2013} - 141)^{11} \equiv r \pmod{100}$.

За да достигнем до A започваме от сравнението $143 \equiv 43 \pmod{100}$.

Повдигаме го на трета степен: $143^3 \equiv 43^3 = 79507 \equiv 7 \pmod{100}$.

Оттук: $143^4 = 143^3.143 \equiv 43.7 = 301 \equiv 1 \pmod{100}$.

Следователно $143^{2012} = (143^4)^{503} \equiv 1 \pmod{100}$ и $143^{2013} \equiv 143 \equiv 43 \pmod{100}$.

Имаме $141 \equiv 41 \pmod{100}$ и като извадим последните две сравнения, получаваме: $143^{2013} - 141 \equiv 43 - 41 \equiv 2 \pmod{100}$. Тогава $A \equiv 2^{11} = 2048 \equiv 48 \pmod{100}$.

Търсените две цифри са 4 (за десетици) и 8 (за единици).

б) Аналогично се показва, че търсените две цифри са 2 и 4. □

Задача 1.2.14. *Да се намерят цифрите x и y от десетичния запис на числото*

а) $A = \overline{3x54y2}$*, ако е известно, че* $24 \mid A$.

б) $B = \overline{4x87y6}$*, ако е известно, че* $56 \mid B$.

Решение. а) Тъй като $24 = 8.3$ и $(8, 3) = 1$, то е достатъчно да намерим цифрите x и y от десетичния запис на числото A, за които $8 \mid A$ и $3 \mid A$.

Едно число по-голямо от 1000 се дели на 8 точно когато последните три цифри от десетичния му запис се делят на 8. За да се дели на 8 числото A, трябва да намерим цифрата y така, че $8 \mid \overline{4y2}$, т.е. $\overline{4y2} \equiv 0 \pmod{8}$. Но $\overline{4y2} = 4.10^2 + y.10 + 2 \equiv$

$2y+2 \equiv 0 \pmod 8$. Лесно се съобразява, че само за цифрите $y = 3$ и $y = 7$ е изпълнено горното сравнение. Така числото $A = A_1 = \overline{3x5432}$ или $A = A_2 = \overline{3x5472}$.

По-нататък числото A ще се дели на 3, ако сумата от цифрите му се дели на 3, т.е. трябва да намерим цифрата x така, че $3 \mid (3 + x + 5 + 4 + y + 2)$, т.е. $x + y + 2 \equiv 0 \pmod 3$. В двата случая имаме съответно $x + 3 + 2 \equiv x + 2 \equiv 0 \pmod 3$ за A_1 или $x + 7 + 2 \equiv x \equiv 0 \pmod 3$ за A_2. Така за A_1 цифрата $x = 1$, $x = 4$ или $x = 7$, а за A_2 цифрата $x = 0$, $x = 3$, $x = 6$ или $x = 9$. Съставете числата от вида A и проверете, че всички се делят на 24.

б) Аналогично на а) се показва, че търсените цифри са: $x = 2$, $y = 3$; $x = 9$, $y = 3$; $x = 6$, $y = 7$. □

Задача 1.2.15. *Да се решат сравненията от първа степен:*

а) $3x + 2 \equiv 0 \ (mod\ 14)$; *б)* $5x + 16 \equiv 0 \ (mod\ 33)$;

в) $5x + 13 \equiv 0 \ (mod\ 30)$; *г)* $237x + 63 \equiv 0 \ (mod\ 47)$;

д) $15x + 20 \equiv 0 \ (mod\ 55)$; *е)* $16x - 28 \equiv 0 \ (mod\ 52)$.

Отг. а) $x \equiv 4 \pmod{14}$; б) $x \equiv 10 \pmod{33}$;
в) няма решение; г) $x \equiv 39 \pmod{47}$;
д) $x \equiv 6, 17, 28, 39, 50 \pmod{55}$;
е) $x \equiv 5, 18, 31, 44 \pmod{52}$;

Задача 1.2.16. *Да се решат системите от сравнения от първа степен:*

а) $\left|\begin{array}{rcl} 5x + 2 & \equiv & 0 \ (mod\ 7) \\ 4x - 6 & \equiv & 0 \ (mod\ 11); \end{array}\right.$ *б)* $\left|\begin{array}{rcl} 2x + 3 & \equiv & 0 \ (mod\ 15) \\ 4x - 7 & \equiv & 0 \ (mod\ 21). \end{array}\right.$

в) $\left|\begin{array}{rcl} 5x & \equiv & 6 \ (mod\ 17) \\ 3x & \equiv & 7 \ (mod\ 13) \\ 26x & \equiv & 17 \ (mod\ 5); \end{array}\right.$ *г)* $\left|\begin{array}{rcl} 4x - 8 & \equiv & 0 \ (mod\ 21) \\ 5x - 6 & \equiv & 0 \ (mod\ 12) \\ 2x + 6 & \equiv & 0 \ (mod\ 15). \end{array}\right.$

Отг. а) $x \equiv 29 \pmod{77}$; б) няма решение;
в) $x \equiv 297 \pmod{1105}$;
г) $x \equiv 128 \pmod{252}$;

Задача 1.2.17. *Да се намери най-малкото естествено число, което при деление на 3, 5, 7, 11 дава съответно остатъци 1, 2, 3, 9.*

Отг. 262.

Задача 1.2.18. *Намерете цифрите x, y и z от десетичния запис на числата $A = \overline{xyz138}$, $B = \overline{x1y3z8}$ и $C = \overline{138xyz}$, ако $7 \mid A, B$ при деление с 11 дава остатък 5 и C при деление с 13 дава остатък 6.*

Отг. $x = 3$, $y = 1$, $z = 3$; $x = 4$, $y = 9$, $z = 5$.

1.3 Функция на Ойлер. Теорема на Ойлер - Ферма

Твърдение 1.3.1. *Ако a и b са цели числа, а p е просто число, то*

$$(a+b)^p \equiv a^p + b^p \ (mod\ p).$$

Доказателство: Като използваме формулата на Нютон и факта, че биномните коефициенти $\binom{p}{k} \equiv 0 \pmod{p}$, за $k = 1, 2 \ldots, p-1$ (Задача 1.1.32), получаваме

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p \\ &\equiv a^p + b^p \pmod{p}.\end{aligned}$$

□

Следствие 1.3.2. *Ако a и b са цели числа, p е просто число и m е естествено число, то*

$$(a+b)^{p^m} \equiv a^{p^m} + b^{p^m} \ (mod\ p).$$

Упътване. Използвайте Твърдение 1.3.1 и индукция по m.

Следствие 1.3.3. *Ако a_1, a_2, ..., a_k ($k \geq 1$ са цели числа, а p е просто число, то*

$$(a_1 + a_2 + \ldots + a_k)^p \equiv {a_1}^p + {a_2}^p + \ldots + {a_k}^p \ (mod\ p).$$

Упътване. Използвайте Твърдение 1.3.1 и индукция по k.

