Глава 1

Аритметика

1.1 Аксиоми на Пеано. Делимост и деление с остатък.

Спокойно можем да кажем, че естествените числа $\mathbb{N} = \{1, 2, 3, \ldots\}$ съпътстват човечеството от появяването му. Навярно разглеждането им като най-древната и основополагаща математическа система е дало основание на Кроненер да заяви (говорейки за математиката), че Бог е създал естествените числа, а всичко останало е творение на Човека. Естествените числа са възникнали и служат като показател за количеството предмети в дадено множесто. Изказано с математически термини това означава, че естествените числа представят (кардинални числа са на) различните класове равномощни крайни множества.

Независимо, че аксиоматичния подход в математиката датира поне от Евклид, то към формализиране на свойствата на естествените числа се пристъпва чак в 19 век, когато активно започва да се работи за поставяне на цялата математика на аксиоматични основи. Най-популярна, използвана и днес, става аксиоматиката предложена от италианския математик Дж. Пеано в негова книга излязла в 1889 г. Сходна аксиоматика е предложил и Р. Дедекинд в 1888 г.

Аксиоматичното построяване на естествените числа е предмет на курсовете по логика и основи на математиката. Затова без да се стремим към прецизност само ще го скицираме - по-скоро за да информираме читателя за съществуването на такава проблематика, отколкото да я излагаме.

Аксиоматика на Пеано. Съществува поне една система $(\mathbb{N}, S, 1)$ състояща се от множество $\mathbb{N}$, функция S ("съпоставяне на наследник"), дефинирана и приемаща стойности в $\mathbb{N}$, и елемент отбелязван с 1, такива че

Аксиома 1 $1 \in \mathbb{N}$.

Аксиома 2 *За всяко $x \in \mathbb{N}$ съществува еднозначно определен наследник $S(x) \in \mathbb{N}$.*

Аксиома 3 $S(x) \neq 1$, *(т.е. 1 не е наследник на никой елемент).*

Аксиома 4 *За всяко $x, y \in \mathbb{N}$ от $S(x) = S(y)$ следва $x = y$.*

Аксиома 5 *(*Принцип на математическата индукция *) Ако едно подмножество $M \subset \mathbb{N}$ удовлетворява условията:*

(i) $1 \in M$
(ii) *от* $x \in M$ *следва* $S(x) \in M$ *за всяко* x *с това свойство, то* $M \equiv \mathbb{N}$.

Непосредствено от аксиомите следва, че за $x \in \mathbb{N}$ е в сила или $x = 1$ или съществува единствено $y \in \mathbb{N}$, такова че $S(y) = x$.

Така зададена системата на Пеано е еднозначно определена, в смисъл, че всеки две системи $(\mathbb{N}, S, 1)$ и $(\mathbb{N}', S', 1')$ са изоморфни. (Както отбелязахме по-горе тук няма да прецезираме това понятие.)

Показва се, че в $\mathbb{N}$ могат да се дефинират и то еднозначно бинарни операции събиране, $(x, y) \to x + y$, и умножение, $(x, y) \to x \cdot y$, така че за всяко $x, y \in \mathbb{N}$ да са изпълнени свойствата:

P1. $x + 1 = S(x)$.

P2. $x + S(y) = S(x + y)$.

P3. $x \cdot 1 = x$.

P4. $x \cdot S(y) = (x \cdot y) + x$.

Въведените бинарни операции са комутативни, асоциативни и е в сила дистрибутивния закон.

Вместо 1 в аксиоматиката на Пеано може да се постави 0, т.е. да се построи направо съвкупността на неотрицателните цели числа. Тогава P1 и P3 се заместват съответно с равенствата $x + 0 = x$ и $x \cdot 0 = 0$.

Упражнение 1.1.1 *Покажете, че в този случай, ако дефинираме* $1 = S(0)$, *то* $x + 1 = S(x)$ *и* $x \cdot 1 = x$.

В $\mathbb{N}$ се дефинира релация **по-малко (по-голямо)**: “$<$”(“$>$”).

Дефиниция 1.1.1 *Казваме, че* $a < b$, *ако съществува* $u \in \mathbb{N}$, *такова че* $b = a + u$. *Записваме този факт и като* $b > a$. *Със знака* $a \leq b$ *ще означаваме, че е изпълнено* $a < b$ *или* $a = b$.

Твърдение 1.1.2 *Нека* $a, b, c \in \mathbb{N}$. *В сила са:*

1. *За всеки* $a, b \in \mathbb{N}$ *е изпълнено точно едно от отношенията* $a < b$, $a = b$ *или* $a > b$.
2. *от* $a < b$ *и* $b < c$ *следва* $a < c$.
3. *от* $a < b$ *следва* $a + c < b + c$ *за всяко* $\in \mathbb{N}$.
4. *от* $a < b$ *следва* $a \cdot c < b \cdot c$ *за всяко* $\in \mathbb{N}$.

Дефиниция 1.1.3 *Нека* $a > b$. *Единственото* $u \in \mathbb{N}$, *такова че* $a = b + u$ *наричаме разлика на* a *и* b. *Бележим с* $a - b$.

Твърдение 1.1.4 *Отношението “$\leq$” е релация на наредба (т.е. 1)* $x \leq x$; *2)* $x \leq y$ *и* $y \leq x \Rightarrow x = y$; *3)* $x \leq y$ *и* $y \leq z \Rightarrow x \leq z$.*), относно която* $\mathbb{N}$ *е линейно наредено.*

$\mathbb{N}$ се разширявя с добавяне на нула 0, така че $a + 0 = a$ за всяко $a \in \mathbb{N}$, и с добавяне на *отрицателните цели числа*: в разширената съвкупност за всяко $a \in \mathbb{N}$ съществува еднозначно определен елемент $-a$, такъв че $a + (-a) = 0$.

Полученото множество се нарича *пръстен на целите числа* $\mathbb{Z}$ и притежава следните свойства:
За всеки $a, b, c \in \mathbb{Z}$ е изпълнено

1. $a + b = b + a$,
2. $(a + b) + c = a + (b + c)$,
3. $a + 0 = a$,
4. $a + (-a) = 0$,
5. $ab = ba$,
6. $(ab)c = a(bc)$,
7. $a(b + c) = ab + ac$,
8. $1 \cdot a = a$.

