Подільність цілих невідємних чисел
Лекція

1. Відношення подільності на множині цілих невідємних чисел. Властивості відношення подільності.
2. Подільність суми, різниці, добутку.
3. Ознаки подільності чисел у десятковій системі числення. Загальна ознака подільності Паскаля. Прості і складені числа. Теореми про дільники натурального числа. Решето Ератосфена.
4. Кратне, спільне кратне, найменше спільне кратне, його властивості.
5. Дільник, спільний дільник, найбільший спільний дільник, його властивості.
6. Основна теорема арифметики. Канонічний розклад чисел.
7. Знаходження НСК та НСД за допомогою канонічного розкладу.
8. Взаємно-прості числа. Ознаки подільності на складені числа. Алгоритм Евкліда.

1. Відношення подільності на множині цілих невідємних чисел. Властивості відношення подільності.

Для цілих невід'ємних чисел віднімання і ділення є частковими операціями. Якщо для віднімання існує проста ознака виконуваності, то для ділення вона не існує. Пошуки таких ознак почалися давно. Вони привели не тільки до відкриття ряду ознак, а й до встановлення важливих властивостей чисел, пов'язаних з розглядом спеціального відношення, яке називається *відношенням подільності.*

Про довільні цілі невід'ємні числа a і b кажуть, що a знаходиться у відношенні подільності з b або що *a ділиться на b* (позначається $a \vdots b$), якщо існує ціле невід'ємне число x таке, що
$a = b \cdot x$:

$\forall a, b \in N_0 : a \vdots b \Leftrightarrow \exists x \in N_0 : a = b \cdot x.$

З означення відношення подільності випливають наслідки.

Наслідок. Нуль ділиться на будь-яке ціле невід'ємне число:
$\forall a, b \in N_0 : 0 \vdots a.$

Наслідок. Будь-яке ціле невід'ємне число ділиться на одиницю:
$\forall a, b \in N_0 : a \vdots 1.$

Відношення подільності на множині цілих невід'ємних чисел:
1) рефлексивне: $\forall a \in N_0 : a \vdots a$;
2) антисиметричне: $\forall a, b \in N_0 : (a \vdots b) \wedge (b \vdots a) \Rightarrow (a = b)$;
3) транзитивне: $\forall a, b, c \in N_0 : (a \vdots b) \wedge (b \vdots c) \Rightarrow (a \vdots c)$;
4) незв'язне.

Зауваження. Відношення подільності на множині цілих невід'ємних чисел слід відрізняти від операції ділення у цій множині: пару чисел, яка належить цьому відношенню, не можна ототожнювати з результатом операції ділення, що ставиться їй у відповідність.

На основі означень відношення подільності, частки і ділення з остачею одержуємо наслідки.

Наслідок. Для довільних цілого невід'ємного числа a і натурального числа b число a ділиться на b тоді і тільки тоді, коли при діленні a на b з остачею остача дорівнює нулю.

Наслідок. Для довільних цілого невід'ємного числа a і натурального числа b число a ділиться на b тоді і тільки тоді, коли існує частка чисел a і b.

Необхідною умовою подільності натуральних чисел є така теорема.

Теорема. Для довільних натуральних чисел a і b, якщо a ділиться на b, то a не менше b, зокрема, якщо $a \neq b$, то $a > b$.

2. Подільність суми, різниці і добутку

Відношення подільності цілих невід'ємних чисел пов'язане з операціями над ними. На цей зв'язок вказують такі теореми.

Теорема. Якщо кожен із доданків ділиться на задане число, то й сума ділиться на це число.

Доведення.

Доведення теореми проведемо для випадку двох доданків. Нехай a_1, a_2 і b – довільні цілі невід'ємні числа такі, що $a_1 \vdots b$ і $a_2 \vdots b$. Звідси за означенням подільності

$$a_1 = b \cdot x_1,\ a_2 = b \cdot x_2, \qquad x_1, x_2 \in N_0.$$

Додамо одержані рівності почленно:

$$a_1 + a_2 = b \cdot x_1 + b \cdot x_2 .$$

На основі дистрибутивності множення відносно додавання

$$a_1 + a_2 = b \cdot (x_1 + x_2).$$

Число $x = x_1 + x_2$ є цілим невід'ємним числом як сума цілих невід'ємних чисел. Отже, $a_1 + a_2 = b \cdot x$, $x \in N_0$. Тому за означенням подільності $(a_1 + a_2) \vdots b$.

Аналогічно доводиться така теорема.

Теорема. Якщо зменшуване і від'ємник діляться на дане число, то й різниця ділиться на це число.

Вираз, у якому є тільки операції додавання і віднімання, називається *алгебраїчною сумою,* а його компоненти – *доданками.* Із розглянутих теорем одержуємо наслідок.

Наслідок. Якщо алгебраїчна сума кількох чисел і кожний її доданок, за винятком одного, діляться на задане число, то й цей доданок ділиться на задане число.

Теорема. Якщо у добутку кількох чисел хоч один із множників ділиться на задане число, то й добуток ділиться на це число.

Доведення.

Доведення проведемо для випадку двох множників. Нехай a_1, a_2 і b – довільні цілі невід'ємні числа такі, що, наприклад, $a_1 \vdots b$. З того, що $a_1 \vdots b$, за означенням подільності випливає

$$a_1 = b \cdot x_1,\ x_1 \in N_0.$$

Тоді $a_1 \cdot a_2 = (b \cdot x_1) \cdot a_2 = b \cdot (x_1 \cdot a_2)$.

Але $x = x_1 \cdot a_2$ є цілим невід'ємним числом як добуток цілих невід'ємних чисел. Тому $a_1 \cdot a_2 = b \cdot x,\ x \in N_0$.

Отже, за означенням подільності $a_1 \cdot a_2 \vdots b$.

З властивостей відношення подільності та теореми одержуємо наслідок.

Наслідок. Якщо число ділиться на добуток кількох чисел, то воно ділиться на кожний множник.

Вказані теореми називаються відповідно теоремами про подільність суми, різниці і добутку.

3. Ознаки подільності

У зв'язку з тим, що процес ділення одного числа на друге досить трудомісткий, нелегко з'ясувати істинність висловлення
" $a \vdots b$" при безпосередньому діленні одного числа на друге, а тому виникає задача пошуку одержання відповіді без виконання ділення.