Дефиниция 1.3.4. *Нека n е естествено число. Броят на естествените числа, ненадминаващи n и взаимно прости с n ще наричаме функция на Ойлер и ще означаваме с $\varphi(n)$. Ако $n = 1$, то $\varphi(n) = 1$.*

Очевидно $\varphi(n)$ е естествено число и $1 \leq \varphi(n) \leq n-1$ при $n \geq 1$. Например $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(7) = 6$, $\varphi(24) = 8$;

Твърдение 1.3.5. *а) Ако p е просто число, то $\varphi(p) = p - 1$.*

б) Ако p е просто число и $\alpha \in \mathbb{N}$, то $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.

Твърдение 1.3.6. *Ако $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$, т.е. функцията на Ойлер $\varphi(n)$ е мултипликативна числова функция.*

Доказателство: Да запишем числата $1, 2, \ldots, ab$ в следната таблица

$$\begin{vmatrix} 1 & 2 & \ldots & a \\ a+1 & a+2 & \ldots & 2a \\ \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & \ldots & ba \end{vmatrix},$$

която е с b реда и a стълба. Ще преброим числата в тази таблица, които са взимно прости едновременно с a и с b.

Нека първо забележим, че в кой да е стълб на таблицата всеки две числа са сравними по модул a, а в първия ѝ ред има точно $\varphi(a)$ на брой числа, взаимно прости с a. Така в таблицата има точно $\varphi(a)$ на брой стълба, в които се намират числата взаимно прости с a.

От друга страна, кой да е стълб на таблицата съдържа b на брой числа, които са две по две несравними по модул b. Наистина, ако $ia + k \equiv ja + k \pmod{b}$, $i \neq j$, $0 \leq i < j \leq b-1$, ще имаме $b \mid (j-i)a$. Но $(a,b) = 1$ и значи $b \mid (j-i)$, което е невъзможно, тъй като $0 \neq j - i < b$. Така числата от този стълб дават всевъзможните остатъци при деление на b, т.е. са сравними по модул b с числата $0, 1, \ldots, b-1$, взети в някакъв ред. Следователно точно $\varphi(b)$ от тях са взимно прости с b.

Получихме, че в таблицата има $\varphi(a)$ стълба, състоящи се от числа, взаимно прости с a (и други такива числа в таблицата няма) и във всеки от тези $\varphi(a)$ стълба има по $\varphi(b)$ числа, взаимно прости с b. Следователно, таблицата съдържа точно $\varphi(a)\varphi(b)$ числа, взаимно прости както с a, така и с b. Но едно число е взаимно просто както с a, така и с b, точно когато е взаимно просто с ab, а по дефиницията на функцията на Ойлер в таблицата има $\varphi(ab)$ такива числа. Така $\varphi(ab) = \varphi(a)\varphi(b)$. □

Като използваме Твърдение 1.3.5 б) и неколкократно Твърдение 1.3.6 получаваме следната обща формула за пресмятане на функцията на Ойлер за дадено естествено число.

Твърдение 1.3.7. *Ако $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ е каноничното разлагане на естественото число $n > 1$ в произведение на прости множители, то*

$$\varphi(n) = {p_1}^{\alpha_1 - 1} \ldots {p_k}^{\alpha_k - 1}(p_1 - 1) \ldots (p_k - 1) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Всяка система от $\varphi(n)$ на брой естествени числа, които са несравними по модул n и са взаимно прости с модула n ще наричаме *приведена (редуцирана) система от остатъци по модул n*. Ясно е, че $\varphi(n)$ на брой естествените числа, ненадминаващи n и взаимно прости с n е една такава приведена система от остатъци, която да означим с $r_1, r_2, \ldots, r_{\varphi(n)}$. От Теоремата за деление с остатък лесно се съобразява, че на всяка произволна приведена система от остатъци по модул n можем взаимно еднозначно да съпоставим приведената система от остатъци $r_1, r_2, \ldots, r_{\varphi(n)}$. По-точно от всяка пълна система от остатъци по модул n може да се избере единствена подсистема, която е приведена система от остатъци по модул n.

Пример 1.3.8. *Нека $n = 12$. Тогава $0, 1, \ldots, 11$ и $-5, -4, \ldots, 4, 5$ са пълни системи остатъци по модул 12. Съответните приведени системи от остатъци по модул 12 са: $1, 5, 7, 11$ и $-5, -1, 1, 5$.* ♢

Теорема 1.3.9. ***(Теорема на Ферма)**. Ако a е цяло число и p е просто число, то*

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

Еквивалентно: ако a е цяло число и p е просто число, неделящо a, то

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Да отбележим, че Теоремата на Ферма не може да се "обърне", т.е. от сравнението $a^p \equiv a \pmod{p}$ не следва непременно, че p е просто число. Освен това Теоремата на Ферма е частен случай на следната теорема.

Теорема 1.3.10. ***(Теорема на Ойлер – Ферма)***. *Нека a е цяло число, n е естествено число и $(a, n) = 1$. Тогава*

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

В частност, ако p е просто число и $p \nmid a$, то $a^{p-1} \equiv 1 \ (mod\ p)$.

Нека a е цяло число, $n > 1$ е естествено число и $(a, n) = 1$. Най-малкото естествено число k, за което

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

се нарича *показател на a по модул n*. Казваме още, че *a принадлежи на показател k по модул n*. Да отбележим, че не всяко цяло число a притежава показател по модул n. По-точно, цяло число a има показател по модул n тогава и само тогава, когато $(a, n) = 1$. Казваме, че *a е примитивен корен по модул n*, когато $(a, n) = 1$ и a принадлежи на показател $\varphi(n)$ по модул n.

Твърдение 1.3.11. *Ако $(a, n) = 1$ и a принадлежи на показател k по модул n, то*

$$a^m \equiv 1 \ (mod\ n)$$

тогава и само тогава, когато $k \mid m$ (m е естествено число). В частност $k \mid \varphi(n)$.

Твърдение 1.3.12. *Ако $(a, n) = 1$ и $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ е каноничното разлагане на n, то показателят на a по модул n е равен на НОК на показателите на a по модулите $p_i^{\alpha_i}$, $i = 1, 2, \dots, t$.*

Теорема 1.3.13. ***(Теорема на Уилсън)***. *Нека p е просто число. Тогава*

$$(p-1)! \equiv -1 \ (mod\ p).$$

Еквивалентно: $(p-2)! \equiv 1 \ (mod\ p)$.

