3 НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК, НАЙМЕНШЕ СПІЛЬНЕ КРАТНЕ І АЛГОРИТМ ЕВКЛІДА, ЇХ ВЛАСТИВОСТІ ТА ВЗАЄМНА ПРОСТОТА

Нехай $a, b \in \mathbb{Z}$. Кажуть, що ціле число d є *спільним дільником* a і b, якщо $a \vdots d$ і $b \vdots d$.

Нехай $a, b \in \mathbb{Z}$. Ціле число d називається *найбільшим спільним дільником* (*НСД*) чисел a і b, якщо

- d – спільний дільник a і b;
- якщо d' – спільний дільник a і b, то $d \vdots d'$.

Позначення: $d = \text{НСД}(a, b)$ або $d = \gcd(a, b)$ або $d = (a, b)$.

Зауважимо, що НСД двох цілих чисел (якщо він існує) єдиний з точністю до знака. А саме, якщо d і d' – два найбільших спільних дільника чисел a і b, то з означення випливає, що $d' \vdots d$ і $d \vdots d'$, звідки випливає, що d і d' асоційовані, тому $d = \pm d'$. Тому важливо розуміти, що вираз $\gcd(a, b)$ не є однозначно визначеним цілим числом, а лише позначає який-небудь з найбільших спільних дільників чисел a і b. Наприклад, якщо $\gcd(a, b) = d$, то і $\gcd(a, b) = -d$.

У словосполученні «найбільший спільний дільник» слово «найбільший» означає не найбільший за величиною, а те, що цей дільник є кратним будь-якого іншого спільного дільника чисел a і b. Наприклад, спільними дільниками чисел 12 і 18 будуть ±1, ±2, ±3, ±6, а найбільшими спільними дільниками цих чисел є 6 і −6 (зауважимо, що за величиною −6 є найменшим серед спільних дільників чисел 12 і 18).

Легко бачити, що $\gcd(0, a) = a$; зокрема, $\gcd(0, 0) = 0$.

Теорема 1 (про існування найбільшого спільного дільника) Найбільший спільний дільник двох цілих чисел a, b існує і представляється у вигляді $d = au_0 + bv_0$ для деяких цілих u_0, v_0.

Доведення.

Якщо $a = b = 0$, то ми вже знаємо, що $\gcd(a, b) = 0$, і доводити нічого. Тепер можна вважати, що $a \neq 0$. Розглянемо множину всіх натуральних чисел виду $au + bv$ для будь-яких цілих u, v і виберемо в ньому найменший ненульовий елемент (ця множина непорожня: наприклад, воно містить $|a|$). Позначимо його через d; з побудови маємо $d = au_0 + bv_0$ для деяких цілих u_0, v_0. Покажемо, що d є спільним дільником a і b. Поділимо a на d із остачею: $a = dq + r = (au_0 + bv_0)q + r$, звідки $r = a(1 - u_0 q) + b(-v_0 q)$. Однак, $r < d$ – натуральне число, а d було найменшим натуральним числом, що подаються у вигляді $d = ax + by$. Отже, $r = 0$ і a ділиться на d. Аналогічно, b ділиться на d.

Доведемо тепер, що d – це найбільший спільний дільник a і b. Нехай d' – деякий спільний дільник a і b: $a \vdots d'$ і $b \vdots d'$. Тоді за властивостями подільності $au_0 \vdots d'$, $bv_0 \vdots d'$, і $au_0 + bv_0 = d \vdots d'$, що й було потрібно.

Вираз $d = au_0 + bv_0$ називається *лінійним поданням НСД*.

Поняття найбільшого спільного дільника легко узагальнюється на довільну скінченну кількість чисел, а саме: d називається найбільшим спільним дільником чисел $a_1, a_2, ..., a_n$, якщо d задовольняє такі умови:

– $a_1 \vdots d, a_2 \vdots d, ..., a_n \vdots d$;

– якщо $a_1 \vdots c, a_2 \vdots c, ..., a_n \vdots c$, то $d \vdots c$.

Цілком аналогічно випадку двох чисел доводиться, що найбільший спільний дільник довільного набору чисел $a_1, a_2, ..., a_n$ існує і визначений з точністю до знаку. Він позначається $\text{НСД}(a_1, a_2, ..., a_n)$ або $\gcd(a_1, a_2, ..., a_n)$. І в загальному випадку для однозначності братимемо лише додатне значення найбільшого спільного дільника.

