ОСНОВИ ТЕОРІЇ ЧИСЕЛ

з дисципліни «Дискретна математика»
Виконала
студентка 311-КІ-19 групи
Овсянецька Віра

План

1. Властивості простих чисел.
   1.1. Прості властивості ділимості.
   1.2. Основні властивості НСД цілих чисел.
   1.3. Основні властивості НСК цілих чисел.
   1.4. Основні властивості взаємно простих чисел.
   1.5. Алгоритм Евкліда.
2. Числові послідовності.
   2.1. Обмежені і необмежені послідовності.
   2.2. Арифметична прогресія.
   2.3. Властивості арифметичної прогресії.
   2.4. Геометрична прогресія. Властивості геометричної прогресії.
   2.5. Ряд Фібоначчі. Властивості чисел ряду Фібоначчі.

1 Властивості простих чисел

Означення. Натуральне число називається **простим**, якщо воно ділиться тільк само на себе і на 1.

Означення. Натуральне число називається **складеним**, якщо воно має дільника, відмінного від самого себе і 1;

Число 1 не вважається ні простим, ні складеним. Це пов'язано з тим, що 1 є так званим *оборотним елементом* множини цілих чисел, тобто будь-яке число можна поділити на 1, а прості числа цією властивістю не володіють.

Будь-яке натуральне число, відмінне від 1, можна подати як добуток простих співмножників, *причому* єдиним чином (з точністю до перестановки співмножників) - цей факт називається **основною теоремою арифметики**.

Разом з цими фактами слід пам'ятати і наступні.

Складені числа мають в своєму розкладі на прості множники хоча б два (не обов'язково різних) множники, а прості - рівно один множник; одиниця – не має множників взагалі.

Для будь-якого простого числа p і будь-якого натурального числа a існує цілий невід'ємний **степінь входження** p в розклад a, і він визначений однозначно. Якщо в розкладі a немає множника p, то степінь дорівнює 0. Якщо множник присутній - степінь входження дорівнює кількості простих множників, рівних p в розкладанні a. Позначається цей степінь входження через $v_p(a)$.

Два натуральних числа a і b рівні тоді і тільки тоді, коли $v_p(a) = v_p(b)$ для будь-якого простого p.

Іншими словами: два числа рівні тільки тоді, коли степені входження в них всіх простих множників однакові.

Якщо натуральне число $n = a \cdot b$ то для будь-якого простого p: $v_p(n) = v_p(a) + v_p(b)$.

Іншими словами: степінь входження будь-якого простого множника в число n дорівнює сумі його степенів входження в a і b. Дане твердження випливає з того, що розклад добутку чисел на прості множники є об'єднанням їх розкладів.

Число a ділиться на число b тільки тоді, коли будь-який простий множник входить в a в не меншій степені, ніж в b, тобто $v_p(a) \geq v_p(b)$ для будь-якого простого p. В інакшому випадку, якщо для якогось множника p ця умова не виконується, то при діленні утворюється дріб з множником p у знаменнику, який не знищується. Дана умова перевіряється тільки для простих множників, які входять в розклад b. Для тих, що не входять степінь входження буде рівний нулю $v_p(b) = 0$ що у будь-якому випадку не більше $v_p(a)$.

Означення. Число **a ділиться на b** (або b ділиться на a), якщо існує таке число c, що $a = b \cdot c$

При цьому число c називається **часткою від ділення** a на b.

Позначається: $a \vdots b$ (a ділиться на b) або $b | a$ (b ділить a).

Якщо a ділиться на b, і частку від ділення позначити за c, то $v_p(c) = v_p(a) - v_p(b)$ для будь-якого простого p.

Іншими словами: степінь входження будь-якого простого множника в число c дорівнює різниці його степенів входження в a і b.

Прості властивості ділимості

1. Якщо $a \vdots b$ і c – частка від ділення, то c – єдинне.

