

**Міністерство освіти і науки України
Дніпровський національний університет імені Олеся Гончара**

Кафедра математичного аналізу і теорії функцій

А.М. Пасько

**ПОДІЛЬНІСТЬ ЦІЛИХ ЧИСЕЛ І ПОВ'ЯЗАНІ З НЕЮ
ЗАДАЧІ**

**Дніпро
2019**

У посібник уміщено основну теорему арифметики (про розклад цілих чисел на прості множники), ретельно доведену на елементарному, доступному для школярів рівні. Розглянуто алгоритм Евкліда пошуку найбільшого спільного дільника, і метод розв'язання лінійних діофантових рівнянь, що ґрунтується на цьому алгоритмі. В кінці посібника міститься низка цікавих задач на цілі числа, розв'язання яких передбачає застосування різних властивостей цілих чисел, пов'язаних із подільністю. Посібник може бути використано як у середній школі, як джерело матеріалу для факультативних занять із математики, так і у вищих навчальних закладах, у процесі підготовки студентів – майбутніх педагогів.

Рекомендовано до друку Вченою радою
механіко-математичного факультету (протокол № 5 від 22 січня 2019 р.)

Рецензенти:

С. Б. Вакарчук, доктор фіз.-мат. наук, професор кафедри економіки і моделювання бізнес-процесів університету імені Альфреда Нобеля;

Я. С. Бондаренко, кандидат фіз.-мат. наук, доцент кафедри статистики й теорії ймовірностей Дніпровського національного університету імені Олеся Гончара.

Подільність цілих чисел і пов'язані
з нею задачі

Автор: канд. фіз.-мат. наук, доц. А. М. Пасько,

© Пасько А.М. 2019

Вступ

З давніх-давен питання, пов'язані з подільністю цілих чисел, знаходяться в центрі уваги вчених – математиків. Зокрема, вже давні греки розрізняли натуральні числа на прості та складені. «Начала» Евкліда містять один із найкрасивіших математичних фактів – так звану основну теорему арифметики про розклад будь-якого натурального числа на прості множники. Ця теорема широко використовується, зокрема для відомих «шкільних» методів одержання найбільшого спільного дільника і найменшого спільного кратного. Утім, попри свою важливість і таке широке використання, сама основна теорема арифметики, та методи пошуку найбільшого спільного дільника і найменшого спільного кратного, зі зрозумілих причин, лишаються, в курсі шкільної математики, доволі слабо (або взагалі не) обґрунтованими. Запропонований посібник покликаний частково компенсувати цю ваду. Він містить у собі детальне обґрунтування основної теореми арифметики та деяких інших питань, пов'язаних із подільністю цілих чисел. В кінці посібника міститься низка цікавих задач на цілі числа, розв'язання яких передбачає застосування різних властивостей цілих чисел, пов'язаних із подільністю. Посібник може бути використано як у середній школі, як джерело матеріалу для факультативних занять із математики, так і у вищих навчальних закладах, у процесі підготовки студентів – майбутніх педагогів.

§1. Найбільший спільний дільник

Безліч властивостей цілих чисел випливає з можливості виконувати над цілими числами операцію **ділення з остачею**. Нехай $a \text{ і } b$ — цілі числа і $b \neq 0$. Тоді існують такі цілі числа $q \text{ і } r$, при чому $0 \leq |r| < b$, що

$$a = q \cdot b + r. \quad (1)$$

Число q при цьому називають **часткою**, а r — **остачею** від ділення a на b . Рівність $r = 0$ у співвідношенні (1) рівносильна тому, що число a ділиться на b . Цей факт записують у вигляді $b|a$ (запис $b|a$ зручно читати як «число b ділить число a »).

Якщо $a \text{ і } b$ — два ненульових цілих числа, і число c таке, що $c|a$ і $c|b$, то c називається **спільним дільником** чисел $a \text{ і } b$. Зазначимо, що довільні два числа завжди мають спільний дільник; такими є числа 1 і -1 . Якщо інших спільних дільників немає, то числа $a \text{ і } b$ називаються **взаємно простими**.

Число називається **найбільшим спільним дільником** чисел $a \text{ і } b$ (НСД), якщо: 1) $a \text{ і } b$ є спільним дільником чисел $a \text{ і } b$ і 2) ділиться на довільний інший спільний дільник чисел $a \text{ і } b$.

