МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

С.В. Кондакова

ТЕОРІЯ ТА ПРАКТИКА ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ. ЧАСТИНА 1. ТЕОРІЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Конспект лекцій
для студентів спеціальності
125 «Кібербезпека»

Київ 2023

УДК 004.056.55
К-64

Рецензент Є. Є. Шабала, канд. техн. наук, доцент

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії протокол № 6 від 31 січня 2023 р.

Кондакова С.В.
К-64 Теорія та практика інфраструктури відкритих ключів. Частина 1. Теорія інфраструктури відкритих ключів: конспект лекцій / С.В. Кондакова. - Київ: КНУБА, 2022. – 32 с.

Інфраструктура відкритих ключів (PublicKeyInfrastructure – PKI) – це інтегрований комплекс методів та засобів (набір служб), приз-начених забезпечити впровадження та експлуатацію криптографіч-них систем із відкритими ключами. Ці ключі можуть використовуватися для автентифікації чи шифру-вання цифрового підпису електронних даних. PKI слугує не тільки для створення цифрових сертифікатів, але і для зберігання величезної кількості сертифікатів і ключів, забезпе-чення резервування і відновлення ключів, взаємної сертифікації, ве-дення списків анульованих сертифікатів і автоматичного відновлен-ня ключів і сертифікатів після закінчення терміну їхньої дії. У курсі передбачається формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики криптографічного захисту інформації та криптографічного аналізу. Методичною основою дисципліни є методи і алгоритми алгебраїчної теорії кодів, які базуються на математичному апараті теорії алгебраїчних блокових кодів, теорії ймовірностей та математичної статистики

Призначено для студентів спеціальності 125 «Кібербезпека».

УДК 004.056.55

© С.В. Кондакова,
© КНУБА, 2023

ЗМІСТ

Лекція 1-2. Основи теорії чисел. Прості числа. 4
Контрольні запитання. 12
Лекція 3-4. Розширений алгоритм Евкліда та криптографічна система RSA. 13
Контрольні запитання. 21
Лекція 5-6. Конгруенції, лишки 22
Контрольні запитання 31

Лекція 1-2. Основи теорії чисел. Прості числа.

Теорія чисел є найстарішим розділом математики. Відомий вчений XIX століття Л. Кронекер говорив “Цілі числа створив Господь, все решта – справа рук людських”. Досить часто можна зустріти погляди на теорію чисел як на розвагу, що досить популярна завдяки нескладним та простим для розуміння умовам задач, хоча теорія чисел знайшла своє застосування у найсерйозніших сферах сучасного суспільства.

Перші системи нумерації чисел склалися більше 5000 років тому у Стародавньому Єгипті і утворювали непозиційну систему числення. До цього часу з непозиційних систем числення зберіглася у використанні римська нумерація, виключно якою користувалися в усіх офіційних документах аж до XVIII століття. Ключовими числами цієї нумерації є I – один, V – п’ять, X – десять, L – п’ятдесят, C – сто, D – п’ятсот, M – тисяча.

Пройшло не менше тисячі років, перш ніж виникла звична нам позиційна система числення, у якій числа від нуля до дев’яти мають індивідуальні позначення. Безумовною перевагою цієї системи є можливість виконання в ній арифметичних дій у письмовому вигляді.

З розвитком електронних обчислювальних машин великого поширення набула двійкова система числення (див. п.1.1, сторінка 10). В цій системі особливо зручно виконувати дії додавання та множення.

Зовнішня простота умови характерна для найскладніших задач теорії чисел. Саме це й надало теорії чисел надзвичайної привабливості та зробило її улюбленою наукою не лише професійних математиків. Вважається, що теорія чисел стала систематичною і самостійною наукою, починаючи з праць і відкриттів П. Ферма (1601 – 1665). Однак найбільші й найцікавіші досягнення в цій галузі з’явилися трохи пізніше і належать Леонарду Ейлеру (1707 – 1783).

Найбільш відомою серед проблем теорії чисел є велика теорема Ферма, а саме, рівняння $x^n + y^n = z^n$ при $n > 2$ і $xyz \neq 0$ не має розв’язків у цілих числах. Вперше ця теорема була опублікована у 1670 році, через 5 років після смерті самого Ферма. Пошуки доведення призвели до появи теорії алгебраїчних чисел, теорії подільності в кільцях, тощо. Однак, незважаючи навіть на премію в 100000 марок, призначену в 1906 році астрономом-любителем Г. Вольфскелем, велика теорема Ферма залишалась недоведеною аж до 1995 року. Ендрю Вайлс довів теорему, скориставшись теорією еліптичних кривих (див. п.2.4), методом, запропонованим лише в останні 10 років, що передували його роботі.

Як уже зазначалося, з теорії чисел нас найбільше цікавитимуть задачі, які пов'язані з поняттям простого числа.

Отже, ціле число p називається простим, якщо $p \neq \pm 1$ і єдиними його дільниками є числа ± 1 та $\pm p$. Ціле число, яке не є простим і відмінне від ± 1 називається складеним. Надалі найчастіше ми будемо мати справу з простими натуральними числами. Доведемо три фундаментальні теореми про прості числа.

Теорема (Евкліда). Множина простих чисел нескінченна.

Доведення. Доведення проведемо методом від супротивного. Припустимо, що множина простих чисел скінченна і складається з чисел $p_1, p_2, \ldots, p_s$, де p_s – найбільше просте число. Тоді число $n = p_1 p_2 \ldots p_s + 1$ – складене, оскільки воно більше за p_s. Якщо число складене, то воно повинно мати дільники, найменший з яких природно повинен бути простим числом. Отже, цей дільник – одне із чисел $p_1, p_2, \ldots, p_s$. Нехай цим дільником є p_k, де $1 \leq k \leq s$. Тоді $n \vdots p_k$, $p_1 \cdot p_2 \cdot \ldots \cdot p_s \vdots p_k$. Звідси, $n - p_1 p_2 \ldots p_s = 1 \vdots p_k$, що неможливо, оскільки $p_k > 1$. Таким чином припущення неправильне, множина простих чисел є нескінченною. Теорему доведено.

Теорема (про інтервали). У натуральному ряді існують як завгодно довгі інтервали, що не містять жодного простого числа.

Доведення. Нехай n – деяке натуральне число. Тоді числа

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n+1$$

утворюють послідовність n складених чисел, оскільки діляться відповідно на числа $2, 3, \ldots, n+1$. Всі ці числа в натуральному ряді йдуть підряд. Теорему доведено.

Враховуючи тільки що доведену теорему, досить несподіваним є факт існування великої кількості простих чисел, що відрізняються одне від одного лише на два. Наприклад, 5 і 7, 11 і 13, 41 і 43, 101 і 103, 109 619 і 109 621, $1\,000\,061\,087$ і $1\,000\,061\,089$. В межах 100 000 таких пар 1 000, а в межах $1\,000\,000$ – $8\,000$ пар. Існує навіть припущення, що таких чисел нескінченно велика кількість.

Теорема (основна теорема арифметики). Будь-яке натуральне число $n > 1$ або є простим, або його можна єдиним чином записати у вигляді добутку простих чисел.

Доведення. Спочатку доведемо існування розкладу. Нехай n – довільне натуральне число. Якщо n просте, то твердження теореми справедливе. Нехай n – складене. Тоді $n = p_1 n_1$, де p_1 – найменший простий дільник n. Якщо n_1 –

просте, то твердження теореми справедливе. Нехай n_1 – складене, тоді $n_1 = p_2 n_2$, де p_2 – найменший простий дільник n_1 і т. д. Через кілька кроків процес закінчиться, оскільки в ряді натуральних чисел $n > n_1 > n_2 > \ldots$ може бути не більше ніж n членів. Тоді $n = p_1 p_2 \ldots p_{s-1} p_s$.

Єдиність розкладу числа n доведемо, використовуючи метод математичної індукції. Для $n = 2$ твердження теореми справедливе. Припустимо справедливість його для всіх натуральних k таких, що $2 \le k < n$ і доведемо справедливість для n.

Нехай $n = p_1 p_2 \ldots p_s$ і $n = q_1 q_2 \ldots q_t$ – два розклади числа n в добуток простих множників. Тоді правильна рівність

$$p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t. \qquad (1)$$

Оскільки $q_1 q_2 \ldots q_t \vdots q_1$, то $p_1 p_2 \ldots p_s \vdots q_1$ і принаймні один із співмножників p_i, $1 \le i \le s$, ділиться на q_1. Припустимо, що $p_1 \vdots q_1$. Для простих чисел це можливо лише у випадку, коли $p_1 = q_1$. Поділивши обидві частини рівності (1) на число p_1, отримуємо

$$p_2 \ldots p_s = q_2 \ldots q_t.$$

Оскільки $p_2 \ldots p_s < n$, то за припущенням $s - 1 = t - 1$ і при необхідній нумерації $p_2 = q_2$, $p_3 = q_3$, …, $p_s = q_s$. Тоді $s = t$ і єдиність розкладу числа n доведено.

Таким чином, згідно з основною теоремою арифметики, будь-яке складене число n може бути подане у вигляді

$$n = p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s},$$

де показники $l_1, l_2, \ldots, l_s$ називаються кратностями простих множників у розкладі числа n. У n може бути s різних простих дільників, однак загальне число простих дільників дорівнює $l_1 + l_2 + \ldots + l_s$.

