МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

Розрахунково-графічна робота

з курсу «Технології захисту інформації»

Тема: «Елементи теорій груп, кілець, полів, теорії чисел та теорії ймовірності в криптографії»

Виконав:

студент IV курсу

групи ДА-32

Колінько Анжела

Київ – 2017

Зміст

[Вступ 3](#_Toc478410763)

[1. Арифметика лишків 5](#_Toc478410764)

[2. Групи, кільця, поля 6](#_Toc478410765)

[2.1 Групи 6](#_Toc478410766)

[2.2 Кільця 7](#_Toc478410767)

[2.3 Поля 8](#_Toc478410768)

[3. Функція Ейлера 10](#_Toc478410769)

[4. Мала теорема Ферма 16](#_Toc478410770)

[5. Парадокс днів народження 18](#_Toc478410771)

[Висновок 21](#_Toc478410772)

[Джерела 22](#_Toc478410773)

# Вступ

Довгий час наука криптографія була засекречена, тому що застосовувалася, в основному, для захисту державних і військових секретів. Термін "криптологія" навіть не можна було вимовляти тим, хто професійно працював в цій галузі, не кажучи вже про відкриті публікації на цю тему. У відкритих організаціях, як навчальних, так і науково-дослідних, ніхто криптологією офіційно не займався. Слово "криптологія" вперше з'явилося у нас в перекладній статті Дж. Л. Мессі "Введення в сучасну криптології" в тематичному випуску ТІІЕР, т.76, № 5 за 1988 рік [6]. Висвітлюючи класичні питання криптології, вона може служити хорошим вступом в предмет.

В даний час, методи і засоби криптографії використовуються для забезпечення інформаційної безпеки не тільки держави, але і приватних осіб і організацій. Справа тут зовсім не обов'язково в секретах, а в тому, що зараз дуже великий обмін інформацією відбувається в цифровому вигляді через відкриті канали зв'язку. До цієї інформації можливо застосування загроз недружнього ознайомлення, накопичення, підміни, фальсифікації і т.д. Найбільш надійні методи захисту від таких загроз дає саме криптографія.

Математичні методи, використовувані в криптографії, неможливо успішно освоїти без знання таких алгебраїчних структур, як групи, кільця і поля. Тому знання і вміння працювати з цими об'єктами є необхідною умовою для підготовки фахівців в області захисту інформації. В силу властивої методам криптографії специфіки, великий інтерес представляє безліч цілих чисел і різні алгебраїчні структури на його базі. Математична криптографія виникла як наука про шифрування інформації, тобто як наука про криптосистеми. Великий вплив на розвиток криптографії надали в середині двадцятого століття роботи американського математика Клода Шеннона. У класичній шеноневській моделі системи секретного зв'язку мають місце два учасника, що повністю довіряють один одному , яким необхідно передавати між собою інформацію, не призначену для третіх осіб. Така інформація називається конфіденційною або секретною. Звідси виникає задача забезпечення конфіденційності, тобто захист секретної інформації від противника. Це завдання, принаймні історично, - перше завдання криптографії. Воно традиційно вирішується за допомогою криптосистем.

При обміні інформацією між учасниками часто виникає ситуація, коли інформація не є конфіденційною, але важливий факт надходження повідомлень в неспотвореному вигляді, тобто наявність гарантії, що ніхто не зможе підробити повідомлення. Така гарантія називається забезпеченням цілісності інформації і становить друге завдання криптографії. Для запобігання загрози контролю за джерелами інформації (звідки пересилаються повідомлення) необхідна система контролю за доступом до ресурсів, яка повинна відповідати двом, здавалося б, взаємно виключаним вимогам. По-перше, кожен бажаючий повинен мати можливість звернутися до цієї системи анонімно, а по-друге, при цьому все ж довести своє право на доступ до ресурсів. Прикладом можуть служити паперові купюри. Якщо ресурсом є деякий товар, то наявність у покупця достатньої кількості купюр є доказом його права на доступ до ресурсу. З іншого боку, хоча кожна паперова купюра і має унікальний номер, відстежувати купюри по номерам практично неможливо, тобто не можна визначити, хто її використовував і в яких платежах. Аналог цієї властивості в криптографії називається невідслідковуваністю. Забезпечення невідслідковуваності – третє завдання криптографії.