Безпосередньо з означення НСД не впливає навіть факт його існування для будь-якої пари цілих чисел. Звісно, цей факт широко відомий, відомий зі школи навіть алгоритм пошуку НСД. Але, якщо ретельно проаналізувати цей алгоритм, виявиться, що він спирається на основну теорему арифметики, яку нам іще належить довести. Тож, насамперед, обґрунтування потребує сам факт існування НСД цілих чисел $a \text{ і } b$.

Поряд із числами $a \text{ і } b$ розглянемо всі можливі числа вигляду

$$v = xa + yb \quad (2)$$

де $x \text{ і } y$ — довільні цілі коефіцієнти. Числа такого вигляду ми називатимемо **лінійними комбінаціями** чисел $a \text{ і } b$.

Теорема 1. Для будь-якої пари ненульових цілих чисел $a \text{ і } b$, їх НСД існує і є їх лінійною комбінацією.

Доведення. Позначимо множину лінійних комбінацій чисел $a \text{ і } b$ через M . Зазначимо, що множина M містить, зокрема, і самі числа a (для $y = 0, x = 1$) і b (для $x = 0, y = 1$), а також число 0 ($x = 0, y = 0$). Всі числа v з множини M є, очевидно, цілими числами. Якщо v належить M , то і $-v$ також належить M (якщо $v = xa + yb$, то $-v = (-x)a + (-y)b$). Зауважимо ще одну властивість чисел v із M , яке нам зразу знадобиться: всі такі числа діляться на всі спільні дільники чисел $a \text{ і } b$. Дійсно, якщо $c|a$ і $c|b$, і, скажемо, $a = a'c$ і $b = b'c$, то $v = xa + yb = xa'c + yb'c = (xa' + yb')c$, тобто $c|v$. Нехай тепер $d \neq 0$ — найменше по модулю число серед усіх ненульових чисел M . Ми покажемо, що d і є НСД чисел $a \text{ і } b$. Властивість 2) означення НСД воно задовольняє, оскільки її за-

довольняють усі числа з M . Потрібно тільки ще встановити, що воно задовольняє і властивість 1), тобто d – спільний дільник чисел a і b . Покажемо, що $d|a$. Оскільки d належить M , то його можна подати у вигляді $d = sa + tb$, де s і t – цілі числа. Поділимо a на d з остачею, тобто знайдемо такі числа q і r , $|r| < |d|$, що $a = qd + r$.

Але тоді і остача r повинна належати множині M . Дійсно, $r = a - qd = a - q(sa + tb) = (1 - qs)a - qtb$.

Згадаймо тепер, що $|r|$ найменше за модулем серед ненульових чисел множини M , а число $|r|$ менше $|d|$. Тоді $r = 0$. Дослівно також доводиться подільність $d|a$. Теорему доведено.

Виникає питання: чи визначений НСД чисел a і b однозначно? Відповідь, звичайно, негативна, якщо число d задовольняє властивості 1) і 2) означення НСД, то і $-d$ також їх задовольняє. Та цим уся неоднозначність і вичерпується. Дійсно, нехай d і d' – два НСД чисел a і b . Оскільки d задовольняє властивість 2), а d' – властивість 1), то $d'|d$. Але, аналогічно, $d|d'$. Отже, $\alpha = \frac{d}{d'}$ і $\frac{d'}{d} = \frac{1}{\alpha} = \frac{1}{\alpha}$ – цілі числа. Але єдині цілі числа, обернені до яких також цілі, – це числа 1 і -1 . Отже, $\alpha = 1$ або $\alpha = -1$, звідки $d' = d$ або $d' = -d$. Якби ми в означенні НСД затребували, щоб це число було додатне, то можна було б сказати, що НСД двох ненульових цілих чисел існує і однозначно визначений.

Далі ми позначатимемо НСД чисел a і b через (a, b) .

Перейдемо до розгляду пар взаємно простих чисел. Ми вже зустрічались з цим поняттям. Повторимо його означення.

Цілі числа $a \neq 0$ і $b \neq 0$ називаються взаємно простими, якщо вони не мають спільних дільників, відмінних від 1 та -1 , тобто їх НСД дорівнює 1.

Із теореми 1 випливає, що якщо $(a, b) = 1$, то 1 можна подати у вигляді

$$1 = sa + tb \quad (3)$$

з належними цілими числами s і t . Навпаки, якщо рівність (3) виконується для деяких s і t , то a і b взаємно прості. Дійсно (див. доведення теореми 1), $d = (a, b)$ – це найменше по модулю число серед чисел які не дорівнюють нулю вигляду $xa + yb$. Значить, якщо (3) виконується, то $|d| \leq 1$ і $d \neq 0$, тож $d = \pm 1$.

