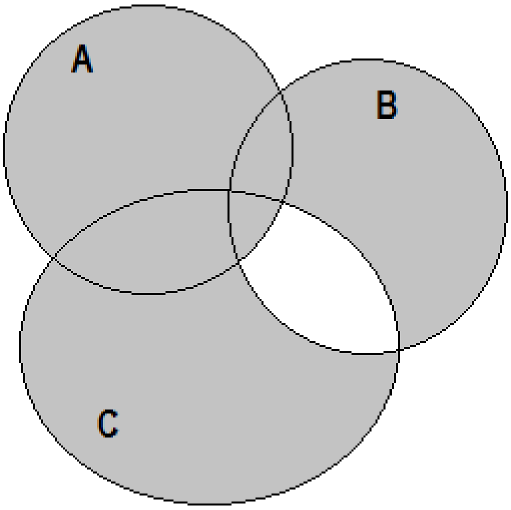
Останнє, що потрібно знати з доведення, все інше у вас уже буде на лабораторних заняттях.

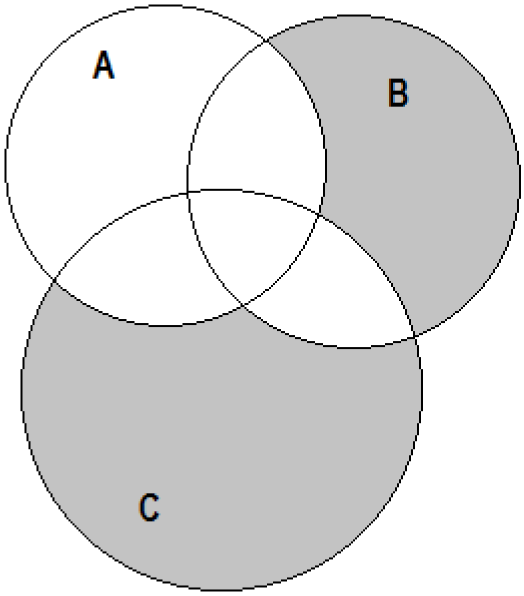
Дехто просить вас довести, що об'єднання з симетричною різницею підкорюється закону дистрибутивності:

4) $A \cup (B \Delta C) = (A \cup B) \Delta (A \cup C)$

Перше, що ви робите, – це малюєте діаграмки і дивитеся – працює чи не працює. Ми казали, що для 3 множин – 64 випадки діаграм, але ми розглядаємо один: якщо на ньому працює, то починаємо доводити, якщо ні – то більше нічого не треба робити. Хоча насправді треба.



$A \cup (B \Delta C)$



$(A \cup B) \Delta (A \cup C)$

Для того, щоб особисто мене переконати – ви повинні навести контр-приклад.

Тобто Ви повинні навести 3 множини: A, B і C. Бажано в явному вигляді, але це не обов'язково, для яких оця рівність не буде виконуватися.

Давайте наведемо якусь множину.

Наприклад: $A = \{1, 2, 3\}$, $B = \{2, \Psi(\textit{ялинка})\}$, $C = \{3, \Omega(\textit{їжачок})\}$. *Оскільки множини B і C не перетинаються, то їх семетрична різниця міститиме всі елементи.*

Отже, $A \cup (B \Delta C) = \{1, 2, 3\} \cup \{2, 3, \Psi, \Omega\} = \{1, 2, 3, \Psi, \Omega\}$, – тобто це буде множина ліворуч.

Множина праворуч: $(A \cup B) \Delta (A \cup C) = \{1, 2, 3, \Psi\} \Delta \{1, 2, 3, \Omega\} = \{\Psi, \Omega\}$.

Звідси множини $\{1, 2, 3, \Psi, \Omega\}$ і $\{\Psi, \Omega\}$ не рівні між собою. Отже, задана рівність не є коректна.

Ось такий контр приклад мене задовольнить повністю.

Чи все вам зрозуміло із доведення тверджень на множинах?

Насправді на… але ви ще дійдете до цього на лабораторних роботах.

Добре. То ж продовжуємо далі.