Алгоритм знаходження простих дільників числа n, який слідує з доведення основної теореми арифметики, легко зрозуміти та запрограмувати. Поступово намагаючись розділити задане числа на числа 2, 3, 5, 7, … рано чи пізно буде знайдено його прості дільники, або ж з'ясовано, що n також просте. При цьому перебирати доведеться серед чисел, які менші за $\left[\sqrt{n}\right]$. Справді, складене число повинно мати хоча б два дільники, тобто $n = a \cdot b$. Очевидно, що $a \le \sqrt{n}$ або $b \le \sqrt{n}$ (інакше їх добуток був би більшим від n). Вперше на цей факт звернув увагу Фібоначчі (Леонардо Пізанський).

Зовнішня простота умови задачі часто характерна для найскладніших проблем теорії простих чисел, що залишаються нерозв'язаними на протязі століть. Щоб мати уявлення про складність розв'язання, яку приховує досить проста умова завдання, наведемо деякі приклади.

Чи правильно, що для будь-якого простого числа p різниця $2^{p-1}-1$ ділиться на p?

Чи існує таке просте число p, що $2^{p-1}-1$ ділиться на p^3?

Чи правильно, що будь-яке парне число, яке більше за 2, можна подати у вигляді суми двох простих чисел?

Чи існують два послідовних натуральних числа, відмінних від 8 та 9, кожне з яких є степенем простого числа?

Чи будь-яке непарне просте число можна подати у вигляді суми двох квадратів натуральних чисел?

Чи нескінченна множина пар простих чисел p, $p+2$?

Чи нескінченна множина таких простих чисел p, що число 2^p-1 також просте?

Питання 1) та 2) дуже схожі між собою Більш того, порівнюючи їх, можна навіть припустити, що друге питання легше за перше. Адже для його розв'язання достатньо просто навести приклад простого числа, яке задовольняє вказаній властивості, а в першому питанні подібну властивість необхідно довести для всіх простих чисел. Однак позитивна відповідь на перше питання була отримана Ферма в XVII столітті, а друге питання чекає свого розв'язання і досі.

Третє питання є знаменитою гіпотезою Гольдбаха, яку він сформулював більше двохсот років тому, однак досі її ніхто не зміг ні довести, ні спростувати. Четверте питання відоме під назвою гіпотези Каталана, відповідь на нього також невідома. Однак відомо, що якщо різниця між деяким кубом та деяким квадратом дорівнює ± 1, то цей куб дорівнює 8, а квадрат дорівнює 9. Доведення цього факту належить Ейлеру та не є дуже складним.

Відповідь на питання 5) негативна. Якщо остача від ділення простого числа p на 4 дорівнює 3, то не існує таких цілих чисел x та y, що $x^2+y^2=p$. Цей результат належить Ферма. Він же показав, що якщо залишок від ділення простого числа p на 4 дорівнює 1, то знайдуться цілі числа x та y, сума квадратів яких x^2+y^2 ділиться на p.

Питання 6) – це знаменита теорема про прості числа-близнюки. Відповідь на це питання невідома. Відомо, що нескінченною є множина простих чисел,

множина простих чисел виду $a+kr$, де a та r – взаємно прості. Відомо також, що єдине є число $p=3$, для якого $p+2$ та $p+4$ прості. Питання ж 6) ніби схоже на ці, проте його досі нікому не вдалося розв'язати.

Відповідь на питання 7) також невідома, незважаючи на те, що числа такого типу, названі числами Мерсенна, активно вивчаються вже не одне століття. Доведено лише, що , якщо n – складене, то число 2^n-1 також є складеним.

В сучасних умовах у багатьох випадках користуються кодами з назвою "система шифрування з відкритим ключем". Такі системи були введені у 1976 році вченими Стенфордського та (незалежно) Каліфорнійського університетів. З них широко використовується та найбільш відома система RSA (1978 р., Rivest, Shamir, Adleman), яка базується на теорії простих чисел. В її основі лежать операції, які легко виконуються в одному напрямку і складно у зворотному. Наприклад, легко знайти, що $17\cdot 19=323$. Визначити ж , що число 323 має множниками лише числа 17 і 19 значно складніше.

Отже, для реалізації системи RSA необхідно мати два великих простих числа p та q: для кодування повідомлень за допомогою RSA користуються числом $n=pq$, а для декодування шифровки RSA потрібно знати числа p і q. Безпека системи RSA визначається тим, що розкласти число n на множники p та q (тобто, іншими словами, провести факторизацію числа) важко, оскільки вони дуже великі.

Проблема факторизації є найстарішою у теорії чисел. Вона досить просто вирішується безпосередньою перевіркою для невеликих чисел, проте надзвичайно ускладнюється зі збільшенням порядку числа. Так, на даному етапі відомо, що число $2^{2^{14}}+1$, яке складається з 4993 цифр, складене, однак досі не відомий жоден з його співмножників.

Приклад 1. Розкласти на прості множники число 299. (Провести факторизацію числа 299).

Очевидно, що відразу не так просто вказати дільники цього числа. В шкільному курсі математики як правило розкладають на прості множники невеликі числа, серед дільників яких є 2, 3 або 5, що важливо для початкового розуміння поняття простого числа, проте є малоефективним на практиці. В даному прикладі, для того, щоб розкласти 299 на множники, необхідно пошукати дільники серед простих чисел 2, 3, 5, 7, 11, 13 та 17, оскільки $\left[\sqrt{299}\right]=17$. Числа два, три та п'ять навіть не перевіряємо, оскільки 299 непарне, сума його цифр не ділиться на 3 (дорівнює 20) і 299 не закінчується на

0 чи 5. Серед решти чисел знаходимо, що $299 = 13 \cdot 23$ – це і є шуканий розклад числа на прості множники.

Найгіршим в плані тривалості при застосуванні цього алгоритму є випадок, коли число n виявляється простим. Тоді необхідно виконати до $\left[\sqrt{n}\right]$ ділень, що досить проблематично при великому n. Існує багато інших алгоритмів розкладу цілих чисел на множники, проте жоден з них не можна вважати універсальним. Ефективність використання того чи іншого алгоритму залежить від особливостей самого n. Так, якщо n не дуже велике, або є підстави сподіватися на невеликий простий дільник, то доцільно використовувати розглянутий алгоритм послідовної перевірки. Якщо n має дільник, який не дуже відрізняється від $\sqrt{n}$, то ефективним буде алгоритм Ферма.

Нехай n – дане число і m – найменше ціле, для якого $m^2 > n$. Утворимо числа

$$m^2 - n,\ \ (m+1)^2 - n,\ \ (m+2)^2 - n,\ \ \ldots \qquad (2)$$

Якщо якесь з цих чисел є точним квадратом, отримаємо рівняння $x^2 - n = y^2$, звідки $n = x^2 - y^2 = (x-y)(x+y)$.

Отже, для розв'язання прикладу 1 за алгоритмом Ферма, знаходимо $m = 18$, оскільки $18^2 = 324 > 299$. Шукаючи числа (1), вже на першому кроці отримаємо $18^2 - 299 = 25 = 5^2$. Отже, за формулою різниці квадратів,

$n = 18^2 - 5^2 = (18-5)(18+5) = 13 \cdot 23$.

Приклад 2. Задумайте довільне трицифрове число. Припишіть до нього справа таке саме число. Знайдене шестицифрове число поділіть на 7. Потім знайдену частку поділіть на 11, а нову частку – на 13. Чому знову отримали попереднє число?

Розв'язання. $abcabc = abc000 + abc = abc(1000+1) = abc \cdot 1001$. Розкладаючи число 1001 на множники, маємо $1001 = 7 \cdot 11 \cdot 13$.

Питання про розподіл простих чисел у натуральному ряді – одна з найскладніших задач теорії чисел. Численні спроби багатьох математиків дати точну формулу кількості простих чисел серед перших n чисел натурального ряду виявилися марними: прості числа розподілені серед натуральних дуже неодноманітно. Так в інтервалі від 1 до 100, у першій сотні, є 25 простих чисел, у другій сотні їх 21, у третій – 16, у восьмій – 14 і т. д. Але це не означає, що кількість простих чисел у кожній наступній сотні зменшується. Так, у дев'ятій сотні їх 15, більше, ніж у восьмій і шостій сотнях. Ще Гауссом було

встановлено, що 26379-та сотня не має жодного простого числа, у той час як 27050-та сотня містить 17 простих чисел, тобто більше ніж третя.

Такою ж складною та нерозв'язаною проблемою є проблема пошуку формули простих чисел. Найбільше, що на даному етапі може запропонувати теорія чисел – це функції, серед значень яких прості числа зустрічаються досить часто. Найбільш відомими є функції, які задаються формулами

$$M(n) = 2^n - 1, \qquad F(n) = 2^{2^n} + 1, \qquad p^{\#} + 1, \qquad x^2 + y^2 + 1.$$

де n – натуральне число. Числа з першої формули називаються числами Мерсенна (Марен Мерсенн – священик та математик-любитель сімнадцятого століття), а з другої – числами Ферма. Третя формула називається прайморіальною формулою. Прайморіал $p^{\#}$ – це добуток всіх простих чисел, менших або рівних p, четверта формула – многочлен.

Про числа Мерсенна відомо, що вони є багатим джерелом простих чисел. Відомо, що якщо число n в показнику степеня складене, то складеним буде і $M(n)$. $M(p)$ може бути як простим, так і складеним. Більш того, найбільші з відомих на сьогодні чисел є саме числами Мерсенна. Чи нескінченною є множина простих чисел Мерсенна дотепер невідомо.