Це спостереження дозволяє довести теорему.

Теорема 2. Якщо $a|bc$ і $(a, b) = 1$, то $a|c$.

Доведення. Оскільки $(a, b) = 1$, то знайдуться такі числа s і t , що

$$1 = sa + tb. \quad (4)$$

Помножимо рівність (4) на c . Маємо

$$c = (sc)a + t(bc).$$

Обидва доданки в правій частині діляться на a , отже, c ділиться на a . Теорему доведено.

Нам іще знадобиться таке твердження.

Теорема 3. Якщо число a взаємно просте з числами b і c , то воно взаємно просте з добутком bc .

Доведення. Оскільки $(a, b) = 1$, то знайдуться цілі числа s і t , які задовольняють рівність

$$1 = sa + tb.$$

Аналогічно, оскільки $(a, c) = 1$, то

$$1 = ua + vc$$

для належних u і v . Перемноживши почленно ці дві рівності, отримаємо

$$\begin{aligned} 1 &= (sa + tb)(ua + vc) = \\ &= sua^2 + savc + tbua + tbvc = \\ &= (sua + svc + tbu)a + (tv) \cdot (bc). \end{aligned}$$

Позначимо $m = sua + svc + tbu$ і $n = tv$, тоді m і n – цілі числа й

$$1 = ma + n(bc),$$

і це показує, що a і bc взаємно прості.

Методом індукції твердження теореми 3 легко узагальнюється на довільне число співмножників.

Теорема 4. Якщо a взаємно просте з числами $b_1, b_2, \dots, b_k$, то a взаємно просте з добутком $b_1 \cdot b_2 \cdot \dots \cdot b_k$.

§2. Розклад цілих чисел на прості множники

Простим числом називають будь-яке натуральне число, яке має рівно два різні натуральні дільники (одиницю і саме це число). Простими числами, отже є числа

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

Зауважимо, що одиниця, відповідно до цього означення, не є простим числом. Ненульові цілі числа, відмінні від ± 1 , що не є простими, називаються **складеними**.

Теорема 5. (Основна теорема арифметики) Будь-яке ненульове ціле число n можна подати у вигляді добутку

$$n = \pm p_1 \cdot p_2 \cdot \dots \cdot p_r \tag{1}$$

простих чисел $p_1, p_2, \dots, p_r$, причому такий розклад – однозначний із точністю до порядку множників.

Доведення. Очевидно, теорему достатньо довести для випадку додатного n . Для доведення теореми потрібно довести дві речі: існування розкладу (1) і його єдність.

Існування. Для доведення можливості такого розкладу для будь-якого натурального n скористаємось методом математичної індукції:

Базис індукції. Якщо $n = 1$, то сама рівність

$$n = 1$$

і є потрібне представлення: 1 є добутком порожньої множини простих чисел.

Крок індукції. Припустимо, що для всіх натуральних чисел m , менших за n , розкладність у добуток простих чисел уже встановлено. Доведемо тоді, що для числа n теж існуватиме такий розклад. Якщо n – просте число, то

$$n = n$$

i є шуканий розклад (один простий співмножник). Нехай n — число складене. Тоді воно є добутком $n = n_1 \cdot n_2$ двох цілих чисел n_1 і n_2 , кожне з яких відмінне від 1 і n і, отже, $n_1 < n$ і $n_2 < n$. Але тоді, відповідно до припущення індукції, розкладність чисел n_1 і n_2 у добуток простих чисел вже встановлено: якщо

$$n_1 = p_1 \cdot p_2 \cdot \dots \cdot p_r,$$

$$n_2 = q_1 \cdot q_2 \cdot \dots \cdot q_s,$$

де p_j і q_i — прості числа. Маємо $n = p_1 \cdot p_2 \cdot \dots \cdot p_r \cdot q_1 \cdot q_2 \cdot \dots \cdot q_s$, тобто ми отримали бажаний розклад числа n .

Єдиність. Зазначимо, що за самим означенням простого числа два різних простих числа взаємно прості. Доведення однозначності розкладу будемо вести індукцію за n .

Базис індукції. Якщо $n = 1$, то потрібний розклад

$$n = 1,$$

і має місце єдиність розкладу.