2. $a \vdots a$

3. Якщо $a \vdots b$ і $b \vdots c$ то $a \vdots c$

4. Якщо $a \vdots b$ і $b \vdots a$ то або $a = b$ або $a = -b$

5. Якщо $a \vdots b$ і $|b| > |a|$ то $a = 0$

6. Якщо $a \vdots b$ і $a \neq 0$ то $|a| \geq |b|$

7. Для того, щоб $a \vdots b$ необхідно і достатньо, щоб $|a| \vdots |b|$

8. Якщо $a_1 \vdots b$ $a_2 \vdots b$ $a_n \vdots b$ то $(a_1 \pm a_2 \pm \ldots \pm a_n) \vdots b$

Існують прості ознаки, які дозволяють визначити, чи ділиться число, наприклад, на 3, на 5, на 9 і.т.і.

1. Число ділиться на 3, якщо сума його цифр ділиться на 3.

2. Число ділиться на 5, якщо його остання цифра 5 або 0.

3. Число ділиться на 2, якщо на 2 ділиться його остання цифра.

4. Число ділиться на 9, якщо сума його цифр ділиться на 9.

<u>Теорема</u>. Множина простих чисел є нескінченною.

Доведення даної теореми проводиться від супротивного.

Нехай множина простих чисел є скінченною, і число p – найбільше просте число.

Розглянемо натуральне число n, яке є добутком всіх простих чисел, тобто $n = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p$

і додамо до цього числа 1: $n + 1 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p + 1$ Очевидно, що отримане число не ділиться на жодне число від 1 до p, звідси отримуємо, $n = 1$ Але відомо, що $n > 1$ Отримали протиріччя, яке виникло через те, що зробили неправильне припущення. Відповідно, множина простих чисел є нескінченною.

Таким чином, який б, за довжиною, ряд послідовних складених чисел не обирався у ряді натуральних чисел, за ним знайдеться ще нескінченна множина простих чисел.

Алгоритм виділення простих чисел у послідовності натуральних $2,\ldots,n$

(так званий решето Ератосфена) полягає в наступному.

1) Викреслюємо послідовно кожне друге число після 2. Перше незакреслене число 3 є простим.

2) Викреслюємо кожне третє число після 3. Перше незакреслене число 5 є простим.

3) Викреслюємо кожне п'яте число після 5 і т.д., доки не дійдемо до числа, яке більше $\sqrt{n}$

4) Всі числа, які лишаються не закресленими, є простими.

Найбільший спільний дільник (НСД) та найменше спільне кратне (НСК). Взаємно прості числа

<u>Означення</u>. **Спільним дільником** цілих чисел $a_1, a_2, \ldots, a_n$ називається будь-яке ціле число d, таке, що

$$a_1 \vdots d, \quad a_2 \vdots d, \quad a_3 \vdots d, \quad \ldots \quad a_n \vdots d.$$

<u>Приклад</u>. Числа 30, 165 мають спільними дільниками числа 3, -3, 15, -15.

<u>Означення</u>. **Найбільшим спільним дільником (НСД)** цілих чисел $a_1, a_2, \ldots, a_n$ називається такий їх додатній спільний дільник, який ділиться на будь-який інший спільний дільник цих чисел.

Позначення: якщо d є НСД чисел $a_1, a_2, \ldots, a_n$ то записується так: $(a_1, a_2, \ldots, a_n) = d$

Основні властивості НСД цілих чисел

1. $d > 0$
2. $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$
3. Якщо існує ціле число k, таке, що $k \mid a_1, k \mid a_2, \ldots, k \mid a_n$ то $k \mid d$

4. Для будь-яких цілих чисел $a_1, a_2, ..., a_n$ з яких хоча б одне не дорівнює нулю, існує НСД.

Виходячи з властивості 4 існує спосіб знаходження НСД, а саме:

1) спочатку розкласти кожне число на прості множники, записавши розклад у канонічній формі;

2) потім знайти добуток мінімальних степенів простих множників, які входять в розклади.