Задачи

Задача 1.3.14. *Нека a и b са цели числа, а p е нечетно просто число. Да се докаже, че от $a^p + b^p \equiv 0 \ (mod\ p)$ следва $a^p + b^p \equiv 0 \ (mod\ p^2)$.*

Задача 1.3.15. *Нека a и b са цели числа, p е просто число и m е естествено число. Да се докаже, че от $a \equiv b \ (mod\ p^m)$ следва $a^p \equiv b^p \ (mod\ p^{m+1})$.*

Задача 1.3.16. *Да се пресметне:*

а) $\varphi(1024)$. *б)* $\varphi(360)$. *в)* $\varphi(2013)$. *г)* $\varphi(3360)$.

Решение. г) Тъй като $3360 = 2^5.3.5.7$, по Твърдение 1.3.7 имаме $\varphi(3360) = 3360(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) = 768$. □

Отг. а) 512; б) 96; в) 1200.

Задача 1.3.17. *Да се пресметне:*

а) броя на естествените числа, по-малки от 70455 и взаимно прости с 70455.

б) броя на естествените числа, по-малки от 14091 не взаимно прости с 14091.

Отг. а) 28800; б) 6891.

Задача 1.3.18. *Нека* a *и* b *са естествени числа и* $d = (a, b)$, $m = [a, b]$. *Да се докаже, че*

$$\varphi(ab) = d\varphi(m).$$

Задача 1.3.19. *Нека* n *и* k *са естествени числа. Да се докаже, че* $\varphi(n^k) = n^{k-1}\varphi(n)$.

Задача 1.3.20. *Да се решат уравненията:*

а) $\varphi(n) = 12$. *б)* $\varphi(n) = \frac{n}{2}$. *в)* $\varphi(n) = \frac{2n}{3}$. *г)* $\varphi(n) = \frac{\varphi(3n)}{3}$.

Отг. а) 13, 21, 26, 28, 36, 42; б) $n = 2^k, k \in \mathbb{N}$;
в) $n = 3^k, k \in \mathbb{N}$; г) $n = 3k, k \in \mathbb{N}$.

Задача 1.3.21. *Покажете, че числата* $25, 19, 37, -9$ *образуват приведена система от остатъци по модул 8.*

Задача 1.3.22. *Определете приведените системи от остатъци на съставените от вас пълни системи от остатъци (съответно) по модул 5 и по модул 15 в Задача 1.2.11.*

Задача 1.3.23. *Да се намери остатъкът от делението на числото* A *на* b, *ако:*

а) $A = (2013^{97} + 17^{74})^{37}$ *и* $b = 13$; *б)* $A = (90^{1361} + 84^{122})^{13}$ *и* $b = 11$;

в) $A = (85^{73} + 19^{26})^{12}$ *и* $b = 21$; *г)* $A = (2013^{65} + 47^{1001} + 21^9)^{373}$ *и* $b = 20$.

Решение. а) Тъй като $(2013, 13) = 1$, от Теорема на Ферма имаме

$$2013^{12} \equiv 1 \pmod{13}.$$

От свойствата на сравненията следва, че $2013^{96} \equiv 1 \pmod{13}$, откъдето

$$2013^{97} \equiv 2013 \equiv 11 \pmod{13}.$$

Аналогично, $(17, 13) = 1$ и по Теорема на Ферма имаме

$$17^{12} \equiv 1 \pmod{13}.$$

Тогава $17^{72} \equiv 1 \pmod{13}$, откъдето

$$17^{74} \equiv 17^2 = 289 \equiv 3 \pmod{13}.$$

Имаме $2013^{97} + 17^{74} \equiv 11 + 3 \equiv 1 \pmod{13}$, откъдето

$$A = (2013^{97} + 17^{74})^{37} \equiv 1^{37} \equiv 1 \pmod{13},$$

т.е $r = 1$.

г) Тъй като $(2013, 20) = 1$ и $\varphi(20) = 8$, от Теорема на Ойлер – Ферма имаме

$$2013^{\varphi(20)} = 2013^8 \equiv 1 \pmod{20}.$$

Тогава

$$2013^{65} \equiv 2013 \equiv 13 \pmod{20}.$$

Аналогично, $(47, 20) = 1$ и $(21, 20) = 1$. По Теорема на Ойлер – Ферма имаме

$$47^{\varphi(20)} = 47^8 \equiv 1 \pmod{20} \quad \text{и} \quad 21^{\varphi(20)} = 21^8 \equiv 1 \pmod{20},$$

откъдето получаваме съответно, че са в сила сравненията

$$47^{1001} \equiv 47 \equiv 7 \pmod{20} \quad \text{и} \quad 21^9 \equiv 21 \equiv 1 \pmod{20}.$$

Следователно

$$A = (2013^{65} + 47^{1001} + 21^9)^{373} \equiv (13 + 7 + 1)^{373} \equiv 1^{373} \equiv 1 \pmod{20},$$

т.е $r = 1$. □

Отг. б) $r = 2$; в) $r = 1$.

Задача 1.3.24. *Да се намерят последните две цифри в десетичния запис на числото A, ако:*

а) $A = 173^{43}$ *б)* $A = 1337^{81}$.

Отг. а) 7 и 3; б) 3 и 7.

Задача 1.3.25. *Нека p и q са различни прости числа. Да се докаже, че е изпълнено сравнението*

$$p^{q-1} + q^{p-1} \equiv 1 \ (mod\ pq).$$

Задача 1.3.26. *Да се докаже, че за всяко нечетно просто число p съществуват безбройно много естествени числа n, за които $n.2^n + 1$ се дели на p.*

Задача 1.3.27. *Да се докаже, че ако a принадлежи на показател k по модул n, а b принадлежи на показател l по модул n и $(k, l) = 1$, то ab принадлежи на показател kl по модул n.*

Решение. Нека ab принадлежи на показател m по модул n, т.е.

$$(ab)^m \equiv 1 \pmod{n}.$$

Повдигайки това сравнение на степен l получаваме

$$(a^{lm})(b^{lm}) \equiv 1 \pmod{n},$$

откъдето

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

Съгласно Твърдение 1.3.11 имаме, че k дели lm и тъй като $(k, l) = 1$, то k дели m. Аналогично се показва, че l дели m, така че kl дели m. Тъй като

$$(ab)^{kl} \equiv 1 \pmod{n},$$

то и m дели kl. Следователно $m = kl$. □

Задача 1.3.28. *Да се докаже, че ако $n > 1$ е естествено число и $(n-1)! + 1 \equiv 0 \ (mod\ n)$, то n е просто число, т.е. твърдението от Теоремата на Уилсън е обратимо.*

Решение. Нека $n > 1$ е естествено число, за което е изпълнено сравнението $(n-1)! + 1 \equiv 0 \pmod{n}$. Нека d е естествен делител на n и $d < n$. Тогава d участва като множител в $(n-1)!$, т.е. $d \mid (n-1)!$. По условие имаме, че n дели $[(n-1)! + 1]$, а значи и $d \mid [(n-1)! + 1]$. Така $d \mid (n-1)!$ и $d \mid [(n-1)! + 1]$. Следователно $d \mid 1$, т.е. $d = 1$. Получихме, че n няма естествени делители, различни от 1 и n, така че n е просто число. □

Задача 1.3.29. *Да се докаже, че равенството*

$$(p-1)! + 1 = p^m$$

не е изпълнено за никои естествени числа m и $p > 5$.