Крок індукції. Припустимо, що доказувана властивість вже встановлена для всіх чисел $m < n$. Нехай

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l$$

— два розклади числа n в добуток простих чисел $p_1, p_2, \dots, p_k$ і $q_1, q_2, \dots, q_l$ відповідно. Ми стверджуємо, що просте число p_k зустрічається серед простих чисел $q_1, q_2, \dots, q_l$. Дійсно, якби це було не так, тобто $p_k \neq q_i, i = 1, 2, \dots, l$, то p_k було б взаємно просте зі всіма числами q_i , а отже, відповідно до теореми 4 воно було б взаємно просте з їх добутком, тобто з числом n . Але це неможливо, бо $p_k | n$, p_k . Отже, p_k дорівнює якомусь із простих чисел q_i . Можна вважати, що $p_k = q_l$, оскільки в протилежному разі такої рівності можна було б добитися перестановкою співмножників q_i .

Отже, отримуємо:

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_{k-1} \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_{l-1} \cdot p_k,$$

звідки

$$m = \frac{n}{p_k} = p_1 \cdot p_2 \cdot \dots \cdot p_{k-1} = q_1 \cdot q_2 \cdot \dots \cdot q_{l-1}.$$

Але $m < n$ і, за припущенням індукції, для m твердження теореми вже доведено, тобто $k - 1 = l - 1$, послідовності $p_1, p_2, \dots, p_{k-1}$ і $q_1, q_2, \dots, q_{l-1}$ містять одні й ті самі прості числа, і відповідні прості числа зустрічаються в двох представленнях одне й те саме число разів, а оскільки $p_k = q_l$, то це ж слушно і для послідовностей $p_1, p_2, \dots, p_{k-1}, p_k$ і $q_1, q_2, \dots, q_{l-1}, q_l$. Теорему доведено.

§3. Алгоритм Евкліда пошуку найбільшого спільного дільника

Відомий зі школи алгоритм пошуку НСД передбачає розклад числа на прості множники. Зараз ми познайомимось із іншим методом знаходження найбільшо-

го спільного дільника, який носить назву **алгоритм Евкліда**. Нехай a, b – цілі числа. Для визначеності припустимо, що $|a| \geq |b|$.

Перший крок. Ділимо a на b з остачею:

$$a = q_1 \cdot b + r_1, \quad |r_1| < |b|. \quad (1)$$

Якщо $r_1 = 0$, то $b|a$ і $(a, b) = b$. Якщо $r_1 \neq 0$, і переходимо до наступного кроку.

Другий крок. Ділимо b на r_1 :

$$b = q_2 \cdot r_1 + r_2, \quad |r_2| < |r_1|. \quad (2)$$

Якщо $r_2 \neq 0$, то робимо

Третій крок.

$$r_1 = q_3 \cdot r_2 + r_3, \quad |r_3| < |r_2|. \quad (3)$$

і так далі. На кожному кроці нова остача менше остачі з попереднього кроку, $|b| > |r_1| > |r_2| > \dots$,

і на якомусь k -му кроці ($k < |b|$) остача дорівнюватиме нулю:

k -ий крок.

$$r_{k-2} = q_k \cdot r_{k-1}. \quad (k)$$

Покажемо, що остання ненульова остача r_{k-1} є шуканим (a, b) . Дійсно, ми маємо ланцюжок рівностей:

$$(1) \quad a = q_1 \cdot b + r_1,$$

$$(2) \quad b = q_2 \cdot r_1 + r_2,$$

$$(3) \quad r_1 = q_3 \cdot r_2 + r_3,$$

.....

$$(k-1) \quad r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-1},$$

$$(k) \quad r_{k-2} = q_k \cdot r_{k-1}.$$

Із останньої рівності маємо $r_{k-1}|r_{k-2}$, із передостанньої та $r_{k-1}|r_{k-2}$ випливає, що $r_{k-1}|r_{k-3}$. Із попередньої рівності аналогічно робимо висновок, що $r_{k-1}|r_{k-4}$ і, піднімаючись таким чином до все більш і більш ранньої рівності, робимо висновок, що $\dots, r_{k-1}|r_2, r_{k-1}|r_1, r_{k-1}|b, r_{k-1}|a$. Ми бачимо, що r_{k-1} – спільний дільник чисел a і b .

Нехай тепер $c|a$ і $c|b$. Тоді з (1), (2), ..., (k-1) послідовно отримаємо: $c|r_1, c|r_2, \dots, c|r_{k-1}$. Таким чином, r_{k-1} – справді НСД чисел a і b .