<u>Приклад</u>. Знайти НСД чисел 5775, 15246, 399. Розкладемо числа на прості множники:

$$5775 = 3 \cdot 5^2 \cdot 7 \cdot 11, \quad 15246 = 2 \cdot 3^2 \cdot 7 \cdot 11^2, \quad 399 = 3 \cdot 7 \cdot 19$$

Знайдемо добуток мінімальних степенів простих чисел, які входять в розклади: $d = 2^0 \cdot 3 \cdot 5^0 \cdot 7 \cdot 11^0 \cdot 19^0 = 27$

Таким чином $(5775, 15246, 399) = 27$

<u>Означення</u>. **Найменшим спільним кратним (НСК)** цілих чисел $a_1, a_2, ..., a_n$ називається найменше додатне яке ділиться на всі ці числа.

Позначення: якщо m є НСК чисел $\mathbf{a_1, a_2, ..., a_n}$ то записується так: $m = [a_1, a_2, ..., a_n]$

Основні властивості НСК цілих чисел

1. $m > 0$

2. $a_1 \vdots m, a_2 \vdots m, ..., a_n \vdots m$

3. Якщо $M > 0$ і $a_1 \vdots M, ..., a_n \vdots M$ то $m \le M$

<u>Означення</u>. Числа a і b називаються **взаємно простими**, якщо НСД цих чисел дорівнює 1.

Основні властивості взаємно простих чисел

1. Якщо a і p – цілі числа, причому p – просте, то або $a \vdots p$ або числа a і p взаємно прості.
2. НСК двох взаємно простих чисел дорівнює їх добутку.
3. Для того, щоб число a ділилось на взаємно прості числа b і c, необхідно і достатньо, щоб воно ділилось на їх добуток.
4. Якщо $a \cdot b \vdots c$ причому $(a, c) = 1$ то $b \vdots c$

Алгоритм Евкліда

Щоб знайти найбільший спільний дільник двох чисел, є дуже простий спосіб,

відомий під назвою **алгоритму Евкліда,** або **способу послідовного ділення**.

Алгоритм Евкліда полягає в наступному. Нехай дано натуральні числа *a* і *b,* $a > b$

1. Ділимо перше число на друге; дістанемо остачу $r_1 (r_1 < b)$
2. Тепер *b* поділимо на $r_2 (r_2 < r_1)$
3. Ділимо r_1 на r_2 і т. д.

Оскільки після кожного наступного кроку утворюється остача, менша від попередньої,

то через скінченну кількість кроків дістанемо остачу, яка дорівнює нулю: ділення відбудеться націло і процес зупиниться.

Остання відмінна від нуля остача r_k на яку націло ділиться остача r_{k-1} і буде найбільшим спільним дільником чисел *a* і *b*.

Запишемо сказане як ланцюжок рівностей:

$$\begin{aligned}
a &= bq + r_1, \\
b &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
&\vdots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k, \\
r_{k-1} &= r_k q_k.
\end{aligned}$$

З останньої рівності випливає, що r_k є дільником r_{k-1} $r_k = (r_k, r_{k-1})$ З передостанньої рівності випливає, що r_k ділить також r_{k-2} і $r_k = (r_{k-1}, r_{k-2})$ Так, послідовно піднімаючись кроками вгору, дістанемо, що $r_k = (a, b)$

Приклад. Знайти НСД чисел 9765 і 6944.

$$9765 = 6944 \cdot 1 + 2821,$$

$$6944 = 2821 \cdot 2 + 1302,$$

$$2821 = 1302 \cdot 2 + 217,$$

$$1302 = 217 \cdot 6.$$

Отже $(9765, 6944) = 217$

2. Числові послідовності

<u>Означення.</u> Якщо кожному натуральному числу n поставлено у відповідність число x_n

то говорять, що задана **послідовність** $x_1, x_2, ..., x_n = \{x_n\}$

Числа $x_1, x_2, ..., x_n$ називаються **членами послідовності**, а член з номером n - її n-им членом.

Спільний елемент послідовності є функцією від n.

$$x_n = f(n)$$

Таким чином послідовність може розглядатись як функція.

Задати послідовність можна різними способами – головне, щоб був вказаний спосіб отримання будь-якого члена послідовності.