Да отбележим, че от Задача 1.3.28 следва, че $p > 5$ е просто число. Освен това при $p = 2, 3, 5$ имаме $1! + 1 = 2^1$, $2! + 1 = 3^1$ и $4! + 1 = 5^2$.

Задача 1.3.30. *Да разгледаме простите числа p със свойството: съществува просто число $q < p$ такова, че p дели $(q-1)! + 1$. Да се докаже, че има безбройно много такива прости числа p.*

Задача 1.3.31. *Нека $p > 1$ е естествено число. Да се докаже, че числата p и $p+2$ са едновременно прости тогава и само тогава, когато е изпълнено сравнението*

$$4[(p-1)! + 1] + p \equiv 0 \ (mod\ p(p+2)).$$

1.4 Други важни функции от Теория на числата

В този параграф ще представим списък с известни функции от Теория на числата и някои техни свойства, необходими за материала по Висша алгебра. Разбира се, свойствата на една такава функция - $\varphi(n)$ разгледахме подробно в предния параграф.

Първата числова функция, която ще разгледаме тук е функцията $[x]$. Нека x е реално число. Най-голямото цяло число, което не надминава x, се нарича *цяла част на* x и се означава с $[x]$ (чете се "скобка x"). Така $[x] \leq x < [x]+1$ и $[x] = x$ само ако x е цяло число. Числото $\{x\} = x - [x]$ се нарича *дробна част на* x; $0 \leq \{x\} < 1$. За всяко реално число x имаме $x = [x] + \{x\}$. В сила са следните свойства:

1. Ако x и y са реални числа и $x \leq y$, то $[x] \leq [y]$.

2. Нека x е реално число. Тогава

$$[-x] = \begin{cases} -[x], & \text{ако } x \text{ е цяло число,} \\ -[x]-1, & \text{ако } x \text{ не е цяло число.} \end{cases}$$

3. Ако x е реално число, а n е цяло число, то $[x+n] = [x] + n$.

4. Ако m и $n > 1$ са цели числа, то частното, получено при делението на m с n е равно на $[\frac{m}{n}]$. В частност, ако m и n са естествени числа, то $[\frac{m}{n}]$ е броят на естествените числа, ненадминаващи m и кратни на n.

5. Ако x е реално число, а n е естествено число, то $[\frac{x}{n}] = [\frac{[x]}{n}]$.

6. За две реални числа x и y са в сила неравенствата

$$[x] + [y] \leq [x+y] \leq [x] + [y] + 1.$$

7. Ако x е реално число, а n е естествено число, то

$$n[x] \leq [nx] \leq n[x] + n - 1.$$

8. Ако p е просто число, а n е естествено число и $n \geq p$, то

$$\binom{n}{p} \equiv [\frac{n}{p}] \pmod{p}.$$

Под *аритметична функция* ще разбираме функция, която е определена за всяко естествено число и не е тъждествено равна на нула. Една аритметична функция $f(n)$ се нарича *мултипликативна*, ако за всеки две естествени числа a и b, за които $(a,b) = 1$, е изпълнено равевнството $f(ab) = f(a)f(b)$. Лесно се съобразява, че за всяка мултипликативна функция имаме $f(1) = 1$. Да напомним, че в предния параграф показахме, че функцията на Ойлер - $\varphi(n)$ е мултипликативна функция.

Броят на различните прости делители на естественото число n ще означаваме с $\nu(n)$, $\nu(1) = 0$. Функцията $\nu(n)$ не е мултипликативна (за a и b, $(a,b) = 1$, е в сила $\nu(mn) = \nu(m) + \nu(n)$), но функцията $2^{\nu(n)}$ е мултипликативна функция.

Друга мултипликативна функция е функцията $\lambda(n)$, определена по следния начин: $\lambda(1) = 1$ и ако $n > 1$, то $\lambda(n) = (-1)^k$, където k е броят на простите делители на естественото число n (броени с техните кратности).

Пример за немултипликативна функция е функцията $\delta(n)$, дефинирана за всяко естествено число n по следния начин:

$$\delta(n) = \begin{cases} 0, & \text{ако } n \text{ не е степен на просто число,} \\ \log p, & \text{ако } n > 1 \text{ е степен на просто число.} \end{cases}$$

С $\tau(n)$ ще означаваме броя на естествените делители на естественото число n. С $\sigma(n)$ ще бележим сумата на всички тези естествени делители на числото n, а с $\pi(n)$ ще означаваме тяхното произведение. Функциите $\tau(n)$ и $\sigma(n)$ са мултипликативни, докато $\pi(n)$ не е мултипликативна функция. Естествено число n се нарича съвършено, ако $\sigma(n) = 2n$.

Нека $f(n)$ е произволна аритметична функция. Функцията $F(n) = \sum_{d|n} f(d)$, където сумирането е по всички естествени делители на числото n, ще наричаме *функция-сума на функцията* $f(n)$. Функцията-сума $F(n)$ на дадена аритметична функция $f(n)$ е мултипликативна тогава и само тогава, когато самата $f(n)$ е мултипликативна.

Нека $n > 1$ е естествено число и $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ е каноничното му разлагане. За така определените по-горе функции са в сила следните равенства:

$$\pi(n) = n^{\frac{1}{2}\tau(n)};$$

$$\tau(n) = \prod_{i=1}^{t}(k_i + 1) = (k_1 + 1)(k_2 + 1)\dots(k_t + 1);$$

$$\sigma(n) = \prod_{i=1}^{t} \frac{{p_i}^{k_i+1} - 1}{p_i - 1} = \frac{{p_1}^{k_1+1} - 1}{p_1 - 1} \frac{{p_2}^{k_2+1} - 1}{p_2 - 1} \dots \frac{{p_t}^{k_t+1} - 1}{p_t - 1};$$

$$\sum_{i=1}^{n} \tau(i) = \tau(1) + \tau(2) + \ldots + \tau(n) = [\frac{n}{1}] + [\frac{n}{2}] + \ldots + [\frac{n}{n}] = \sum_{i=1}^{n} [\frac{n}{i}];$$

$$\sum_{i=1}^{n} \sigma(i) = \sigma(1) + \sigma(2) + \ldots + \sigma(n) = 1.[\frac{n}{1}] + 2.[\frac{n}{2}] + \ldots + n.[\frac{n}{n}] = \sum_{i=1}^{n} i.[\frac{n}{i}];$$

$$F(n) = \prod_{i=1}^{t}(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{k_i}));$$

$$\sum_{d|n} \varphi(d) = n;$$

$$\sum_{d|n} \delta(d) = \log n.$$

Освен това е в сила неравенството $\dfrac{n^2}{2} < \varphi(n)\sigma(n) < n^2$.