Потужність скінченної множини A – це кількість її елементів. Потужність зазвичай позначається $|A|$ (A за модулем, але це не модуль – це потужність), іноді – #A (шляхом застосування символу октото́рп (від лат. octothorpe — вісім ніг (кінців)), який називають дієзом, але це не дієз).

Введемо визначення. **Об'єднання** двох множин називається **диз'юнктним**, якщо ці множини не перетинаються. Я в цьому випадку буду писати, що C одержано ось таким об'єднанням множин A та B. Я підкреслюю, що якщо я пишу ось таким піддоном:

$A \coprod B$, – то це означає : $C = A \coprod B \Leftrightarrow \begin{cases} C = A \cup B \\ A \cap B = \varnothing \end{cases}$. Далі ми ось цю кон'югацію назвемо розбиттям множини С – і це значно коротше, ніж «диз'юнктне об'єднання множин».

Навіщо я це ввожу? Тому, що у мене є ціла теорема.

Чому дорівнює потужність диз'юнктного об'єднання двох множин?

Теорема. Якщо $C = A \coprod B \Rightarrow |C| = |A| + |B|$.

Це настільки очевидна теорема, що я не знаю як вам її довести, щоб не забрати всю пару. Тому лише схематично окреслю: якщо у нас множини скінченні, тобто кількість елементів виражається певним натуральним числом. Я їх можу всі перенумерувати. Тобто я перенумеровую всі елементи множини А, я перенумеровую всі елементи множини В, – потім я починаю перекидати їх в множину С і от: номери множини А я зберігаю, а номери елементів з В я збільшую на потужність А. Звідси в С будуть елементи з номерами від 1 до $|A| + |B|$. *Тобто загальна кількість елементів буде* $|A| + |B|$.

... Ну знаєте, яка в планіметрії найскладніша теорема? Прямокутник існує. Це очевидне твердження, але його треба доводити з аксіоматики Евкліда. Це було одне з видатних досягнень німецьких математиків XIX ст. Коли вони аксіому про те, що існує прямий кут вивели з трьох попередніх аксіом Евкліда. Це була 4-та аксіома, її викреслили.

Ми наразі будемо нею користуватися.

Сформулюємо наслідок.

Наслідок: $A = \coprod_{i=1}^{n} A_i = A_1 \coprod A_2 \coprod ... \coprod A_n$ – якщо у мене є *n*-множин $A_1, A_2, ..., A_n$, які не перетинаються попарно і я їх диз'юнктно об'єдную, тоді потужність $|A| = \sum_{i=1}^{n} |A|_i = |A_1| + |A_2| + ... + |A_n|$.

Як цей наслідок доводиться? Беремо n-ту множину і всі попередні – це буде дез'юнктне об'єднання двох множин – буде сума, потім беремо (n-1)-множину і всі попередні – буде знову сума і так далі... *Так все зрозуміло. Якщо не зрозуміло – промедитуйте, поки не стане зрозуміло.* ☺

Лема 1. $|A \setminus B| = |A| \setminus |A \cap B|$.

Доведення. Розглянемо дві множини: $X = A \setminus B$ і $\mathrm{Y} = \mathrm{A} \cap \mathrm{B}$. Що буде об'єднанням цих двох множин? $X \cup Y = (A \setminus B) \cup (A \cap B) = (A \cap \overline{B}) \cup (A \cap B) = A \cap (B \cup \overline{B}) = A \cap U = A$. (*використано дистрибутивність*). А якщо я перетну ці дві множини?

$$X \cap Y = (A \setminus B) \cap (A \cap B) = A \cap \overline{B} \cap A \cap B = A \cap B \cap \overline{B} = A \cap \varnothing = \varnothing$$

(*за асоціативністю прибрали дужки*).