# 1. Арифметика лишків

Ідея арифметики залишків по суті дуже проста і схожа на «арифметику годин», з якою ви знайомитеся в дитинстві. «Арифметика годин» пов'язана з перерахунком часу з 24-годинної системи в 12-годинну і назад, адже в добі 24 години, а на циферблаті їх всього 12. Робиться це досить просто: щоб перевести значення в 24-годинний системі в 12-годинну, досить розділити його на 12. Залишок від ділення і буде шуканим значенням в 12-годинної системою. Наприклад, 13:00 у 24-годинний системі –- те ж саме, що і одна годину на 12-годинний, оскільки залишок від ділення 13 на 12 дорівнює 1. [1]

Пояснимо більш чітко, що таке арифметика залишків. Перш за все ми фіксуємо позитивне натуральне число N, яке називається модулем. Якщо різниця двох цілих чисел b-а ділиться на N без остачі, то пишуть а=b(modN) і говорять, що числа а і b порівняні по модулю N. Очевидно, що в цьому випадку числа а і b мають один і той же залишок від ділення на N. Звідси назва «арифметика залишків». Якщо ясно з якого модулю N відбувається порівняння то можна писати просто ab.

Наприклад, 18 (mod 7) = 4, -18 (mod 7) = 3.

Оператор модуля схожий на оператор% в мові програмування C, за тим винятком, що в значення цього оператора зазвичай невід'ємні.

Наприклад, в мовах С або Java оператор модуля діє так: (-3) У, 2 = -1, а ми будемо думати, що (-3) (mod 2) = 1.

Всі можливі залишки від ділення чисел на N утворюють множину Z/NZ = {0,. . . , N-1}. Оскільки всі порівняні між собою за модулем N цілі числа мають один і той же залишок, ми можемо вважати, що елемент х Z/NZ зображує цілий клас чисел виду х + kN, де k Z. Таким чином, оперуючи цілими числами по модулю N, ми будемо вважати всі порівняні між собою числа рівними один одному і використовувати традиційний знак «=» замість «».

На множині Z/NZ є дві основні операції - додавання і множення. Вони визначаються звичайним шляхом, наприклад, (11 + 13) (mod 16) = 24 (mod 16) = 8, рскільки 24=1•16+8, і (11•13)(mod 16)=143(mod 16)=15, оскільки 143=8•16+15.

# 2. Групи, кільця, поля

Додавання і множення по модулю N працюють майже так само, як арифметичні операції над дійсними і цілими числами. Зокрема, вони мають такі властивості:

1. Замкнутість по додаванню:

∀ a, b ∈ Z/NZ: a + b ∈ Z/NZ

2. Асоціативність додавання:

∀ a, b, с ∈ Z/NZ : (a+b)+c=a+(b+c)

3. Нуль є одиничним елементом (або одиницею) по додаванню:

∀ a ∈ Z/NZ: a+0=0+a=а

4. Завжди існує зворотний елемент по додаванню (протилежний):

∀a ∈ Z/NZ: а+(N-а)=(N-а)+а=0

5. Комутативність додавання:

∀ a, b ∈ Z/NZ: a+b=b+a

6. Замкнутість множення:

∀ a, b ∈ Z/NZ: a\*b ∈ Z/NZ

7. Асоціативність множення:

∀a, b, с ∈ Z/NZ: (а\*b)\*с=а\*(b\*с)

8. Число 1 є одиничним елементом (одиницею) по множенню:

∀ a ∈ Z/NZ: а•1=1•а=а

9. Множення і додавання пов'язані законом дистрибутивності:

∀ a, b, c ∈ Z/NZ: (a+b)\*c=a\*c+b\*c

10. Комутативність множення:

∀ a, b ∈ Z/NZ: a\*b=b\*a

## 2.1 Групи

**Визначення 1**. Групою називається множина з операцією, яка

- замкнута,

- володіє одиницею,

- асоціативна;

- щодо неї кожен елемент має зворотній.

Групу з комутативною операцією називають комутативною або абелевою. Майже всі групи, що зустрічаються в криптографії, – абелеві, оскільки саме властивість комутативності надає їм криптографічний інтерес. Отже, будь-яка множина з операцією, що задовільняє властивостям 1, 2, 3 і 4 з перерахованих вище, називається групою, а якщо операція задовольняє ще й властивості 5, то – абелевою групою.

Група називається мультиплікативною якщо ми записуємо її операцію як множення, тобто крапкою:

f=g\*h і g5=g\*g\*g\*g\*g

Таку групу ми позначаємо (G,•) в тому випадку, коли можливі сумніви щодо використовуваної в ній операції. групу називають адитивно якщо її операція записується як додавання:

f=g+h і 5\*g=g+g+g+g+g

Для адитивних груп ми використовуємо позначення (G, +). Абелева група називається циклічною, якщо в ній є такий спеціальний елемент (твірний), що будь-який інший елемент групи виходить багаторазовим застосуванням до нього груповий операції.