Множество с въведени в него две бинарни операции събиране, "+", и умножение "$\cdot$", така че са изпълнени горните свойства се наричат *комутативен пръстен с единица.*

Целите числа притежават и следното свойство: от $ab = 0$ следва $a = 0$ или $b = 0$. Ако това е изпълнено се казва, че пръстенът е без делители на нулата. Комутативен пръстен с 1 и без делители на нулата се нарича *област на цялост.*

В сила е следната важна и много често използвана теорема:

Теорема 1.1.5 *Всяко непразно множество от естествени числа има най-малък елемент.*

Доказателство. Нека $A \subseteq \mathbb{N}$, $A \neq \emptyset$. Да допуснем, че в A няма най-малък елемент и да разгледаме множеството

$$B = \{x \in \mathbb{N} \,|\, x < y, \text{ за всяко } y \in A\}.$$

Ако $x \in A \cap B$, то $x < x$, което е невъзможно. Следователно $A \cap B = \emptyset$, т.е.

$$B \subseteq \overline{A} = \mathbb{N} \setminus A.$$

Използвайки математическа индукция (Аксиома 5) ще докажем, че $B \equiv \mathbb{N}$. Наистина $1 \in B$, защото в противния случай 1 би бил най-малък елемент на A. Нека сега $x \in B$. Тогава за всяко $y \in A$ е в сила $x < y$, откъдето получаваме $S(x) \leq y$. Ако $S(x) \in A$, то $S(x)$ ще бъде най-малък елемент, което противоречи на допускането. Следователно $S(x) < y$ за всяко $y \in A$, откъдето $S(x) \in B$. И така за всяко $x \in B$ следва $S(x) \in B$. В такъв случай принципът на математическата индукция ни дава $B \equiv \mathbb{N}$. Но тогава $A = \emptyset$. Противоречието се дължи на неправилното ни допускане.

Теорема 1.1.6 *За всеки две цели числа a и b, $b \neq 0$, съществуват еднозначно определени $q, r \in \mathbb{Z}$, такива че*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Доказателство. Нека $b > 0$. Да разгледаме множеството

$$M = \{a - bx \,|\, x \in \mathbb{Z},\, a - bx \geq 0\}$$

В него има поне един елемент: например $a - b(-a^2) = a^2b + a \geq 0$. В такъв случай M е непразно множество от цели неотрицателни числа. Съгласно Теорема 1.1.5 в M има минимално число $r \geq 0$. Нека q е стойността на x, при която се получава r, т.е. $r = a - bq$. Ако допуснем, че $r \geq b$, то $0 \leq r - b = a - b(q+1) \in M$, което противоречи на избора на r. Следователно $0 \leq r < b$. С това съществуването е доказано. Остава да покажем единственоста.
Да допуснем, че $a = bq + r = bq_1 + r_1$. Тогава $r - r_1 = b(q_1 - q)$. Но $|r - r_1| < b$. Следователно равенството е възможно само при $q - q_1 = r - r_1 = 0$.
В случая $b < 0$ намираме $a = (-b)q_1 + r$ и полагаме $q := -q_1$.

Теорема 1.1.6 е еквивалентна със следното твърдение

Теорема 1.1.7 *За всеки две цели числа a и $b \neq 0$ съществува $k, l \in \mathbb{Z}$, такива че*

$$kb \leq a < lb, \text{ където } |k - l| = 1.$$

Доказателството на тази еквивалентност предоставяме за упражнение на читателя.

Дефиниция 1.1.8 *Казваме, че $a \in \mathbb{Z}$ **дели** $b \in \mathbb{Z}$, когато съществува $q \in \mathbb{Z}$, такова че $b = aq$, т.е. когато при деление на a се получава остатък нула. Бележим $a|b$.*

Понятието делимост може да се дефинира не само за целите числа, а и в други алгебрични структури, където то запазва почти без изменение свойствата си. Затова ще ги изложим за произволна *област на цялост, т.е. комутативен пръстен с единица и без делители на нулата.* Читател, който не е свикнал да борави с тези алгебрични понятия, може да си мисли, че това е $\mathbb{Z}$ или някое от множествата от всички полиноми с рационални, реални или комплексни коефициенти.

Нека R е област на цялост. Например R съвпада с $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ или $\mathbb{C}[x]$.

Дефиниция 1.1.9 *Един елемент $x \in R$ наричаме **обратим** в R, когато съществува $y \in R$, такъв че $xy = 1$.*

Твърдение 1.1.10 *Съвкупността от обратимите елементи на R е комутативна група относно умножението. (Ще я бележим с R^*.)*

Доказателство. Нека $\alpha, \beta \in R^*$. В такъв случай съществуват α_1, β_1, такива че $\alpha\alpha_1 = \beta\beta_1 = 1$. Очевидно $\alpha_1, \beta_1 \in R^*$. Освен това $(\alpha\beta)(\alpha_1\beta_1) = (\alpha\alpha_1)(\beta\beta_1) = 1$, т.е. $\alpha\beta$ е обратим в R. Комутативния и асоциативния закон са в сила, тъй като са изпълнени в R.

Пример 1.1.1 Ето как изглеждат групите от обратимите елементи на някои добре познати пръстени

1. $\mathbb{Z}^* = \{\pm 1\}$

2. $\mathbb{Q}[x]^* = \mathbb{Q}^*$, $\mathbb{R}[x]^* = \mathbb{R}^*$ и $\mathbb{C}[x]^* = \mathbb{C}^*$.

Дефиниция 1.1.11 *Два елемента $a, b \in R$ наричаме* ***асоциирани****, ако съществува обратим елемент $\epsilon \in R^*$, такъв че $a = \epsilon b$. Бележи се с $a \sim b$.*

Лесно се проверява, (което предоставяме на читателя като упражнение) че е в сила следното твърдение:

Твърдение 1.1.12 *Релацията асоциираност е релация на еквивалентност и разбива R на непресичащи се класове от асоциирани помежду си елементи.*

Целите числа се разбиват на двойки асоциирани числа $\{n, -n\}$. Всеки клас асоциирани полиноми се състои от всички произведения на даден полином с произволна константа, т.е. съвпада с $\{af(x) \,|\, a \in P\}$ $(P = \mathbb{Q}, \mathbb{R}, \mathbb{C})$.

Дефиниция 1.1.13 *Казваме, че $a \in R$* ***дели*** *$b \in R$, когато съществува $q \in R$, такова че $b = aq$. Бележим $a|b$.*

Твърдение 1.1.14 *За всяко $a, b, c \in R$ са в сила:*

(1) *$a|0$, $\epsilon|a$, $a|a\epsilon$ за всяко $\epsilon \in R^*$.*

(2) *$a|b$ влече $a\epsilon|b$, за всяко $\epsilon \in R^*$.*

(3) *$a|b$ и $b|c$ влече $a|c$.*

(4) *$a|b$ и $b|a$ влече $a \sim b$. (В $\mathbb{Z}$ това означава $|a| = |b|$.)*

(5) *$a|b$ влече $a|bc$, за всяко $c \in R$.*

(6) *$a|b$ и $a|c$ влече $a|(b \pm c)$.*

(7) *Ако $c \neq 0$, то $ac|bc$ тогава и само тогава, когато $a|b$.*

(8) *В $\mathbb{Z}$ $a|b$ влече $|b| \geq |a|$.*

> ***Доказателство.*** Всички свойства следват директно от дефинициите. За илюстрация ще докажем (4): Условието дава, че съществуват $q_1, q_2 \in R$, такива че $b = aq_1$ и $a = bq_2$. Следователно $a = aq_1q_2$, т.е. $a(1 - q_1q_2) = 0$. Но R е без делители на нулата, което влече $1 = q_1q_2$. Следователно q_1 и q_2 са обратими. При $R = \mathbb{Z}$ асоциираността означава $a = \pm b$.