Приклад 1 Знайти довжину найкоротшої арифметичної прогресії, членами якої будуть числа 15, 69, 105 і 189.

Розв'язання.

У найкоротшій прогресії числа 15 і 189 повинні бути крайніми членами. Можна вважати, що 15 – перший член, а 189 – останній. Різниця двох довільних членів арифметичної прогресії завжди ділиться на різницю d цієї прогресії. Тому d ділить кожне з чисел 69−15=54, 105−69=36, 189−105=84. Щоб прогресія була найкоротшою, її різниця має бути найбільшою. Отже, d=$\text{НСД}(54, 36, 84) = 6$.

Тепер із рівності $189 = 15 + 6 \cdot (n-1)$ знаходимо $n = 30$, тобто найкоротша прогресія містить 30 членів.

Практичний спосіб для знаходження найбільшого спільного дільника – алгоритм Евкліда.

Лема 1 Нехай $a, b, q, r \in \mathbb{Z}$. Якщо $a = bq + r$, то $\gcd(a, b) = \gcd(b, r)$.

Доведення.

Дійсно, нехай $d = \gcd(a, b)$ і $d' = \gcd(b, r)$. З одного боку, $a \vdots d$, $b \vdots d$, звідки $(a - bq) = r \vdots d$, і з означення $d' = \gcd(b, r)$ випливає, що $d' \vdots d$. Крім того, $b \vdots d'$, $r \vdots d'$, звідки $bq + r = a \vdots d'$, і з означення $d = \gcd(a, b)$ слід, що $d \vdots d'$. Ми отримали, що $d' \vdots d$ і $d \vdots d'$; це означає, що $d = \pm d'$, і тому $\gcd(a, b) = \gcd(b, r)$.

Нехай $a, b \in \mathbb{Z}$. Потрібно знайти $\gcd(a, b)$. Зауважимо, що $\gcd(a, b) = \gcd(|a|, |b|)$, тому можна вважати, що $a, b \in \mathbb{N}$. Якщо одне з чисел a, b дорівнює 0, мета досягнута. Інакше нехай для визначеності $a \geq b > 0$. Ділимо з залишком a на b: $a = bq_0 + r_0$. Застосуємо до пари (b, r_0) ту ж операцію (тепер ми знаємо, що $b > r_0$): $b = r_0 q_1 + r_1$ і так далі: $r_0 = r_1 q_2 + r_2$, ... У нас виникає монотонно спадний ряд чисел

$$a \geq b > r_0 > r_1 > ... , \qquad (1.1)$$

члени якого визначаються послідовно за допомогою ділення з остачею. Отже, процес колись зупиниться (остача стане дорівнювати нулю). Ми стверджуємо, що останній ненульовий залишок в цьому ланцюжку дорівнює $\gcd(a, b)$.

Теорема 2 Остання ненульова остача r_k з послідовності остач (1.1) є найбільшим спільним дільником чисел a і b.

Доведення.

Використовуючи лему 1.1 і правило побудови послідовності (1.1), отримуємо ланцюжок рівностей

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{k-1}, r_k) = r_k.$$

Метод обчислення $\gcd(a, b)$, який випливає з теореми 1.3, називається *алгоритмом Евкліда*.

Більш того, алгоритм Евкліда дозволяє знаходити і лінійне представлення НСД. Дійсно, в кінці алгоритму ми приходимо до пари $(d, 0)$ і лінійне представлення очевидно: $d = d \cdot 1 + 0 \cdot 0$. На кожному кроці ми переходимо від пари (a, b) до пари (b, r), де $a = bq + r$; якщо ми вже знаємо, що $d = bx' + ry'$, то, підставляючи $r = a - bq$, маємо $d = bx' + (a - bq)y' = ay' + b(x' - qy')$.

Приклад 2 Обчислити найбільший спільний дільник чисел:

а) 9367 і 4318;

б) 525 і 231.

Розв'язання.

а) застосуємо алгоритм Евкліда:

$$9367 = 2 \cdot 4318 + 731,$$
$$4318 = 5 \cdot 731 + 663,$$
$$731 = 1 \cdot 663 + 68,$$
$$663 = 9 \cdot 68 + 51,$$
$$68 = 1 \cdot 51 + 17,$$
$$51 = 3 \cdot 17 + 0.$$

Остання ненульова остача дорівнює 17, тому $\gcd(9367, 4318) = 17$.