Якщо g – твірна циклічної групи G, ми пишемо G=<g>. У мультиплікативному випадку кожен елемент h групи G можна записати у вигляді h=gx, а в адитивному – h=x\*g, де x в обох випадках – деяке ціле число, яке називають дискретним логарифмом елемента h по основі g.

## 2.2 Кільця

**Визначення 2**. Кільце - це безліч R з двома операціями, додаванням і множенням, що традиційно позначаються «+» і «•», які мають властивості 1-9. [1]

Ми можемо позначати кільце разом з його операціями трійкою (G, •, +). Якщо виявиться, що множення в даному кільці комутативне (властивість 10), то ми будемо називати його комутативним кільцем. Множина залишків Z/NZ з операціями додавання і множення теж є комутативним кільцем, яке часто називають кільцем лишків за модулем N, Кільце лишків – один з центральних об'єктів криптографії, на властивостях якогозасновано багато методів шифрування.

## 2.3 Поля

Вирішуючи рівняння виду ах=(mod N),ми приходимо до питання про існування мультиплікативного зворотного у числа а по модулю N. Інакше кажучи, необхідно з'ясувати, чи існує число с, що задовольняє рівності ас=са=1(mod N)?

Таке число з природно позначити через а-1, Як вже було зазначено, зворотний до а існує тільки тоді, коли a і N взаємно прості, тобто НСД (а,N)=1. Особливо цікавий випадок простого модуля N=р – просте, оскільки при цьому для будь-якого ненульового елемента а Z/NZ знайдеться єдине рішення рівняння ах=1(mod p).

Отже, якщо р - просте число, то будь-який ненульовий елемент в Z/pZ має мультиплікативний зворотній. Кільця з такою властивістю називаються полями.

**Визначення 3**. Полем називається множина (G,•,+) з двома операціями, що володіє додатковими властивостями:

- (G,+) - абелева група з одиничним елементом О,

- {G\{0},•) - абелева група з одиничним елементом 1,

- (G,•,+) задовольняє закону дистрибутивності.

Отже, поле – це коммутативное кільце, в якому кожен ненульовий елемент має зворотній.

Визначимо множину оборотних елементів в Z/NZ як

(Z/NZ)\*={х Z/NZ | НСД(х,N)=1}.

Для загального кільця А позначення А\* закріплено для найбільшої його підмножини елементів, які утворюють групу по множенню. У нашій ситуації легко перевірити, що множина (Z/NZ)\* – група по множенню з числом елементів (N), де () – функція Ейлера.//TODO;

У спеціальному випадку, коли N=р – просте число, отримуємо: (Z/pZ)\*={l,. . . , p - 1},оскільки кожен ненульовий елемент кільця Z/pZ взаємно простий з р і тому має зворотній. Іншими словами, Z/pZ є скінченним полем, яке зазвичай називається полем лишків за модулем р і позначається символом Fр. Як випливає з визначення, мультиплікативна група F\* поля F збігається з множиною F\{0} (немає такого числа, щоб при множенні на нуль отримати 1(mod N). Тому в 0 немає оберненого). У випадку поля лишків отримуємо

Fp=Z/pZ={0, ..., р-1} і Fp\*=(Z/pZ)\*={1, ..., р-1}

Таким чином з 10 властивостей:

– якщо виконуються властивості 1-4 включно (по груповій операції)– то це група

– якщо виконуються властивості 1-5 включно (по груповій операції) – то це абелева група

– якщо виконуються властивості 1-9 включно – то це кільце

– якщо виконуються властивості 1-10 включно – то це комутативне кільце

– якщо виконуються властивості 1-10 включно, а також кожен елемент крім одиничного за додаванням (крім нуля) має зворотній – то це поле.

# 3. Функція Ейлера

Одна з центральних завдань арифметики залишків - це рішення рівняння а•x=b(mod N), тобто пошук елемента х Z/NZ, який задовольняє цій рівності.

Лінійне рівняння ах=b з дійсними коефіцієнтами при а0 завжди вирішується. Якщо ж розглядати його над кільцем цілих чисел, то відповідь знайдеться не завжди. Наприклад, не існує цілого числа x, яке перетворює рівняння 2x=5 в правильну рівність. Таким чином, постає питання: за яких умов на а, b і N рівняння ах=b(mod N) має рішення і як їх всі знайти?

ах=b(mod N) => a\*x=k\*N+b

Розглянемо 3 випадики:

– якщо НСД (а, N)=1, то існує рівно одне рішення. Воно може бути знайдено за допомогою проміжного числа с, що задовольняє рівняння аc=1(mod N), після чого шукане невідоме х обчислюється за формулою х=bс(mod N). *Доведення:*

ах=b(mod N) =>|домножимо обидві частини на c| =>axc=bc(mod N) =>|комутативність| => acx=bc(mod N) => |аc=1(mod N)| => x=bc(mod N).