Тобто ці дві множини X та Y в об'єднанні дають А, а в перетині – Ø. Тому множина А диз'юнктно розбивається на X та Y: $A = X \coprod \mathrm{Y}$. А тому я можу застосувати теорему і тоді: $|A| = |X| + |Y| = |A \setminus B| + |A \cap B|$. *А що нас просять довести? Те ж саме нас просять довести.*

Чи все вам зрозуміло? Чи є у вас питання? :-)

Лема 2. Якщо мені потрібно об'єднати дві множини і обчислити потужність, то мені потрібно взяти потужність А, додати потужність В і відняти потужність їх перетину:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Ця лема, насправді, у різних варіація повторюється майже у всіх розділах математики. Скажімо, будете ви систему лінійних рівнянь досліджувати, ось там буде: кількість вхідних змінних і вихідних змінних описується через потужність апарату та потужність образу. Добре.

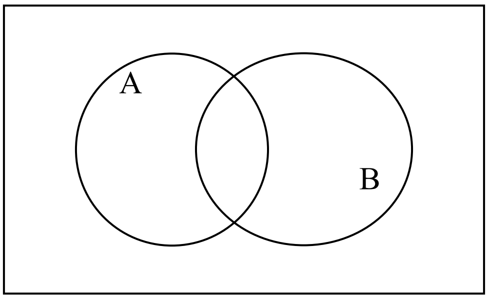
Або інше: якщо ви візьмете максимум двох чисел, візьмете мінімум двох чисел – і їх додасте, то це все рівно, що додати ці два числа. ☺... Потім зрозумієте.

Доведення (*воно взагалі просте*).

Я множину перетину А з В можу представити як: $A \cup B = B \coprod (A \setminus B)$. **Вдома доведіть це самостійно.**

Звідси і за допомогою леми 1 випливає, що потужність об'єднання двох множин це: $|A \cup B| = |B| + |A \setminus B| = |B| + |A| - |A \cap B|$.

Як це виглядає візуально?



Потужність – це площа цього кола. Як знайти площу цієї фігури, яка складається з двох кіл? Ви берете площу круга А, площу круга В, а фрагмент їх перетину ви підрахували двічі, а потрібно лише один раз. Тому ми один раз його віднімаємо. *Це зрозуміла ілюстрація. А перед цим було строге доведення.*

Що робити, якщо у мене є об'єднання великої кількості множин, які можуть перетинатися між собою?

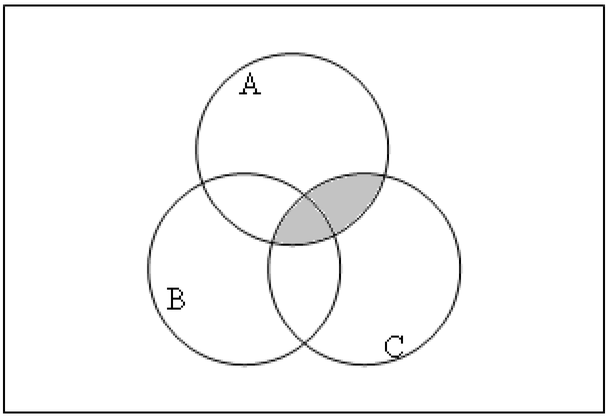
Теорема (формула включень та виключень – *взагалі то це не є формула, це є принцип обрахунку потужності об'єднання множин*) – *один з ваших нічних жахів* ☺

Формула включень та виключень є досить простою, коли ви розумієте принцип, але виглядає досить громісткою.

Якщо у нас є об'єднання множин $A_1, A_2, ..., A_n$ і ми бажаємо дізнатися, яка є там потужність: $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - ... + (-1)^{n-1} |A_1 \cap A_2 \cap ... \cap A_n|$.

Для початку ми беремо потужності кожної множини, потім беремо потужності їх попарних перетинів – і ці потужності ми віднімаємо. Потім ми беремо їх потужності перетинів по три і додаємо, потім беремо по 4 і віднімаємо, потім по п'ять – і додаємо, по 6 – віднімаємо… наприкінці в нас буде перетин всіх *n*-множин – в деяких випадках ми будемо їх додавати, в деяких – віднімати, тому $(-1)^{n-1}$: якщо n – парне, то будемо віднімати, якщо не парне – додавати.

Я зараз просто поясню як це працює.