б) застосуємо алгоритм Евкліда:

$$525 = 231 \cdot 2 + 63,$$
$$63 = 42 \cdot 1 + 21,$$
$$42 = 21 \cdot 2 + 0.$$

Отже $\gcd(525, 231) = 21$.

Відповідь. а) 17; б) 21.

Приклад 3 Один майстер робить на довгій стрічці позначки чинім роівцес через кожні 25 см, а другий – червоним через кожні 36 см, починаючи з одного й того самого місця. Чи може яка-небудь синя позначка виявитися на відстані 1 см від якої-небудь червоної?

Розв'язання.

Нехай x і y – кількість позначок, зроблених першим і лруним майстрами відповідно. Відповідь на запитання задачі буде ствердною, якщо рівняння $25x - 36y = 1$ матиме розв'язок у натуральних числах.

Застосуємо алгоритм Евкліда до чисел 36 і 25:

$$36 = 25 \cdot 1 + 11,$$
$$25 = 11 \cdot 2 + 3,$$
$$11 = 3 \cdot 3 + 2,$$
$$3 = 2 \cdot 1 + 1.$$

Перепишемо ці рівності наступним чином:

$$11 = 36 - 25 \cdot 1,$$
$$3 = 25 - 11 \cdot 2,$$
$$2 = 11 - 3 \cdot 3,$$
$$1 = 3 - 2 \cdot 1.$$

Звідси

$$1 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11 = 4 \cdot (25 - 11 \cdot 2) - 11 = 4 \cdot 25 - 9 \cdot 11 =$$
$$= 4 \cdot 25 - 9 \cdot (36 - 25 \cdot 1) = 13 \cdot 25 - 9 \cdot 36.$$

Отже, $13 \cdot 25 - 9 \cdot 36 = 1$, тобто пара $(13; 9)$ є розв'язком рівняння $25x - 36y = 1$.

Відповідь: може.

Приклад 4 Зобразити найбільший спільний дільник чисел 9367 і 4318 у вигляді лінійної комбінації цих чисел.

Розв'язання.

Скористаємось ланцюжком рівностей з розв'язання приклада 1.16а. Будемо мати:

$$17 = 1 \cdot 68 - 1 \cdot 51 = 1 \cdot 68 - 1 \cdot (1 \cdot 663 - 9 \cdot 68) = 10 \cdot 68 - 1 \cdot 663 =$$
$$10 \cdot (1 \cdot 731 - 1 \cdot 663) - 1 \cdot 663 = 10 \cdot 731 - 11 \cdot 663 =$$
$$= 10 \cdot 731 - 11 \cdot (1 \cdot 4318 - 5 \cdot 731) = 65 \cdot 731 - 11 \cdot 4318 =$$
$$= 65 \cdot (9367 - 2 \cdot 4318) - 11 \cdot 4318 = 65 \cdot 9367 - 141 \cdot 4318.$$

Відповідь: $\gcd(9367, 4318) = 17 = 65 \cdot 9367 - 141 \cdot 4318.$

Твердження 1 (властивості НСД)

1) $\gcd(x, y) = x$ тоді й тільки тоді, коли $y \vdots x$;

2) $\gcd(\gcd(x, y), z) = \gcd(x, \gcd(y, z)) = \gcd(x, y, z)$;

3) $\gcd(zx, zy) = z \cdot \gcd(x, y)$;

4) якщо $x > y$, то $\gcd(x, y) = \gcd(x - y, y)$.

Доведення.

1) Якщо $\gcd(x, y) = x$, то $y \vdots x$ за визначенням. Назад, нехай $y \vdots x$, тоді x – загальний дільник x і y, і якщо d' – якийсь спільний дільник x, y, то, зокрема, $x \vdots d'$. Отже, $\gcd(x, y) = x$.

2) Будь-який спільний дільник $\gcd(x, y)$ і z є спільним дільником x, y і z; то ж можна сказати про будь-який спільний дільник x і $\gcd(y, z)$.