Ще завършим този параграф с известната функция на Мьобиус. Тя се означава

с $\mu(n)$ и се дефинира по следния начин:

$$\mu(n) = \begin{cases} 1, & \text{ако } n = 1, \\ 0, & \text{ако } n \text{ се дели на квадрат на цяло число, по-голямо от 1,} \\ (-1)^r, & \text{ако } n \text{ е произведение на } r \text{ различни прости числа.} \end{cases}$$

Функцията на Мьобиус е мултипликативна функция. Нека $n > 1$ е естествено число, $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ е каноничното му разлагане и $f(n)$ е произволна мултипликативна функция. В сила са следните равенства:

$$\sum_{d|n} \mu(d) f(d) = \prod_{i=1}^{t} (1 - f(p_i));$$

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{ако } n = 1, \\ 0, & \text{ако } n > 1; \end{cases}$$

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n};$$

$$\sum_{d|n} \mu(d)\tau(d) = (-1)^t;$$

$$\sum_{d|n} \tau(d)\mu(\frac{n}{d}) = 1;$$

$$\sum_{d|n} \mu(d)\sigma(d) = (-1)^t p_1 p_2 \dots p_t;$$

$$\sum_{d|n} \sigma(d)\mu(\frac{n}{d}) = n;$$

$$\prod_{d|n} d^{\mu(d)} = \begin{cases} 1, & \text{ако } n \text{ не е степен на просто число,} \\ p^{-1}, & \text{ако } n > 1 \text{ е степен на простото число } p. \end{cases}$$

За произволна мултипликативна функция $f(n)$ и съответната за нея функция-сума $F(n)$ е в сила следната формула на Мьобиус за обръщане

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}).$$

Глава 2

Класове остатъци по модул n

Нека n е фиксирано естествено число. Да напомним от първа глава, че множеството на класовете остатъци по модул n означихме с $\mathbb{Z}_n$. По-точно, ако $a \in \mathbb{Z}$ и $a = nk + r$, $0 \leq r < n$, класът с представител a означихме с

$$\overline{a} = \overline{r} = \{b \in \mathbb{Z} \mid b \equiv r (\mathrm{mod}\ n),\ 0 \leq r < n\}.$$

Тогава класовете остатъци по модул n е множеството

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

със съответни представители коя да е пълна система от остатъци по модул n. В тази глава за по-голямо удобство (без ограничение на общността) ще използваме за представител на класа остатъци $\overline{i}$ по модул n съответното цяло число $0 \leq i \leq n-1$.

Да отбележим, че основните числови множества $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ са безкрайни, докато $\mathbb{Z}_n$ е крайно множество с n елемента.

По-надолу ще разгледаме подробно множеството $\mathbb{Z}_n$. Ще въведем операции събиране и умножение на елементите му и ще покажем редица важни свойства на така въведените действия.

2.1 Събиране и умножение в $\mathbb{Z}_n$

В множеството $\mathbb{Z}_n$ въвеждаме операция събиране по следния начин.

Дефиниция 2.1.1. *Нека $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Сума на елементите $\overline{a}$ и $\overline{b}$ наричаме елемента $\overline{a+b} \in \mathbb{Z}_n$, т.е. $\overline{a} + \overline{b} := \overline{a+b}$.*

Твърдение 2.1.2. *Операцията събиране в $\mathbb{Z}_n$ е коректно дефинирана, т.е. не зависи от избора на представители на съответните класове.*

Доказателство. Нека $\overline{a} + \overline{b} = \overline{a+b}$ и да изберем други представители $\overline{a_1}$ и $\overline{b_1}$ съответно на класовете $\overline{a}$ и $\overline{b}$, т.е. $a_1 \equiv a \pmod{n}$ и $b_1 \equiv b \pmod{n}$. Тогава $a_1 + b_1 \equiv a + b \pmod{n}$, т.е. $a_1 + b_1 \in \overline{a+b}$ и значи $\overline{a_1 + b_1} = \overline{a+b}$. □

От Твърдение 2.1.2 следва още, че множеството $\mathbb{Z}_n$ е затворено относно въведената в него операция събиране, т.е. сумата на кои да са два елемента от множеството $\mathbb{Z}_n$ е елемент на множеството $\mathbb{Z}_n$. В сила са следните свойства.

$(1.^+)$ За всеки три елемента $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ е изпълнено $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$.

Свойство $(1.^+)$ показва, че операцията събиране в $\mathbb{Z}_n$ е асоциативна и можем да записваме просто $\overline{a + b + c}$.

$(2.^+)$ За всеки два елемента $\overline{a}, \overline{b} \in \mathbb{Z}_n$ е изпълнено $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

Свойство $(2.^+)$ показва, че операцията събиране в $\mathbb{Z}_n$ е комутативна.

$(3a.^+)$ За всяко $\overline{a} \in \mathbb{Z}_n$ имаме $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$.

Елементът $\overline{0}$ играе роля на неутрален елемент (нулев елемент, нула) относно операцията събиране, т.е. действието на операцията върху него и всеки друг елемент оставя елемента в себе си.

$(3b.^+)$ Елементът $\overline{0}$ е единственият неутрален елемент относно операцията събиране в $\mathbb{Z}_n$.

$(4a.^+)$ За всяко $\overline{a} \in \mathbb{Z}_n$ съществува елемент $\overline{x} \in \mathbb{Z}_n$, за който $\overline{a} + \overline{x} = \overline{x} + \overline{a} = \overline{0}$.

Доказателство. Нека $\overline{a}$ е произволен елемент на $\mathbb{Z}_n$. Тогава елементът $\overline{x_0} = \overline{n - a} \in \mathbb{Z}_n$ изпълнява нужното свойство. Наистина, $\overline{a} + \overline{x_0} = \overline{a} + \overline{n - a} = \overline{a + n - a} = \overline{n} = \overline{0}$. Аналогично $\overline{x_0} + \overline{a} = \overline{n - a} + \overline{a} = \overline{n - a + a} = \overline{n} = \overline{0}$. □

Елементът $x_0 = \overline{n - a} \in \mathbb{Z}_n$ ще означаваме с $-\overline{a}$ и ще казваме, че е противоположен на $\overline{a}$ елемент. При това $-\overline{a} = \overline{-a} = \overline{n - a}$.

$(4b.^+)$ Противоположният $-\overline{a}$ на всеки елемент $\overline{a}$ се определя еднозначно от $\overline{a}$, т.е. противоположният на даден елемент е единствен.