Ознакою подільності одного натурального числа на інше називається необхідна і достатня умова, при виконанні якої одне число ділиться на інше, причому перевірка умови виконується легше, ніж безпосереднє ділення.

Багато ознак подільності натуральних чисел одержують із загальної ознаки подільності Паскаля.

Теорема (загальна ознака подільності Паскаля).

Для того щоб натуральне число $a = \overline{a_n a_{n-1} \ldots a_1 a_{0g}}$, записане у позиційній системі числення з основою g, ділилося на натуральне число b, необхідно і достатньо, щоб на b ділилася сума

$$r = a_0 + a_1 \cdot r_1 + a_2 \cdot r_2 + ... + a_n \cdot r_n,$$

де $r_1, r_2, ... r_n$ – остачі від ділення $g, g^2, ..., g^n$ на число b.

Доведення.

Розглянемо запис числа a у позиційній системі числення з основою g :

$$a = a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + ... + a_2 \cdot g^2 + a_1 \cdot g + a_0 \quad (1)$$

На основі ділення з остачею степені основи системи числення запишуться:

$$g = b \cdot q_1 + r_1, \quad r_1 < b;$$
$$g^2 = b \cdot q_2 + r_2, r_2 < b;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$g^n = b \cdot q_n + r_n, \quad r_n < b.$$

Підставляючи значення $g, g^2, ..., g^n$ у (l), дістанемо

$$a = a_n \cdot (b \cdot q_n + r_n) + ... + a_2 \cdot (b \cdot q_2 + r_2) + a_l \cdot (b \cdot q_1 + r_l) + a_0. \quad (2)$$

На основі законів операцій множення і додавання цілих невід'ємних чисел рівність (1) можна записати так:

$$a = b \cdot (a_n \cdot q_n + ... + a_2 \cdot q_2 + a_l \cdot q_1) +$$
$$+ (a_n \cdot r_n + ... + a_2 \cdot r_2 + a_1 \cdot r_1 + a_0).$$

Якщо ввести позначення $q = a_n \cdot q_n + ... + a_2 \cdot q_2 + a_1 \cdot q_1$ і $r = a_n \cdot r_n + ... + a_2 \cdot r_2 + a_1 \cdot r_1 + a_0$, то одержимо рівність

$$a = b \cdot q + r. \quad (3)$$

З рівності (3) матимемо:

1. За теоремою про подільність добутку число $b \cdot q$ ділиться на b. Якщо і другий доданок r ділиться на b, то за теоремою про подільність суми $a \vdots b$.

2. Навпаки, якщо число r ділиться на число b, то за наслідком і число a ділиться на b.

Цим самим доведено, що

$$a \vdots b \Leftrightarrow r \vdots b.$$

Користуючись теоремою, можна встановлювати ознаку подільності на довільне задане натуральне число у позиційній системі числення з будь-якою основою. Найбільш вживаними є ознаки подільності на 2, 3, 4, 5, 9, 11 і 25 у десятковій системі числення, деякі з них відомі ще з середньої школи.

Теорема. Для того щоб натуральне число $\overline{a = a_n a_{n-1} \ldots a_1 a_0}$, записане у десятковій системі числення, ділилося:

1) на 2, необхідно і достатньо, щоб a_0 ділилося на 2;

2) на 5, необхідно і достатньо, щоб остання його цифра була 0 або 5;

3) на 3 (або 9), необхідно і достатньо, щоб на 3 (або 9) ділилося число $a_0 + a_1 + a_2 + ... + a_n$;

4) на 4, необхідно і достатньо, щоб число $a_0 + 2\,a_1$ ділилося на 4;

5) на 11, необхідно і достатньо, щоб на 11 ділилася різниця $(a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)$;

6) на 25, необхідно і достатньо, щоб на 25 ділилося число

$\overline{a_1 a_0}$.

Доведення.

Усі ознаки доводяться на основі ознаки Паскаля. Як приклад доведемо ознаку подільності на 11.

Розглянемо десятковий запис числа

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0.$$

Знаходимо остачі r_1, r_2, ... r_n при діленні 10, 10^2..., 10^n на 11.

$$10 = 11 \cdot 0 + 10,\ r_1 = 10,$$

$$10^2 = 99 + 1 = 11 \cdot 9 + 1,\ r_2 = 1.$$

Взагалі, якщо $n = 2k,\ k \in N$, то

$$10^{2k} = \underbrace{99 \ldots 9}_{2k\ разів} + 1 = 11g + 1,\ r_{2k} = 1.$$

Якщо ж

$$n = 2k + 1,\ k \in N,$$

$$\text{то } 10^{2k+1} = 10^{2k} \cdot 10 = (11g + 1) \cdot 10 =$$

$$= 11 \cdot (10g) + 10, \text{ отже, } r_{2k+1} = 10.$$

А тому маємо

$$r = a_0 + 10\, a_1 + a_2 + 10\, a_3 + a_4 + 10\, a_5 + \ldots =$$

$$= (a_0 + a_2 + a_4 + ...) + 10(a_1 + a_3 + a_5 + ...).$$

Якщо до правої частини одержаної рівності додати і відняти вираз ($a_1 + a_3 + a_5 + ...$), то можна записати

$$r = ((a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)) + 11(a_1 + a_3 + a_5 + ...).$$

Звідси, за властивостями відношення подільності та ознакою Паскаля дістанемо

$a \vdots 11 \Leftrightarrow ((a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)) \vdots 11.$

Наприклад, число 153623 не ділиться на 11, бо (3 + 6 + 5) – – (2 + 3 + 1) = 8, і 8 не ділиться на 11, а число 150623 ділиться на 11, бо (3+ 6+ 5) – (2 + 0+ 1)= 11, і 11 ділиться на 11.

Прості і складені числа

Як відомо, для довільного цілого невід'ємного числа a і натурального числа b, якщо a ділиться на b, то число b називається дільником числа a.

Множину цілих невід'ємних чисел за кількістю натуральних дільників можна розбити на такі чотири класи:

1) клас, єдиним елементом якого є число нуль, що має безліч дільників;

2) клас, єдиним елементом якого є число 1, що має єдиний дільник;

3) клас, елементи якого мають два дільники;

4) клас, елементи якого мають більше як два дільники, але їх скінченна кількість.

