Дискретна математика - 2

Змістовий модуль 7. Теорія чисел і криптографія

Тема 6. Подільність і модулярна арифметика.

План лекції

- Подільність і модулярна арифметика
- Прості числа

Подільність і модулярна арифметика

Матеріал, який ми вивчатимемо в цій темі, ґрунтується на понятті подільності. Ділення цілого числа на додатне ціле дає в результаті частку й остачу. Вивчення остач веде до модулярної арифметики, яка відіграє важливу роль у математиці й значно використовується в комп'ютерних науках. Ми розглянемо застосування модулярної арифметики до шифрування повідомлень.

Ділення

Коли ціле число ділять на інше ненульове ціле, то частка може бути, а може й не бути цілою. Наприклад, $12/4 = 3$ – ціле, а $13/4 = 3.25$ – ні. Це проводить до такого означення.

Нехай a та b – цілі числа та $a \neq 0$. Говорять, що a *ділить* b, якщо існує таке ціле c, що $b = ac$. Еквівалентне формулювання: a *ділить* b, якщо b/a – ціле. Коли a ділить b, говорять, що a – *фактор* або *дільник* b, і що b *кратне* a. Запис $a \mid b$ означає, що a ділить b. Якщо a **не** ділить b, то використовують запис $a \nmid b$.

Приклад. Нехай n та d – додатні цілі. Скільки додатних цілих не більших n діляться на d? Усі додатні цілі, які діляться на d, можна записати формі dk, де k – додатне ціле. Отже, кількість додатних цілих, які діляться на d і не більших n дорівнює кількості цілих чисел k, для яких $0 < dk \leq n$, тобто $0 < k \leq n/d$. Отже, є $\lfloor n/d \rfloor$ додатних цілих не більших n, які діляться на d.

У теоремі 3.1 сформульовано головні властивості подільності цілих чисел.

Теорема 3.1. Нехай a, b, c – цілі числа, причому $a \neq 0$. Тоді:

(*а*) якщо $a \mid b$ і $a \mid c$, то $a \mid (b + c)$;

(*б*) якщо $a \mid b$ то $a \mid bc$ для всіх цілих c;

(*в*) якщо $a \mid b$ і $b \mid c$, то $a \mid c$.

Доведення пропонується як вправа.

Наслідок. Якщо a, b, c – цілі числа, де $a \neq 0$, такі, що $a \mid b$ і $a \mid c$, то $a \mid (mb + nc)$ для будь-яких цілих m і n.

Доведення. Із частини (*б*) теореми 3.1 слідує, що $a \mid mb$ і $a \mid nc$ для будь-яких цілих m і n. Із частини (*а*) теореми 3.1 слідує, що $a \mid (mb + nc)$.

Коли ціле число ділять на додатне ціле, то виникають частка й остача.

Теорема 3.2. Нехай a – ціле число, d – додатне ціле. Тоді існують єдині цілі q і r, $0 \le r < d$, такі, що $a = dq + r$.

> У рівності, поданій у теоремі 3.2, d називають дільником, a – діленим, q – часткою, r – остачею. Наступний запис використовують для частки й остачі:
>
> $$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

Зауваження. Зазначимо, що a **div** d та a **mod** d за фіксованого d є функціями на множині цілих чисел. Більше того, коли a – ціле та d – додатне ціле, більше за 1, то $a \textbf{ div } d = \lfloor a/d \rfloor$ і $a \textbf{ mod } d = a - d\lfloor a/d \rfloor$. Справді, за теоремою 3.2 маємо $a = dq + r$, де $0 \le r < d$. Поділивши рівність на d, одержимо $a/d = q + (r/d)$, де $0 \le (r/d) < 1$. Із означення випливає, що $q = \lfloor a/d \rfloor$. Із рівняння випливає, що $r = a - dq$. Це й доводить друге твердження.

Приклад. Знайдемо частку й остачу від ділення 101 на 11. Маємо $101 = 11 \cdot 9 + 2$. Отже, частка від ділення 101 на 11 становить $9 = 101 \textbf{ div } 11$, а остача становить $2 = 101 \textbf{ mod } 11$.