Серед чисел Ферма простих відомо дуже мало – це $F(0), F(1), \ldots, F(4)$, хоча досі не доведена і не спростована гіпотеза про те, що простих чисел Ферма необмежена кількість. Сам Ферма помилково припускав, що всі числа такого типу прості. Існує теорема, за якою дільник числа $F(n)$ повинен мати вигляд $2^{n+1} \cdot k + 1$, де $k = 0, 1, 2, \ldots$. Виходячи з цієї теореми, дільники, наприклад числа $F(5) = 4\ 294\ 967\ 297$ слід шукати серед чисел $2^{5+2} \cdot k + 1 = 128 \cdot k + 1$, тобто серед чисел 1, 257, 385, 513, 641. Безпосереднім діленням, переконуємося, що 641 – дільник $F(5)$.

Третя формула задає прості числа при $p = 2(3),\ p = 3(7),\ p = 5(31),\ p = 7(211),\ p = 11(2311)$. Взагалі ж на даному етапі знайдено 16 таких простих чисел, найбільше з яких відповідає $p = 24\,027$ та нараховує 10387 знаків.

У відношенні четвертої формули у 1962 році було доведено, що при цілих x та y вона дає нескінченно багато простих чисел.

Відомо багато теорем, які є критерієм для перевірки того, чи є дане натуральне число простим. Зокрема,

Теорема (Вільсона). Натуральне число $n > 0$ просте тоді і тільки тоді, коли число $(n-1)! + 1$ ділиться на n.

Теорема . Для довільного простого числа p число $2^p - 2$ ділиться на p.

Якщо ж не ставити завдання задати просте число аналітично, то одним з найстаріших методів виписування простих чисел є решето Ератосфена. Метод отримав назву решета, оскільки коли його застосовувати до списку натуральних чисел, складені числа будуть відсіюватись, а прості затримаються. Іноді назву пояснюють тим, що Ератосфен, щоб отримати таблицю простих чисел не підкреслював, а проколював складені числа. Решето Ератосфена, як і інші відомі алгоритми знаходження простих чисел, має переваги та недоліки. До переваг слід віднести простоту програмування та відсутність необхідності знаходити окремі дільники, а до недоліків – неефективність при пошуку дуже великих простих чисел.

Використання решета Ератосфена ґрунтується на наступному правилі. Якщо натуральне число a не ділиться на жодне просте число p таке, що $p \le \sqrt{a}$, то a – просте, в іншому випадку a – складене.

Отже, виписуємо всі непарні цілі числа від 3 до n (в нашому прикладі $n = 51$): 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51.

Парні слід відкинути відразу, оскільки крім 2 всі вони складені. Починаємо просіювати список. Перше число в списку – 3. Починаючи з наступного числа у списку, викреслюємо з нього кожне третє число: 3, 5, 7, ~~9~~, 11, 13, ~~15~~, 17, 19, ~~21~~, 23, 25, ~~27~~, 29, 31, ~~33~~, 35, 37, ~~39~~, 41, 43, ~~45~~, 47, 49, ~~51~~

Таким чином викреслили зі списку всі числа, які кратні трьом та більші за саму трійку.

Вибираємо найменше число зі списку, яке більше трьох і ще не викреслене. Це 5. Викреслюємо кожне п’яте число зі списку, починаючи відлік від семи.

3, 5, 7, ~~9~~, 11, 13, ~~15~~, ~~17~~, 19, ~~21~~, 23, ~~25~~, ~~27~~, 29, 31, ~~33~~, ~~35~~, ~~37~~, ~~39~~, 41, 43, ~~45~~, ~~47~~, 49, ~~51~~

Тепер треба викреслювати кожне сьоме число, починаючи рахувати від 9. Не викресленим до цього серед чисел 21, 35, 49 є лише 49. Його і викреслюємо.

3, 5, 7, ~~9~~, 11, 13, ~~15~~, ~~17~~, 19, ~~21~~, 23, 25, ~~27~~, 29, 31, ~~33~~, ~~35~~, ~~37~~, ~~39~~, 41, 43, ~~45~~, ~~47~~, ~~49~~, ~~51~~

На цьому, згідно з правилом, треба просіювання простих чисел припинити, оскільки наступним не викресленим числом є 11, а $11^2 = 121 > 51$.

Справді, перевіряємо наступне число – 11. 33 вже викреслено. Перевіряємо 13, і т. д. Насправді жодне з чисел, які залишилися у списку після

викреслювання кожного сьомого, викреслені не будуть. Отже, прості числа, які не перевищують 51 мають вигляд

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Контрольні запитання.

Довести теорему Евкліда про нескінченність множини простих чисел.

Довести фундаментальну теорему арифметики про інтервали.

Довести основну теорему арифметики про єдиність розкладу цілого числа на прості множники.

Провести факторизацію чисел 437, 483, 943, 6293 методом спроб або за алгоритмом Ферма.

Показати, що довільне просте число, крім двійки, можна записати або у вигляді $4n+1$, або у вигляді $4n+3$.

Що таке числа Мерсенна та Ферма? Навести приклади.

Використовуючи алгоритм решета Ератосфена, виписати прості числа з інтервалу 1000 – 1050.

Лекція 3-4. Розширений алгоритм Евкліда та криптографічна система RSA.

Вище була сформульована ідея однієї з криптографічних систем – системи RSA, звідки безпосередньо слідує, що для безпечної її реалізації необхідно навчитися певним чином добирати великі числа: по два на кожного користувача.

Розглянемо основні поняття ділення цілих чисел, які допоможуть збагнути принцип роботи системи шифрування з відкритим ключем та системи електронного цифрового підпису.

<u>Ціле число</u> a <u>ділиться на ціле число</u> b, якщо існує таке ціле число c, що виконується умова $a = b \cdot c$, де a – ділене або кратне числа b, b – дільник, c – частка. Нуль ділиться на будь-яке ціле число. Число a ділиться на нуль тоді і тільки тоді, коли $a = 0$.

Ділення націло числа a на число b позначають $a \vdots b$, якщо a не ділиться на число b, то позначають $a \not\vdots b$.

<u>Розділити</u> ціле число a на ціле число $b \neq 0$ з остачею означає знайти два цілих числа q і r таких, що 1) $a = bq + r$; 2) $0 \le r < |b|$, де a – ділене, b – дільник, q – неповна частка, r – остача від ділення. В спеціальній літературі зустрічаються різні способи позначення остачі від ділення, наприклад $r = R_b(a)$, $r = a(\mathrm{mod}\, b)$. Ми будемо користуватися останньою формою запису.

Теорема 1. Для будь-яких цілих чисел a та b, де $b \neq 0$, завжди існує одна і лише одна пара цілих чисел q і r таких, що $a = bq + r$, де $0 \le r < |b|$, причому q дорівнює цілій частині числа $\frac{a}{b}$: $q = \left[\frac{a}{b}\right]$.

Доведення. Існування. Оскільки числа a та b – цілі, $b \neq 0$, то число $\frac{a}{b}$ – раціональне. Позначимо через q цілу частину числа $\frac{a}{b}$: $q = \left[\frac{a}{b}\right]$. Нагадаємо, що цілою частиною дійсного числа x називається таке найбільше ціле число q, що не перевищує x, тобто $0 \le x - [x] < 1$. Тоді $0 \le \frac{a}{b} - q < 1$. Помноживши останні нерівності на $b > 0$, отримуємо: $0 \le a - bq < b$. Позначимо число $a - bq = r$, тоді $a = bq + r$, де $0 \le r < b$.

При $b < 0$ позначаємо $b_1 = -b > 0$ і за аналогією повторюємо доведення.

Єдиність. Нехай існує дві пари цілих чисел таких, що

$a = bq + r$, де $0 \le r < b$; (3)

$a = bq_1 + r_1$, де $0 \le r_1 < b$, (4)

і нехай $r \ge r_1$. Віднімаючи від рівності (3) рівність (4), маємо $0 = b(q - q_1) + (r - r_1)$, або $b(q_1 - q) = r - r_1 \ge 0$. Тоді $(r - r_1) \vdots b$, причому $0 \le r - r_1 < b$. Отже, це можливо лише у випадку, коли $r - r_1 = 0$. Тоді $r = r_1$, $b(q_1 - q) = 0$. Звідси $q_1 - q = 0$, тобто $q_1 = q$. Теорему доведено.

Приклад 3. Знайти q і r, якщо $a = 23$, $b = 2$.

Розв'язання: $23 = 2 \cdot 11 + 3$; $q = 11$, $r = 1$.

Приклад 4. Довести, що жодне із чисел виду $3k + 2$, $k \in Z$, не може бути квадратом цілого числа.

Розв'язання. Припустимо, що існує таке число s, що $s^2 = 3k + 2$. За попередньою теоремою, для чисел s та 3 існує єдина пара таких чисел q та r, що $s = 3q + r$, де $r = 0,1,2$.

Нехай $r = 0$. Тоді $s^2 = 3k + 2 = 9q^2$, звідки $2 = 9q^2 - 3k = 3(3q - k)$, що означає $2 \vdots 3$, а це неможливо, тому $r \ne 0$.

Нехай $r = 1$. Тоді $s^2 = 3k + 2 = (3q + 1)^2 = 9q^2 + 6q + 1$, звідки $2 - 1 = 9q^2 + 6q - 3k = 3(3q^2 + 2q - k)$, а це означає, що $1 \vdots 3$, що також неможливо, отже $r \ne 1$.