1.2 Най-голям общ делител. Алгоритъм на Евклид.

Нека R е област на цялост. Както вече отбелязахме читател, който не е запознат с това алгебрично понятие може да счита, че R съвпада с някое от множествата $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ или $\mathbb{C}[x]$.

Дефиниция 1.2.1 ***Най-голям общ делител*** *(НОД) на $a, b \in R$ наричаме елемент $d \in R$ определен със свойствата:*

1. *$d|a$ и $d|b$,*

2. *ако $d_1|a$ и $d_1|b$, то $d_1|d$.*

Бележим $d = (a, b)$.

Теорема 1.2.2 *Най-големият общ делител е определен с точност до асоциираност.*

> ***Доказателство.*** Ако d и d_1 удовлетворяват условия 1 и 2 от дефиницията, то $d|d_1$ и $d_1|d$. Следователно $d \sim d_1$ съгласно Твърдение 1.1.14. (В случая $R = \mathbb{Z}$, ако d удовлетворява дефиницията, то и $-d$ я удовлетворява.)

Затова в конкретните R се поставя допълнително трето условие, с което НОД се определя еднозначно. Когато $R = \mathbb{Z}$ се изисква НОД да е положителен. Оставяме на читателя да докаже, че с това допълнително условие при целите числа дефиницията е еквивалентна с определението (a, b) да е най-големият измежду всички общи делители на a и b. Когато R е пръстен от полиноми над $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$ допълнителното условието е $d(x)$ да е със старши коефициент равен на 1.

Аналогично можем да дефинираме най-голям общ делител на n елемента. Условията за $d = (a_1, a_2, \dots, a_n)$ изглеждат съответно

1. $d|a_i,\ i = 1, 2, \dots, n$,

2. ако $d_1|a_i$ за всяко $i = 1, \dots, n$, то $d_1|d$.

Теорема 1.2.3 *В сила са следните свойства:*

(1) $(a, ab) \sim a$ *за всяко* $a, b \in R$.

(2) $(a, \epsilon b) = (a, b)$ *за всяко* $\epsilon \in R^\star$.

(3) $(a, b - qa) = (a, b)$ *за всяко* $a, b, q \in R$.

(4) $(a, (b, c)) = ((a, b), c) = (a, b, c)$ *за всяко* $a, b, c \in R$.

(5) $(ac, bc) \sim (a, b)c$ *за всяко* $a, b, c \in R$.

(6) $(a, b) = (a, c) = 1$, *то* $(a, bc) = 1,\ \ a, b, c \in R$.

Доказателство. (1) е очевидно.
(2): Нека $d = (a, b)$ и $d_1 = (a, \epsilon b)$. Тогава $d|a$ и $d|\epsilon b$, откъдето следва $d_1|d$. Но аналогично получаваме и $d|d_1$.
(3): Нека $d = (a, b)$ и $d_1 = (a, b - qa)$. От $d|a$ и $d|b$ следва $d|d_1$. Обратно, $d_1|a$ и $d_1|(b - aq)$ влече $d_1|a$ и $d_1|b$, т.е. $d_1|d$.
(4): Нека $d = (a, b, c)$ и $d_1 = ((a, b), c)$. От $d|a$, $d|b$ и $d|c$ следва $d|(a, b)$ и $d|c$, откъдето $d|d_1$. Обратно, $d_1|(a, b)$ и $d_1|c$, дава $d_1|a$, $d_1|b$ и $d_1|c$, т.е. $d_1|d$.
(5): $(a, b)c \mid ac$ и $(a, b)c \mid bc$, което влече $(a, b)c \mid (ac, bc)$. Следователно $(ac, bc) = c(a, b)t$, т.е. $ac = c(a, b)tu$ и $bc = c(a, b)tv$. Но тогава $a = (a, b)tu$ и $b = (a, b)tv$, т.е. $(a, b)t$ трябва да е делител на a и b. Следавателно $(a, b)t \sim (a, b)$, което влече $t \in R^*$. Но това означава $(ac, bc) \sim c(a, b)$.
(6): $(a, bc) = ((a, ac), bc) = (a, (ac, bc)) = (a, c) = 1$.

Дефиниция 1.2.4 *Казваме, че елементите $a, b \in R$ са **взаимнопрости**, ако $(a, b) = 1$.*

Твърдение 1.2.5 *$d = (a, b)$ тогава и само тогава, когато $a = da_1$, $b = db_1$ и $(a_1, b_1) = 1$.*

Доказателство. Доказателството оставяме за упражнение на читателя.

Нека $A \subset \mathbb{Z}$ е непразно подмножество на $\mathbb{Z}$ със свойството, че за всяко $a, b \in A$ е в сила $a \pm b \in A$. Очевидно $0 \in A$. Подмножество A с това свойство се нарича *адитивна подгрупа* на $\mathbb{Z}$.

Лема 1.2.6 *Ако A е адитивна подгрупа на $\mathbb{Z}$, то съществува $n \in A$, такова че*

$$A = n\mathbb{Z} = \{0, \pm n. \pm 2n, \pm 3n, \ldots\}.$$

Доказателство. Нека A^+ е подмножеството от положителните числа в A. Съгласно Теорема 1.1.5 съществува минимално число $n \in A^+$. Тъй като за всяко $k \in A$ числото $-k$ също е в A, то n е минималното по абсюлютна стойност ненулево число в A. Нека $k \in A$. Да допуснем, че n не дели k, т.е. $k = qn + r$, където $n > r > 0$. Но $r = k - qn \in A$, което води до противоречие с избора на n. Следователно $n \mid k$ за всяко $k \in A$.

Теорема 1.2.7 *Всеки две цели числа a, b имат най-голям общ делител $d = (a, b)$ и съществуват $u, v \in \mathbb{Z}$, такива че $d = ua + vb$.*

Доказателство. Лесно се проверява, че $A = \{ax + by \mid x, y \in \mathbb{Z}\}$ е адитивна подгрупа на $\mathbb{Z}$. Тогава съгласно Лема 1.2.6 съществува $d \in A$, такова че $A = d\mathbb{Z}$. Но тогава d е общ делител на a и b и съществуват $u, v \in \mathbb{Z}$, така че $d = ua + vb$. От последното веднага следва, че е изпълнено и условие 2 на дефиницията.