Приклад. Знайдемо частку й остачу від ділення –11 на 3. Маємо $-11 = 3 \cdot (-4) + 1$. Отже, частка від ділення –11 на 3 становить $-4 = -11 \textbf{ div } 3$, а остача становить $1 = -11 \textbf{ mod } 3$.

Зазначимо, що остача не може бути від'ємною, навіть через рівність $-11 = 3\cdot(-3) - 2$. Справді, $r = -2$ не задовольняє умову $0 \le r < 3$.

Зазначимо також, що ціле число a подільне на ціле число d тоді й тільки тоді, коли при діленні a на d одержимо нульову остачу.

Множину всіх можливих остач при діленні на m позначають як Z_m – це множина всіх цілих невід'ємних чисел, менших ніж m, тобто $\mathrm{Z}_m = \{0, 1, 2, \ldots, m-1\}$.

Зауваження. Мови програмування мають один, можливо, два оператори для модулярної арифметики. Такий оператор позначають як mod (BASIC, Maple, Mathematica, EXCEL, SQL), % (C, C++, Java, Python), rem (Ada, Lisp) тощо. Потрібно бути уважним під час використання цих операторів, бо для $a < 0$ деякі з них повертають $a - m\lceil a/m \rceil$ замість правильної відповіді a **mod** $m = a - m\lfloor a/m \rfloor$ (див. попереднє зауваження). Також, на відміну від a **mod** m, деякі з цих операторів визначені для $m < 0$, і навіть для $m = 0$.

Модулярна арифметика

Почнемо з простого прикладу модулярної арифметики. Якщо відрахувати 14 годин від 15 години біжучого дня, то одержимо 5 годину наступного дня: $(15 + 14)$ **mod** $24 = 5$. Тут 29 поділено на 24 і записано остачу.

Оскільки часто цікавими є тільки остачі, то використовують спеціальний запис для них. Ми завжди можемо використовувати запис a **mod** m для подання остачі від ділення цілого числа a на додатне ціле m. Зараз ми введемо інший, але співвіднесений запис, який указує, що два цілих числа мають одну й ту саму остачу від ділення їх на додатне ціле m.

Нехай a і b – цілі числа, а m – додатне ціле. Тоді говорять, що *a конгруентне до b за модулем m*, якщо m ділить $a - b$. Це записують як $a \equiv b \pmod{m}$. Якщо a та b не конгруентні, то пишуть $a \not\equiv b \pmod{m}$.

Хоча обидва записи $a \equiv b \pmod{m}$ і a **mod** $m = b$ містять «mod», вони репрезентують фундаментально різні концепції. Перший репрезентує відношення на множині цілих чисел, тоді як другий репрезентує функцію. Проте відношення $a \equiv b \pmod{m}$ і функція **mod** m тісно пов'язані – це складає зміст теореми 3.3.

Теорема 3.3. Нехай a, b – цілі числа, m – додатне ціле. Для того, щоб $a \equiv b \pmod{m}$, необхідно й достатньо, щоб a **mod** $m = b$ **mod** m.

Приклад.

$21 \equiv 9 \pmod{6}$, тому що 6 ділить $21 - 9 = 12$, а $21 \not\equiv 11 \pmod{6}$, бо 6 не ділить $21 - 11 = 10$.

Концепцію конгруентності наприкінці вісімнадцятого століття досліджував видатний німецький математик Карл Фрідріх Гаус (1777–1855). Поняття конгруентності відіграє важливу роль у розвитку теорії чисел. У теоремі 3.4 сформульовано важливий для роботи з конгруенціями результат.

Теорема 3.4. Нехай m – додатне ціле число. Цілі числа a та b конгруентні за модулем m тоді й тільки тоді, коли існує ціле k таке, що $a = b + km$.

Доведення. Якщо $a \equiv b \pmod{m}$, то за означенням $m \mid (a - b)$. Отже, існує таке ціле k, що $a - b = km$, звідки $a = b + km$. Навпаки, якщо існує ціле k таке, що $a = b + km$, то $km = a - b$. Звідси випливає, що m ділить $a - b$, отже, $a \equiv b \pmod{m}$.