– якщо НСД (а, N) 1 і b ділиться на g=НCД(а, N), то рівняння матиме g рішень. *Доведення:*

ах=b(mod N) =>|поділимо обидві частини рівняння на g, a/g і N/g – цілі тому, що g=НCД(а, N), а b/g – ціле тому, що за умовою b ділиться на g | => (a/g)x=(b/g)(mod N/g) => |позначимо a'=a/g, b'=b/g, N'=N/g | => a'x=b'(mod N') => |НСД (а', N')=НCД(а/g, N/g)=(НCД(а, N))/g=g/g=1 => маємо перший випадок => дане рівняння має 1 розв’язок x'=b'\*c, де a'c=1| => x'=b'\*c. Інші розв’язки даного рівняння задовольняють формулі x=x'+i\*N', де i=1,2,…,g-1. Таким чином розв’язків буде g-1+1=g.

– в інших випадках рішень немає.

Ситуація, коли НСД (а, N) = 1, настільки важлива, що для неї вводиться спеціальну назву. Кажуть, що числа а і N взаємно прості.

Число елементів кільця Z/NZ, взаємно простих з N, дається функцією Ейлера () і дорівнює (N). Значення (N) можна знайти за розкладом числа N на прості множники. Якщо

,

де pi - різні прості числа, то

(N)=

Зауважимо, що останнє твердження дуже важливе з точки зору криптографії: по розкладенню числа N на прості множники легко обчислити значення (N). Особливий інтерес представляють такі окремі випадки:

1. Якщо р просте, то (p)=р-1.

2. Якщо р і q - прості числа і рq,то (pq)=(p-l) (q-l).

*Доведення:*

Функція Ейлера (m), це функція, яка дорівнює кількості натуральних чисел, менших m і взаємно простих з m. Число m взаємно просте з усіма натуральними числами (і з одиницею). [2]

Візьмемо ряд натуральних чисел до m

1, 2, 3, ..., m.

Визначимо, скільки в цьому ряду чисел, взаємно простих з m. Так як одиниця взаємно проста з одиницею, то

φ (1) = 1.

Далі, число 2 взаємно просто з 1, тоді φ (2) = 1, число 3 взаємно просте з 1 і 2, тоді φ (3) = 2. Продовжуючи отримаємо: φ (4) = 2, φ (5) = 4, і т.д.

Сформулюємо такі завдання.

Завдання 1. Нехай a1, a2, a3, ... всі відмінні один від одного прості множники числа m. Знайти число тих чисел, які не діляться ні на одне з чисел a1, a2, a3, ....

Більш спільне завдання має наступний вигляд:

Завдання 2. Нехай a1, a2, a3, ... взаємно прості числа, які входять множниками в m. Знайти число всіх чисел, які не діляться ні на одне з чисел a1, a2, a3, ....

Візьмемо ряд натуральних чисел до m:

1, 2, 3, ..., m. (1)

Виключимо з ряду (1) всі ті числа, які діляться на a1. Це такі числаhttp://matworld.ru/images/euler-function/img1.jpg

Їх число дорівнює http://matworld.ru/images/euler-function/img2.jpg (m цілочисленно ділиться на a1, a2, a3… тому, що це його прості множники). Виключимо ці числа з ряду (1). тоді залишаться

http://matworld.ru/images/euler-function/img3.jpg (2)

числа, які не діляться на a1. Позначимо множину цих чисел через A1.

З чисел ряду A1 потрібно виключити всі ті числа, які кратні a2. Це ті числа з ряду (1), які діляться на a2 і не діляться на a1. Числа ряду (1), які діляться на a2 наступні:

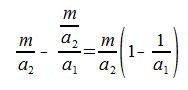
http://matworld.ru/images/euler-function/img4.jpg

Їх кількість дорівнює http://matworld.ru/images/euler-function/img5.jpg.