Нехай $r = 2$. Тоді $s^2 = 3k + 2 = (3q + 2)^2 = 9q^2 + 12q + 4$. Оскільки $4 - 2 = 3k - 9q^2 - 12q = 3(k - 3q^2 - 4q)$, то, як і в першому випадку, $2 \vdots 3$, знову прийшли до суперечності. Оскільки інших варіантів для r не існує, припущення про існування такого s, що $s^2 = 3k + 2$ неправильне. Приклад розв'язано.

Ціле число c називається спільним дільником цілих чисел a та b, якщо $a \vdots c$ і $b \vdots c$.

Число 0 може бути спільним дільником чисел a і b тоді і лише тоді, коли $a = 0$ і $b = 0$.

Найбільшим спільним дільником цілих чисел a та b, одночасно не рівних нулю, називається такий додатній спільний дільник, який ділиться на будь-який інший спільний дільник цих чисел. Позначається $d = (a,b)$ або НСД(a,b).

Для чисел a і b, які одночасно дорівнюють нулю, поняття найбільшого спільного дільника не вводиться. Якщо $НСД(a,b) = 1$, то числа a та b називають взаємно простими.

Взаємно прості числа відіграють у математиці наскільки важливу роль, що ними визначається навіть окрема функція. Функція Ейлера $\varphi(m)$ – числова функція, значення якої для будь-якого натурального числа m дорівнює кількості натуральних чисел, взаємно простих з m, які не перевищують m.

На практиці для обчислення значення функції Ейлера користуються наступною теоремою та наслідками з неї.

Теорема 2. Якщо число p - просте, то $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$, де $k \in N$.

Наслідок 1. Якщо число p - просте, то $\varphi(p) = p - 1$.

Наслідок 2. Якщо натуральне число n розкласти на прості множники, причому $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, то значення функції Ейлера обчислюється за формулою $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$.

Знаходження НСД двох чисел здійснюється за алгоритмом Евкліда, який ще називається методом послідовного ділення з остачею. Цей алгоритм ґрунтується на двох лемах.

Лема 1. Нехай a і b – цілі числа, $b > 0$. Якщо $a \vdots b$, то $НСД(a,b) = b$.

Лема 2. Якщо $a = bq + r$, де a, b і r відмінні від нуля цілі числа, то $НСД(a,b) = НСД(b,r)$.

Доведення. Нехай $d = НСД(a,b)$, $d_1 = НСД(b,r)$. Тоді $a \vdots d$, $b \vdots d$, а отже $a - bq = r \vdots d$. Це означає, що d – спільний дільник чисел b і r, тобто $d_1 \vdots d$. Оскільки $d_1 = НСД(b,r)$, то $b \vdots d_1$ і $r \vdots d_1$, а значить $bq + r = a \vdots d_1$, тобто d_1 – спільний дільник чисел a та b. Тоді $d \vdots d_1$. Оскільки d та d_1 – натуральні числа, то $d = d_1$. Лему доведено.

Приклад 5. Розглянемо послідовність натуральних чисел у якій кожне число, починаючи з третього, є сумою двох попередніх:

1, 1, 2, 3, 5, 8, 13, 21, …

Ці числа називають числами Фібоначчі (1180 – 1240). Вони, зокрема, цікаві тим, що відношення кожного наступного числа послідовності Фібоначчі до попереднього (починаючи з четвертого): $\frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \ldots$ наближено задають відношення довжини відрізка до більшої його частини в золотому перерізі. Алгебраїчне знаходження золотої середини відрізка $AB = a$ зводиться до

розв'язання рівняння $\frac{a}{x}=\frac{x}{a-x}$, яке ще називають характеристичним рівнянням Фібоначчі. Золотий переріз відомий як найбільш гармонічний спосіб ділення на частини, який знайшов своє відображення в багатьох творах світового мистецтва. Сам термін «Золотий переріз» був введений Леонардом да Вінчі (1452 – 1519).

Довести, що найбільший спільний дільник двох послідовних членів послідовності Фібоначчі дорівнює одиниці, тобто два сусідні числа Фібоначчі є взаємно простими.

Доведення. Нехай u_k - k-й член послідовності Фібоначчі. Тоді за означенням $u_{k+1}=u_k+u_{k-1}$. Останню суму можна розглядати як результат ділення u_{k+1} на u_k: $u_{k+1}=u_k\cdot 1+u_{k-1}$, де $q=1$, $r=u_{k-1}$. За лемою 2 $НСД(u_{k+1},u_k)=НСД(u_k,u_{k-1})$. Аналогічно, оскільки за означенням $u_k=u_{k-1}\cdot 1+u_{k-2}$, за лемою 2 $НСД(u_k,u_{k-1})=НСД(u_{k-1},u_{k-2})$.

Повторюючи дію k раз, підійдемо до перших членів послідовності, для яких твердження про те, що вони взаємно прості, не викликає сумніву. Отже

$НСД(1,2)=НСД(2,3)=\ldots=НСД(u_{k+1},u_k)=1$, для $k=\overline{2,\infty}$. Твердження доведено.

<u>Алгоритм Евкліда</u>, або спосіб послідовного ділення з остачею, полягає в наступному: нехай a та b – цілі числа, причому $0<b<a$. Поділимо з остачею a на b: $a=bq_0+r_1$, $0\le r_1<b$. Якщо $r_1=0$, то $a\vdots b$, і, в силу леми 1, $НСД(a,b)=b$.

Нехай $0<r_1<b$. Тоді b ділимо з остачею на r_1: $b=r_1q_1+r_2$, $0\le r_2<r_1$.

Якщо $r_2=0$, то $b\vdots r_1$ і, за лемами 1 та 2, $НСД(a,b)=НСД(b,r_1)=r_1$.

Нехай $0<r_2<r_1$. Ділимо з остачею r_1 на r_2: $r_1=r_2q_2+r_3$, $0\le r_3<r_2$ і т. д. Процес вважається закінченим, коли отримаємо остачу, що дорівнює нулю. Легко переконатися, що отриманий алгоритм є скінченний. Дійсно, остачі r_1, r_2, … за означенням є цілими додатними числами і задовольняють умову $b>r_1>r_2>\ldots$. Але таких остач може бути не більше b. Отже через кілька кроків отримаємо $r_{n+1}=0$. Запишемо отримані рівності:

$$
\begin{aligned}
&a = bq_0 + r_1, \quad \text{де} \quad 0 < r_1 < b;\\
&b = r_1 q_1 + r_2, \quad \text{де} \quad 0 < r_2 < r_1;\\
&r_1 = r_2 q_2 + r_3, \quad \text{де} \quad 0 < r_3 < r_2;\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad \text{де} \quad 0 < r_n < r_{n-1};\\
&r_{n-1} = r_n q_n, \quad r_{n+1} = 0.
\end{aligned}
\tag{5}
$$

Використовуючи леми 1 та 2, з рівностей (5) отримаємо:

$НСД(a,b) = НСД(b,r_1) = НСД(r_1,r_2) = ... = НСД(r_{n-1},r_n) = r_n > 0$.

Отже справедлива наступна теорема.

Теорема 3. Для будь-яких цілих чисел a і b, одночасно не рівних нулю, НСД завжди існує і дорівнює останній відмінній від нуля остачі, отриманій за алгоритмом Евкліда.

Приклад 5. Знайти найбільший спільний дільник чисел 1232 та 98.

Розв'язання. Послідовне ділення з остачею за схемою (5) виглядатиме так

$1232 = 98 \cdot 12 + 56;$

$98 = 56 \cdot 1 + 42;$

$56 = 42 \cdot 1 + 14;$

$42 = 14 \cdot 3.$

Останній відмінний від нуля залишок дорівнює 14. Отже, $НСД(1232, 98) = 14$.

Слід відмітити, що неповні частки від ділення не враховуються при підрахунку найбільшого спільного дільника.

В криптографії можливість використання будь-якого алгоритму визначається складністю цього алгоритму. Існує кілька оцінок складності алгоритму Евкліда. Зокрема, найбільш можлива кількість кроків алгоритму Евкліда для заданих чисел a та b за формулою, виведеною Ламе (1795 – 1870), не перевищує $\left[\log_{|\Phi|}(\sqrt{5}n)\right] - 2 \approx \left[4,785 \cdot \lg n + 1,672\right] - 2$, де $n = \max\{a,b\}$, $|\Phi| = \dfrac{1+\sqrt{5}}{2}$ – модуль кореня характеристичного рівняння послідовності Фібоначчі. Тому, наприклад, для будь-якої пари чисел, менших за мільйон, алгоритм спрацьовує не більше ніж за $\left[4,785 \cdot 6 + 1,672\right] - 2 = 30 - 2 = 28$ кроків.

Для отримання секретного ключа за системою шифрування RSA необхідно вміти знаходити лінійне подання НСД двох чисел, тобто вміти знайти x та y такі, що $a \cdot x + b \cdot y = \text{НСД}(a,b)$. Наступну теорему іноді ще називають <u>розширеним алгоритмом Евкліда</u>.

Теорема 4 (про лінійне подання НСД). Якщо d – найбільший спільний дільник чисел a і b, то існують цілі числа x та y такі, що

$a \cdot x + b \cdot y = d$.

Доведення. З рівностей (5) знаходимо

$r_1 = a - bq_0$;

$r_2 = b - r_1 q_1$;

$r_3 = r_1 - r_2 q_2$;

.....