Розглянемо числовий приклад: $a = 858, b = 253$. Маємо:

$$(1) \quad 858 = 3 \cdot 253 + 99,$$

$$(2) \quad 253 = 2 \cdot 99 + 55,$$

$$(3) \quad 99 = 1 \cdot 55 + 44,$$

$$(4) \quad 55 = 1 \cdot 44 + 11,$$

$$(5) 44 = 4 \cdot 11,$$

звідки $(858, 253) = 11$.

Поряд із поняттям найбільшого спільного дільника часто зустрічається поняття найменшого спільного кратного. Нехай a, b – ненульові цілі числа. Ненульове число k називають **найменшим спільним кратним** (НСК) чисел a, b , якщо: 1) k є спільним кратним чисел a, b , тобто ділиться на кожне з цих чисел; 2) будь-яке інше спільне кратне цих чисел ділиться на k .

Теорема 6. Нехай a, b – ненульові цілі числа. Тоді їх найменше спільне кратне k існує і пов’язане з найбільшим спільним дільником d співвідношенням

$$k = \frac{ab}{d}.$$

Доведення. Нехай M – множина всіх відмінних від нуля спільних кратних чисел a, b . Множина $M \neq \emptyset$, оскільки містить у собі щонайменше одне число – добуток ab . Розглянемо довільне число $m \in M$. Оскільки m – кратне числа a , то $m = ah$ для деякого ненульового цілого h . Але також m – кратне числа b , тобто ah ділиться на b .

Оскільки $d = (a, b)$, то $a = a_1 d$, $b = b_1 d$. Якби a_1 та b_1 мали відмінний від ± 1 спільний дільник w , то можна було б записати

$$a = a_2 w d, \quad b = b_2 w d,$$

і a та b мали б спільний дільник wd , що входить у суперечність із означенням НСД. Отже, a_1, b_1 – взаємно прості.

Оскільки $ah = a_1 d h$ ділиться на $b = b_1 d$, то $a_1 h$ ділиться на b_1 . Числа a_1 і b_1 – взаємно прості, отже, за теоремою 2, h ділиться на b_1 . Запишемо число m як

$$m = ah = ab_1 \frac{h}{b_1} = a \frac{b}{d} \frac{h}{b_1} = \frac{ab}{d} \frac{h}{b_1}.$$

Оскільки $h \neq 0$ ділиться на b_1 , то $t = \frac{h}{b_1}$ – ціле ненульове число, отже

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

Таким чином, множина M має вигляд

$$M = \left\{ \frac{ab}{d} t : t = \pm 1, \pm 2, \pm 3, \dots \right\}.$$

Ясно, що всі числа множини M діляться на число $\frac{ab}{d}$, тобто $\frac{ab}{d} = k$ – найменшому спільному кратному чисел a, b . Теорему доведено.

Зауваження. З доведення теореми видно, що НСК двох цілих чисел визначено неоднозначно, якщо k дорівнює НСК чисел a і b , то протилежне число $-k$ – теж їх НСК. Але ця неоднозначність – рівно тією ж мірою, що неоднозначність НСД – з точністю до знаку. Рівність

$$k = \frac{ab}{d}$$

при цьому виконується окремо для додатних значень НСД та НСК, окремо – для від’ємних.

Алгоритм Евкліда та теорема 6 дозволяють знаходити НСК двох цілих чисел, оминаючи їх розклад на прості множники. Наприклад, вище ми знайшли, що $\text{НСД}(858, 253) = 11$, тоді, за теоремою 6 їх НСК дорівнює

$$k = \frac{858 \cdot 253}{11} = 19734.$$

Проілюструємо можливості алгоритму Евкліда на ще одному прикладі: знайти НСД та НСК чисел $a = -231$, $b = -140$. Очевидно, що для пошуку НСД та НСК двох цілих чисел можна замість самих цих чисел брати їх модулі. Застосуємо алгоритм Евкліда для пошуку $\text{НСД}(231, 140)$. Маємо ланцюжок рівностей:

$$231 = 140 \cdot 1 + 91;$$

$$140 = 91 \cdot 1 + 49;$$

$$91 = 49 \cdot 1 + 42;$$

$$49 = 42 \cdot 1 + 7 \text{ і}$$

$$42 = 7 \cdot 6.$$

Бачимо, що остання ненульова остача дорівнює 7, тобто $\text{НСД}(231, 140) = 7$.

Тепер, відповідно до теореми 6

$$\text{НСК}(231, 140) = \frac{231 \cdot 140}{7} = 4620.$$

Наведемо ще одну теорему, корисну для відшукування НСД.