Ці числа можна представити у вигляді ka2, де k пробігає натуральні числа

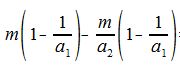
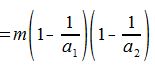
http://matworld.ru/images/euler-function/img6.jpg (3)

Для того, щоб ka2 не ділився на a1 необхідно і достатньо, щоб k не ділився на a1 (тому що a1 і a2 взаємно прості числа). Потрібно знайти кількість чисел з ряду (1), які діляться на a1 і виключити їх з ряду (3). http://matworld.ru/images/euler-function/img5.jpg ділиться на a1 тому m ділиться на a1, m ділиться на a2 і m ділиться на a1a2 (a1, a2 входять множниками в m). Завдання по відношенню числа http://matworld.ru/images/euler-function/img5.jpgта ж, що і завдання по відношенню числа m, яке ми вирішили за допомогою формули (2). З ряду A1 потрібно виключити числа, які діляться на a1. Тоді взявши замість m число http://matworld.ru/images/euler-function/img5.jpgотримаємо

 (4)

(4) – число тих чисел ряду A1, які не діляться на a1 або це число тих чисел ряду (1), які діляться на a2 і не діляться на a1.

З огляду на (2) і (4) отримаємо число тих чисел ряду (1), які не діляться ні на a1, ні на a2:

  (5)

Позначимо множину цих чисел через A2. Далі видалимо з A2 ті числа, які діляться на a3. Це ті числа з ряду (1), які діляться на a3 і не діляться на a1 і a2.

Числа ряду (1), які діляться на a3 наступні:

http://matworld.ru/images/euler-function/img9.jpg

Їх кількість дорівнюєhttp://matworld.ru/images/euler-function/img10.jpg.

Ці числа можна представити у вигляді ka3, де k пробігає натуральні числа

http://matworld.ru/images/euler-function/img11.jpg (6)

Для того, щоб ka3 не ділився на a1 і a2 необхідно і достатньо, щоб k не ділився на a1 і a2 (тому що a3 і a1 а також a3 і a2 числа взаємно прості). Потрібно знайти кількість чисел з ряду (1), які діляться на a1 і a2 і виключити з ряду (6). http://matworld.ru/images/euler-function/img10.jpg ділиться на a1 і a2, так як m ділиться на a1, m ділиться на a2 і m ділиться на a1a2a3 (a1, a2, a3 входять множниками в m). Завдання по відношенню числа http://matworld.ru/images/euler-function/img10.jpg та ж, що і завдання по відношенню числа m, яке ми вирішили за допомогою рівняння (5). Число тих чисел ряду (6), які не діляться ні на a1 ні на a2 (або число тих чисел ряду (1), які діляться на a3 і не діляться ні на a1, ні на a2):

http://matworld.ru/images/euler-function/img12.jpg

Тоді число тих чисел ряду (1), які не діляться ні на a1, ні на a2, ні на a3:

http://matworld.ru/images/euler-function/img13_1.jpghttp://matworld.ru/images/euler-function/img13_2.jpghttp://matworld.ru/images/euler-function/img13_3.jpg

Позначимо множину цих чисел через A3. Міркуючи таким чином, отримаємо, що число Ai тих чисел ряду (1), які не діляться на a1, a2, ..., ai дорівнює

http://matworld.ru/images/euler-function/img14_1.jpghttp://matworld.ru/images/euler-function/img14_2.jpg (7)

Ми отримали число тих чисел ряду (1), які не діляться на числа a1, a2, ..., ai. Отримаємо формулу для чисел a1, a2, ..., ai, ai + 1, де ai + 1 також входить множником в m і взаємно просте з a1, a2, ..., ai.

Щоб знайти число тих чисел ряду (1), які не діляться на a1, a2, ..., ai + 1, потрібно з множини (7) виключити числа кратні ai + 1. Це ті числа ряду (1), які не діляться на a1, a2, ..., ai і діляться на ai + 1.

Всі числа ряду (1), які діляться на ai + 1, наступні:

http://matworld.ru/images/euler-function/img15_1.jpghttp://matworld.ru/images/euler-function/img15_2.jpg

тобто це числа kai + 1, де k = 1, 2, ..., m / ai + 1 і для того, щоб kai + 1 не ділилося на a1, a2, ..., ai необхідно і достатньо, щоб k не ділилося на a1, a2, ..., ai. Тому з ряду Ai потрібно виключити стільки чисел, скільки існує в ряду

http://matworld.ru/images/euler-function/img16.jpg

чисел, які не діляться на a1, a2, ..., ai, тобто

http://matworld.ru/images/euler-function/img17.jpg

Якщо виключити ці числа з ряду Ai, то залишаться ті числа цього ряду, які не діляться на числа a1, a2, ..., ai + 1. Їх число дорівнює

http://matworld.ru/images/euler-function/img18_1.jpghttp://matworld.ru/images/euler-function/img18_2.jpghttp://matworld.ru/images/euler-function/img18_3.jpg

Ми довели наступну теорему:

Теорема 1. Якщо a1, a2, ..., aq, все різні взаємно прості числа, що входять в m, то число чисел, які не діляться ні на одне з чисел a1, a2, ..., aq і входять в ряд m дорівнює:

http://matworld.ru/images/euler-function/img19_1.jpghttp://matworld.ru/images/euler-function/img19_2.jpg (8)

Таким чином справедлива і наступна теорема:

Теорема 2. Якщо a1, a2, ..., aq, все різні прості числа, що входять в m, то число чисел, взаємно простих з m і входять в ряд

1, 2, ..., m

визначається формулою (8).