Следствие 1.2.8 *Нека $d = (a, b)$. Равенството $d = u_1 a + v_1 b$ е в сила тогава и само тогава, когато $u_1 = u - kb/d$, $v_1 = v + ka/d$ за някое $k \in \mathbb{Z}$.*

Забележка 1.1 *Подгрупата A от Лема 1.2.6 притежава и свойството, че произведението на всеки неин елемент с произволно цяло число остава в A. Адитивна подгрупа на един пръстен, която притежава горното свойство се нарича идеал. Ако всички елементи на един идеал са кратни на фиксиран негов елемент (както е за A), то идеалът се нарича главен, а пръстен, в който всеки идеал е главен - пръстен от главни идеали. За такива пръстени е в сила следния по-общ резултат:*

Теорема 1.2.9 *В област от главни идеали R всеки n елемента $a_1, a_2, \dots, a_n$ имат най-голям общ делител d и*

$$d = u_1a_1 + u_2a_2 + \cdots + u_na_n,$$

за подходящи $u_i \in R$.

Твърдение 1.2.10 *Ако $a \mid bc$ и $(a, b) = 1$, то $a \mid c$.*

Доказателство. Съгласно Теорема 1.2.7 съществуват $u, v \in \mathbb{Z}$, такива че $ua + vb = 1$. Следователно $uac + vbc = c$, откъдето и $a \mid bc$ получаваме твърдението.

Твърдение 1.2.11 *Ако $a \mid c,\ b \mid c$ и $(a, b) = 1$, то $ab \mid c$.*

Доказателство. От условието $c = ac_1$. Но $b \mid c$ и $(a, b) = 1$. Тогава предното твърдение ни дава, че $b \mid c_1$. Следователно $c = ab \cdot c_2$.

Лема 1.2.12 *Ако $a = bq + r,\ \ 0 \le r < |b|$, то $(a, b) = (b, r)$.*

Доказателство. Съгласно (3) на Теорема 1.2.3 $(b, r) = (b, a - bq) = (a, b)$.

Алгоритъм на Евклид за намиране на НОД и числата u, v.

Да извършим описаната по-долу поредица от деление с остатък.

$$\begin{array}{ccll}
a & = & bq_1 + r_1, & 0 < r_1 < |b| \\
b & = & r_1q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 & = & r_2q_3 + r_3, & 0 < r_3 < r_2 \\
\dots & \dots & \dots\dots\dots\dots\dots\dots & \dots\dots\dots\dots\dots\dots \\
r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1}q_n, &
\end{array}$$

Тъй като $r_1 > r_2 > \cdots > r_{n-1} > 0$, то съществува номер n, така че $r_n = 0$. Съгласно Лема 1.2.12 е изпълнено $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = r_{n-1}$.
Замествайки $r_1 = a - bq_1$ във второто равенство получаваме $r_2 = (-q_2)a + (1 + q_1q_2)b$. Замествайки r_2 в третото равенство и продължавайки аналогично ще намерим u, v, такива че $r_{n-1} = ua + vb$.

Да положим

$$u_0 = 0, \quad u_1 = 1, \quad u_j \stackrel{\text{def}}{=} u_{j-2} - q_ju_{j-1}$$
$$v_0 = 1, \quad v_1 = -q_1, \quad v_j \stackrel{\text{def}}{=} v_{j-2} - q_jv_{j-1}.$$

Лема 1.2.13 *В сила са следните свойства:*

(1) $r_j = a\,u_j + b\,v_j$;

(2) $u_{j-1}v_j - u_jv_{j-1} = (-1)^j$;

(3) $r_{j-1}u_j - r_ju_{j-1} = (-1)^jb$;

(4) $r_{j-1}v_j - r_jv_{j-1} = (-1)^ja$.

Доказателство. Равенствата могат лесно да се докажат с метода на математическата индукция. Директната проверка показва, че са в сила за $j = 1, 2$. Предполагаме, че твърденията са вярни за стойности $< j$ и ще покажем валидността им за j. Проверката ще извършим само за (2), като оставяме за читателя останалите случаи.

$$\begin{aligned} & u_{j-1}v_j - u_jv_{j-1} \\ & \quad = \quad u_{j-1}\,(v_{j-2} - q_jv_{j-1}) - (u_{j-2} - q_ju_{j-1}))v_{j-1} \\ & \quad = \quad -[u_{j-2}v_{j-1} - u_{j-1}v_{j-2}] = -(-1)^{j-1} = (-1)^j. \end{aligned}$$

При $j = n-1$ получаваме числата u и v с помощта, на които се представя най-големият общ делител $d = ua + vb$.

В теория на числата често се ползва символът $\lfloor x \rfloor$, наричан *цяла част на* x.

Дефиниция 1.2.14 *Функцията* $\lfloor x \rfloor$ *се дефинира за всяко реално* x*, като най-голямото цяло число* $\le x$.
Горната дефиниция може да се изкаже и като : $\lfloor x \rfloor$ е единственото цяло число удовлетворяващо $x - 1 < \lfloor x \rfloor \le x$, или $\lfloor x \rfloor$ е единственото цяло число, такова че $x = \lfloor x \rfloor + \alpha$, $0 \le \alpha < 1$. Ако $a = bq + r,\ 0 \le r < |b|$, то очевидно

$$\left\lfloor \frac{a}{b} \right\rfloor = \begin{cases} q, & \text{при b>0,} \\ q-1, & \text{при b<0.} \end{cases}$$

При така въведеното означение $q_j = [r_{j-2}/r_{j-1}]$.

Реализация на алгоритъма: Да считаме, че $a > b > 0$. Разглеждаме наредените тройки $W_i = (r_i, u_i, v_i)$, които се задават рекурентно с $W_{-1} = (a, 1, 0),\ W_0 = (b, 0, 1)$ и

$$W_{i+1} = W_{i-1} - q_{i+1}W_i, \ \text{ където } q_{i+1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor.$$

Упражнение 1.2.1 *Докажете, че* $(a, b) = r_{i-1},\ u = u_{i-1}$ *и* $v = v_{i-1}$*, където* i *е такова, че* $r_i = 0$.

За удобство при ръчни изчисления пресмятанията можем да записваме в таблица с четири стълба.

a	1	0	**q**
b	0	1	q_1
r_1	u_1	v_1	q_2
r_2	u_2	v_2	q_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-1}	u_{n-1}	v_{n-1}	q_n
0			

Първите три колони на всеки ред представляват текущата стойност на тройката W_i, а последният стълб (от втория ред нататък) съдържа текущото състояние на частното q. Търсените стойности на d, u, v се появявят в реда предхождащ появата на нула в първия стълб. В първата позиция на този ред е НОД (a, b), а втората и третата са съответно u и v.

Алгоритъм 1 *Данни:* a, b *цели числа* $(a > b > 0)$
Резултат: $d = (a, b),\ u,\ v$ цели числа
Променливи: $A = (a_1, a_2, a_3),\ B = (b_1, b_2, b_3)$ и $C = (c_1, c_2, c_3)$ са три масива, които ще се изменят в процеса на изпълнение на програмата; q е цяло число.
$A := (a, 1, 0),\ B := (b, 0, 1),\ C := (1, 0, 0).$
while $c_1 \neq 0$ do
  $q := \lfloor \frac{a_1}{b_1} \rfloor, \quad C := A - qB, \quad A := B, \quad B := C$
else
  $d := a_1,\ u := a_2,\ v := a_3.$

Пример 1.2.1 Да намерим НОД $(29, 25)$ и числата u, v от Теорема 1.2.7. Както отбелязахме пресмятанията записваме в таблица с четири стълба. Първите три колони на всеки три последователни реда представляват текущите стойности на тройките A, B, C, а последният стълб (от втория ред нататък) съдържа текущото състояние на частното q.