Числа останніх двох класів посідають у математиці особливе місце. Вони становлять обсяги двох важливих понять. Натуральне число, більше

одиниці, називається:

1) *простим,* якщо воно має своїми дільниками тільки одиницю і саме себе;

2) *складеним,* якщо воно має не менше трьох дільників.

Наприклад, за цим означенням числа 2, 3,5,7, 11, 13, 17, 19 – прості, а числа 4, 6, 8, 9, 10, 12 складені. Теореми виражають властивості простих і складених чисел.

Теорема. Якщо просте число ділиться на натуральне число більше одиниці, то ці числа рівні.

Доведення.

Нехай p – просте число і $a > 1$ – натуральне число таке, що $p \vdots a$. p – просте число, тоді за означенням воно має своїми дільниками лише 1 і p. $a > 1$ і є дільником p. Отже, $a = p$.

Теорема. Для довільних натурального числа a і простого числа p має місце одне і тільки одне з відношень: або a ділиться на p, або вони взаємно прості.

Доведення.

Нехай a – довільне натуральне число, а p – довільне просте число. Розглянемо НСД (a, p). Можливі лише два такі випадки: або НСД $(a, p) = 1$, тоді числа a і p взаємно прості; або

$$\text{НСД}\ (a, p) = d > 1.$$

Звідси одержуємо, що $p \vdots d$. За попередньою теоремою маємо, що $p = d$, а тому $a \vdots p$.

Теорема. Добуток кількох натуральних множників ділиться на просте число тоді і тільки тоді, коли хоч один із множників ділиться на просте число.

Теорема. Кожне натуральне число, більше одиниці, має принаймні один простий дільник.

Наслідок. Найменший, відмінний від одиниці, дільник натурального числа є числом простим.

Теорема (теорема Евкліда). Множина простих чисел нескінченна.

Доведення.

Доведемо теорему методом від протилежного. Припустимо, що множина простих чисел скінченна, тобто, що вона складається з простих чисел $p_1, p_2, ..., p_n$. Розглянемо число

$g = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Число g натуральне і більше одиниці, а тому воно має

принаймні один простий дільник. Таким простим числом не може бути жодне з простих чисел $p_1, p_2, ..., p_n$, бо число g при діленні на кожне з них дає в остачі 1. Отже, існує просте число, відмінне від чисел $p_1, p_2, ..., p_n$. Значить, наше припущення про скінченність множини простих чисел хибне.

Простим чи складеним є задане натуральне число, більше від 1, встановлюється на основі теореми, яка може бути використана як критерій простоти натурального числа.

Теорема. Якщо натуральне число a, більше одиниці, не ділиться на жодне з простих чисел, квадрати яких не перевищують a, то число a просте.

Доведення.

Доведемо теорему методом від протилежного. Припустимо, що число a складене. Тоді за властивістю простих чисел найменший його дільник, більший від 1, є числом простим. Позначимо його g. Матимемо

$$a = g \cdot a_1, \quad 1 < g < a, \quad a_1 > 1.$$

За вибором числа g воно є найменшим дільником числа a, більшим від одиниці, і простим, а тому $g \le a_1$. Звідси за монотонністю множення цілих невід'ємних чисел $g^2 \le a_1 \cdot g$, тобто $g^2 \le a$. Отже, g є простим дільником числа a, квадрат якого не перевищує a, а це суперечить умові теореми.

З теореми одержуємо наслідок.

Наслідок. Найменший простий дільник натурального числа не перевищує кореня квадратного з даного числа.

Задача. Встановити, простим чи складеним є число 967.

Роз'язання.

Для того, щоб встановити простим чи складеним є число 967, потрібно перевірити, чи є його дільниками всі прості числа від 2 до 31, бо $31^2 = 961 < 967$, а $32^2 = 1024 > 967$.

За ознаками подільності встановлюємо, що число 967 не ділиться на прості числа 2, 3, 5 і 11. Безпосередньо перевіряємо, що це число не ділиться на прості числа 7, 13, 17, 19, 23, 29 і 31.

Отже, число 967 не ділиться на жодне з простих чисел, квадрати яких не перевищують числа 967, а тому воно буде простим.

Відповідь: число 967 – просте.

Прості числа у натуральному ряді розподілені нерівномірно. Можна вказати досить великі проміжки натурального ряду, в яких немає жодного простого числа. Наприклад, серед чисел виду

$$n! + 2, n! + 3, n! + 4, ..., n! + n$$

при достатньо великому n немає жодного простого числа. Нагадаємо, що $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$. Разом із тим, існують послідовні непарні числа, що є простими. Такими, зокрема, є числа 3 і 5, 5 і 7, 11 і 13, 17 і 19,..., 1000061087 і 1000061089, ...

Для вивчення розподілу простих чисел у натуральному ряді та інших задач теорії чисел потрібно знати всі прості числа, які не перевищують заданого натурального числа. Для розв'язання цієї задачі є спеціальний метод, який називається *решетом Ератосфена.*

Суть його полягає у такому.

1. Виписують всі натуральні числа від 2 до n:

2,3,4,5,6,7,8,9,10,11, 12, ...,n. (1)

2. Число 2 ділиться тільки на 1 і саме на себе, отже, воно є простим. Викреслюють у ряді (1) усі числа, кратні двом, крім самого числа 2.

3. Перше, наступне за 2, невикреслене число буде 3. Воно не ділиться на 2 (інакше його б викреслили). Отже, 3 ділиться тільки на 1 і саме на себе, а тому також буде простим. Викреслюють усі числа, кратні 3, крім самого числа 3.

4. Перше, наступне за 3, невикреслене число буде 5. Воно не ділиться ні на 2, ні на 3. Отже, 5 ділиться тільки на 1 і саме на себе, тому воно також буде простим. Викреслюють усі числа, кратні 5, крім самого числа 5 і т. д.

Процес буде закінчено, коли одержимо просте число p таке, що $p^2 \le n$, але для першого, наступного за p, невикресленого простого числа p_1 $p_1^2 > n$. Усі невикреслені числа від 2 до n будуть простими.