$r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$;

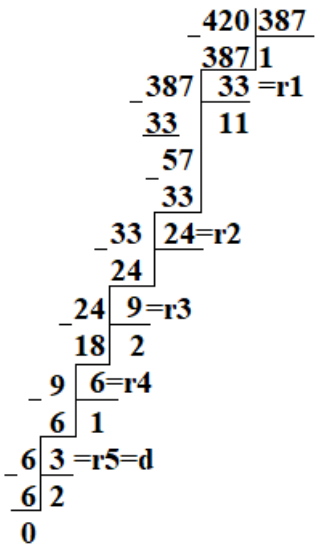
$r_n = d = r_{n-2} - r_{n-1} q_{n-1}$.

Послідовно підставляючи замість r_{n-2}, r_{n-1}, …, r_1 їх лінійні подання, отримаємо $d = ax + by$.

Для обчислення найбільшого спільного дільника та його лінійного подання існує кілька досить зручних форм запису. Одна з них продемонстрована у наступному прикладі.

Приклад 6. Знайти лінійне подання НСД чисел 387 та 420.

Розв'язання. Тут $a = 420$, $b = 387$. Виконавши ділення за алгоритмом Евкліда, отримаємо



Звідси можна записати систему рівнянь

$a = 420 = 1 \cdot b + r_1$

$b = 11 \cdot r_1 + r_2$

$r_1 = 1 \cdot r_2 + r_3 = r_2 + r_3$

$r_2 = 2 \cdot r_3 + r_4$

$r_3 = 1 \cdot r_4 + d = r_4 + d$

Поступово рухаючись від п'ятого рівняння до першого отримаємо

$d = r_3 - r_4 = r_3 - (r_2 - 2r_3) = -r_2 + 3r_3 = -r_2 + 3(r_1 - r_2) =$
$= 3r_1 - 4r_2 = 3r_1 - 4(b - 11r_1) = -4b + 47r_1 = -4b + 47(a - b) = 47a - 51b$

Перевірка. $47 \cdot 420 - 51 \cdot 387 = 19740 - 19737 = 3$.

Відповідь: 3= $d = 47a - 51b$.

Навчившись розкладати число на прості множники, ділити цілі числа, знаходити значення функції Ейлера та виконувати розширений алгоритм Евкліда, можна перейти до ознайомлення з принцип роботи відомої системи RSA та електронного цифрового підпису на прикладі невеликих чисел.

Нагадаємо, що для реалізації цієї системи необхідно мати два прості числа p та q. На практиці це випадкові великі прості числа, які знищуються після формування числа $n = p \cdot q$, та чисел l та d, які є відповідно відкритим та секретним ключем шифру. Функція Ейлера, $\varphi(n) = (p-1)(q-1)$. Візьмемо довільне $1 \le l < \varphi(n)$ таке, що НСД($l, \varphi(n)$)=1. Тоді за розширеним алгоритмом Евкліда існує єдине $1 \le d < \varphi(n)$ таке, що $dl + y\varphi(n) = 1$.

Отже, нехай x - повідомлення, яке потрібно зашифрувати. Шифрування здійснюється за формулою $RSA(x) = x^l (\mathrm{mod}\, n) = c$, тобто знаходять остачі від ділення числа x^l на n. Для розшифрування використовують секретний ключ шифру d та формулу $x = c^d (\mathrm{mod}\, n)$.

Як правило повідомленнями є тексти, які можна подати у вигляді цілого числа, якщо кожній букві поставити у відповідність порядок її розміщення у певному алфавіті. Зокрема,

а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16

н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ю	я	ь
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

При цьому зліва чисел, які позначаються однією цифрою, приписують 0, щоб уникнути неоднозначності при оберненому перетворенні чисел на відповідні букви). Інтервал між словами можна позначати числом 33 або 00.

Приклад 7. Доберемо 2 довільні прості числа. Нехай $p = 3$, $q = 11$. Визначимо $n = pq = 3 \cdot 11 = 33$. Тоді значення функції Ейлера $\varphi(33) = (3-1)(11-1) = 20$. Вибираємо відкритий ключ l, такий, що НСД $(l, 20) = 1$. В нашому випадку допустимими значеннями числа l є числа: 3, 7, 9, 11, 13, 17, 19. Знову ж таки, щоб уникнути громіздких обчислень, беремо $l = 3$.

За допомогою розширеного алгоритму Евкліда формуємо секретний ключ d: $d \cdot 3 + y \cdot 20 = 1$.

Записуємо

$$
\begin{array}{r|l}
20 & 3 \\ \hline
-18 & 6 \\ \hline
3 & 2=r1 \\ \hline
-2 & 1 \\ \hline
2 & 1=r2=d \\ \hline
-2 & 2 \\ \hline
0 &
\end{array}
$$

Звідси отримуємо систему рівностей $\begin{cases} \varphi(n) = 6l + r_1 \\ l = r_1 + 1. \end{cases}$

Тому $1 = l - (\varphi(n) - 6l) = 7l - \varphi(n)$. Отже, секретний ключ $d = 7$.

Публікується відкритий ключ $(l, n) = (3, 33)$ за допомогою якого учасники системи секретного зв'язку зашифровують свої повідомлення і відправляють їх адресату.

Нехай таким повідомленням буде прізвище виданого вченого XVIII століття - Ейлер: е – 6, й – 13, л – 15, е – 6, р – 20. Щоб уникнути операцій з великими числами, будемо кодувати та розкодовувати за допомогою алгоритму RSA кожну букву окремо, хоча на практиці на кожному такті шифрування беруть відразу досить великий блок відкритого тексту, тобто можна прийняти $x = 613150620$.

Тоді RSA(е)=RSA(6) = $6^3 (\mathrm{mod}\, 33) = 27$, оскільки $216 = 33 \cdot 6 + 18$;

RSA(й)=RSA(13) = $13^3 (\mathrm{mod}\, 33) = 19$, оскільки $2197 = 33 \cdot 66 + 19$;

RSA(л)=RSA(15) = $15^3 (\mathrm{mod}\, 33) = 9$, оскільки $3375 = 33 \cdot 102 + 9$;

RSA(р)=RSA(20) = $20^3 (\mathrm{mod}\, 33) = 14$, оскільки $8000 = 33 \cdot 242 + 14$.

Отримали зашифроване повідомлення $c = 1819091814$, якому відповідає беззмістовний набір букв.

Для розшифровування розбиваємо його на блоки по 2 елементи і, користуючись секретним ключем $d = 7$, знаходимо:

$18^7 (\mathrm{mod}\, 33) = 612220032 (\mathrm{mod}\, 33) = 6$, $612220032 = 33 \cdot 18552122 + 6$;

$19^7 (\mathrm{mod}\, 33) = 893871739 (\mathrm{mod}\, 33) = 13$, $893871739 = 33 \cdot 27087022 + 13$;

$9^7 (\mathrm{mod}\, 33) = 4782969 (\mathrm{mod}\, 33) = 15$, так як $4782969 = 33 \cdot 144938 + 15$;

$14^7 (\mathrm{mod}\, 33) = 105413504 (\mathrm{mod}\, 33) = 20$, так як $105413504 = 33 \cdot 3194348 + 20$, тобто маємо початкову числову комбінацію.

Алгоритм електронного підпису виглядає наступним чином. Нехай M - повідомлення, яке необхідно підписати. Тоді підпис здійснюється за формулою $C = M^d (\bmod n)$, звідки (M, C) - повідомлення з підписом. Перевірка підпису виконується за формулою $C^l (\bmod n) = M'$. Якщо існує таке ціле число k, що $M = M' + nk,\ k \in \mathrm{N}$, то підпис вірний.

Приклад 8. Нехай треба підписати повідомлення «ні», тобто «1711». Візьмемо секретний ключ попереднього прикладу, $d = 7$. Тоді $1711^7 (\bmod 33) =$ 19 і $(M, C) = (1711, 19)$. Перевіряємо отриманий підпис, $19^3 (\bmod 33) = 28 = M'$. Оскільки в результаті додавання до числа 28 числа кратного 33 отримуємо 1711 (28+51·33=1711), можна стверджувати, що підпис правильний.

У нашому прикладі секретний ключ можна легко знайти перебором. На практиці це виконати неможливо, оскільки рекомендована довжина блоку відкритого тексту n складає в даний час біля двохсот цифр для приватних осіб, чотирьохсот та більше шестисот цифр відповідно для комерційної та таємної інформації. При цьому ці числа вимушені весь час збільшуватися через швидке вдосконалення комп'ютерної техніки. Так у 1977 році творці системи RSA використовували n, яке мало 129 цифр. На той час ними було підраховано, що для злому такої системи потрібно буде $40 \cdot 10^{15}$ років. Проте у 1986 році 129-значне число було розкладене на множники завдяки оновленим комп'ютерам та об'єднаним зусиллям користувачів Інтернетом. Для цього знадобилося 8 місяців роботи 600 комп'ютерів добровольців з 25 різних країн.

Контрольні запитання.

1. Сформулювати правило ділення цілих чисел.
2. Довести теорему про ділення цілих чисел з остачею.
3. Що називається найбільшим спільним дільником чисел? Дільником чисел?
4. Які числа є взаємно простими?
5. Обчислити $\varphi(25)$, $\varphi(152)$, $\varphi(113)$.
6. Довести, що два послідовні числа послідовності Фібоначчі взаємно прості.
7. Довести правильність алгоритму Евкліда для знаходження найбільшого спільного дільника двох цілих чисел.
8. Сформулювати розширений алгоритм розширений алгоритм Евкліда.
9. Знайти лінійне зображення найбільшого спільного дільника чисел 2345 і 1125.
10. Розшифрувати (200615010018230804), якщо $(l, n) = (7; 33)$.