29	1	0	q
25	0	1	1
4	1	-1	6
1	-6	7	4
0			

Търсените стойности се появявят в четвъртия ред - реда предхождащ появата на нула в първия стълб. В първата позиция на този ред е НОД $(29, 25) = 1$, а втората и третата са съответно $u = -6$ и $v = 7$. Следователно

$$29 \cdot (-6) + 25 \cdot 7 = 1.$$

Дефиниция 1.2.15 ***Най-малко общо кратно*** *(НОК) на* $a_1, a_2, \ldots, a_n \in R$ *наричаме елемент* $m \in R$ *определен със свойствата:*

1. $a_i \,|\, m,\ i = 1, \ldots, n,$ *и*
2. *ако* $a_i | m_1,\ i = 1, \ldots, n,$ *то* $m \,|\, m_1.$

Бележим $m = [a_1, , a_2, \ldots, a_n].$

Най-малкото общо кратно е определено с точност до асоциираност. В $\mathbb{Z}$ се взема положителното число.

Твърдение 1.2.16 *В сила са следните свойства:*

(1) $[a, b, c] = [[a, b], c]$ *за всяко* $a, b, c \in R.$

(2) $[ac, bc] \sim c[a, b]$ *за всяко* $a, b, c \in R.$

(3) $[a, b] \sim \dfrac{ab}{(a, b)}$ *за всяко ненулево* $a, b \in R.$

(4) $[a, b, c] \sim \dfrac{abc}{(ab, bc, ac)}$ *за всяко ненулево* $a, b, c \in R.$

(5) $([a_1, , a_2, \ldots, a_n]) = (a_1) \cap (a_2) \cap \cdots \cap (a_n)$, *където* (x) *е главния идеал породен от* x.

Доказателство. Оставяме го за упражнение на читателя.

Твърдение 1.2.17 $(a^n - 1\,,\, a^m - 1) = a^d - 1$, *където* $d = (n, m)$.

Доказателство. Нека $n \geq m$. Разсъждаваме индуктивно по m. При $m = 1$ твърдението е вярно: $(a^n - 1\,,\, a - 1) = a - 1$. Да предположим, че е вярно за стойности по-малки от m. Ще докажем за m.
Нека $n = mq + r$. Тогава

$$a^n - 1 = a^{mq}a^r - 1 = (a^{mq} - 1)a^r + a^r - 1 = (a^m - 1)A + (a^r - 1).$$

Съгласно Лема 1.2.12 и индукционното допускане

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

Но $(m, r) = (n, m) = d$, с което доказателството е завършено.

Линейни диофантови уравнения.

Дефиниция 1.2.18 *Линейно диофантово уравнение се нарича линейно уравнение с цели коефициенти*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \quad a_i, b \in \mathbb{Z}, \tag{1.1}$$

чиито решение търсим в цели числа.

Теорема 1.2.19 *Линейното диофантово уравнение (1.1) има решение в цели числа тогава и само тогава, когато най-големият общ делител* $(a_1, a_2, \ldots, a_n)$ *дели* b.

Доказателство. Необходимостта е очевидна - всеки общ делител на коефициентите трябва да дели свободния член b. Обратно, нека $d = (a_1, a_2, \ldots, a_n)$ дели b. Съгласно Теорема 1.2.9 съществуват $u_1, \ldots, u_n \in \mathbb{Z}$, такива че

$$d = u_1a_1 + u_2a_2 + \cdots + u_na_n.$$

Умножавайки по b/d получаваме, че

$$\left(\frac{u_1b}{d}, \frac{u_2b}{d}, \ldots, \frac{u_nb}{d}\right)$$

е решение.

Теорема 1.2.20 *Ако линейното диофантово уравнение*

$$ax + by = c$$

има поне едно решение (x_0, y_0) *в цели числа, то всички решения се получават по формулата*

$$\begin{aligned} x &= x_0 + \tfrac{b}{(a,b)}t \\ y &= y_0 - \tfrac{a}{(a,b)}t, \end{aligned} \tag{1.2}$$

където $t \in \mathbb{Z}$.

Доказателство. Директната проверка показва, че така зададено (x, y) е решение. Ако (x_1, y_1) и (x_2, y_2) са две решения, то разликата им удовлетворява $ax + by = 0$, откъдето се получават и горните формули.

Пример 1.2.2 Да решим системата линейни диофантови уравнения

$$\left| \begin{array}{ll} 2x + 5y - 11z & = 1 \\ x - 12y + 7z & = 2 \end{array} \right.$$

Изключвайки x получаваме система еквивалентната на дадената:

$$\left| \begin{array}{ll} x & = 12y - 7z + 2 \\ 29y - 25z & = -3 \end{array} \right.$$

Следвайки горната теорема решаваме второто уравнение в цели числа. Съгласно Пример 1.2.1 НОД $(29, 25) = 1$ и $29 \cdot (-6) + 25 \cdot 7 = 1$, откъдето

$$29 \cdot (-6) \cdot (-3) + 25 \cdot 7 \cdot (-3) = -3.$$

Следователно $y = 18 - 25t,\ z = 21 - 29t,\quad t = 0, \pm 1, \pm 2, \dots$. Замествайки полученото в първото уравнение получаваме x. И така

$$\begin{array}{ll} x & = 71 - 97t \\ y & = 18 - 25t \\ z & = 21 - 29t \end{array}, \qquad t = 0, \pm 1, \pm 2, \dots .$$

1.3 Прости числа. Основна теорема на аритметиката.

Дефиниция 1.3.1 *Цялото число p се нарича* ***просто****, ако $p \neq 0, \pm 1$ и се дели само на ± 1 и $\pm p$.*

Тъй като p е просто тогава и само тогава, когато и $-p$ е просто, то много често когато се говори за прости числа се разбира съвкупността от положителните прости числа.

Твърдение 1.3.2 *Цялото число p е просто тогава и само тогава, когато за всяко a, b, за които $p \mid ab$ следва $p|a$ или $p|b$.*

Доказателство. *Необходимост.* Нека p е просто число и да предположим, че p не дели a. Тогава $(a, p) = 1$ и съгласно Теорема 1.2.7 съществуват $u, v \in \mathbb{Z}$, така че $ua + vp = 1$. Умножавайки с b получаваме $b = uab + vbp$, откъдето следва $p|b$.
Достатъчност. Нека p притежава свойството, че за всяко a, b, за които $p \mid ab$ следва $p|a$ или $p|b$. Нека $p = ab$. Тогава $p \mid ab$ и следователно $p|a$ или $p|b$. Но това влече $a, b = \pm 1,\ \pm p$.