Теорема 7. Нехай a, b – ненульові цілі числа. Тоді $(a, b) = (a, a - b)$.

Доведення. Зазначимо, що будь-який спільний дільник чисел a, b є спільним дільником чисел $a, a - b$. Навпаки, будь-який спільний дільник чисел $a, a - b$ є спільним дільником чисел a та $b = a - (a - b)$. Отже, множина спільних дільників чисел a, b збігається з множиною спільних дільників чисел $a, a - b$. А значить і найбільші спільні дільники цих двох пар чисел збігаються. Теорему доведено.

Проілюструємо цю теорему, знайшовши НСД чисел 517, 141. Послідовно застосовуючи до цих чисел теорему 7, одержуємо:

$$(517, 141) = (517 - 141, 141) = (376, 141) = (376 - 141, 141) = (235, 141) = (235 - 141, 141) = (94, 141) = (94, 141 - 94) = (94, 47) = (94 - 47, 47) = (47, 47) = 47.$$

§4. Алгоритм Евкліда і лінійні діофантові рівняння з двома змінними

В теоремі 1 ми встановили, що $(a, b) = d$ можна подати у вигляді $d = s \cdot a + t \cdot b$,

але доведення не мало жодної вказівки на те, як знайти відповідні числа s і t . За допомогою алгоритму Евкліда ця задача розв’язується дуже просто. Ми не будемо

описувати процедури в загальному випадку, а пояснимо її на вже розібраному числовому прикладі.

Отже, потрібно знайти такі цілі числа s і t , що

$$11 = s \cdot 858 + t \cdot 253.$$

Випишемо ще раз послідовність викладок алгоритму Евкліда, за допомогою яких ми знайшли НСД цих чисел:

$$(1) 858 = 3 \cdot 253 + 99,$$

$$(2) 253 = 2 \cdot 99 + 55,$$

$$(3) 99 = 1 \cdot 55 + 44,$$

$$(4) 55 = 1 \cdot 44 + 11,$$

$$(5) 44 = 4 \cdot 11,$$

Із (4), (3), (2), (1) послідовно одержуємо:

$$11 = 55 + (-1) \cdot 44,$$

$$44 = 99 + (-1) \cdot 55,$$

$$55 = 253 + (-2) \cdot 99,$$

$$99 = 858 + (-3) \cdot 253.$$

Підставляючи, тепер, у перше з виписаних щойно рівностей вираз для 44 із другого, потім для 55 – вираз із наступної рівності і так далі, одержуємо:

$$\begin{aligned} 11 &= 55 + (-1) \cdot (99 + (-1) \cdot 55) = \\ &= 2 \cdot 55 + (-1) \cdot 99 = \\ &= 2 \cdot (253 + (-2) \cdot 99) + (-1) \cdot 99 = \\ &= 2 \cdot 253 + (-5) \cdot (858 + (-3) \cdot 253) = \\ &= (-5) \cdot 858 + 17 \cdot 253. \end{aligned}$$

Остаточно: $s = -5, t = 17$.

Читачу легко уяснити собі, як застосовується алгоритм в загальному випадку. Рівності ті, що виникають в алгоритмі Евкліда при знаходженні НСД чисел

a і b , дозволяють розв'язати в цілих числах рівняння вигляду

$$d = xa + yb,$$

(де $d = (a, b)$).

Взагалі, рівняння вигляду

$$xa + yb = c, \tag{1}$$

де a, b, c – заданні цілі числа, для якого шукаємо цілочисловий розв'язок x, y , називають **лінійним діофантовим рівнянням** з двома невідомими. Лінійним воно називається тому, що невідомі x і y входять у нього в першому степені. Термін «діофантове» вказує на те, що коефіцієнти рівняння – цілі числа і що розв'язки також шукають цілочислові.

Дослідимо питання про всі розв'язки рівняння (1). Зазначимо, спочатку, що не будь-яке рівняння такого вигляду має розв'язок. Дійсно, якщо рівняння (1) має розв'язок в цілих числах, скажімо, $x = x_0, y = y_0, c = x_0 a + y_0 b$, і якщо НСД цих

чисел $d = (a, b)$, то, оскільки $d|a, d|b$, число d ділить обидва множники в правій частині і, отже, також ділить c . Звідси робимо висновок, що для існування цілочислового розв'язку рівняння (1) необхідно, щоб права частина рівняння ділилась на НСД чисел a і b .