Лекція 5-6. Конгруенції, лишки

В попередньому параграфі було розглянуто основи теорії чисел та описано ряд алгоритмів, за допомогою яких можна знайти найбільший спільний дільник двох чисел, отримати дільники числа та розкласти його на прості множники, визначити, чи є простим задане число. Проте істотним недоліком цих алгоритмів є те, що їх практично не можна застосувати до великих чисел, а саме з такими числами має справу сучасна криптографія. Наприклад, треба показати, що $F(23471)$ ділиться на число $5\cdot 2^{23\,473}+1$. Користуючись логарифмами, нескладно показати, що число $F(23471)$ містить більше ніж $10^{7\,063}$ знаки. Отже, безпосереднім діленням факт подільності встановити проблематично. Для цього стає в нагоді теорія конгруенцій, яка є основою сучасної криптографії. В перекладі на українську congruent, congruous означає порівняння, зокрема в російськомовній літературі за теорією конгруенцій закріпилася назва «теория сравнений».

Щоб мати уявлення про конгруентні числа, достатньо подивитись на рис. 2.1. Числа, записані в одному секторі, є конгруентними за модулем а) 3, б)8; в)12 відповідно.

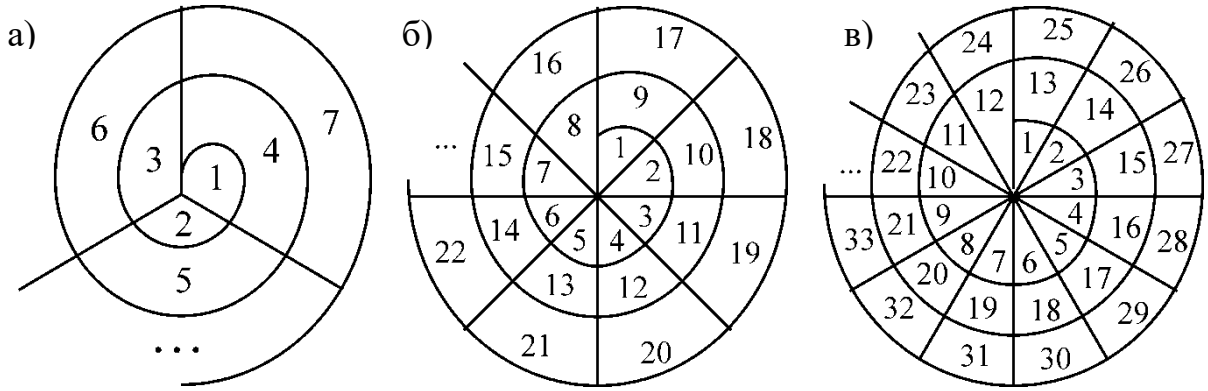


Рис. 2.1

При операціях з конгруентними числами варто пам’ятати основний принцип: будь-яке ціле число можна замінити на конгруентне йому за модулем. Тобто числа, які стоять в одному секторі при еквівалентних перетвореннях можна змінювати на інші з цього ж сектора.

Для двох чисел a та b, конгруентних за модулем m, використовують запис $a\equiv b(\mathrm{mod}\,m)$. Наприклад, дивлячись на малюнок, можна записати $1\equiv 7(\mathrm{mod}\,3)$, $1\equiv 17(\mathrm{mod}\,8)$, $3\equiv 15(\mathrm{mod}\,12)$.

Зручність використання конгруентних чисел демонструє загальноприйнятий формат годинників. Наприклад, коли говорять, що робочий день закінчується о шостій годині, насправді всім зрозуміло, що мається на

увазі 18.00, тобто $18 \equiv 6(\mathrm{mod}12)$. Конгруентними числами користувалися досить давно, наприклад їх використовували ще стародавні астрономи та астрологи. Проте чіткого означення та систематизації теорія набула в XIX ст. завдяки працям К. Гаусса (1777 – 1855).

Для перевірки чисел на конгруентність найчастіше користуються наступним означенням.

Означення 1. Два цілі числа a та b називаються конгруентними за модулем m, якщо різниця $a-b$ ділиться на m, $(a-b)\vdots m$.

Приклад 1. $26 \equiv 1(\mathrm{mod}5)$, оскільки $26-1=25\vdots 5$;

$-23 \equiv 7(\mathrm{mod}10)$, оскільки $-23-7=-30\vdots 10$.

Нескладно показати, що означенню 1 еквівалентні наступні два означення.

Означення 2. Два цілі числа a та b називаються конгруентними за модулем m, якщо при діленні на m вони дають однакові остачі.

Приклад 2. $26 \equiv 1(\mathrm{mod}5)$, оскільки $26=5\cdot 5+1$ і $1=0\cdot 5+1$;

$-23 \equiv 7(\mathrm{mod}10)$, оскільки $-23=-3\cdot 10+7$ і $7=0\cdot 10+7$.

Означення 3. Два цілі числа a та b називаються конгруентними за модулем m, якщо вони пов'язані співвідношенням $a=b+mt$, де $t \in Z$.

Приклад 3. $26 \equiv 1(\mathrm{mod}5)$, оскільки $26=1+5\cdot 5$;

$-23 \equiv 7(\mathrm{mod}10)$, оскільки $-23=7+10\cdot(-3)$.

В залежності від ситуації будемо користуватися одним з цих трьох рівнозначних означень.

З поняттям конгруенції тісно пов'язане ще одне ключове поняття, яке широко використовується у криптографії.

Число r, $0 \le r \le m-1$, називається лишком числа a за модулем m, якщо $a \equiv r(\mathrm{mod}\, m)$.

Приклад 4. Знайти лишок числа $a=2351$ за модулем $m=2$.

Розв'язання. Очевидно, що для модуля рівного 2, $r=1$ для всіх непарних чисел, яким є задане за умовою a.

Множина **всіх цілих чисел** r, конгруентних числу a за модулем m, називається класом лишків за модулем m. Позначається $K_a^{(m)}$. На рис. 2.1 елементи кожного з секторів утворюють клас лишків за відповідним модулем $K_a^{(3)}$, $K_a^{(8)}$, $K_a^{(12)}$. Очевидно, що кожному модулю m відповідає рівно m різних класів лишків.

Конгруенції зручні тим, що для них зберігаються властивості звичайних числових рівностей.

Конгруенції за одним і тим же модулем можна почленно додавати;

Конгруенції за одним і тим же модулем можна почленно віднімати;

Доданок, що стоїть у якій-небудь частині конгруенції, можна переносити в іншу частину, змінивши знак на протилежний;

До обох частин конгруенції можна додати (або від обох частин конгруенції можна відняти) одне і те саме ціле число;

До будь-якої з частин конгруенції можна додати (або відняти) довільне ціле число, кратне модулю;

Конгруенції за одним і тим же модулем можна почленно перемножувати;

Обидві частини конгруенції можна помножити на одне і те саме ціле число;

Обидві частини конгруенції можна піднести до одного і того самого натурального степеня, тобто, якщо $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$, де $n \in N$.

Обидві частини конгруенції можна поділити на їх спільний дільник, взаємно простий з модулем;

Обидві частини конгруенції і модуль можна помножити на одне і те саме натуральне число;

Обидві частини конгруенції і модуль можна поділити на будь-який їхній спільний натуральний дільник;

Якщо конгруенція має місце за кількома модулями, то вона матиме місце і за модулем, що дорівнює їхньому найменшому спільному кратному;

Якщо конгруенція має місце за модулем m, то вона матиме місце і за будь-яким натуральним дільником d цього модуля;

Якщо $a \equiv b(\mathrm{mod}\, m)$, то НСД$(a,m)$=НСД$(b,m)$.

Користуючись одним з трьох означень конгруентності, лемами 1, 2 попереднього параграфа, можна показати правильність цих властивостей. Для прикладу доведемо властивість 1, властивість 4 та властивість 9.

Нехай $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$. Отже, за означення 3, $a = b + mt_1$, $c = d + mt_2$, де $t_1, t_2 \in Z$. Додамо почленно ці дві рівності. Отримаємо $a + c = b + d + m(t_1 + t_2)$, тобто, за означенням $a + c \equiv b + d(\mathrm{mod}\, m)$.

Додаючи до конгруенції $a \equiv b(\mathrm{mod}\, m)$ тривіальну конгруенцію $c \equiv c(\mathrm{mod}\, m)$, як наслідок з властивості 1, отримаємо правильну конгруенцію $a + c \equiv b + c(\mathrm{mod}\, m)$. Тобто властивість 4 доведено.

Нехай $ak \equiv bk(\mathrm{mod}\, m)$, де НСД$(k,m) = 1$. Тоді, за означенням 1, $ak - bk = (a-b)k \vdots m$. З теорії чисел відомо, що у випадку взаємно простих k та m це можливо лише тоді, коли $(a-b) \vdots m$, тобто правильним буде $a \equiv b(\mathrm{mod}\, m)$.

Приклад 5. Довести, що $2^{625} \equiv 2(\mathrm{mod}10)$.

Розв'язання. За означенням можна показати, що правильною є конгруенція $2^2 \equiv -1(\mathrm{mod}5)$. Тоді, за властивістю 8 правильною буде і конгруенція $(2^2)^{312} \equiv (-1)^{312}(\mathrm{mod}5)$, тобто $2^{624} \equiv 1(\mathrm{mod}5)$. Скориставшись властивістю 10, помножимо отриману конгруенцію на 2, в результаті чого отримаємо $2^{625} \equiv 2(\mathrm{mod}10)$.