Пример 2.1.3. *В $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ таблицата за събиране има следния вид.*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Противоположният на елемента $\overline{2}$ е елементът $\overline{4}$, т.е. $-\overline{2} = \overline{-2} = \overline{6 - 2} = \overline{4}$. Разбира се $-\overline{4} = \overline{2}$. Елементите $\overline{1}$ и $\overline{5}$ са противоположни един на друг, т.е. $-\overline{1} = \overline{5}$ и $-\overline{5} = \overline{1}$. Елементът $\overline{3}$ съвпада със своя противоположен, т.е. $-\overline{3} = \overline{3}$. ♢

Пример 2.1.4. *В $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \ldots, \overline{6}\}$ таблицата за събиране има следния вид.*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

Освен това $-\overline{1} = \overline{6}$, $-\overline{2} = \overline{5}$, $-\overline{3} = \overline{4}$, $-\overline{4} = \overline{3}$, $-\overline{5} = \overline{2}$ *и* $-\overline{6} = \overline{1}$. ♢

По-нататък в множеството $\mathbb{Z}_n$ може да се въведе и операция умножение по следното правило.

Дефиниция 2.1.5. *Нека* $\overline{a}, \overline{b} \in \mathbb{Z}_n$. *Произведение на елементите* $\overline{a}$ *и* $\overline{b}$ *наричаме елементъ̀т* $\overline{ab} \in \mathbb{Z}_n$, *т.е.* $\overline{a}.\overline{b} := \overline{ab}$.

Твърдение 2.1.6. *Операцията умножение в* $\mathbb{Z}_n$ *е коректно дефинирана, т.е. не зависи от избора на представители на съответните класове.*

Доказателство. Нека $\overline{a}.\overline{b} = \overline{ab}$ и да изберем други представители $\overline{a_1}$ и $\overline{b_1}$ съответно на класовете $\overline{a}$ и $\overline{b}$, т.е. $a_1 \equiv a \pmod n$ и $b_1 \equiv b \pmod n$. Тогава $a_1 b_1 \equiv ab \pmod n$, т.е. $a_1 b_1 \in \overline{ab}$ и значи $\overline{a_1 b_1} = \overline{ab}$. □

От Твърдение 2.1.6 следва още, че множеството $\mathbb{Z}_n$ е затворено относно въведената в него операция умножение, т.е. произведението на кои да са два елемента от множеството $\mathbb{Z}_n$ е елемент на множеството $\mathbb{Z}_n$. Очевидно за всяко $\overline{a} \in \mathbb{Z}_n$ имаме, че $\overline{a}\overline{0} = \overline{0}\overline{a} = \overline{0}$. В сила са следните свойства.

(1.*) За всеки три елемента $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ е изпълнено $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$.

Свойство (1.*) показва, че операцията умножение в $\mathbb{Z}_n$ е асоциативна и можем да записваме просто $\overline{abc}$.

(2.*) За всеки два елемента $\overline{a}, \overline{b} \in \mathbb{Z}_n$ е изпълнено $\overline{a}\overline{b} = \overline{b}\overline{a}$.

Свойство (2.*) показва, че операцията умножение в $\mathbb{Z}_n$ е комутативна.

(3*a*.*) За всяко $\overline{a} \in \mathbb{Z}_n$ имаме $\overline{a}\overline{1} = \overline{1}\overline{a} = \overline{a}$.

Елементът $\overline{1}$ играе роля на неутрален елемент (единичен елемент, единица) относно операцията умножение.

(3*b*.*) Елементът $\overline{1}$ е единственият неутрален елемент относно операцията умножение в $\mathbb{Z}_n$.

Пример 2.1.7. *В* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ *таблицата за умножение има следния вид.*

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Да отбележим, че $\overline{2}.\overline{3} = \overline{0}$ *и* $\overline{3}.\overline{4} = \overline{0}$. *Освен това* $\overline{5}.\overline{5} = \overline{1}$. ♢

Пример 2.1.8. *В* $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \ldots, \overline{6}\}$ *таблицата за умножение има следния вид.*

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Да отбележим, че $\overline{2}.\overline{4} = \overline{1}$, $\overline{3}.\overline{5} = \overline{1}$ *и* $\overline{6}.\overline{6} = \overline{1}$. ♢

Операциите събиране и умножение в $\mathbb{Z}_n$ се съгласуват от следващото свойство, което показва, че в $\mathbb{Z}_n$ са в сила дистрибутивните закони.

($1.^{+*}$) За всеки три елемента $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ са изпълнени

$$(\overline{a} + \overline{b})\overline{c} = \overline{ac} + \overline{bc} \quad \text{и} \quad \overline{a}(\overline{b} + \overline{c}) = \overline{ab} + \overline{ac}.$$

Например, в $\mathbb{Z}_6$ от Примери 2.1.3 и 2.1.7 по Свойство ($1.^{+*}$) следва, че $\overline{3}.\overline{5} + \overline{3}.\overline{3} = \overline{3}(\overline{5} + \overline{3}) = \overline{3}.\overline{2} = \overline{0}$.

Дефиниция 2.1.9. *Нека* $\overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$. *Ако за* $\overline{a}$ *съществува елемент* $\overline{x} \in \mathbb{Z}_n$, *за който* $\overline{a}.\overline{x} = \overline{x}.\overline{a} = \overline{1}$, *ще казваме, че* $\overline{a}$ *е обратим елемент (в противен случай ще казваме, че* $\overline{a}$ *е необратим елемент). Елементът* $\overline{x}$ *ще означаваме с* $\overline{a}^{-1}$ *и ще го наричаме обратен на елемента* $\overline{a}$. *Очевидно елементът* $\overline{x} = \overline{a}^{-1}$ *също е обратим елемент и* $\overline{x}^{-1} = (\overline{a}^{-1})^{-1} = \overline{a}$. *Освен това* $\overline{0}$ *е необратим елемент, а* $\overline{1}^{-1} = \overline{1}$.

Ако $\overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$ е обратим елемент. Обратният $\overline{a}^{-1}$ на $\overline{a}$ елемент се определя еднозначно от $\overline{a}$, т.е. обратният на обратим елемент е единствен.

Твърдение 2.1.10. *Нека* $\overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$. *Елементът* $\overline{a}$ *е обратим тогава и само тогава, когато* $(a, n) = 1$.