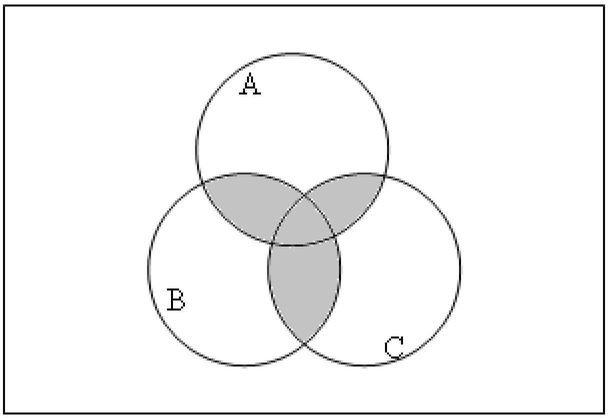
Розглянемо 3 множини А, В, С. Я хочу обчислити потужність об'єднання цих двох множин, тобто площу цієї фігури.

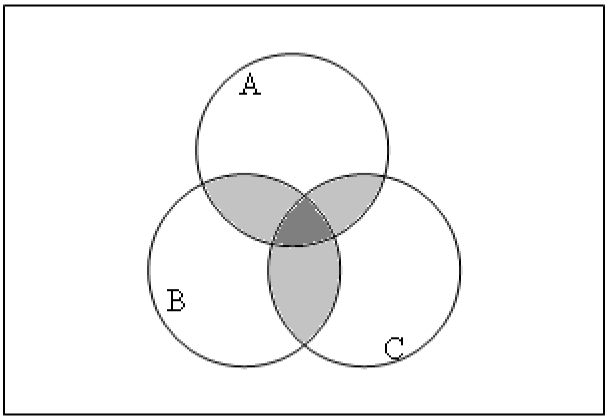
Спочатку я беру площу кожного кола:

$|A| + |B| + |C| -$

Але перетин двох множин А та С я порахувала двічі – в одному колі і в іншому колі. Тому його треба відняти. Так само треба відняти перетин множин А та В, В та С.

$-|A \cap B| - |A \cap C| - |B \cap C| +$





Але подивимося на середній шматочок. Що це за шматочок? Це перетин всіх трьох множин – це елементи, які належать всім трьом множинам одночасно. Спочатку я цей шматочок тричі додала в кожному колі, а потім я його тричі відняла в кожному колі – і він зник! А я повинна його порахувати. Тому потім мені потрібно його повернути:

$$|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|.$$

І ось ми одержали формулу включень, виключень для 3 множин.

Коли ми беремо для чотирьох множин. Графічно це не можна назвати «красиво». Тому я не буду цього малювати. Але там буде так само: ви додаєте потужності кожної множини, але певні елементи, що належать двом множинам ви порахували двічі, тому ви повинні їх відняти. Але виявляється певні елементи, що належать 3 і більше множинам – ви скільки раз додали, стільки й відняли, – треба їх повернути. Ви їх повертаєте, але при цьому елементи, що належали 4 і більше множинам ви + , - , + – додали зайву кількість разів (*чому ми <u>формулу назвали «включень та виключень» – ми на кожному кроці уточнюємо, уточнюємо, уточнюємо, поки не доходимо до самого кінця, – де дуже все точно… і якщо ви зрозумієте цей принцип: +1, - по два, + по три, - по чотири, + по 5, - по 6…, – то ця формула не буде визивати у вас жодних труднощів… А якщо ви просто будете зубрити… ☺</u>*).

<u>Теорема (формула включень та виключень). Взагалі то це не «формула», це є принцип: як рахувати певні об'єкти множин, що перетинаються. У</u> нас було n-множин $A_1, A_2, ..., A_n$, які ми об'єднували між собою і їх загальна потужність обчислювалася як:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| - \sum_{i<j}|A_i\cap A_j| + \sum_{i<j<k}|A_i\cap A_j\cap A_k| - ... + (-1)^{n-1}|A_1\cap A_2\cap ...\cap A_n| \qquad (1)$$

(сума потужностей кожної множини, мінус сума потужностей їх <u>всіх можливих попарних перетинів</u>, + сума потужностей їх <u>всіх можливих перетинів по три</u>, *<u>- по чотири, + по 5, - по 6… і т.д. І на останок – їх загальний перетин, який може бути або з «+» або з «-» – в залежності від їх кількості</u>*).