Приклад 6. Знайти остачу від ділення 12331^{12331} на 9 (знайти лишок числа 12331^{12331} за модулем 9).

Розв'язання. Згадуючи критерій подільності чисел на 9, запишемо правильну конгруенцію $12331 \equiv 1(\mathrm{mod}9)$, правильність якої нескладно перевірити ще й за означенням. Скориставшись властивістю 8, отримаємо $12331^{12331} \equiv 1(\mathrm{mod}9)$, тобто, за означенням конгруентності, шукана остача дорівнює 1.

Приклад 7. Знайти останню цифру числа 7^{7^7}.

Розв'язання. Завдання цього прикладу можна сформулювати як і у прикладі 5, тобто знайти остачу від ділення 7^{7^7} на 10.

Визначимо спершу якому числу є конгруентним показник степеня 7^7. Очевидно, що $7 \equiv -3(\mathrm{mod}10)$, а $9 \equiv -1(\mathrm{mod}10)$. Тоді, піднісши до квадрату обидві частини першої конгруенції (властивість 8), в силу транзитивності, отримаємо

$7^2 \equiv -1(\mathrm{mod}10)$, отже $7^4 \equiv 1(\mathrm{mod}10)$ (за властивістю 8). Тому $7^7 = 7^4 \cdot 7^2 \cdot 7 \equiv 1 \cdot (-1) \cdot (-3) = 3(\mathrm{mod}10)$. Звідси

$7^{7^7} \equiv 7^3 \equiv 3(\mathrm{mod}10)$.

Наступні дві теореми, теорема Ейлера, та її частинний випадок мала теорема Ферма, значно спрощують та скорочують розв'язання завдань, подібних до тих, які розглянуті у прикладах 5 – 7.

Теорема (мала теорема Ферма). Якщо a - довільне ціле число, то для будь-якого простого p, такого, що НСД$(a, p) = 1$, справедливою є конгруенція

$a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

З малою теоремою Ферма пов'язана гіпотеза, яка відома під назвою китайської: «ціле число n тоді і тільки тоді є простим, коли $2^n - 2$ ділиться на n, тобто $2^{n-1} \equiv 1(\mathrm{mod}\, n)$». Сформульована вона була у V столітті, проте лише у IX столітті її було дещо спростовано. Тобто, якщо p - довільне просте число,

то справді $2^{p-1} \equiv 1(\bmod p)$, проте це справедливо і для деяких складених чисел. Наприклад, $2^{340} \equiv 1(\bmod 341)$, хоча число $341 = 11 \cdot 31$ є складеним. Останнє твердження буде доведене у прикладі 7.

Тут слід відзначити, що незважаючи на хибність китайської гіпотеза її успішно використовують при розробці тестів, що досліджують числа на простоту. Якщо для деякого натурального n вдається знайти таке a, що

$$a^{n-1} \not\equiv 1(\bmod n), \qquad (6)$$

то n - складене (a достатньо брати з інтервалу $1 < a < n-1$). Якщо ж для всіх перевірених a

$$a^{n-1} \equiv 1(\bmod n), \qquad (7)$$

то n може бути простим. Складені числа, для яких виконується мала теорема Ферма називають псевдопростими, число a з (6) називається свідком складеності числа n. Враховуючи, що псевдопрості числа зустрічаються досить рідко (наприклад, між 1 і 10^9 є 50 847 544 простих і лише 5 597 псевдопростих для $a = 2$), розглянутий спосіб можна використовувати поряд з методом поступової перевірки та методом факторизації Ферма (див. приклад 1, ст. 80).

Теорема (Ейлера). Якщо a - довільне ціле число, то для будь-якого натурального m, такого, що НСД$(a,m) = 1$, справедливою є конгруенція

$$a^{\varphi(m)} \equiv 1(\bmod m).$$

Доведення. Нехай числа $r_1, r_2, \ldots, r_{\varphi(m)}$ утворюють систему найменших невід'ємних лишків за модулем m. Оскільки $(a,m) = 1$, то, числа $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ також утворюють зведену систему лишків за модулем m.

Нехай

$$\begin{aligned} &ar_1 \equiv \rho_1 (\bmod m), \\ &ar_2 \equiv \rho_2 (\bmod m, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &ar_{\varphi(m)} \equiv \rho_{\varphi(m)} (\bmod m), \end{aligned} \qquad (8)$$

де $\rho_1, \rho_2, \ldots \rho_{\varphi(m)}$ – система найменших невід'ємних лишків за модулем m.

Числа цієї системи попарно не конгруентні між собою за модулем m. Оскільки їх всього $\varphi(m)$, то вони утворюють зведену систему найменших невід'ємних лишків за модулем m, тобто числа $\rho_1, \rho_2, \ldots \rho_{\varphi(m)}$ – це ті ж самі числа $r_1, r_2, \ldots r_{\varphi(m)}$, але записані в іншому порядку. Тоді добутки цих чисел рівні:

$$r_1 r_2 \ldots r_{\varphi(m)} = \rho_1 \rho_2 \ldots \rho_{\varphi(m)},$$

причому, зважаючи на те, що $(r_i, m) = 1$, $(\rho_i, m) = 1$ для всіх $i = 1, 2, \ldots, \varphi(m)$, $(r_1 r_2 \ldots r_{\varphi(m)}, m) = 1$, $(\rho_1 \rho_2 \ldots \rho_{\varphi(m)}, m) = 1$.

Перемножимо конгруенції набору:

$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv \rho_1 \rho_2 \ldots \rho_{\varphi(m)} (\bmod m)$.

Поділивши обидві частини даної конгруенції на число $r_1 r_2 \ldots r_{\varphi(m)} = \rho_1 \rho_2 \ldots \rho_{\varphi(m)}$, отримаємо $a^{\varphi(m)} \equiv 1 (\bmod m)$. Теорему доведено.

Приклад 8. Довести, що $2^{340} \equiv 1 (\bmod 341)$.

Розв'язання. Очевидно, що НСД$(2, 341) = 1$, отже можна скористатися теоремою Ейлера. $\varphi(341) = 341\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{31}\right) = 300$, тому $2^{300} \equiv 1 (\bmod 341)$.

$2^{10} = 1024 = 341 \cdot 3 + 1$, тому $2^{10} \equiv 1 (\bmod 341)$, а отже $2^{40} \equiv 1 (\bmod 341)$ і як наслідок після по членного множення $2^{240} \equiv 1 (\bmod 341)$.

Приклад 9. Знайти остачу від ділення а) 5029^{10000} на 11; б) 15^{150} на 228.

Розв'язання. а) оскільки $p = 11$ - просте, $5025 \not\vdots 11$ і $\varphi(11) = 10$, за теоремою Ферма $5029^{10} \equiv 1 (\bmod 11)$. Піднісши обидві частини конгруенції до тисячного степеня, отримаємо $5029^{10000} \equiv 1 (\bmod 11)$. Тобто, шукана остача дорівнює 1.

б) $228 = 2^2 \cdot 3 \cdot 19$, $15 = 3 \cdot 5$, тому НСД$(228, 15) = 3$. Для того, щоб мати змогу використати теорему Ейлера, розглянемо конгруенції за модулем $228 : 3 = 76$. Оскільки $\varphi(76) = 76 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{19}\right) = 4 \cdot 18 = 72$, за теоремою Ейлера $5^{72} \equiv 1 (\bmod 76)$, $3^{72} \equiv 1 (\bmod 76)$, піднісши до квадрату, отримаємо

$5^{144} \equiv 1 (\bmod 76)$, $3^{144} \equiv 1 (\bmod 76)$. Скориставшись властивістю 10, перейдемо до початкового модуля

$5^{144} \cdot 3 \equiv 3 (\bmod 228)$, $3^{145} \equiv 3 (\bmod 228)$, а після почленного множення, матимемо

$5^{144} \cdot 3^{146} \equiv 9 (\bmod 228)$. Залишилося знайти остачу від ділення 5^6 та 3^4 на модуль 228. Ці остачі обчислюємо безпосередньо. Оскільки $5^6 = 15625 = 68 \cdot 228 + 121$, $3^4 = 81$, правильною буде конгруенція

$5^{150} \cdot 3^{150} \equiv 9 \cdot 121 \cdot 81 \equiv 177 \cdot 81 \equiv (-3) \cdot 9 \equiv 201 (\bmod 228)$. Останні перетворення можна було не виконувати, а знайти $9 \cdot 121 \cdot 81 = 88209 = 386 \cdot 228 + 201$. Проте краще за можливості уникати операцій з великими числами. В будь-якому випадку, відповідь буде 201.

Однією з центральних задач арифметики лишків є задача розв'язання рівняння

$$ax \equiv b(\bmod m). \qquad (9)$$

Рівняння (9) ще називають лінійною конгруенцією або конгруенцією з одним невідомим.

Якщо НСД$(a,m)=1$, то за розширеним алгоритмом Евкліда можна знайти такі $x, y \in Z$, що $xa + ym = 1$. Звідси, за означенням конгруентних чисел,

$$xa \equiv 1(\bmod m). \qquad (10)$$

Ціле число x називається <u>оберненим</u> до a за модулем m, якщо виконується конгруенція (10). Часто можна зустріти позначення $a^{-1}(\bmod m)$. Якщо вважати рівними числа, що належать одному класу лишків, то число $a^{-1}(\bmod m)$ для взаємно простих чисел a та m визначається однозначно, тобто йому відповідає один клас лишків за модулем m. Розв'язання рівняння (6) у загальному випадку слід виконувати у такій послідовності.