Дійсно. Будь-яке число, яке не ділиться ні на один з простих множників, що входять до складу m є взаємно простим з m. Тоді враховуючи теорему 1, отримуємо підтвердження цієї теореми.

Знайдену формулу можна переписати і в іншому вигляді. Якщо a1, a2, a3, ... все різні прості числа, що входять множниками в m, то

http://matworld.ru/images/euler-function/img20.jpg

тоді

http://matworld.ru/images/euler-function/img21_1.jpghttp://matworld.ru/images/euler-function/img21_2.jpghttp://matworld.ru/images/euler-function/img21_3.jpg

# 4. Мала теорема Ферма

Якщо p- просте число і a- ціле число, що не ділиться на p, то a p-1-1 ділиться на p, тобто

ap-1≡1(mod p) (1)

Мала теорема Ферма є окремим випадком теореми Лагранжа і служить основою одного з тестів на простоту.

*Доведення:*

Для доведення теореми буде потрібно наступна лема. [3]

Лема. Для будь-якого простого числа p і цілого числа k не кратного p, добуток k і чисел 1, 2, 3, ..., p-1:

k·1, k·2, k·3, ..., k·(p-1)

при діленні на p в залишку дають ті ж самі числа 1, 2, 3, ..., p-1, можливо записані в деякому іншому порядку.

*Доведення* леми. Добуток числа k з будь-яким з чисел 1, 2, 3, ..., p-1 не ділиться на p. Отже, при діленні k·1, k·2, k·3, ..., k·(p-1) на p не може бути нульового залишку.

Доведемо, що всі залишки різні. Припустимо, зворотнє. Нехай добутки ka і kb при діленні на p дають однакові залишки, тоді ka-kb=k(a-b) ділиться на p. Але це неможливо, оскільки a-b не ділиться на p (тому що |a-b|<p) і k не ділиться на p (за умовою). Значить всі залишки різні. Існує лише p-1 різних ненульових залишків від ділення на p і всі вони менше p. Лема доведена.

Згідно з доведеною вище лемою, залишки від ділення чисел a, 2a, 3a, ..., (p-1) a збігаються з числами 1,2,3, ..., p-1 з точністю до перестановки. тоді

a·2a·3a ...(p-1)a≡1·2·3...(p-1) (mod p).

Звідси

ap-1(p-1)!≡(p-1)! (mod p) (2)

З виразу (2) випливає, що

ap-1(p-1)!-(p-1)!=(ap-1-1)(p-1)! (3)

ділиться на p. Так як всі співмножники 1, 2, 3, ..., p-1 виразу (p-1)! взаємно прості з p, то ap-1-1 ділиться на p або можна записати:

ap-1≡1(mod p).

Теорема доведена.

Альтернативне формулювання малої теореми Ферма відрізняється тим, що не вимагає, щоб a не ділилося на p.

Теорема 1. Якщо p - просте число, то для кожного цілого числа a

ap≡a(mod p) (4)

Іншими словами, якщо p - просте число, то для кожного цілого числа a, ap-a ділитися на p.

*Доведення*. Якщо a ділиться на p, то ap-a=a(ap-1-1) ділиться на p. Вираз (4) еквівалентна виразу a·ap-1≡1·a(mod p). Якщо ж a не ділиться на p (НСД(a,p)=1), то найбільший спільний дільник чисел a і p дорівнює 1. Тоді з виразу am≡bm mod (p) => a≡b mod (p/λ) [4], де λ це найбільший спільний дільник чисел m і p, маємо: a·ap-1≡1·a(mod p) еквівалентний виразу ap-1≡1(mod p).

# 5. Парадокс днів народження

Щоб зрозуміти причину назви парадоксу, оцінимо ймовірність збігу днів народжень двох людей з деякою групи. Деякі наївно вважають, що така ймовірність дуже мала, вважаючи практично неможливим збіг чиєїсь дати народження з його власною. [5]

У групі, що складається з 23 або більше осіб, ймовірність збігу днів народження (число і місяць) хоча б у двох людей перевищує 50%. Наприклад, якщо в класі 23 учня або більше, то більш імовірно те, що у когось з однокласників дні народження припадуть на один день, ніж те, що у кожного буде свій неповторний день народження.