Ми з вами розглянули певний приклад для 3 множин. Чому воно будується саме так. А зараз ми це все <u>доведемо методом математичної індукції</u>.

Доведення.

Що у нас іде на першому кроці в методі математичної індукції? ***База****. Яку ми візьмемо базу?* **Якщо розглянути 1 множину $n=1$, то як буде виглядати формула включень та виключень?** $|A|=|A_1|$ (*потужність однієї множини, об'єднаної самої з собою – це буде сума цієї множини і все, бо в нас не буде попарних перетинів, бо в нас лише одна множина*). **Побачили, що для $n=1$ формула вироджується, тобто з**

формули залишається тривіальна рівність. Цього насправді достатньо, щоб довести цю формулу методом математичної індукції, але що буде, якщо $\mathrm{n}=2$?

$\mathrm{n}=2$: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ – (*сума потужностей множин, мінус потужність всіх можливих перетинів; оскільки у нас лише 2 множини – у нас лише один попарний перетин*).

Це ми доводили – це лема 2.

Насправді ця рівність, якщо ви будете брати замість множин A_1, A_2 – все більше і більше множин – вона дозволить вам вивести ось цю формулу.

Отже, крок – **індукція**.

Нехай для $\forall\mathrm{n}$-множин формула вірна. Нам потрібно буде його вивести декілька раз для різних випадків.

Позначимо $\mathrm{B} = \bigcup_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{A}_\mathrm{i}$ (об'єднання n-множин через B). І додамо ще одну множину з індексом $n+1$: $|B \cup A_{n+1}| =$

Що можна сказати про потужність цієї множини? За лемою 2:

$|B \cup A_{n+1}| = |B| + |A_{n+1}| - |B \cap A_{n+1}| =$.

Якщо замість B підставити, що це об'єднання n-множин:

$$|B \cup A_{n+1}| = |B| + |A_{n+1}| - |B \cap A_{n+1}| = \left|\bigcup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1}\right| =$$

Але, якщо у мене є об'єднання, яке я потім перетинаю певною множиною, то я можу скористатися властивістю дистрибутивності: я можу перетин внести в дужки:

$$|B \cup A_{n+1}| = |B| + |A_{n+1}| - |B \cap A_{n+1}| = \left|\bigcup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1}\right| = \left|\bigcup_{\mathrm{i}=1}^{\mathrm{n}} A_i\right| + |A_{n+1}| - \left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right|$$

Так? Згодні?

За припущенням індукції потужність $\left|\bigcup_{i=1}^{n} A_i\right|$ множини розписується згідно формули (1) і тут будуть фігурувати всі можливі сполучення множин від першої – до n-тої, – так, як потрібно за формулою. Множина $A_{\mathrm{n}+1}$, яка включається в першу суму – суму потужностей множин.

$\left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right|$ – це об'єднання n-множин; і ми рахуємо їх потужність. За припущенням індукції я знову можу застосувати формулу (1). Але множини будуть інші. Якщо я буду це окремо розписувати:

$-\left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right| = -\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{A}_\mathrm{i} \cap A_{i+1}|$ зрозумілий крок? Добре. Плюс сума потужностей попарних перетинів:

$-\left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right| = -\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{A}_\mathrm{i} \cap A_{i+1}| + \sum_{1 \le i \le j \le n} |A_i \cap A_{n+1} \cap A_j \cap A_{n+1}| =$ але, якщо я двічі перетинаю з однією і тією ж самою множиною – це все рівно, що перетнути з нею 1 раз, тому:

$= -\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{A}_\mathrm{i} \cap A_{i+1}| + \sum_{1 \le i \le j \le n} |A_i \cap A_{n+1} \cap A_j| -$. Зрозуміло?