<u>Приклад.</u> $\{x_n\} = \{(-1)^n\}$ або $\{x_n\} = -1;1;-1;1;...$

$$\{x_n\} = \{\frac{\sin \pi n}{2}\} \quad \text{або} \quad \{x_n\} = 1;0;1;0;...$$

Для послідовностей можна визначити наступні **операції**:

1) Множення послідовності на число m: $m\{x_n\} = \{mx_n\}$ тобто $mx_1, mx_2, ..., mx_n$

2) Додавання (віднімання) послідовностей: $\{x_n\} \pm \{y_n\} = \{x_n \pm y_n\}$

3) Множення послідовностей: $\{x_n\} \cdot \{y_n\} = \{x_n \cdot y_n\}$

4) Ділення послідовностей: $\dfrac{\{x_n\}}{\{y_n\}} = \left\{\dfrac{x_n}{y_n}\right\}$ при $\{y_n\} \neq 0$

Обмежені і необмежені послідовності

Означення. Послідовність $\{x_n\}$ називається **обмеженою**, якщо існує таке число $M > 0$ що для будь-якого n вірна нерівність:

$$|x_n| < M$$

тобто всі члени послідовності належать проміжку $(-M; M)$

Означення. Послідовність $\{x_n\}$ **називається обмеженою зверху, якщо для** будь-якого n існує таке число M, що

$$x_n \leq M$$

Означення. Послідовність $\{x_n\}$ називається **обмеженою знизу**, якщо для будь-якого n існує таке число M, що

$$x_n \geq M$$

Приклад. Послідовність $\{x_n\} = n$ – обмежена знизу $\{1, 2, 3, ...\}$

Означення. Число a називається **межею** послідовності $\{x_n\}$ якщо для будь-якого позитивного $\varepsilon > 0$ існує такий номер N, що для всіх $n > N$ виконується умова $|a - x_n| < \varepsilon$

$$\lim\{x_n\} = a$$

В цьому випадку говорять, що послідовність $\{x_n\}$ **сходиться** до a при $n \to \infty$

Якщо відкинути будь-яке число членів послідовності, то виходять нові послідовності, при цьому якщо сходиться одна з них, то сходиться і інша.

Приклад 1. Довести, що межа послідовності $\frac{(-1)^n}{n}$ дорівнює 0, тобто $\lim\left\{\frac{(-1)^n}{n}\right\} = 0$

Нехай при $n > N$ вірно $\left|0 - \frac{(-1)^n}{n}\right| < \varepsilon$ тобто $\frac{1}{n} < \varepsilon$ Це вірно при $n > \frac{1}{\varepsilon}$

таким чином, якщо за N взяти цілу частку від $\frac{1}{\varepsilon}$ то твердження, приведене вище, виконується.

Приклад 2. Показати, що при $n \to \infty$ послідовність $\left\{3, 2\frac{1}{2}, 2\frac{1}{3}, 2\frac{1}{4}, ..., 2 + \frac{1}{n}\right\}$ має межею число 2.

Результат: $\{x_n = 2 + \frac{1}{n};\ \frac{1}{n} = x_n - 2\}$ Очевидно, щ існує таке число n, що

$|x_n - 2| = \left|\frac{1}{n} < \varepsilon\right|$ тобто $\lim\{x_n\} = 2$

Теорема. Послідовність не може мати більш за одну межу.

Теорема. Якщо $x_n \to a$ то $|x_n| \to |a|$

Теорема. Якщо $x_n \to a$ то послідовність $\{x_n\}$ обмежена.

Слід зазначити, що зворотне твердження невірне, тобто через обмеженість послідовності не виходить її збіжність.

Приклад. Послідовність $x_n = \begin{cases} 1 + \frac{1}{n}, & \text{при парному } n \\ 2 - \frac{1}{n}, & \text{при непарному } n \end{cases}$ не має межі, хоча $|x_n| \le 2$

Арифметична прогресія

Означення. Числова послідовність $\{a_n\}$ кожен член якої, починаючи з другого, дорівнює попередньому, з доданим до нього одним і тим же числом d називається **арифметичною прогресією**.

Число d називається **різницею** арифметичної прогресії:

$$a_{n+1} = a_n + d \qquad (1)$$

Число a_1- називається **першим членом** арифметичної прогресії.