Для 60 і більше осіб ймовірність такого збігу перевищує 99%, хоча 100% вона досягає, згідно з принципом Діріхле, тільки тоді, коли в групі не менше 367 чоловік (рівно на 1 більше, ніж число днів у високосному році; з урахуванням високосних років).

Таке твердження може здатися неочевидним, тому що ймовірність збігу днів народження двох чоловік з кожним днем в році (1/365=0.27%), помножена на число осіб у групі (23), дає лише (1/365)\*23=6.3%. Проте число можливих пар (=(23 × 22)/2=253) значно перевищує число людей в групі (253> 23). Таким чином, твердження не є парадоксом в науковому сенсі: логічного протиріччя в ньому немає, а парадокс полягає лише у відмінностях між інтуїтивним сприйняттям ситуації людиною і результатами математичного розрахунку.

Потрібно визначити ймовірність того, що в групі з n осіб як мінімум у двох з них дні народження співпадуть.

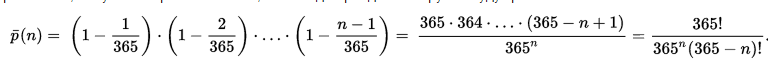
Нехай дні народження розподілені рівномірно, тобто приймемо, що:

– в році 365 днів (немає високосних років);

– в групі немає людей, які очевидно народилися в один день (наприклад, близнюків);

– народжуваність не залежить від дня тижня, пори року та інших факторів.

Розрахуємо спочатку  – імовірність того, що в групі з n людей дні народження всіх людей будуть різними. Якщо n> 365, то в силу принципу Діріхле ймовірність  дорівнює нулю. Якщо ж , то будемо міркувати таким чином. Візьмемо навмання одну людину з групи і запам'ятаємо його день народження. Потім візьмемо навмання іншу людину, при цьому ймовірність того, що у неї день народження не співпаде з днем народження першої людини, дорівнює . Потім візьмемо третю людину; при цьому ймовірність того, що його день народження не співпаде з днями народження перших двох, дорівнює . Міркуючи за аналогією, ми дійдемо до останньої людини, для якої ймовірність неспівпадання його дня народження з усіма попередніми дорівнюватиме . Перемножуючи всі ці ймовірності, отримуємо ймовірність того, що всі дні народження в групі будуть різними:



Тоді ймовірність того, що хоча б у двох осіб з n дні народження співпадуть, дорівнює



Значення цієї функції перевищує 1/2 при n = 23, при цьому ймовірність збігу дорівнює приблизно 50.73%, а . Список значень n і відповідної ним вірогідності наведено в таблиці нижче.

|  |  |
| --- | --- |
| n | p(n) |
| 10 | 12% |
| 20 | 41% |
| 30 | 70% |
| 50 | 97% |
| 100 | 99.99996% |
| 200 | 99.9999999999999999999999999998% |
| 300 | ( 1 − 7×10−73 ) × 100% |
| 350 | ( 1 − 3×10−131 ) × 100% |
| 367 | 100% |

Дану задачу можна переформулювати в термінах класичної «задачі про збіги». нехай:

– урна містить M куль (в даному випадку M – кількість днів у році, прийнята рівною 365 дням);

– кулі пронумерованих числами 1, 2, ..., M;

– вибираємо кілька вибірок по n куль з урни (в даному випадку n – кількість людей в групі);

– вилучені кулі повертаються в урну після кожної вибірки;

вибірки вважаються впорядкованими, тобто вибірки {1, 2, 4, 6 \} і {4, 2, 6, 1 \} вважаються різними.

Потрібно порахувати вірогідність події, що полягає у відсутності повторень у вибірці. Всі розрахунки аналогічні наведеним вище.

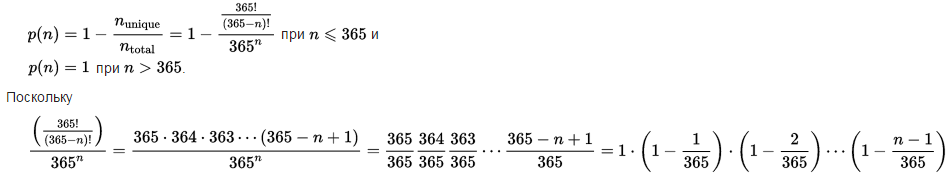
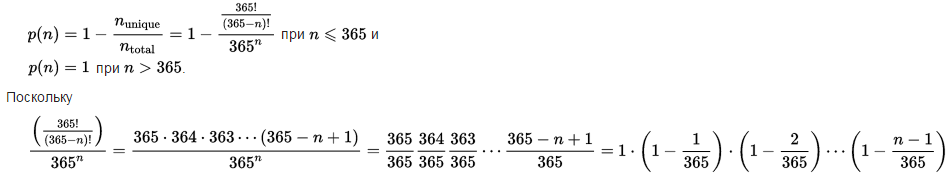
Існує ще один метод визначення ймовірністі:

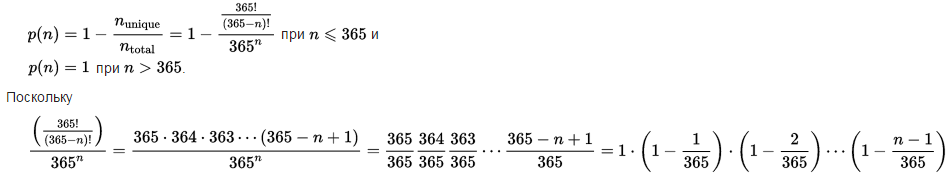
Ймовірність збігу днів народження у двох осіб, що входять в групу з n людей, можна також розрахувати з використанням формул комбінаторики. За формулою Хартлі кількість можливих варіантів днів народження дорівнює 

Кількість можливих варіантів днів народження, в яких дні не повторюються (розміщення з 365 по n), складе

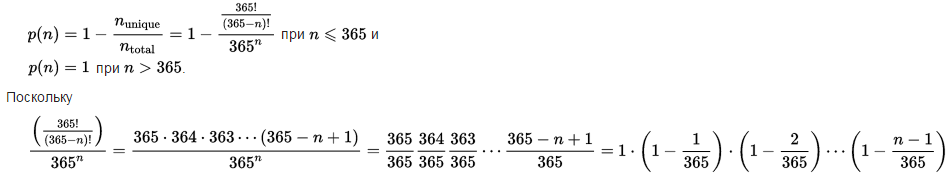


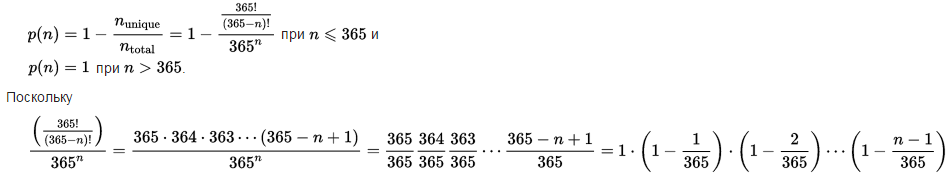
Якщо рядки вибираються випадково (з рівномірним розподілом), ймовірність спів падіння днів народження хоча б у двох людей, дорівнює

, при  і

 при n> 365.

Оскільки





ця формула еквівалентна представленій вище.

# Висновок

Криптографія є багатим джерелом важких математичних задач, а математика – однієї з основ криптографії. Історія показує, що рано чи пізно розвиток математичних методів і техніки призводить до того, що завдання, які здавалися нерозв'язними, вирішуються [7].

В останні десятиліття в криптографії стали з'являтися шифри, стійкість яких обґрунтовується складністю вирішення суто математичних задач: розкладання великих чисел на множники, рішення рівнянь в цілих числах та інше.

Методи і результати різних розділів математики (зокрема, алгебри, комбінаторики, теорії чисел, теорії алгоритмів, теорії ймовірностей і математичної статистики) використовуються як при розробці шифрів, так і при їх дослідженнях, зокрема, при пошуку методів розкриття шифрів.

# Джерела

1. Н. Смарт. Криптография. Москва:Техносфера, 2005. 528 с.

2. Функция Эйлера. Доказательство // Мир математики URL: http://matworld.ru/teorija-chisel/eulers-function.php (дата звернення: 27.03.2017).

3. Малая теорема Ферма // Мир математики URL: http://matworld.ru/teorija-chisel/malaja-teorema-ferma.php (дата звернення: 27.03.2017).

4. Сравнение чисел по модулю // Мир математики URL: http://matworld.ru/teorija-chisel/sravnenie-po-modulju.php#utv5 (дата звернення: 27.03.2017).

5. Парадокс дней рождения // Википедия URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%B0%D0%B4%D0%BE%D0%BA%D1%81\_%D0%B4%D0%BD%D0%B5%D0%B9\_%D1%80%D0%BE%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F (дата звернення: 27.03.2017).

6. Математические основы криптологии // Информационно-коммуникационные технологии в образовании URL: http://www.ict.edu.ru/ft/004940/16.pdf (дата звернення: 27.03.2017).

7. О применениях математики в криптографии // Математическая составляющая URL: http://book.etudes.ru/toc/cryptography/ (дата звернення: 27.03.2017).