Наприклад, рівняння

$$9x + 15y = 7$$

розв'язку немає, оскільки 7 не ділиться на $3 = (9, 15)$. Навпаки, якщо $d|c$, то рівняння (1) має цілочисловий розв'язок, і ми навіть знаємо, як такий розв'язок знайти. Дійсно, нехай $c = c'd$, і нехай s і t — такі цілі числа (їх можна знайти за допомогою алгоритму Евкліда), що

$$d = as + bt.$$

Тоді

$$c = c'd = a(sc') + b(tc'),$$

тобто $x_0 = sc', y_0 = tc'$ — розв'язок рівняння (1).

Розв'яжемо, наприклад, діофантове рівняння

$$33 = 858x + 253y. \quad (2)$$

Вище ми показали, що

$$11 = 858 \cdot (-5) + 253 \cdot 17.$$

Умножаючи цю рівність почлено на 3, отримуємо

$$33 = 858 \cdot (-15) + 253 \cdot 51.$$

І так, $x = -15, y = 51$ — розв'язок рівняння (2). Не слід думати, що знайдений розв'язок єдиний. Взагалі, якщо діофантове рівняння вигляду (1) має бодай один розв'язок, то воно має безліч розв'язків. Дослідимо це питання більш детально: дамо доведення сформульованого твердження і знайдемо загальний вигляд всіх можливих розв'язків рівняння (1). Почнемо зі з'ясування загального вигляду.

Припустимо, що ми вже знаємо, що поряд з цілочисловими розв'язками x_0, y_0 рівняння (1) має ще розв'язок x_1, y_1 . Маємо:

$$c = ax_0 + by_0,$$

$$c = ax_1 + by_1.$$

Віднімаючи другу рівність із першої, одержуємо:

$$a(x_0 - x_1) + b(y_0 - y_1) = 0,$$

або

$$a(x_0 - x_1) = b(y_1 - y_0). \quad (3)$$

Для $d = (a, b)$ візьмемо $a' = \frac{a}{d}, b' = \frac{b}{d}$, тобто

$$a = a'd,$$

$$b = b'd,$$

де a' і b' — взаємно прості числа. Скорочуючи рівність (3) на d , приходимо до такої рівності

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Оскільки a', b' — взаємно прості, $a'|(y_1 - y_0)$ і, аналогічно, $b'|(x_0 - x_1)$. Узявши

$$y_1 - y_0 = a'k_1,$$

$$x_0 - x_1 = b'k_2,$$

маємо $a'b'k_1 = a'b'k_2$, звідки $k_1 = k_2 = k$. Таким чином, остаточно

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k, \quad (4)$$

$$x_1 = x_0 - b'k = x_0 - \frac{b}{d}k, \quad (5)$$

де k — деяке ціле число.

Навпаки, легко перевірити, що якщо x_0, y_0 — розв'язок рівняння (1), то всі пари чисел (4), (5) при цілих значеннях k дають розв'язки рівняння (1). Дійсно,

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 - \frac{b}{d}k\right) + b\left(y_0 + \frac{a}{d}k\right) = \\ &= ax_0 + by_0 + \left(-\frac{ab}{d}k + \frac{ab}{d}k\right) = \\ &= c + 0 = c. \end{aligned}$$

Отже, якщо x_0, y_0 — розв'язок рівняння (1), то всі числа вигляду $x_0 - \frac{b}{d}k, y_0 + \frac{a}{d}k$

є також розв'язками (значить, розв'язків, в будь-якому разі, безліч — по одному для кожного k) й інших розв'язків немає.

Для прикладу розв'яжемо ще одне діофантове рівняння.

$$45x - 37y = 25.$$

Оскільки НСД(45;37)=1, то рівняння має безліч розв'язків.

Щоб знайти (x_0, y_0) застосуємо алгоритм Евкліда:

$$\begin{aligned} 45 &= 37 \cdot 1 + 8; \\ 37 &= 8 \cdot 4 + 5; \\ 8 &= 5 \cdot 1 + 3; \\ 5 &= 3 \cdot 1 + 2; \\ 3 &= 2 \cdot 1 + 1. \end{aligned}$$

Отже $d = 1$. Запишемо алгоритм Евкліда в зворотному напрямку:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - 1(5 - 3 \cdot 1) = 3 - 5 + 3 \cdot 1 = 2 \cdot 3 - 5 = 2 \cdot (8 - 5 \cdot 1) - 5 = \\ &= 2 \cdot 8 - 2 \cdot 5 - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (37 - 8 \cdot 4) = 2 \cdot 8 - 3 \cdot 37 + 12 \cdot 8 = \\ &= 14 \cdot 8 - 3 \cdot 37 = 14 \cdot (45 - 37 \cdot 1) - 3 \cdot 37 = 14 \cdot 45 - 14 \cdot 37 - 3 \cdot 37 = \\ &= 45 \cdot 14 - 37 \cdot 17. \end{aligned}$$

Отже, $(14; 17)$ — частинний розв'язок рівняння $45x - 37y = 1$.