Доказателство. Нека първо $(a, n) = 1$. Тогава от тъждеството на Безу (Твърдние 1.1.8) съществуват цели числа u и v, такива че $au + nv = 1$, откъдето в $\mathbb{Z}_n$ е изпълнено равенството $\overline{a}.\overline{u} + \overline{n}.\overline{v} = \overline{1}$. Но $\overline{n} = \overline{0}$, откъдето $\overline{a}.\overline{u} = \overline{1}$ и значи $\overline{a}$ е обратим елемент, като $\overline{a}^{-1} = \overline{u}$ е обратният на $\overline{a}$. Обратно, нека $\overline{a} \in \mathbb{Z}_n$, $\overline{a} \neq \overline{0}$ е обратим елемент и нека $\overline{a}^{-1} = \overline{u} \in \mathbb{Z}_n$ е обратният на $\overline{a}$, т.е. $\overline{1} = \overline{a}.\overline{u}$. Да допуснем, че $(a, n) = d > 1$ и нека $a = a_1 d$, $n = n_1 d$. Тогава $0 < n_1 < n$ и значи $\overline{n_1} \neq \overline{0}$ в $\mathbb{Z}_n$. Сега, като умножим равенството $\overline{1} = \overline{a}.\overline{u}$ с $\overline{n_1}$, получаваме $\overline{n_1} = \overline{n_1}.\overline{au} = \overline{n_1 au} = \overline{n_1 a_1 du} = \overline{n a_1 u} = \overline{n}.\overline{a_1 u} = \overline{0}$, противоречие. □

От дефиницията на функцията на Ойлер и Твърдение 2.1.10 следва, че броят на обратимите в $\mathbb{Z}_n$ елементи е точно $\varphi(n)$. Ако p е просто число, то в $\mathbb{Z}_p$ имаме, че всяко $\overline{a} \neq \overline{0}$ е обратим елемент, тъй като $(a, p) = 1$ за всяко $0 < a \leq p - 1$.

Твърдение 2.1.11. *Нека $\overline{a} \neq \overline{0}$ е необратим елемент в $\mathbb{Z}_n$. Тогава съществува необратим елемент $\overline{b} \in \mathbb{Z}_n$, $\overline{b} \neq \overline{0}$, такъв че $\overline{a}.\overline{b} = \overline{0}$. В общия случай елементът $\overline{b}$ не е единствен.*

Доказателство. Нека $\overline{a} \neq \overline{0}$ е необратим елемент в $\mathbb{Z}_n$, т.е. имаме $0 < a \leq n-1$ и $(a, n) = d > 1$. Нека $a = a_1 d$ и $n = n_1 d$. От една страна имаме $(a_1, n) = 1$ и от Твърдение 2.1.10 следва, че елементът $\overline{a_1} \neq \overline{0}$ е обратим. Нека $(\overline{a_1})^{-1} = \overline{u} \in \mathbb{Z}_n$ е обратният на $\overline{a_1}$, т.е. $\overline{1} = \overline{a_1 u}$. Умножаваме последното равенство с $\overline{d} > \overline{1}$ и получаваме $\overline{d} = \overline{d a_1 u} = \overline{d a_1}\,\overline{u} = \overline{au}$. От друга страна, от $n = n_1 d$ имаме $0 < n_1 < n$ и значи $\overline{n_1} \neq \overline{0}$. Сега умножаваме равенство $\overline{d} = \overline{au}$ с $\overline{n_1}$ и получаваме $\overline{0} = \overline{n} = \overline{n_1 d} = \overline{n_1 au} = \overline{a}.\overline{un_1}$. Тогава за елемента $\overline{b} = \overline{un_1}$ имаме $\overline{a}.\overline{b} = \overline{0}$ и $\overline{b} \neq \overline{0}$. (Ако допуснем, че $\overline{b} = \overline{un_1} = \overline{0}$, то като умножим това равенство с $\overline{a_1}$ обратния на $\overline{u}$ елемент, получаваме $\overline{n_1} = \overline{a_1 u n_1} = \overline{a_1}\,\overline{0} = \overline{0}$, противоречие). □

Елементите, които удовлетворяват Твърдение 2.1.11 се наричат делители на нулата в $\mathbb{Z}_n$.

Пример 2.1.12. *В $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ обратимите елементи са $\overline{1}$ и $\overline{5}$, като $(\overline{5})^{-1} = \overline{5}$. Делители на нулата са $\overline{2}$, $\overline{3}$ и $\overline{4}$, като са в сила равенствата $\overline{2}.\overline{3} = \overline{0}$, $\overline{3}.\overline{4} = \overline{0}$ (виж Пример 2.1.7).* ♢

Пример 2.1.13. *В $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \ldots, \overline{6}\}$ всеки ненулев елемент е обратим, като $(\overline{2})^{-1} = \overline{4}$, $(\overline{3})^{-1} = \overline{5}$, $(\overline{4})^{-1} = \overline{2}$, $(\overline{5})^{-1} = \overline{3}$, $(\overline{6})^{-1} = \overline{6}$ и няма делители на нулата (виж Пример 2.1.8).* ♢

За операциите събиране и умножение в $\mathbb{Z}_n$ са в сила и следните свойства.

($2.^{+*}$) За всеки два елемента $\overline{a}, \overline{b} \in \mathbb{Z}_n$ е изпълнено $(-\overline{a})\overline{b} = \overline{a}(-\overline{b}) = -\overline{ab}$.

($3.^{+*}$) За всеки два елемента $\overline{a}, \overline{b} \in \mathbb{Z}_n$ можем да определим $\overline{a} - \overline{b} = \overline{a} + (-\overline{b}) = \overline{a - b} \in \mathbb{Z}_n$. В този случай операцията ще наричаме изваждане, а елемента $\overline{a - b} = \overline{a} - \overline{b}$ – разлика на $\overline{a}$ и $\overline{b}$.

($4.^{+*}$) За всеки три елемента $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ са изпълнени равенствата $(\overline{a} - \overline{b})\overline{c} = \overline{ac} - \overline{bc}$ и $\overline{c}(\overline{a} - \overline{b}) = \overline{ca} - \overline{cb}$.

2.2 K-кратни и степени в $\mathbb{Z}_n$

Дефиниция 2.2.1. *Сумата на k елемента, равни на $\overline{a}$ ще наричаме k-то кратно на $\overline{a}$ и ще бележим с $k\overline{a}$, като са в сила зависимостите: $k\overline{a} = \overline{ka}$ и $k(-\overline{a}) = -\overline{ka}$. От $n\overline{a} = \overline{na} = \overline{0}$ следва $(n + k)\overline{a} = k\overline{a}$, т.е. достатъчно е да разглеждаме k-кратните на $\overline{a}$ само за $1 \leq k \leq n - 1$.*

Твърдение 2.2.2. *Ако $\overline{a} \neq \overline{0}$ е обратим в $\mathbb{Z}_n$ елемент, то за $1 \leq k \leq n-1$ всички k-кратни на $\overline{a}$ са ненулеви, т.е. за $1 \leq k \leq n-1$ имаме $k\overline{a} \neq \overline{0}$. В частност, ако p е просто число, за всяко $\overline{a} \neq \overline{0}$ и за $1 \leq k \leq p-1$, k-кратните на $\overline{a}$ са ненулеви в $\mathbb{Z}_p$.*

Доказателство. Нека $\overline{a} \neq \overline{0}$ е обратим в $\mathbb{Z}_n$ елемент и допуснем, че за някое k $(1 \leq k \leq n-1)$ имаме $k\overline{a} = \overline{0}$. Умножаваме последното равенство с обратния на