Наприклад, щоб скласти таблицю простих чисел, які не перевищують 1000, викреслювання потрібно закінчити при $p = 31$, тому що $31^2 = 961 < 1000$. Для наступного за 31 числа, тобто для числа 32, маємо $32^2 = 1024 > 1000$, а тому й поготів для наступного за 31 простого числа будемо мати таку ж нерівність.

Зауваження.

1. Щоб викреслити всі складені числа, кратні простому числу p, не потрібно знати ознаки подільності на p, для цього досить у ряді (1) викреслити кожне p-те число після числа p, враховуючи й ті, які вже раніше були викреслені.

2. Викреслювання чисел, кратних простому числу p, слід починати з p, тому що всі складені числа між p і p^2 уже викреслені як кратні простим числам, меншим від p.

4. Спільні кратні і найменше спільне кратне кількох натуральних чисел

Нехай $a_1, a_2, a_3, ...,a_n$ – довільні натуральні числа. Натуральне число, яке ділиться на кожне із заданих чисел, називається їх *спільним кратним,* а найменше із спільних кратних – їх *найменшим спільним кратним* і позначається НСК($a_1, a_2, a_3, ...,a_n$).

Множина спільних кратних для натуральних чисел $a_1, a_2, a_3, ...,a_n$ нескінченна. Це випливає з того, що за теоремою про подільність добутку число $a_1 \cdot a_2 \cdot a_3 \cdot ... \cdot a_n$ є спільним кратним заданих чисел, а тому і кожне число виду

$$(a_1, a_2, a_3, ...,a_n) \cdot k, \text{ де } k \in N,$$

також буде їх спільним кратним. За принципом найменшого числа у множині

спільних кратних існує найменше число, яке і буде найменшим спільним кратним заданих чисел. Отже, для довільних натуральних чисел a_1, a_2, a_3, ...,a_n їх найменше спільне кратне існує і причому єдине.

З означення найменшого спільного кратного випливає теорема.

Теорема. Для довільних натуральних чисел a і b, якщо a ділиться на b, то a і буде найменшим спільним кратним заданих чисел:

$$\forall a, b \in N : a \vdots b \Rightarrow \text{НСК}(a, b) = a.$$

Основну властивість найменшого спільного кратного виражає така теорема.

Теорема. Кожне спільне кратне кількох натуральних чисел ділиться на їх найменше спільне кратне.

Доведення.

Нехай a_1, a_2, a_3, ...,a_n – довільні натуральні числа, m = НСК (a_1, a_2, ...,a_n) і M – довільне спільне кратне цих чисел. Поділимо M на m з остачею:

$$M = m \cdot g + r, \quad r < m. \qquad (1)$$

M і m – спільні кратні чисел a_1, a_2, a_3, ...,a_n, тоді для кожного i = 1, 2, ..., n $M \vdots a_i$ і $m \vdots a_i$.

За теоремою про подільність добутку, $m \cdot g \vdots a_i$ i = 1,2, ...,n.

Отже, у рівності (1) усі члени, крім одного r, діляться на кожне з чисел a_i i= 1, 2, ..., n. Звідси за наслідком $r \vdots a_i$, i = 1, 2, ..., n.

Оскільки $r < m$ є найменшим спільним кратним заданих чисел, то r = 0 і $M = m \cdot g$, тобто $M \vdots m$.

5. Спільні дільники і найбільший спільний дільник кількох натуральних чисел

Нехай a_1, a_2, ...,a_n – довільні натуральні числа. Натуральне число, на яке ділиться кожне із заданих чисел, називається їх *спільним дільником,* а найбільший із спільних дільників – їх *найбільшим спільним дільником* і позначається НСД (a_1, a_2, ...,a_n). Множина спільних дільників декількох натуральних чисел є непорожньою і скінченною. Це випливає з того, що число 1 – спільний дільник довільних натуральних чисел, а дільник числа не перевищує його. Тоді за принципом найбільшого числа у множині спільних дільників заданих чисел існує найбільше число, яке і буде найбільшим спільним дільником заданих чисел. Отже, для довільних натуральних чисел a_1, a_2, ...,a_n їх найбільший спільний дільник завжди існує і причому єдиний.

З означення найбільшого спільного дільника випливає теорема.

Теорема. Для довільних натуральних чисел a і b, якщо a ділиться на b, то їх найбільший спільний дільник дорівнює b:

$$\forall a, b \notin N : a \vdots b \Rightarrow \text{НСК}(a, b) = b.$$

Основну властивість найбільшого спільного дільника виражає така теорема.

Теорема. Довільний спільний дільник заданих натуральних чисел є дільником їх найбільшого спільного дільника.

Доведення.

Нехай $a_1, a_2, ..., a_n$ – довільні натуральні числа, D = НСД ($a_1, a_2, ..., a_n$) і d – їх довільний спільний дільник. Тоді за означенням найбільшого спільного дільника $D \geq d$. Припустимо, що D не ділиться на d. Нехай m = НСК (D, d).

Оскільки $\overline{D \vdots d}$, то $m > D$. Числа D і d є спільними дільниками кожного із чисел a_i, i = 1,2, ..., n, тобто кожне з даних чисел є спільним кратним чисел d і D. За основною властивістю найменшого спільного кратного кожне з чисел a_i, i= 1, 2, ... , n, буде кратним числу m, тобто m є їх спільним дільником. А це неможливо, бо D – найбільший спільний дільник чисел $a_1, a_2, ..., a_n$. Одержане протиріччя і доводить теорему.

Властивості найменшого спільного кратного і найбільшого спільного дільника двох натуральних чисел

Між найменшим спільним кратним і найбільшим спільним дільником двох натуральних чисел існує зв'язок, який виражається такою теоремою.

Теорема. Для довільних натуральних чисел a і b їх найменше спільне кратне дорівнює добутку даних чисел, що ділиться на їх найбільший спільний дільник:

$$\forall a, b \in N: \; НСК\ (a, b) = \frac{ab}{НСД\ (a, b)}.$$

Доведення.