Далі буде сума перетинів потужностей по 3:

$$= -\sum_{\mathrm{i}=1}^{\mathrm{n}} |\mathrm{A}_\mathrm{i} \cap A_{i+1}| + \sum_{1 \le i \le j \le n} |A_i \cap A_{n+1} \cap A_j| - \sum_{1 \le i \le j \le k \le n} |A_i \cap A_{n+1} \cap A_j \cap A_{n+1} \cap A_k \cap A_{n+1}| =$$

$$=-\sum_{i=1}^{n}\left|A_i \cap A_{i+1}\right| + \sum_{1\le i\le j\le n}\left|A_i \cap A_{n+1} \cap A_j\right| - \sum_{1\le i\le j\le k\le n}\left|A_i \cap A_{n+1} \cap A_j \cap A_k\right| + \ldots + (-1)^n\left|A_1 \cap A_2 \cap \ldots \cap A_{n+1}\right|$$

Що ми бачимо? Що в цій сумі: $\left|B \cup A_{n+1}\right| =$, – яку ми починали розглядати потужність об'єднання $n+1$-множини буде сума потужностей кожної множини, «-» сума потужностей їх попарних перетинів, потім буде «+» сума їх перетинів по три,… по чотири,… по 5… по 6… в кінці – сума потужностей всіх множин і цю суму ми трактуємо як $(-1)^{(n+1)-1}$ (*щоб формули збігалися*).

Тобто, якщо у мене вірна ця формула для n-множин, то ось ми довели, що вона буде вірна для $n+1$ – множини.

Далі індукційний перехід: якщо вона вірна для $n=1$, то буде вірна для $n=2$; якщо вона вірна для $n=2$, то буде вірна для $n=3$ і т.д.

До речі питання: чому індукційний перехід є перервним? Тобто чому мені ось цих двох тверджень справедливості бази та коректності переходу від n до $n+1$ достатньо, щоб довести твердження для довільного n?

Тому, що якщо мені дадуть певне конкретне число n – я побудую доведення цього твердження за скінченну кількість кроків: я починаю з бази і застосовую n-кроків індукційного класу. Тут ключовим є те, що для кожного натурального n я можу побудувати доведення за скінченну кількість кроків. Якщо б у мене індукція вимагала нескінченної кількості кроків, то ми б ніколи не дочекалися твердження про істинність.

Зрозуміло? Чи є у вас питання до цього доведення?

Приклади. Бо без прикладів не буде.

Приклади.

1) з того, що для вас найбільш близьке… для математиків досить часто потрібні прості числа – <u>великі прості числа, дуже великі прості числа!</u> І певної формули, яка дозволяє генерувати прості числа – її немає! Тому зазвичай генерують випадкове число – і перевіряють чи є воно простим чи ні. Існують алгоритми – тести на перевірку простоти, але вони доволі складні – і вимагають певного часу для свого виконання. А оскільки простих чисел не так багато, то нам потрібно декілька разів генерувати випадкові числа, щоб знайти просте. Але можна спочатку, коли ви згенерували число – перевірити чи ділиться воно на 2, на 3, на 5, на 7 – на мої прості числа, які ми знаємо. Якщо ділиться, то воно вже точно не просте. Так?

То ж питання: якщо ми перевіряємо подільність числа, обраного з інтервалу $[1, N]$, на 2, на 3, на 5, то скільки чисел ми таким чином можемо відкинути? Ці множини чисел, які окремо діляться на 2, на 3 і на 5 – вони перетинаються. Бо у вас, звісно, є множини, які діляться на ці числа одночасно (числа, які одночасно діляться на 2 і на 5 тощо). Тому треба застосувати формулу включень та виключень. Спочатку беремо потужність по одному. Скільки чисел буде ділитися на 2? Половина (для зручності будемо вважати, що N ділиться на 30):

$$=\frac{N}{2}+$$

Скільки чисел ділиться на 3? Кожне третє – третина:

$$=\frac{N}{2}+\frac{N}{3}+$$

Скільки на 5? 1/5:

$=\frac{N}{2}+\frac{N}{3}+\frac{N}{5}-$. Добре.