знайти $a^{-1}(\bmod m)$. Для цього за розширеним алгоритмом Евкліда необхідно знайти лінійне зображення одиниці через числа a та m, тобто знайти такі λ_1 та λ_2, що $\lambda_1 a + \lambda_2 m = 1$. Тоді $a^{-1}(\bmod m) = \lambda_1$.

помножити ліву та праву частини рівняння (9) на знайдене λ_1, звідки $x \equiv b\lambda_1(\bmod m)$.

Виникає природне запитання: за яких умов, накладених на a, b та m, рівняння (9) має єдиний розв'язок, знайдений за попереднім? Виявляється існування та єдність розв'язку рівняння (9) залежить від найбільшого спільного дільника чисел a та m.

Теорема (існування та кількості розв'язків конгруенції з одним невідомим). Нехай дано конгруенцію (9). Тоді, якщо

НСД$(a,m)=1$, то рівняння (9) має єдиний розв'язок;

НСД$(a,m)=d>1$ і число b не ділиться на d, то рівняння (9) не має розв'язків;

НСД$(a,m)=d>1$ і число b ділиться на d, то рівняння (9) має d розв'язків.

З доведенням цієї теореми можна ознайомитися, наприклад, в [14, сторінка 201-202].

Приклад 10. Розв'язати конгруенцію $2x - 1 \equiv 7(\bmod 15)$.

Розв'язання. Перетворивши задану конгруенцію у відповідності до властивостей 3, 9, отримаємо розв'язок $x \equiv 4 (\mathrm{mod}\, 15)$.

Приклад 11. Розв'язати конгруенцію $28x \equiv 33 (\mathrm{mod}\, 43)$.

Розв'язання. Оскільки НСД$(28, 43) = 1$, скористаємося розширеним алгоритмом Евкліда для знаходження $28^{-1} (\mathrm{mod}\, 43)$. Отримаємо

$$
\begin{array}{r|l}
43 & 28 \\ \hline
-28 & 1 \\ \hline
28 & 15 = r1 \\ \hline
-15 & 1 \\ \hline
15 & 13 = r2 \\ \hline
-13 & 1 \\ \hline
13 & 2 = r3 \\ \hline
-12 & 6 \\ \hline
2 & 1 = r4 = d \\ \hline
-2 & 2 \\ \hline
0 &
\end{array}
$$

Звідси $m = a + r_1$, $a = r_1 + r_2$, $r_1 = r_2 + r_3$, $r_2 = 6r_3 + 1$, а отже $1 = r_2 - 6(r_1 - r_2) = 7r_2 - 6r_1 = 7(a - r_1) - 6r_1 = 7a - 13r_1 = 7a - 13(m - a) = 20a - 13m$.

Тому $28^{-1} (\mathrm{mod}\, 43) = 20$, виконуючи п.2 алгоритму та відповідні спрощення, отримаємо

$$x \equiv 33 \cdot 20 (\mathrm{mod}\, 43) \equiv 3 \cdot 11 \cdot 2 \cdot 2 \cdot 5 (\mathrm{mod}\, 43) \equiv 3 \cdot 44 \cdot 5 (\mathrm{mod}\, 43) \equiv 15 (\mathrm{mod}\, 43).$$

Навчившись розв'язувати рівняння (9), природно приступити до розв'язування систем рівнянь:

$$\begin{cases} x \equiv t_1 (\mathrm{mod}\, m_1), \\ x \equiv t_2 (\mathrm{mod}\, m_2), \\ \dots\dots\dots\dots\dots\dots, \\ x \equiv t_s (\mathrm{mod}\, m_s). \end{cases} \qquad (11)$$

Єдність розв'язку такої системи гарантує наступна теорема.

Китайська теорема про лишки. Нехай маємо k попарно взаємно простих натуральних чисел $m_1, m_2, \dots, m_k$. Тоді система (11) має один і лише один розв'язок $K_x^{(m_1 m_2 \dots m_k)}$.

Приклад 12. Розв'язати систему

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 3), \\ x \equiv 4 (\mathrm{mod}\, 5), \\ x \equiv 2 (\mathrm{mod}\, 7), \\ x \equiv 5 (\mathrm{mod}\, 11). \end{cases}$$

Розв'язання. З першого рівняння системи означенням 3 $x = 1 + 3t_1$, тому друга конгруенція набуде вигляду $1 + 3t_1 \equiv 4(\mathrm{mod}\,5)$, тобто $t_1 \equiv 1(\mathrm{mod}\,5)$ (властивість 9), що означає $t_1 = 1 + 5t_2$, тому $x = 1 + 3(1 + 5t_2) = 4 + 15t_2$. Отриманий вираз для x підставляємо у третє рівняння: $15t_2 \equiv -2(\mathrm{mod}\,7)$, а оскільки $15 \equiv 1(\mathrm{mod}\,7)$, то $t_2 \equiv -2 \equiv 5(\mathrm{mod}\,7)$, тобто $t_2 = 5 + 7t_3$, а $x = 4 + 15(5 + 7t_3) = 79 + 105t_3$. Після підстановки у останнє рівняння: $79 + 105t_3 \equiv 5(\mathrm{mod}11)$, $105t_3 \equiv -74 \equiv 3(\mathrm{mod}11)$. Оскільки $105 \equiv 6(\mathrm{mod}11)$, то $2t_3 \equiv 1(\mathrm{mod}11)$. Множимо ліву та праву частину на 6: $12t_3 \equiv 6(\mathrm{mod}11)$, або $t_3 \equiv 6(\mathrm{mod}11)$, звідки $t_3 = 6 + 11t_4$, а $x = 79 + 105(6 + 11t_4) = 709 + 1155t_4$ і 709 – шуканий розв'язок за модулем $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, $x \equiv 709(\mathrm{mod}1155)$.

В астрономії системи конгруенцій виникають при необхідності визначення часу «параду планет» з різними періодами обертання, в системах захисту такі задачі виникають, зокрема, в ситуації, коли сейф може бути відкритий лише за одночасної присутності певної кількості осіб, які володіють фрагментами ключа.

Нехай маємо ключ, який є деяким натуральним числом n. Потрібно розподілити цей ключ між s осіб, тобто розподілити його на фрагменти ключа. При цьому розбиття ключа на фрагменти повинно відповідати двом умовам:

ключ n легко знайти, якщо відомо k і більше його фрагментів;

ключ n важко визначити, якщо відомо менше k його фрагментів.

Фрагментами ключа на практиці беруть впорядковану пару взаємно простих чисел $(t_i, m_i), i = \overline{1,s}$. Тоді таємний ключ n можна отримати, взявши найменше додатне число, яке задовольняє розв'язок системи (11): $n \equiv x(\mathrm{mod}\, m_1 m_2 ... m_s)$. Зрозуміло, що чим менше буде відомо рівнянь цієї системи, тим серед більшої кількості варіантів доведеться методом проб шукати невідомий ключ.

Контрольні запитання

1. Що означає запис $a \equiv b (\bmod m)$?
2. Довести еквівалентність трьох означень конгруентності.
3. Користуючись кожним з трьох означень довести, що числа -724 і 322 конгруентні за модулем 3.
4. Кожну з властивостей 1 - 14 конгруенцій проілюструвати конкретним числовим прикладом;
5. Довести властивості 1 – 14 конгруенцій;
6. Серед чисел 4, 57, 8, 13 вибрати такі, що є конгруентними 3 за модулем 5.
7. Із яких чисел складається клас лишків $K_1^{(5)}$?
8. Користуючись теоремою Ферма, показати, що $(2^{70} + 3^{70}) \vdots 13$.
9. Користуючись теоремою Ейлера, знайти остачу від ділення

   а) 19^{71} на 12; в) 341^{291} на 48; д) 592^{192} на 65;

   б) 473^{193} на 45; г) 499^{245} на 60; е) 428^{200} на 75.
10. Знайти лишок числа a за модулем m, якщо

    а) $a = 2351$, $m = 2$, б) $a = 321\,671$, $m = 14$.
11. Розв'язати конгруенції:

    а) $3x \equiv 2 (\bmod 4)$, б) $5x \equiv -2 (\bmod 13)$, в) $21x \equiv 25 (\bmod 26)$.
12. Знайти найменше число, яке ділиться на 7, а при діленні на 2, 3, 4, 5, 6 дає остачу 1.
13. Розв'язати систему:

    а) $\begin{cases} x \equiv 1 (\bmod 2), \\ x \equiv 2 (\bmod 5), \\ x \equiv 5 (\bmod 12). \end{cases}$ б) $\begin{cases} x \equiv 2 (\bmod 3), \\ x \equiv 3 (\bmod 5), \\ x \equiv 2 (\bmod 7). \end{cases}$
14. Яким може бути код, якщо його фрагменти задають пари чисел $\{(11,19),(13,17),(17,13),(19,11),(23,7)\}$?

Навчальне видання

КОНДАКОВА Світлана Віталіївна

ТЕОРІЯ ТА ПРАКТИКА ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ. ЧАСТИНА 1. ТЕОРІЯ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Конспект лекцій

Редагування та коректура *А.М. Кондакової*
Комп'ютерне верстання *М.М. Власенко*

Підписано до друку 02.02.2023 Формат 60 х 84 1/ 16
Ум. друк. арк. 1,86. Обл.-вид. арк. 1,16
Електронний документ. Вид. № 10/І-16 Зам. 40/1-16

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р.