Арифметична прогресія **зростаюча**, якщо її різниця більше нуля $d > 0$

або **спадна** в протилежному випадку $d < 0$

Число S_n називається **сумою** n перших членів арифметичної прогресії:

$$S_n = \frac{a_1 + a_n}{2} \cdot n \qquad (2)$$

Властивості арифметичної прогресії

1. $a_n = a_1 + (n-1) \cdot d$

2. $a_n = \dfrac{a_{n-1} + a_{n+1}}{2}, \ \ \forall n > 1$

3. $S_n = \dfrac{2a_1 + d \cdot (n-1)}{2} \cdot n$

Геометрична прогресія

Означення. Числова послідовність $\{b_n\}$ перший член якої відмінний від нуля, а кожен член, починаючи з другого, дорівнює попередньому, помноженому на одне і те ж число $q \neq 0$ називається **геометричною прогресією**.

Число q називається **знаменником** прогресії:

$$b_{n+1} = b_n \cdot q \qquad (3)$$

Число b_1 - називається **першим членом** геометричної прогресії.

Число S_n називається **сумою** n перших членів геометричної прогресії.

$$S_n = \frac{b_1(q^n - 1)}{q - 1} \qquad (4)$$

Число P_n називається добутком n перших членів геометричної прогресії.

$$P_n = (a_1 \cdot a_n)^{\frac{n}{2}} \qquad (5)$$

Властивості геометричної прогресії

1. $b_n = b_1 \cdot q^{n-1}$
2. $b_n^2 = b_{n-1} \cdot b_{n+1}, \forall\ n > 1$
3. $S_n = \dfrac{b_n q - b_1}{q - 1}$
4. Якщо $|q| \le 1$ і послідовність нескінченна, тобто $n \to \infty$ то $S_n = \dfrac{b}{1 - |q|}$

Ряд Фібоначчі

1, 1, 2, 3, 5, 8, 13, 21, ...

Закон створення членів цієї послідовності дуже простий: перші два члени - одиниці,

а потім кожний наступний член дорівнює сумі двох попередніх.

Наприклад, 2=1+1, 3=1+2, 5=2+3, 8=3+5 і т. д.: 1, 1, 2, 3, 5, 8, 13, 21, ...

Будь-яка пара сусідніх чисел ряду Фібоначчі задовольняє одному з рівнянь

$$x^2 - xy - y^2 = 1$$

або

$$x^2 - xy - y^2 = -1$$

причому більше число є значенням невідомого x, а менше - значенням невідомого y.

Властивості чисел ряду Фібоначчі

1. Принцип створення членів цього ряду приводить до наступного співвідношення між будь-якими його трьома членами, які стоять поруч

S_{n-2}, S_{n-1}, S_n

$$S_n = S_{n-1`} + S_{n-2}$$

Ця формула дає можливість по перших двох членах ряду встановити його третій член,

по другому і третьому - четвертий, по третьому і четвертому - п'ятий і т. д.

2. Щоб відразу отримати будь-який член ряду s_n знаючи лише номер n

його місця, допомагають два ірраціональні числа $a_1 = \frac{1+\sqrt{5}}{2}$ та $a_2 = \frac{1-\sqrt{5}}{2}$

$$s_n = \frac{a_1^n - a_2^n}{\sqrt{5}}$$

3. Сума n перших членів ряду Фібоначчі на 1 менша від (n+2)-го члена того ж ряду

$$s_1 + s_2 + \ldots + s_n = s_{n+2} - 1$$

4. Сума квадратів чисел ряду Фібоначчі виражається через добуток двох сусідніх членів того ж ряду:

$$s_1^2 + s_2^2 + \ldots + s_n^2 = s_n \cdot s_{n-1}$$

5. $$s_1 + s_3 + \ldots + s_{2n-1} = s_{2n}$$

6. $$s_2 + s_4 + \ldots + s_2 = s_{2n+1} - 1$$

7. В ряду Фібоначчі кожне третє число – парне, кожне четверте ділиться на 3,

кожне п’яте ділиться на 5,

а кожне п’ятнадцяте – на 10.

ВИСНОВОК

Опрацювавши теоретичну частину, що стосується важливих алгоритмів,властивостей основи теорії чисел , вам залишається тільки практикуватися.