Твърдение 1.3.2 позволява да се даде еквивалентна дефиниция на просто число. В действителност тя се взема за дефиниция на алгебричното понятие прост елемент, а първата дефиниция за определение на неразложим елемент.

Нека R е област на цялост.

Дефиниция 1.3.3 *Елементът $q \in R$ наричаме **неразложим** в R, ако $q \neq 0$, не е обратим (т.е. $q \not\sim 1$) и от $q = ab$ следва $a \sim 1$ или $b \sim 1$. Ако последното не е изпълнено казваме, че q е разложим.*

Дефиниция 1.3.4 *Елементът $p \in R$ се нарича **прост** в R, когато $p \neq 0$, не е обратим и за всяко a, b, за които $p \,|\, ab$ следва $p|a$ или $p|b$.*

В $\mathbb{Z}$ понятията прост и неразложим елемент съвпадат. Същото остава в сила и за $\mathbb{Q}[x]$, $\mathbb{R}[x]$ и $\mathbb{C}[x]$. Нещо повече, вярна е следната теорема:

Теорема 1.3.5 *В област на цялост R, в която всеки два елемента имат най-голям общ делител, понятията прост и неразложим елемент съвпадат.*

Доказателство. Нека p е прост елемент и $p = ab$. Тогава $p \mid ab$, което влече $p \mid a$ или $p \mid b$. Нека $p \mid a$. Но $a|p$ също. Следователно $p \sim a$ и $b \in R^*$.
Обратно, нека q е неразложим и $q \mid ab$. Ако $q \nmid a$, то $(q, a) = 1$. Но тогава съгласно (5) на Теорема 1.2.3 $(qb, ab) \sim b$, което влече $q \mid b$.

Лема 1.3.6 *Всяко цяло число различно от 0 и ± 1 е или просто число или има прост делител.*

Доказателство. Без ограничение на общност можем да предполагаме, че $a > 1$. Да предположим, че a не е просто. Нека $a = a_1 b_1$. Ако някое от множителите е прост, то твърдението е вярно. Да предположим, че това не е изпълнено и нека $a_1 = a_2 b_2$. Ако никое от a_2 и b_2 не е просто число продължаваме аналогично. Получаваме строго намаляваща редица от естествени числа:

$$a > a_1 > a_2 > \cdots, \quad \text{като } a_{i-1} \,|\, a_i.$$

Но всяко множество от естествени числа има минимален елемент, т.е. съществува a_n, което не се разлага и следователно е просто число. От конструкцията на редицата е ясно, че a_n е делител на a.

Доказаната лема е частен случай на следното твърдение:

Лема 1.3.7 *В област на главни идеали всеки ненулев и необратим елемент има неразложим делител.*

Теорема 1.3.8 ***(Основна теорема на аритметиката)*** *В област от главни идеали всеки ненулев и необратим елемент се разлага в произведение на неразложими множители и това разлагане е единствено с точност до наредба и асоциираност.*

Доказателство. Нека R е област от главни идеали и $a \in R$, $a \neq 0$, е необратим. Съгласно Лема 1.3.7, a или е неразложим или $a = q_1 a_1$, където q_1 е неразложим елемент. Ако $a_1 \sim 1$ или неразложим също, разлагането е получено. В противния случай съществува q_2 неразложим, такъв че $a_1 = q_2 a_2$. Продължавайки получаваме редица

$$a, a_1, a_2, \cdots, \quad \text{като } a_{i-1} \,|\, a_i.$$

Тази редица не може да е безкрайна (в $\mathbb{Z}$ вече го видяхме, а в общия случай също не се обосновава трудно). И така $a = q_1 q_2 \cdots q_n$.
Да предположим, че $a = q_1 q_2 \cdots q_n = p_1 p_2 \cdots p_m$, където q_i и p_j са неразложими елементи. Но в област от главни идеали те се явяват и прости. Следователно q_1 дели някое p_j, например p_1 Това означава, че $q_1 = \epsilon_1 p_1$. Следователно $q_2 \cdots q_n = \epsilon_1 p_2 \cdots p_m$. Продължавайки разсъжденията получаваме $q_i \sim p_i$ и $n = m$.

Следствие 1.3.9 *За всяко цяло число a има и то единствено с точност до наредба представяне*

$$a = \epsilon p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n},$$

където $\epsilon = \pm 1$, p_i са различни прости числа, а k_i естествени числа.

Следствие 1.3.10 *За всеки полином $f(x)$ с коефициенти от полето $\mathbb{F}$ (например $\mathbb{F} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) има и то единствено с точност до наредба представяне*

$$f(x) = a p_1^{k_1}(x) p_2^{k_2}(x) \cdots p_n^{k_n}(x),$$

където $a \in \mathbb{F}$, $p_i(x)$ са различни неразложими над $\mathbb{F}$ полиноми, а k_i - естествени числа.

Следващото твърдение е непосредствено следствие от дефинициите и основната теорема. Доказателството предоставяме на читателя.

Твърдение 1.3.11 *Нека $a = \epsilon_1 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $\alpha_i \geq 0$ и $b = \epsilon_2 p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, $\beta_j \geq 0$, където $\{p_1, p_2, \ldots, p_n\}$ е множеството от всички различни прости числа, които са делители на поне едно от числата a и b. Тогава*

$$(a, b) = \prod_{i=1}^{n} p_i^{\min(\alpha_1, \beta_i)} \qquad [\,a, b\,] = \prod_{i=1}^{n} p_i^{\max(\alpha_1, \beta_i)}.$$

Теорема 1.3.12 *Всяка съставно цяло число n има поне един прост делител ненадминаващ $\sqrt{n}$.*

Доказателство. Да допуснем, че всички прости множители p_i (има поне два) са $> \sqrt{n}$. Тогава $n \geq p_1 p_2 > n$, което е невъзможно.

Следствие 1.3.13 *Ако n не се дели на никое просто число $\leq \sqrt{n}$, то n е просто число.*

Решето на Ератостен. Под това име е известен един елементарен метод за намиране на всички прости числа ненадминаващи дадено n. Свързва се с древногръцкия математик Ератостен (около 200 години преди н.е.) За съжаление той не е пригоден за големи числа. Методът е следния:
Всички естествени числа $\leq n$ се записват последователно (най-често в таблица, например с размери $(\lfloor n/10 \rfloor + 1) \times 10$). Започвайки от 2 се задрасква всяко четно число (т.е. числата през едно) без самото 2. След това се взема първото незадраскано число (в случая 3) и се задраскват всички негови кратни (т.е. през две) без самото число, от което се започва. Тази процедура продължава докато се стигне число $\geq \sqrt{n}$. Съгласно горната теорема всички незадраскани по-големи числа трябва да са прости.
Вместо да се записват числата до n таблицата може да се запълни с единици, които при "задраскване" да се обръщат в нула. Простите числа са номерата на позициите, в които има 1. В табличния запис те се изчисляват лесно. Освен това могат да се запишат само нечетните числа както е направено в таблицата по-долу (с размери $(\lfloor 159/16 \rfloor + 1) \times 8$). В този случай като стигнем незадраскано число m пак се задраска всяко m-то след него.