Нехай d – довільний спільний дільник натуральних чисел a і b. Розглянемо число $M = \frac{ab}{d}$. (1)

Рівність (1) можна записати ще й так:

$$M = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}.$$

Звідси за означенням подільності одержуємо, що M є спільним кратним чисел a і b. Отже, за основною властивістю найменшого спільного кратного будемо мати

$$M = m \cdot t, \; m = \text{НСК}\ (a, b) \text{ і } t \in N. \qquad (2)$$

Скориставшись (2), рівність (1) можна записати

$$m\,t = \frac{ab}{d}$$

Тоді

$$d = \frac{ab}{mt}. \qquad (3)$$

Таким чином, будь-який спільний дільник чисел a і b дорівнює їх добутку, поділеному на число, кратне найменшому спільному кратному даних чисел. Рівність (3) показує, що найбільшим спільний дільник буде при $t = 1$. Враховуючи це, рівність (3) запишеться

$$\text{НСД}\,(a, b) = \frac{ab}{m}.$$

Отже,

$$НСК\,(a, b) = \frac{ab}{НСД\,(a, b)}.$$

З доведеної теореми одержуємо наслідок.

Наслідок. Для того щоб найменше спільне кратне двох чисел дорівнювало їх добутку, необхідно і достатньо, щоб ці числа були взаємно простими.

Теорема не може бути застосована більше, ніж до двох чисел, бо, наприклад, НСК (2, 4, 6) = 12, тоді як за теоремою

$$\text{НСК}(2, 4, 6) = \frac{2 \cdot 4 \cdot 6}{2} = 24.$$

Теорема. Для того щоб спільний дільник d натуральних чисел a і b був їх найбільшим спільним дільником, необхідно і достатньо, щоб числа $\frac{a}{d}$ і $\frac{b}{d}$ були взаємно простими.

Доведення.

Необхідність. Нехай d = НСД (a, b). Доведемо, що числа $\frac{a}{d}$ і $\frac{b}{d}$ – взаємно прості. Припустимо протилежне, тобто, що числа $\frac{a}{d}$ і $\frac{b}{d}$ – не взаємно прості. Отже, вони мають спільний дільник $k > 1$. Тоді $\frac{a}{d} = k \cdot a_1$ і $\frac{b}{d} = k \cdot b_1$.

Звідси

$a = (d \cdot k) \cdot a_1$ і $b = (d \cdot k) \cdot b_1$,

тобто $a \vdots (d \cdot k)$ і $b \vdots (d \cdot k)$, де $(d \cdot k) > d$, що суперечить вибору числа d як найбільшого спільного дільника чисел a і b.

Значить, числа $\frac{a}{d}$ і $\frac{b}{d}$ – взаємно прості.

Достатність. Нехай d є спільним дільником чисел a і b таким, що числа $\frac{a}{d}$ і $\frac{b}{d}$ – взаємно прості. Доведемо, що d =НСД (a, b). Припустимо, d не є найбільшим спільним дільником чисел a і b. Нехай D = НСД (a, b). За основною властивістю найбільшого спільного дільника та необхідною ознакою подільності натуральних чисел матимемо $D = d \cdot k$, де $k > 1$. Звідси видно, що $a \vdots (d \cdot k)$ і $b \vdots (d \cdot k)$. Отже, числа $\frac{a}{d}$ і $\frac{b}{d}$ мають спільний дільник $k > 1$, що суперечить умові.

Теорему можна узагальнити на довільну скінченну сукупність натуральних чисел.

Теорема. Спільний дільник двох натуральних чисел можна виносити за знак їхнього найбільшого спільного дільника і найменшого спільного кратного:

$\forall a, b, c \in N$: НСД ($a \cdot c$, $b \cdot c$) = $c \cdot$ НСД (a, b);

$\forall a, b, c \in N$: НСК ($a \cdot c$, $b \cdot c$) = $c \cdot$ НСК (a, b).

Доведення.

1. Нехай D = НСД (a, b). Розглянемо число $D_1 = c \cdot D$. Матимемо

$$НСД\left(\frac{a \cdot c}{D_1}, \frac{b \cdot c}{D_1}\right) = НСД\left(\frac{a \cdot c}{c \cdot D}, \frac{b \cdot c}{c \cdot D_1}\right) = НСД\left(\frac{a}{D}, \frac{b}{D}\right).$$

За попередньою теоремою числа $\frac{a}{D}$ і $\frac{b}{D}$ будуть взаємно простими, тобто $НСД\left(\frac{a}{D}, \frac{b}{D}\right) = 1$. Отже, $НСД\left(\frac{a \cdot c}{D_1}, \frac{b \cdot c}{D_1}\right) = 1$.

За тією ж теоремою НСД ($a \cdot c$, $b \cdot c$) = D_1. А тому НСД ($a \cdot c$, $b \cdot c$) = $c \cdot$ НСД (a, b).

2. Маємо

$$\text{НСК } (a \cdot c, b \cdot c) = \frac{a \cdot c \cdot b \cdot c}{НСД\ (a \cdot c, b \cdot c)} = \frac{c^2 (a \cdot c)}{c \cdot НСД\ (a,b)} =$$

$$= c \cdot \frac{(a \cdot c)}{НСД\ (a,b)} = c \cdot \text{НСК } (a, b).$$

Отже, НСК ($a \cdot c$, $b \cdot c$) = $c \cdot$ НСК (a, b).

Теорема полегшує знаходження найменшого спільного кратного та

найбільшого спільного дільника двох чисел. Наприклад:

$$НСК(45, 60) = 15 \cdot НСК(3, 4) = 15 \cdot 3 \cdot 4 = 180;$$

$$НСД(45, 60) = 15 \cdot НСД(3, 4) = 15.$$

Теорему також можна узагальнити на довільну скінчену сукупність натуральних чисел.

6. Основна теорема арифметики і канонічний розклад натурального числа

Прості числа відіграють особливу роль у математиці, вони є своєрідними "цеглинками", з яких будується кожне натуральне число, більше одиниці. Це випливає з такої теореми, яку назива*ють основною теоремою арифметики.*

Теорема. Кожне натуральне число, більше одиниці, є або простим, або розкладається у добуток простих множників, причому цей розклад єдиний з точністю до порядку слідування множників.

Доведення.

I. Спочатку покажемо, що кожне натуральне число, більше одиниці, є або простим, або розкладається в добуток простих множників. Для цього скористаємося методом математичної індукції.

1. 2 – просте число. Отже, твердження істинне при $a = 2$.

2. Припустимо, що твердження істинне для довільного натурального числа k такого, що $2 \le k < a$, тобто, що кожне таке число є або простим, або розкладається в добуток простих множників.