Тоді $25 = 45 \cdot (14 \cdot 25) - 37 \cdot (17 \cdot 25) = 45 \cdot 350 - 37 \cdot 425$. Тобто $(x_0, y_0) = (350; 425)$.

Отже всі розв'язки знайдемо за формулами

$$x = 350 + 37k; y = 425 + 45k, k \in \mathbb{Z}.$$

Відповідь: $x = 350 + 37k; y = 425 + 45k, k \in \mathbb{Z}$.

Задачі

1. Доведіть, що якщо p — просте число і $p > 3$, то $p^2 - 1$ ділиться на 24.

2. Доведіть, що якщо $a + b + c$ ділиться на 6, то $a^3 + b^3 + c^3$ ділиться на 6 (a, b, c — цілі числа).
3. Доведіть, що якщо $a^2 + b^2$ ділиться на 7, то $a^2 + b^2$ ділиться і на 49 (a і b — цілі числа).
4. Доведіть, що число $n^2 + 5n + 16$ ні при якому цілому n не ділиться на 169.
5. При яких цілих a обидва корені рівняння $x^2 + ax + 6 = 0$ є цілими числами?
6. Доведіть, що число N має непарне число дільників тоді й тільки тоді, коли N — точний квадрат.
7. Знайдіть кількість натуральних дільників числа $n = 1024$.
8. Знайдіть кількість натуральних дільників числа $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, де $p_1, p_2, \dots, p_m$ — різні прості числа.
9. Які остачі можуть давати точні квадрати при діленні на 3, на 4?
10. Чи може дискримінант квадратного рівняння з цілими коефіцієнтами дорівнювати 23?
11. Довжини всіх сторін прямокутного трикутника — цілі. Чи можуть довжини катетів бути непарними числами?
12. В десятичному записі 12-значного числа N цифри 2 і 9 зустрічаються по два рази, а останні — по одному разу. Чи може N бути точним квадратом?
13. В десяткового запису числа 300 одиниць і декілька нулів (а інших цифр немає). Може це число бути точним квадратом?
14. 1987-значне число a ділиться на 9. Сума цифр a — число b , сума цифр b — число c , сума цифр c — число d . Знайти d .
15. Розв'яжіть в цілих числах рівняння $3^x = 1 + y^2$.
16. Розв'яжіть в цілих числах рівняння $2^x + 1 = y^2$.
17. Розв'яжіть в цілих числах рівняння $x^2 - y^2 = 91$.
18. Розв'яжіть в цілих числах рівняння $x! + y! = (x + y)!$.
19. Розв'яжіть в цілих числах рівняння $1! + 2! + \dots + x! = y^2$.

Література

1. Валах В.Я. Подорож у світ цілих чисел. – К. «Рад. школа», 1978. – 102 с.
2. Виноградов И.М. Основы теории чисел. – Л.-М.: ОГИЗ, 1952. – 180 с.
3. Ивлев Б.М., Абрамов А.М., Дудницын Ю.П., Шварцбурд С.И. Задачи повышенной трудности по алгебре и началам анализа. М.: «Просвещение», 1990. – 48с.
4. Михелович Ш.Х. Теория чисел. – М.: «Высшая школа», 1967. – 336 с.
5. Калужнин Л. А. Основная теорема арифметики. – М.: «Наука», 1969. – 32 с.

Зміст

Вступ	3
§ 1. Найбільший спільний дільник.	4
§ 2. Розклад цілих чисел на прості множники.	6
§ 3. Алгоритм Евкліда пошуку найбільшого спільного дільника.	7
§ 4. Алгоритм Евкліда і лінійні діофантові рівняння з двома змінними.	10
Задачі	14

Подільність цілих чисел і пов'язані
з нею задачі

Автор:

Пасько Анатолій Миколайович

Підписано до друку	2019 р.	Формат 60×84/16.	Папір
Друк	. Ум. друк. арк.	Ум. фарбовідб.	
Обл.-вид. арк.	Тираж 30 пр.	Зам. №	