	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63
65	67	69	71	73	75	77	79
81	83	85	87	89	91	93	95
97	99	101	103	105	107	109	111
113	115	117	119	121	123	125	127
129	131	133	135	137	139	141	143
145	147	149	151	153	155	157	159

1.4 Бройни системи. Сложност на аритметичните операции.

Теорема 1.4.1 *Нека $g > 1$ е естествено число. Всяко естествено число a се представя и то по единствен начин във вида:*

$$a = a_{k-1}g^{k-1} + a_{k-2}g^{k-2} + \cdots + a_1 g + a_0, \ \ 0 \leq a_i \leq g - 1 \tag{1.3}$$

Доказателство. Провеждаме индукция по a. При $a = 1$ твърдението очевидно е вярно. Да предположим, че твърдението е вярно за естествени числа $< a$. Ще го докажем и за a. Както знаем съществуват цели неотрицателни числа n и r : $0 \leq r \leq g - 1$, такива че $a = ng + r$. Но $n < a$. Съгласно индукционното допускане, n се представя по единствен начин във вида (1.3):

$$n = n_{k-1}g^{k-1} + n_{k-2}g^{k-2} + \cdots + n_1 g + n_0,$$

откъдето получаваме

$$a = n_{k-1}g^{k} + n_{k-2}g^{k-1} + \cdots + n_1 g^2 + n_0 g + r.$$

Представянето (1.3) бележим съкратено с $a = (a_{k-1}a_{k-2}\dots a_0)_g$ и го наричаме *представяне на n в бройна система с основа g (g-ична бройна система).* Числото k се нарича *дължина* на a в g-ична бройна система (бележим $\mathrm{length}_g(a) = k$) и казваме, че a е *k-цифрено* g-ично число.

Твърдение 1.4.2 $\mathrm{length}_g(a) = k$ *тогава и само тогава, когато*

$$g^{k-1} \le a < g^k \tag{1.4}$$

и е в сила

$$\mathrm{length}_g(a) = 1 + \lfloor \log_g a \rfloor = 1 + \left\lfloor \frac{\ln a}{\ln g} \right\rfloor . \tag{1.5}$$

Доказателство. Лявото неравенство е очевидно, а дясното следва от

$$a \le \sum_{i=0}^{k-1} (g-1)g^i = g^k - 1.$$

Логаритмувайки (1.4) получаваме и равенството за k.

Представянето (1.3) по естествен начин задава и алгоритмите за запис на едно число n от една бройна система към друга.

Алгоритъм 2 *(към основа g):*
Данни: n, g *цели числа*
Резултат: a_i *цели числа*
Променливи: t, q, i *цели числа*
$i := 0,\ t := n$
while $t > 0$ *do*
$q := \lfloor \frac{t}{g} \rfloor,\ a_i := t - qg,\ i := i + 1,\ t := q$
else
print $a_{i-1}a_{i-2}\dots a_0$

Алгоритъм 3 *(от основа g):*
Данни: g *цяло число,* a_i*,* $i = 0, \dots, k$*, цели числа задаващи* $(a_k a_{k-1}\dots a_0)_g$ *(*a_0 *е младшия разряд)*
Резултат: n *цяло число в десетична бройна система*
Променливи: t, i *цели числа*
$i := k - 1,\ t := a_k;$
while $i \ge 0$ *do*
$t := tg + a_i,\ i := i - 1;$
$n := t,$ *print* $n.$

Означения о-голямо - $O(\cdot)$, и о-малко - $o(\cdot)$.

Дефиниция 1.4.3 *Нека $f(n)$ и $g(n)$ са две функции:* $\mathbb{N} \to \mathbb{R}$. *Казваме, че*

$$f = O(g),$$

когато съществуват положителна константа $c \in \mathbb{R}$ и $n_0 \in \mathbb{N}$, такива че за всяко $n \ge n_0$ е изпълнено

$$|f(n)| \le c|g(n)|.$$

Означението о-голямо показва, че функцията $f(n)$ асимптотически се "доминира с точност до константа" от $g(n)$. Ясно е, че $f = O(g)$ и $g = O(f)$ тогава и само тогава, когато съществуват константи $c_1 > 0$ и $c_2 > 0$, такива че за достатъчно големи n

$$c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|.$$

В този случай двете функции имат "еднакво" асимптотическо поведение и бележим

$$f = \Theta(g).$$

В частност горното е изпълнено, когато $\lim_{n\to\infty} \frac{f(n)}{g(n)} = const > 0$. Случаят, когато тази константа е 1 често се отбелязва с $f \approx g$.

Пример 1.4.1 $\mathrm{length}_g(n) = O(\log_g) = O(\ln n)$, тъй като броят на цифрите при записа на n в различни бройни системи се отличава само на константа.

Изобщо, поради факта, че логаритмите при различни основи се различават с константа, оценките в термините на о-голямо се дават с натуралния логаритъм ln или с логаритъм $\log_2$ при основа 2. За краткост ще означаваме двоичния логаритъм само с $\log$.

Пример 1.4.2 $\ln n = O(n^\epsilon)$, за всяко $\epsilon > 0$, тъй като $\lim_{n\to\infty} \frac{\ln n}{n^\epsilon} = 0$, т.е. $\ln n < n^\epsilon$.

Дефиниция 1.4.4 *Нека $f(n)$ и $g(n)$ са две функции: $\mathbb{N} \to \mathbb{R}$. Казваме, че*

$$f = o(g),$$

когато е изпълнено

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0,$$

т.е. когато $|f(n)| \leq c|g(n)|$ за всяко $c > 0$, колкото и малко да е то.

Съгласно тази дефиниция можем да напишем и $\ln n = o(n^\epsilon)$.

Сега да оценим броя на цифрите при сума и произведение на две числа. Нека $a = (a_{k-1}a_{k-2}\dots a_0)_g$ и $b = (b_{l-1}b_{l-2}\dots b_0)_g$ са съответно k и l цифрени g-ични числа, $k \geq l$. Тъй като $a_i + b_i < 2g$, то $\mathrm{length}_g(a+b) = k$ или $k+1$. Следователно можем да запишем, че

$$\mathrm{length}_g(a+b) = O(\max(k, l)).$$

От неравенствата (1.4) заключаваме, че

$$\mathrm{length}_g(ab) = O(k+l)).$$

Твърдение 1.4.5 $\mathrm{length}(n!) = \Theta(n \ln n)$.