Але у нас є числа, які діляться і на 2 і на 3 – ми їх обрахували двічі, тобто ми повинні відняти всі числа, які одночасно поділяються на 2 і на 3, на 2 і на 5, на 3 і на 5:

$=\frac{\mathrm{N}}{2}+\frac{\mathrm{N}}{3}+\frac{N}{5}-\frac{\mathrm{N}}{6}-\frac{N}{10}-\frac{N}{15}+$

І нарешті числа, які поділяються на 2, на 3 і на 5:

$=\frac{\mathrm{N}}{2}+\frac{\mathrm{N}}{3}+\frac{N}{5}-\frac{\mathrm{N}}{6}-\frac{N}{10}-\frac{N}{15}+\frac{\mathrm{N}}{30}=.$

Якщо суму цих дробів коректно обчислити, то отримаємо:

$=\frac{\mathrm{N}}{2}+\frac{\mathrm{N}}{3}+\frac{N}{5}-\frac{\mathrm{N}}{6}-\frac{N}{10}-\frac{N}{15}+\frac{\mathrm{N}}{30}=\frac{22\mathrm{N}}{30}\approx N\cdot 0{,}7333...$

Тепер: якби у мене було в не число 5, а 4, то формула б виглядала б зовсім інакше, бо множина чисел $\frac{\mathrm{N}}{4}$ була б підмножиною чисел $\frac{\mathrm{N}}{2}$.

Якщо числа не взаємно прості – там потрібно найменше спільне кратне.

Тобто цей тест: якщо ми перевіряємо подільність на 2, 3 та 5, – він відразу викреслює $\frac{3}{4}$ всіх чисел. Якщо взяти перших 10 простих чисел, то можна, здається, до 95%.

Тобто така проста перевірка дуже пришвидшує тестування простоти чисел.

Інший приклад

2) Скільки взагалі існує чисел від 1 до N, які взаємно прості з заданим числом N?

Що таке взаємно прості числа? Взаємно прості числа – це числа, які не мають спільних дільників, окрім одиниці.

Тобто ми повинні обчислити потужність множини таких натуральних чисел, які належать цьому проміжку і не мають нетривіальних спільних дільників із числом N:

$\varphi(M)=\#\{\mathrm{x}\in\mathrm{N}\mid 1\le\mathrm{x}\le\mathrm{N},\text{НД}(\mathrm{x},\mathrm{N})=1\}$

– функція Ойлера (Euler's totient(? Ніхто не знає) function)

Отже, як обчислювати це число?

По-перше, кожне натуральне число ми можемо розкласти на прості дільники. Можемо? В 5 класі ще повинні розкладати. Так?

Тобто я маю число $\mathrm{N}=p_1^{\alpha_1}p_2^{\alpha_2}...p_t^{\alpha_t}$. Можу представити це число, де p-прості числа, а α – це певний степінь. Зветься це канонічний розклад числа.

Отже, якщо у вас число *x* має спільний дільник із числом *n,* то цей спільний дільник повинен ділитися або на p_1, або на p_2, або на p_3, або на p_t. *Це зрозуміло?*

(Якщо у вас $\mathrm{N}=2^{30}$, то які спільні дільники можуть бути в цього числа з іншими числами? 1, 2, $2^2, 2^3,...,2^{30}$; якщо буде $\mathrm{N}=2^{30}\cdot 3^{20}$: будуть усі степені 2-ки, усі степені 3-ки та їх множення; а спільний дільник «5» не буде, тому, що N не ділиться на 5; не може виникнути спільних дільників, окрім добутків степенів цих простих чисел).

Позначимо через A_i множину таких чисел, які лежать в інтервалі від 1 до N і поділяються на задане просте число p_i, яке ми взяли із розкладу нашого числа N: $A_i=\{x\in N\mid 1\le x\le N, x\,\vdots\, p_i\}$.

Тоді що можна сказати про числа з множини A_i? Вони точно не є взаємно простими з N. Бо в них є спільний дільник, щонайменше ось цей – p_i.

Тому функція Ойлера для числа N: це мені потрібно взяти всі числа від 1 до N – і відняти всі числа, що входять до множин A_i. Тобто це буде: $\varphi=N-|A_1\cup A_2\cup\ldots\cup A_t|$. Зрозуміло?