3. Доведемо істинність твердження і для числа a. Оскільки натуральне число a більше одиниці, то воно має принаймні один простий дільник. Позначимо його p_1.

$$a = p_1 k_1 . \qquad (1)$$

У рівності (1) k_1 є натуральним числом, отже, для нього можливі лише два такі випадки: або $k_1 = 1$, або $k_1 > 1$.

Якщо $k_1 = 1$, то число a є простим, і доводжуване твердження у цьому випадку істинне і для a.

Якщо $k_1 > 1$, то внаслідок рівності (1) $2 \le k_1 < a$. Звідси та з припущення одержуємо, що для числа k_1 можливі лише два такі випадки:

а) число k_1 є простим і тоді число a є добутком двох простих множників;

б) число k_1 є складеним і розкладається у добуток простих чисел, тобто $k_1 = p_2 \cdot p_3 \cdot \ldots \cdot p_n$, і тоді $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$.

Отже, твердження істинне для a і у випадку, коли $k_1 > 1$. Таким чином, твердження істинне для a.

Звідси на основі принципу математичної індукції твердження істинне для довільного натурального числа $a \ge 2$.

II. Доведемо тепер, що для складеного натурального числа його

розклад у добуток простих множників єдиний з точністю до порядку слідування множників. Дійсно, нехай складене число a має принаймні два розклади у добуток простих чисел

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n \quad \text{і} \quad a = g_1 \cdot g_2 \cdot \ldots \cdot g_s.$$

Тоді

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n = g_1 \cdot g_2 \cdot \ldots \cdot g_s. \qquad (2)$$

З рівності (2) випливає, що добуток $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ ділиться на просте число g_1, а тому на основі теореми про подільність добутку на просте число робимо висновок, що принаймні один із множників $p_1, p_2, \ldots, p_n$ ділиться на число g_1. Не обмежуючи загальності міркувань, можна вважати, що таким множником є число p_1. Оскільки p_1 і g_1 – прості числа, то на основі теореми про властивість простих чисел $p_1 = g_1$. Скорочуючи обидві частини рівності (2) нарі, матимемо

$$p_2 \cdot p_3 \cdot \ldots \cdot p_n = g_2 \cdot g_3 \cdot \ldots \cdot g_s.$$

Повторюючи аналогічні міркування, через скінченну кількість кроків дістанемо

$$p_1 = g_1 \quad p_2 = g_2, \ldots, p_k = g_k \quad \text{і або } n = s, \text{ або } n \neq s.$$

Покажемо, що $n = s$. Дійсно, якщо припустити, що $n < s$, то

$$1 = g_{n+1} \cdot g_{n+2} \cdot \ldots \cdot g_s,$$

що неможливо, бо добуток простих чисел більший 1. Аналогічно розглядається випадок, коли $n > s$.

Отже, $n = s$ і розклади не відрізняються простими множниками, тобто він єдиний з точністю до порядку слідування множників.

Якщо для складеного натурального числа знайдено його зображення у вигляді добутку простих множників, і у ньому рівні прості множники записано у вигляді степенів простих множників, а самі прості множники розміщені у порядку зростання, то такий запис складеного числа у вигляді добутку простих множників називається *канонічним розкладом натурального числа*

$p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n}$ де $p_1, p_2, \ldots, p_n$ – різні прості дільники числа a і $p_1 < p_2 < \ldots < p_n$.

Якщо натуральне число a є простим, то сам його запис і є канонічним розкладом числа a.

Кажуть, що просте число p *входить у канонічний розклад числа* $a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n}$, якщо воно дорівнює одному з чисел $p_1, p_2, \ldots, p_n$.

На основі поняття канонічного розкладу з основної теореми арифметики одержуємо наслідок.

Наслідок. Канонічний розклад складеного числа єдиний.

Щоб знайти канонічний розклад складеного числа, випробовують його подільність на прості числа у порядку зростання. При цьому користуються відомими ознаками подільності на прості числа. Результати обчислень зручно розташовувати так, як показано у такій задачі.

7. Знаходження найбільшого спільного дільника і найменшого спільного кратного кількох чисел за їх канонічними розкладами

При розгляді кількох натуральних чисел можна вважати, що їх канонічні розклади містять степені одних і тих же простих множників, при цьому показники степенів у деяких з них можуть бути рівні нулю, бо за означенням нульового показника степеня
$x^0 = 1$ для довільного числа $x \neq 0$.

За допомогою канонічного розкладу натуральних чисел можна встановити вигляд їх дільників.

Теорема. Якщо натуральне число a має канонічний розклад

$$a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n},$$

то натуральне число b є його дільником тоді і тільки тоді, коли воно має канонічний розклад

$$b = p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots \cdot p_n^{\beta n} \text{ і } 0 \le \beta_1 \le \alpha_1,$$
$$0 \le \beta_2 \le a_2, \ldots, 0 \le \beta_n \le a.$$

Доведення.

Необхідність. Нехай число $a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n}$ ділиться на число b. Отже, $a = b \cdot g$ або, що те саме, $a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n} = b \cdot g$. Внаслідок єдиності розкладу на прості множники до канонічного розкладу чисел b і g не можуть входити прості числа, відмінні від чисел $p_1, p_2, \ldots, p_n$. А тому

$$b = p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots \cdot p_n^{\beta n} \quad \text{і} \quad g = p_1^{\gamma 1} \cdot p_2^{\gamma 2} \cdot \ldots \cdot p_n^{\gamma n}.$$

Отже,

$$p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n} =$$
$$= (p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots \cdot p_n^{\beta n}) \cdot (p_1^{\gamma 1} \cdot p_2^{\gamma 2} \cdot \ldots \cdot p_n^{\gamma n}) =$$
$$= p_1^{\beta 1 + \gamma 1} \cdot p_2^{\beta 2 + \gamma 2} \cdot \ldots \cdot p_n^{\beta n + \gamma n}.$$

Звідси, завдяки єдиності канонічного розкладу, одержуємо

$$\alpha_1 = \beta_1 + \gamma_1, \quad \alpha_2 = \beta_2 + \gamma_2, \quad \ldots \quad \alpha_n = \beta_n + \gamma_n.$$

Числа α_i, β_i і γ_i є цілими невід'ємними числами, тому з попередніх рівностей $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le a_2, \ldots, 0 \le \beta_n \le a$.