Доказателство. $n!$ е произведение на n числа с дължина ненадминаваща $\operatorname{length}(n)$. Следователно

$$\operatorname{length}(n!) \le n \cdot \operatorname{length}(n) = O(n \ln n).$$

От друга страна нека $m\ :\ 2^{m-1} \le n < 2^m$, т.е. $m = \lfloor \log n \rfloor + 1$. Тогава $2^{m-2} \le n/2 < 2^{m-1}$, откъдето получаваме, че за $k > n/2$

$$\operatorname{length}(k) \ge m - 1 \ge \log n - 2.$$

Следователно

$$\operatorname{length}(n!) > \frac{n}{2}(\log n - 2).$$

Но за всяко $0 < c < 1$ при достатъчно голямо n е в сила

$$\ln n > \frac{2 \ln 2}{1 - c},$$

откъдето $\ln n - 2 \ln 2 > c \ln n$. Следователно

$$\frac{n}{2}(\log n - 2) = \frac{n}{2}\left(\frac{\ln n}{\ln 2} - 2\right) > \frac{c}{2 \ln 2} n \ln n,$$

откъдето получаваме и необходимата ни оценка отдолу

$$\operatorname{length}(n!) > \frac{c}{2 \ln 2} n \ln n.$$

При събиране на две числа a и b, съответно с дължини k и l бита (цифри) трябва да се извършат $\max\{k, l\}$ "елементарни събирания" $a_i + b_i$ и най-много още толкова събирания поради "добавяне към по-високия разряд". В такъв случай общия брой такива събирания е $\le 2 \max(k, l)$. Следователно необходимия брой елементарни операции, т.е. сложноста на събирането е

$$O(\max(\ln a, \ln b)).$$

Ако числата са записани в двоична позиционна система, то елементарните операции са точно побитови операции. В общия случай $a_i + b_i$ отговаря на събиране на две двоични числа от $\le 1 + \lfloor \log g \rfloor$ бита, т.е. изисква $\le 2 + 2\lfloor \log g \rfloor$ битови операции. Но тъй като това е константа, горната оценка остава в сила.

Оттук нататък при оценките за сложност ще предполагаме, че числата са дадени в двоичен запис не само защото така се съхраняват и обработват в компютрите, но и поради гореказаното за влиянието на бройната система върху сложноста.

Нека $k \ge l$. Ако изпълним умножението по стандартната процедура ще са ни необходими lk по битови умножения и събиране на най-много l числа от по $k + l - 1$ бита. Следователно броят на елементарните операции е $O(kl)$, т.е. може да напишем, че сложността на умножението е

$$O(\ln a \cdot \ln b).$$

Нека x, y са две числа от по $n = 2m$ бита. При стандартната процедура ще са необходими $O(n^2)$ операции. В 1982 Карацуба предлага метод за умножение, който изисква по-малко операции. Можем да намерим a, b, c, d от по m бита, така че

$$x = a2^m + b, \qquad y = c2^m + d.$$

Умножавайки ги получаваме

$$xy = v2^n + (u - v - w)2^m + w,$$

където

$$u = (a+b)(c+d),\ v = ac,\ w = bd.$$

Тогава за броя на операциите $M(n)$ имаме

$$M(n) = \begin{cases} k, & \text{m=1}, \\ 3M(m) + kn, & \text{m>1}, \end{cases}$$

където k е константа.
Ако $n \leq 2^l$ и l е минималното естествено число с това свойство, то прилагайки горната оценка за $2^l, 2^{l-1}, \ldots, 2$ получаваме

$$M(2^l) = O(3^l).$$

Но тъй като $l/(l-1) \leq 2$ и клони към 1, когато l расте, то за всяка константа $1 < c < 2$ за достатъчно голямо n е изпълнено $l < c \cdot \log n$, откъдето $3^l < n^{c \cdot \log 3}$. Следователно за достатъчно голямо n

$$M(n) = O(n^\alpha),$$

където $\alpha = c \cdot \log 3 \approx c \cdot 1,585 < 2$, т.е. по-добра е от дадената горе.
Методът може да се прецезира като множителите се разбиват на повече от две части (все едно се представят в бройна система с основа 2^k). Това води до оценка

$$M(n) = O(n^{1+\varepsilon}),$$

където $1 > \varepsilon > 0$.

Най-малко операции изисква (от известните) методът за умножение чрез бързо преобразуване на Фурие. При него

$$M(n) = O(\ln n \cdot \ln(\ln n)).$$

Сега да разгледаме делението $a = bq + r$, където a и b са числа с дължина, съответно k и l бита, $k \geq l$. За осъществяването му са необходими $k - l + 1$ изваждания на l-битови числа. Следователно сложността е $O(l(k - l + 1))$, т.е. можем да напишем, че сложността е

$$O(\ln a \cdot \ln b).$$

Получените оценки са събрани в Таблица 1.1.

операция	сложност
$a \pm b$	$O(max(\ln a, \ln b))$
$a \cdot b$	$O(\ln a \ln b))$
$a = bq + r$	$O(\ln a \ln b)$

Таблица 1.1.

Упражнение 1.4.1 *Покажете, че за броя на операциите при алгоритъма на Евклид за НОД е в сила оценката* $O(\ln a \cdot \ln b)$.

1.5 Допълнителни задачи към Глава 1.

Задача 1.1 *Докажете, че ако* $2^n + 1$ *е просто число, то* $n = 2^k$, *за някое* $k \geq 0$. *(Простите числа от вида* $F_k = 2^{2^k} + 1$ *се наричат прости числа на Ферма.)*

Задача 1.2 *Проверете, че* F_0, F_1, F_2, F_3 *и* F_4 *са прости, но* $F_5 = 641 \cdot 6700417$.

Задача 1.3 *Проверете, че числото на Мерсен* $M_{11} = 2^{11} - 1$ *е съставно число.*

Задача 1.4 *Докажете, че* $\frac{(m+n-1)!}{m!(n-1)!}$ *е цяло число.*

Задача 1.5 *Покажете, че ако* p *и* $8p-1$ *са едновременно прости, то* $8p+1$ *е съставно число.*

Задача 1.6 *Проверете, че стойностите на* $f(x) = x^2+x+41$ *за* $x = -40, -39, \ldots, 0, 1, \ldots, 39$ *са прости числа (за* $x = 0, \ldots, 39$ *са различни).*

Задача 1.7 *Докажете, че не съществува полином* $f(x)$ *с цели коефициенти, за които* $f(n)$ *да е просто за всяка цяла стойност на* n.

Задача 1.8 *Решете диофантовите уравнения*
а) $119x - 29y = 8;$ *б)* $12x - 7y = 15$ *в)* $13x - 153y = 178.$

Задача 1.9 *Решете в цели числа системите*

$$\text{а)} \left|\begin{array}{rcl} 20x + 44y + 50z & = & 10 \\ 17x + 13y + 11z & = & 19 \end{array}\right. ; \qquad \text{б)} \left|\begin{array}{rcrcrcrcr} x_1 & + & x_2 & + & 4x_3 & + & 2x_4 & = & 5 \\ -3x_1 & - & x_2 & & & - & 6x_4 & = & 3 \\ -x_1 & - & x_2 & + & 2x_3 & - & 2x_4 & = & 1 \end{array}\right.$$