3) Якщо $z = 0$, то і зліва, і справа стоїть 0; доводити нічого. Нехай $\gcd(x, y) = d$; $x \vdots d$, $y \vdots d$, звідки $zx \vdots zd$ і $zy \vdots zd$; тому $\gcd(zx, zy) \vdots zd$. Назад,

очевидно, що $zx \vdots z$, $zy \vdots z$, тому $\gcd(zx, zy) \vdots z$. Запишемо $\gcd(zx, zy) = zc$ для деякого c. Отже, $zx \vdots zc$, $zy \vdots zc$, звідки після скорочення (з урахуванням того, що $z \neq 0$) отримуємо $x \vdots c$ і $y \vdots c$. Тому $\gcd(x, y) = d \vdots c$, звідки $zd \vdots zc$, тобто, $zd \vdots \gcd(zx, zy)$

4) Нехай $x \vdots d$ і $y \vdots d$, тоді $(x - y) \vdots d$. Нехай $(x - y) \vdots d_1$ і $y \vdots d_1$, тоді $x \vdots d_1$. Маємо, що будь-який спільний дільник чисел x і y є спільним дільником чисел $(x - y)$ і y. І навпаки, будь-який спільний дільник чисел $(x - y)$ і y є спільним дільником чисел x і y. Отже, множина спільних дільників чисел x і y збігається з множиною спільних дільників чисел $(x - y)$ і y. Звідси $\gcd(x, y) = \gcd(x - y, y)$.

Приклад 5 Знайдіть $\gcd(6n + 3, 3n)$.

Розв'язання.

Скористаємось властивістю 4 НСД. Будемо мати:

$$\gcd(6n + 3, 3n) = \gcd(6n + 3 - 3n, 3n) = \gcd(3n + 3, 3n) =$$
$$= \gcd(3n + 3 - 3n, 3n) = \gcd(3, 3n) = 3.$$

Відповідь. 3.

Числа a і b називаються *взаємно простими*, якщо $\gcd(a, b) = 1$. Позначення: $a \perp b$.

Теорема 3 (критерій взаємної простоти двох чисел) Числа a і b взаємно простими тоді й лише тоді, коли можна підібрати такі цілі числа u_0, v_0, що $au_0 + bv_0 = 1$.

Доведення.

Якщо $a \perp b$, то $1 = au_0 + bv_0$ – лінійне представлення НСД. Навпаки, якщо $au_0 + bv_0 = 1$ і $d = \gcd(a, b)$, то $d \mid au_0$, $d \mid bv_0$, звідки $d \mid au_0 + bv_0 = 1$ і $d = 1$.

Твердження 2 (властивості взаємної простоти) Нехай a, b, c – деякі цілі числа.

1) якщо $a \perp b$ і $a \perp c$, то $a \perp bc$;
2) якщо $c \mid ab$ і $a \perp c$, то $c \mid b$;
3) якщо $b_1 \mid a$, $b_2 \mid a$ і $b_1 \perp b_2$, то $b_1 b_2 \mid a$.

Доведення.

1) $\gcd(a, bc) = \gcd(\gcd(a, ac), bc) = \gcd(a, \gcd(ac, bc)) =$
$$= \gcd(a, c \cdot \gcd(a, b)) = \gcd(a, c) = 1;$$

2) запишемо $au_0 + cv_0 = 1$ і помножимо на b: $abu_0 + cbv_0 = b$. Ми знаємо, що $c \mid ab$, тому $c \mid abu_0$. Крім того, очевидно, що $c \mid cbv_0$. Тому c ділить і їх суму $abu_0 + cbv_0 = b$;

3) $a = b_1 k$ ділиться на b_2, $b_1 \perp b_2$, за попередньою властивістю k ділиться на b_2: $k = b_2 l$, звідки $a = b_1 k = b_1 b_2 l$.

Твердження 3 Якщо $d=\gcd(a,b)$ і $a=a_0d$, $b=b_0d$, то числа a_0 і b_0 взаємно прості.

Доведення.

Зобразимо d у вигляді $d=au_0+bv_0=aa_0d+bb_0d$. Тоді після скорочення на d матимемо: $1=aa_0+bb_0$. Отже, за критерієм взаємної простоти чисел, $\gcd(a_0,b_0)=1$.

Приклад 6 Розв'яжіть у натуральних числах рівняння $x(y-1)^2=8y$.

Розв'язання.

Очевидно, що $y\neq1$. Оскільки ліва частина рівняння кратна $y-1$, то й права частина кратна $y-1$. Знайдемо НСД y і $y-1$:

$$\gcd(y,y-1)=\gcd(y-y+1,y-1)=\gcd(1,y-1)=1.$$

Отже, $y\perp y-1$. Тоді повинно $8\vdots(y-1)^2$. Звідси $(y-1)^2=1$ або $(y-1)^2=4$. З урахуванням того, що $y\in\mathbb{N}$, отримуємо: $y=2$ або $y=3$. Далі: $x=16$ або $x=6$.