Достатність. Нехай число b має такий канонічний розклад, як вказано у теоремі. Тоді число a можна записати

$$a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n} =$$
$$= (p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots \cdot p_n^{\beta n}) \cdot (p_1^{\beta 1 - \gamma 1} \cdot p_2^{\beta 2 - \gamma 2} \cdot \ldots \cdot p_n^{\beta n - \gamma n}).$$

Різниці $\alpha_i - \beta_i$ існують завдяки умові $0 \le \beta_i \le \alpha_i$ $i = 1, 2, \ldots, n$.
З одержаної рівності випливає, що число b є дільником числа a.

З теореми випливають наслідки.

Наслідок. Натуральне число ділиться на просте число тоді і тільки тоді, коли дане просте число входить до його канонічного

розкладу.

Наслідок. Два натуральних числа взаємно прості тоді і тільки тоді, коли їх канонічні розклади не мають спільних простих дільників.

Наслідок. Якщо кожне з двох даних натуральних чисел взаємно просте з третім натуральним числом, то і їх добуток взаємно простий з даним числом.

Теорема також дає можливість за канонічними розкладами кількох натуральних чисел знайти їх найбільший спільний дільник і найменше спільне кратне.

Теорема.

1. Канонічний розклад найбільшого спільного дільника кількох натуральних чисел містить ті ж прості множники, що й канонічні розклади цих чисел, але взяті з найменшими показниками степенів.

2. Канонічний розклад найменшого спільного кратного кількох натуральних чисел містить ті ж прості множники, що й канонічні розклади даних чисел, але взяті з найбільшими показниками степенів.

Доведення.

Нехай задано кілька натуральних чисел і відомі їх канонічні розклади

$$a = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_n^{\alpha n},$$

$$b = p_1^{\beta 1} \cdot p_2^{\beta 2} \cdot \ldots \cdot p_n^{\beta n} \cdot \ldots \cdot l = p_1^{\gamma 1} \cdot p_2^{\gamma 2} \cdot \ldots \cdot p_n^{\gamma n}.$$

Позначимо через μ_1 – найменше, а через ν_1 – найбільше з чисел α_1, β_1, λ_1, тобто

$$\mu_1 = \min\{\alpha_1, \beta_1, \lambda_1\}, \quad \nu_1 = \max\{\alpha_1, \beta_1, \lambda_1\}.$$

Аналогічно

$$\mu_2 = \min\{\alpha_2, \beta_2, \lambda_2\}, \quad \nu_2 = \max\{\alpha_2, \beta_2, \lambda_2\}.$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mu_n = \min\{\alpha_n, \beta_n, \lambda_n\}, \quad \nu_1 = \max\{\alpha_n, \beta_n, \lambda_n\}.$$

На основі введених позначень, щоб довести теорему, потрібно показати, що

$$\text{НСД}(a, b, \ldots, l) = p_1^{\mu 1} \cdot p_2^{\mu 2} \cdot \ldots \cdot p_n^{\mu n}, \qquad (1)$$

$$\text{НСК}(a, b, \ldots, l) = p_1^{\nu 1} \cdot p_2^{\nu 2} \cdot \ldots \cdot p_n^{\nu n}. \qquad (2)$$

Доведемо рівність (1). Нехай $d = p_1^{\mu 1} \cdot p_2^{\mu 2} \cdot \ldots \cdot p_n^{\mu n}$. Тоді за теоремою число d є спільним дільником чисел a, b, ..., l. За основною властивістю найбільшого спільного дільника число d є дільником числа D = НСД (a, b, ..., l). Знову, за теоремою число

$$D = p_1^{\sigma 1} \cdot p_2^{\sigma 2} \cdot \ldots \cdot p_n^{\sigma n} \text{ де } \sigma_1 \geq \mu_i,\ i = 1, 2, \ldots, n.$$

Покажемо, що $\sigma_1 = \mu_i$, $i = 1, 2, \ldots, n$. Дійсно, якби при деякому i_0 було $\sigma_{i0} > \mu_{i0}$ то те з чисел a, b, ..., l, до канонічного розкладу якого входить число $p_{i0}^{\mu i0}$, не ділилося б на D. Отже, с $\sigma_1 = \mu_i$, $i = 1, 2, \ldots, n$, тобто НСД (a, b, ..., l) $= p_1^{\mu 1} \cdot p_2^{\mu 2} \cdot \ldots \cdot p_n^{\mu n}$.

Аналогічно доводиться рівність (2).

Задача. Знайти найбільший спільний дільник і найменше спільне кратне чисел 4680, 7722 і 4368 за їх канонічними розкладами.

Роз'язання.

Знаходимо канонічні розклади даних чисел.

Відповідь: НСД(4680, 7722, 4368) = 78, НСК(4680,7722,4368) = 2162160.

8. Натуральні числа a_1, a_2, ..., a_n називаються *взаємно простими,* якщо їх найбільший спільний дільник дорівнює одиниці, і *попарно взаємно простими,* якщо НСД (a_i, a_j) = 1 для всіх $i \neq j$, $i, j = 1, 2, ..., n$.

Для двох чисел поняття взаємно простих і попарно взаємно простих чисел рівносильні. Якщо ж чисел більше як два, то ці поняття нерівносильні. Очевидно, що завжди, коли числа попарно взаємно прості, то вони і взаємно прості, але обернене твердження хибне. Наприклад, числа 2, 3 і 4 взаємно прості, але вони не будуть попарно взаємно простими, бо НСД (2, 4) = 2.

Теореми про подільність, пов'язані з взаємно простими числами

З поняттям про взаємно прості числа пов'язані дві важливі теореми про подільність.

Теорема. Якщо добуток двох натуральних чисел ділиться на третє натуральне число, яке взаємно просте з одним із множників, то другий множник ділиться на це число:

$$\forall a, b, c \in N : a, b \vdots c \ \wedge \text{НСД}(a, b) = 1 \Rightarrow a \vdots c .$$

Доведення.