$\overline{a}$ елемент и получаваме $(k\overline{a})\overline{a}^{-1} = \overline{ka}\overline{a}^{-1} = \overline{k}(\overline{a}.\overline{a}^{-1}) = \overline{k} = \overline{0} = \overline{0}\overline{a}^{-1}$, противоречие с $\overline{k} \neq \overline{0}$ от $1 \leq k \leq n-1$. Тъй като в $\mathbb{Z}_p$ (p - просто число) всеки елемент $\overline{a} \neq \overline{0}$ е обратим, то $k\overline{a} \neq \overline{0}$, за всяко $\overline{a} \neq \overline{0}$ и за $1 \leq k \leq p-1$. □

От Твърдение 2.1.11 е ясно, че Твърдение 2.2.2 не е изпълнено за необратимите елементи $\overline{a} \neq \overline{0}$ в $\mathbb{Z}_n$. Например 3-кратното на елемента $\overline{2}$ в $\mathbb{Z}_6$ е $3.\overline{2} = \overline{6} = \overline{0}$.

Твърдение 2.2.3. *Нека $m, k \in \mathbb{N}$ и $\overline{a}, \overline{b} \in \mathbb{Z}_n$. В сила са следните равенства*

$$(m+k)\overline{a} = m\overline{a} + k\overline{a} = \overline{(m+k)a},$$

$$m(\overline{a}+\overline{b}) = m\overline{a} + m\overline{b} = \overline{m(a+b)},$$

$$(mk)\overline{a} = m(k\overline{a}) = k(m\overline{a}) = \overline{(mk)a}.$$

Дефиниция 2.2.4. *Произведението на k елемента, равни на $\overline{a}$ ще наричаме k-та степен на $\overline{a}$ и ще бележим с $\overline{a}^k$, като по дефиниция $\overline{a}^0 = \overline{1}$. За всеки обратим елемент $\overline{a}$ е изпълнено $\overline{a}^{-k} = (\overline{a}^{-1})^k = (\overline{a}^k)^{-1}$.*

Твърдение 2.2.5. *Ако $m, k \in \mathbb{N}$, то са в сила равенствата*

$$\overline{a}^m\overline{a}^k = \overline{a}^{m+k},$$

$$(\overline{a}^m)^k = \overline{a}^{mk} = (\overline{a}^k)^m,$$

$$(\overline{ab})^m = \overline{a}^m\overline{b}^m.$$

Доказателство. Ще докажем само последното равенство. За произволни два елемента $\overline{a}$ и $\overline{b}$ на $\mathbb{Z}_n$ като използваме Свойство (2.*) имаме

$$(\overline{ab})^m = \underbrace{(\overline{ab})(\overline{ab})\dots(\overline{ab})}_{m-\text{пъти}} = \underbrace{(\overline{aa}\dots\overline{a})}_{m-\text{пъти}}\underbrace{(\overline{bb}\dots\overline{b})}_{m-\text{пъти}} = \overline{a}^m\overline{b}^m.$$

В доказателството е съществено, че операцията умножение е комутативна. □

Забележка 2.2.6. *При по-голям нечетен модул n, освен като $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, понякога ще записваме класовете остатъци по модул n и по следния еквивалентен начин: $\mathbb{Z}_n = \{-\overline{\frac{n-1}{2}}, \dots, -\overline{1}, \overline{0}, \overline{1}, \dots, \overline{\frac{n-1}{2}}\}$ или $\mathbb{Z}_n = \{\overline{0}, \pm\overline{1}, \dots, \pm\overline{\frac{n-1}{2}}\}$. Например, $\mathbb{Z}_{13} = \{\overline{0}, \pm\overline{1}, \dots, \pm\overline{6}\}$.*

Забележка 2.2.7. *Повечето от получените свойства за елементите на множеството $\mathbb{Z}_n$, относно въведените в него операции събиране и умножение, са аналози на съответни (известни) свойства на целите числа $\mathbb{Z}$ относно обичайните операции събиране и умножение.*

Задачи

Задача 2.2.8. *Да се съставят таблиците за събиране и умножение съответно в:*

а) $\mathbb{Z}_4$; *б)* $\mathbb{Z}_5$; *в)* $\mathbb{Z}_{12}$; *г)* $\mathbb{Z}_{13}$; *д)* $\mathbb{Z}_{16}$.

Да се покаже за всеки елемент кой е неговият противоположен в съответното $\mathbb{Z}_n$, *за* $n = 4, 5, 12, 13, 16$.

Задача 2.2.9. *Да се намерят обратимите елементи и техните обратни елементи в множеството* $\mathbb{Z}_n$ *за:*

а) $n = 5$; *б)* $n = 8$; *в)* $n = 10$; *г)* $n = 12$; *д)* $n = 13$; *е)* $n = 16$.

Задача 2.2.10. *Да се намерят делителите на нулата в множеството* $\mathbb{Z}_n$ *за:*

а) $n = 5$; *б)* $n = 8$; *в)* $n = 10$; *г)* $n = 12$; *д)* $n = 13$; *е)* $n = 16$.

За така намерените елементи намерете поне един друг елемент, за който да е изпълнено Твердение 2.1.11.

Задача 2.2.11. *Да се пресметнат в* $\mathbb{Z}_{12}$ *следните изрази:*

а) $9(\overline{4} + 2.\overline{5})^5$; *б)* $7(\overline{5} + 4.\overline{11})^{13}$; *в)* $(\overline{11}^3.\overline{7}^{-3})^4$; *г)* $(\overline{11}^{-2} + \overline{4}^4 + \overline{3}^5)^3$.

Отг. а) $\overline{0}$; б) $\overline{7}$; в) $\overline{1}$; г) $\overline{8}$.

Задача 2.2.12. *Нека* p *е просто число. Докажете, че за произволно* $\overline{a} \in \mathbb{Z}_p$ *е в сила тъждеството* $\overline{a}^p = \overline{a}$.

Библиография

[1] Г. Генов, Ст. Миховски, Т. Моллов, *Алгебра*, Университетско издателство "Паисий Хилендарски", Пловдив, 2006.

[2] Ст. Додунеков, К. Чакърян, *Задачи по Теория на числата*, Регалия 6, София, 1999.

[3] К. Дочев, Д. Димитров, В. Чуканов, *Ръководство за упражнения по Висша алгебра*, изд. "Наука и изкуство", София, 1976.

[4] Н. Ненов, *Лекции по Висша алгебра*, публикувани на страницата на катедра Алгебра, 2008.

[5] Пл. Сидеров, К. Чакърян, *Записки по алгебра (групи, пръстени, полиноми)*, Веди, София, 2006.

[6] Пл. Сидеров, К. Чакърян, *Задачи по алгебра (групи, пръстени, полиноми)*, Веди, София, 2006.