А чому дорівнює потужність множини A_i? Множина A_i містить всі числа, що діляться на p_i-те (кожне p_i-те число буде ділитися на p_i). Тому: $|\mathrm{A}_\mathrm{i}|=\frac{N}{p_i}$.

А чому дорівнює потужність попарного перетину? $|\mathrm{A}_\mathrm{i}\cap A_j|=$

Перетин цих множин – це всі числа, які поділяються і на p_i і на p_j. Відповідно це буде кожне $p_i p_j$-те число: $\left|A_i \cap A_j\right| = \frac{N}{p_i p_j}$. Так?

Якщо в мене буде перетин по три – це всі числа, що поділяються на $p_i p_j p_k$: $\left|A_i \cap A_j \cap A_k\right| = \frac{N}{p_i p_j p_k}$.

І тоді, якщо ми застосуємо для того виразу: $\varphi = N - \left|A_1 \cup A_2 \cup \ldots \cup A_t\right|$, – формулу включень та виключень, то ми побачимо, що функція Ойлера: $\varphi(N) = N - \sum_{i=1}^{t} \frac{N}{p_i} + \sum_{1 \le i \le j} \frac{N}{p_i p_j} - \sum_{1 \le i \le j \le k} \frac{N}{p_i p_j p_k} + \ldots + (-1)^t \frac{N}{p_i p_j \cdots p_t} =$ («+» сума по 4, «-» сума по 5, «+» сума по 6 і т.д.   В кінці будемо мати ↑)

Якщо ми уважно подивимося на цей вираз, то можна побачити, що це розклад ось цього виразу: $= N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\ldots\left(1 - \frac{1}{p_t}\right)$.

Цей факт я зараз залишаю без доведення, а ви вдома подивіться: доведіть методом математичної індукції.

Нарешті ми можемо перейти до нової теми.

Сьогодні ми повинні розглянути методи конструювання складних множин, коли у вас є певні прості.

Першою такою складною множиною є так званий булеан.

Булеаном множини А ми називаємо **множину всіх її підмножин**.

Традиційне позначення для булеана: 2^A. Але я підкреслюю: це не 2 піднести до степеня множина А, – тобто 2^A – це не операція, це символ, що означає булеан!!! Це лише позначення для булеана.

Є альтернативні позначення для булеана: $P(A)$ або $B(A)$.

Чому саме такий символ (2^A) зараз покажу.

Ну і формальне визначення: $2^A = \{B \mid B \subseteq A\}$ – булеан це є множини, які є підмножинами множини А.

Які є **очевидні властивості булеана**?

$\varnothing \in 2^A$ – пуста множина є елементом будь-якого булеану (бо порожня множина завжди є множиною будь-якої множини);

Наша вихідна множина також завжди є власною підмножиною, тому вона завжди належить нашому булеану: $A \in 2^A$.

Тобто ці дві властивості є тут (які виконуються для будь-яких множин).

А скільки взагалі підмножин буде в нашій множині?

Якщо наша множина А скінченна, то в мене є теорема.

Теорема (про потужність булеана): **якщо** множина **А** є **скінченною** і містить n елементів, то її булеан містить 2^n елементів. Тобто потужність булеану обчислюється за допомогою такого виразу: $\left|2^A\right| = 2^{|A|}$. Або: $|A| = n \Rightarrow \left|2^A\right| = 2^n$. Що одне і те ж саме.

Якщо в мене множина А складається з 1 елемента. То скільки в неї підмножин? 2. Які? Ø та сама множина А.

Якщо в мене множина А складається з 2 елементів: $A = \{a, b\}$, то в мене є: $2^A = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$. Можна перевірити для 3-4 елементів множини. І ми бачимо, що твердження здається коректним. Добре. Нам це потрібно доводити. Як ми це будемо доводити? Методом математичної індукції.

Але це буде один з його способів, який ми сьогодні розглянемо.

(*Математик повинен слідкувати за тим, що він говорить* ☺)