Нехай a, b і c – довільні натуральні числа такі, що

$$a, b \vdots c \text{ і НСД } (a, b) = 1.$$

Доведемо, що $a \vdots c$. Дійсно, за теоремою про подільність добутку, $a \cdot b \vdots b$ і за умовою теореми $a \cdot b \vdots c$. Звідси за основною властивістю найменшого спільного кратного $a \cdot b \vdots$ НСК (b, c). Оскільки числа b і c взаємно прості, то

$$\text{НСК } (b, c) = b \cdot c, \text{ отже, } a \cdot b \vdots b \cdot c.$$

За означенням подільності $a \cdot b = (b \cdot c) \cdot x$ і за монотонністю множення

цілих невід'ємних чисел $a = c \cdot x$, тобто $a \vdots c$.

Теорема. Якщо натуральне число ділиться на кожне з двох взаємно простих чисел, то воно ділиться і на їх добуток:

$$\forall a, b, c \in N : (a \vdots b) \wedge (a \vdots c) \wedge \text{НСД}(b, c) = 1 \Rightarrow a \vdots b \cdot c .$$

Доведення.

Нехай a, b і c – довільні натуральні числа такі, що $a \vdots b$, $a \vdots c$ і НСД(b, c) = 1.

Доведемо, що $a \vdots b \cdot c$. За умовою теореми число a є спільним кратним чисел b і c. На підставі основної властивості найменшого спільного кратного матимемо $a \vdots$ НСК(b, c). Числа b і c взаємно прості, отже, НСК (b, c) = $b \cdot c$, атому $a \vdots b \cdot c$.

Відомо, що коли число ділиться на добуток, то воно ділиться і на кожний множник. Користуючись цим фактом та теоремою, одержуємо наслідок.

Наслідок. Для того щоб натуральне число ділилося на добуток двох взаємно простих чисел, необхідно і достатньо, щоб воно ділилося на кожен із множників.

Одержаний наслідок дає можливість встановлювати ознаки подільності на натуральні числа, які можна подати у вигляді добутку двох взаємно простих чисел. Відзначимо також, що цей наслідок можна застосувати і до множників числа, подільність на яке встановлюється.

Задача. Встановити ознаку подільності на 165.

Число $165 = 3 \cdot 55$, де числа 3 і 55 взаємно прості. На основі наслідку

$$a \vdots 165 \Leftrightarrow a \vdots 3 \wedge a \vdots 55 . \qquad (1)$$

Число $55 = 5 \cdot 11$, де числа 5 і 11 взаємно прості. На основі наслідку

$$a \vdots 55 \Leftrightarrow a \vdots 5 \wedge a \vdots 11.$$

Підставивши в (1) замість $a \vdots 55$ рівносильне йому твердження $a \vdots 5 \wedge a \vdots 11$, одержимо

$$a \vdots 165 \Leftrightarrow a \vdots 3 \wedge a \vdots 5 \wedge a \vdots 11.$$

Отже, число ділиться на 165 тоді і тільки тоді, коли воно ділиться на числа 3, 5 і 11.

За цією ознакою число 8745 ділиться на 165, бо сума його цифр ділиться на 3, закінчується цифрою 5 і

$$(5 + 7) – (4 + 8) = 0 \vdots 11.$$

8. Алгоритм Евкліда

Відомі властивості найменшого спільного кратного і найбільшого спільного дільника двох чисел не завжди дають можливість їх обчислювати. За теоремою 12

$$\forall\, a, b \in N : \text{НСК}(a, b) = \frac{a \cdot b}{НСД\ (a, b)}\ .$$

Отже, достатньо вміти знаходити найбільший спільний дільник двох чисел. Для розв'язання цієї задачі є спеціальний метод, який називається *послідовним діленням,* або *алгоритмом Евкліда.* Теоретичною основою його є теорема про ділення з остачею і така теорема.

Теорема. Для довільних натуральних чисел *a, b, g* і *r*, якщо між ними має місце залежність

$a = b \cdot g + r,$

то множина спільних дільників чисел *a* і *b* дорівнює множині спільних дільників чисел *b* і *r*, зокрема

НСД (*a*, *b*) = НС (*g*, *r*).

Доведення.

Нехай між натуральними числами *a, b, g* і *r* має місце залежність

$$a = b \cdot g + r \qquad (1)$$

1. Якщо *d* – будь-який спільний дільник чисел *a* і *b,* то за теоремою про подільність добутку $b \cdot g \vdots d$. Тоді з рівності (1) за властивістю подільності алгебраїчної суми $r \vdots d$. Отже, кожний спільний дільник чисел *a* і *b* є спільним дільником чисел *b* і *r.*

2. Навпаки, якщо *d* – будь-який спільний дільник чисел *b* і *r,* то за теоремою про подільність добутку і суми $a \vdots d$. Отже, кожний спільний дільник чисел *b* і *r* є спільним дільником чисел *a* і *b.*

З пунктів 1 і 2 доведення випливає, що множини спільних дільників чисел *a* і *b* та *b* і *r* збігаються, а тому і

НСД(*a*, *b*) = НСД(*b*, *r*).

Алгоритм Евкліда полягає у тому, що:

1. Число *a* ділиться на число *b* з остачею r_1

$$a = b \cdot g_1 + r_1, \quad r_1 < b\ .$$

Якщо $r_1 = 0$, то $b = \text{НСД}\ (a, b)$.

2. Якщо $r_1 > 0$, то число *b* ділять на число r_1 з остачею:

$$b = r_1 \cdot\ g_2 + r_2, \quad r_2 < r_1.$$

Якщо $r_2 = 0$, то $r_1 = \text{НСД}\ (b, r_1) = \text{НСД}\ (a, b)$.

3. Якщо $r_2 > 0$, то число r_1 ділять на число r_2 з остачею:

$$r_1 \Rightarrow r_2 \cdot g_3 + r_3, \quad r_3 < r_2$$

Якщо $r_3 = 0$, то

$$r_2 = \text{НСД}\ (r_1,\ r_2) = \text{НСД}\ (b, r_1) = \text{НСД}\ (a, b).$$

4. Якщо $r_3 > 0$, то повторюють ділення аналогічно пункту 3, поки не отримають остачу, рівну нулю.

5. Остання, відмінна від нуля, остача і буде найбільшим спільним дільником чисел *a* і *b.* Процес ділення в алгоритмі Евкліда скінченний, бо

остачі, які є цілими невід’ємними числами, на кожному кроці зменшуються, залишаючись меншими від *b,* а таких чисел не більше як *b*.