Відповідь. $(16;2)$, $(6;3)$.

Нехай $a,b\in\mathbb{Z}$. Ціле число m називається *найменшим спільним кратним* (*НСК*) чисел a і b, якщо

- $m\vdots a$ і $m\vdots b$;
- якщо $n\vdots a$ і $n\vdots b$, то $n\vdots m$.

Позначення: $m=\text{НСК}(a,b)$ або $m=\text{gcm}(a,b)$ або $m=[a,b]$.

Як і для двоїстого поняття найбільшого спільного дільника, слово «найменше» у словосполученні «найменше спільне кратне» розуміється в сенсі подільності, а не величини: це кратне мусить бути дільником будь-якого іншого кратного чисел a і b.

Поняття найменшого спільного кратного легко узагальнюється на довільну скінченну кількість чисел, а саме: m називається найменшим спільним кратним чисел $a_1,a_2,\ldots,a_n$, якщо m задовольняє такі умови:

- $m\vdots a_1, m\vdots a_2, \ldots, m\vdots a_n$;
- якщо $n\vdots a_1, n\vdots a_2, \ldots, n\vdots a_n$, то $n\vdots m$.

Зауважимо, що задача знаходження найменшого спільного знаменника кількох дробів, яка постійно виникає при додаванні чи відніманні дробів, є не що інше як обчислення найменшого спільного кратного знаменників цих дробів.

Теорема 4 Якщо $a\vdots c$ і $b\vdots c$, то $\text{gcm}(a,b)=\dfrac{ab}{c}$.

Доведення.

Якщо $a\vdots c$ і $b\vdots c$, то $a=cn$ і $b=cm$. Тоді $\dfrac{ab}{c}=\dfrac{cncm}{c}=cmn=am=bn$, отже $\dfrac{ab}{c}=\text{gcm}(a,b)$.

Теорема 5 Для натуральних чисел a і b: $\operatorname{gcm}(a,b)=\dfrac{ab}{\gcd(a,b)}$.

Доведення.

Нехай $d=\gcd(a,b)$. Тоді $a=a_0d$, $b=b_0d$ і $\dfrac{ab}{\gcd(a,b)}=a_0b_0d$. Очевидно, що $m=a_0b_0d=b_0a=a_0b$ є спільним кратним чисел a і b.

Нехай тепер M – деяке спільне кратне чисел a і b. Тоді $M=aa_1=bb_1$. За твердженням 1.4 $\gcd(a_0,b_0)=1$, а тому існують такі числа k,l, що $1=ka_0+lb_0$. Помножимо обидві частини цієї рівності на M, матимемо:

$$M=ka_0M+lb_0M=ka_0bb_1+lb_0aa_1=kmb_1+lma_1=m(kb_1+la_1).$$

Отже, $M\vdots m$.

Приклад 7 Обчислити найменше спільне кратне чисел 9367 і 4318.

Розв'язання.

Застосуємо формулу з теореми 1.9 та результат прикладу 1.16а: $\gcd(9367,4318)=17$:

$$\operatorname{gcm}(a,b)=\frac{9367\cdot 4318}{17}=2379218.$$

Відповідь. 2379218.

Приклад 8 Доведіть, що $\forall n\in\mathbb{N}\ \left(n^3-n\right)\vdots 6$.

Доведення.

Маємо $n^3-n=n(n-1)(n+1)$. Оскільки з двох послідовних натуральних чисел одне кратне 2, а з трьох послідовних натуральних чисел одне кратне 3, то $\left(n^3-n\right)\vdots(2\cdot 3)$, тобто $\left(n^3-n\right)\vdots 6$.

Приклад 9 Доведіть, що коли $a\equiv b(\bmod m)$, $a\vdots n$, $b\vdots n$, $m\perp n$, то $\dfrac{a}{n}\equiv\dfrac{b}{n}(\bmod m)$.

Доведення.

Якщо $a\vdots n$, $b\vdots n$, то $a=nk_1$, $b=mk_2$ і $a\equiv b(\bmod m)$, тоді $a-b=n(k_1-k_2)\vdots m$. Оскільки $m\perp n$, то $(k_1-k_2)\vdots m$, тобто $k_1\equiv k_2(\bmod m)$. Звідси $\dfrac{a}{n}\equiv\dfrac{b}{n}(\bmod m)$.