Множину всіх цілих чисел, конгруентних до цілого числа a за модулем m, називають *класом конгруентності* a за модулем m і позначають як $[a]_m$. Відношення конгруентності на множині цілих чисел є відношенням еквівалентності; клас конгруентності $[a]_m$ являє собою клас еквівалентності. Отже, відношення конгруентності здійснює розбиття множини цілих чисел на класи конгруентності. Можна показати, що таки класів (різних) є точно m.

Теорема 3.5. Нехай m – додатне ціле число. Нехай $a \equiv b \pmod{m}$ і $c \equiv d \pmod{m}$. Тоді $a + c \equiv b + d \pmod{m}$ і $ac \equiv bd \pmod{m}$.

Доведення. Оскільки Нехай $a \equiv b \pmod{m}$ і $c \equiv d \pmod{m}$, то за теоремою 3.4 існують цілі числа s і t такі, що $b = a + sm$ і $d = c + tm$.

Отже,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \text{ і}$$
$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Отже, $a + c \equiv b + d \pmod{m}$ і $ac \equiv bd \pmod{m}$.

Наслідок. Нехай m – додатне ціле число і a та b – цілі числа. Тоді

$$(a + b) \textbf{ mod } m = (a \textbf{ mod } m + b \textbf{ mod } m) \textbf{ mod } m$$

і

$$ab \textbf{ mod } m = (a \textbf{ mod } m \cdot b \textbf{ mod } m) \textbf{ mod } m.$$

Доведення. За **означенням** *функції* **mod** m і *конгруентності за модулем* m (позначаємо mod m) можемо записати

$$a \equiv (a \textbf{ mod } m) \pmod{m} \text{ і}$$
$$b \equiv (b \textbf{ mod } m) \pmod{m}.$$

Отже, за теоремою 3.5, матимемо

$$a + b \equiv a \textbf{ mod } m + b \textbf{ mod } m \pmod{m} \text{ і}$$
$$a \cdot b \equiv a \textbf{ mod } m \cdot b \textbf{ mod } m \pmod{m}$$

Тепер рівняння з формулювання наслідку випливають безпосередньо із теореми 3.3.

Арифметика за модулем m

Нагадаємо, що множину всіх можливих остач при діленні на m позначають як $\mathbf{Z}_m$ – це множина всіх цілих невід'ємних чисел, менших ніж m, тобто $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$. На цій множині можна означити арифметичні операції додавання $+_m$ і множення $\cdot_m$.

$$a +_m b = (a+b) \,\mathbf{mod}\, m,$$
$$a \cdot_m b = (a \cdot b) \,\mathbf{mod}\, m.$$

Зауваження. У правій частині двох останніх рівнянь – звичайне додавання і, відповідно, множення цілих чисел.

Операції $+_m$ і $\cdot_m$ називають додаванням і множенням за модулем m і, коли ці операції використовують, то говорять про *арифметику за модулем m*.

Приклад. Обчислимо $7 +_{11} 9$ та $7 \cdot_{11} 9$.

Маємо: $7 +_{11} 9 = (7+9) \,\mathbf{mod}\, 11 = 16 \,\mathbf{mod}\, 11 = 5$; $7 \cdot_{11} 9 = (7 \cdot 9) \,\mathbf{mod}\, 11 = 63 \,\mathbf{mod}\, 11 = 8$.

Операції $+_m$ і $\cdot_m$ задовольняють багато властивостей звичайного додавання і множення цілих чисел.

Операції $+_m$ і $\cdot_m$ на множині $\mathbf{Z}_m$ задовольняють умові *замкненості*: якщо a і b належать $\mathbf{Z}_m$, то і $a +_m b$ та $a \cdot_m b$ належать $\mathbf{Z}_m$.

Множина $\mathbf{Z}_m$ разом з операцією $+_m$ утворює ***абелеву групу***, бо задовольняються такі властивості.

Асоціативність. Якщо a, b і c належать $\mathbf{Z}_m$, то

$$(a +_m b) +_m c = a +_m (b +_m c).$$

Нейтральний елемент. Елемент $0 \in \mathbf{Z}_m$ є нейтральним елементом по додаванню: якщо a належить $\mathbf{Z}_m$, то $a +_m 0 = 0 +_m a = a$.

Обернений елемент. Якщо $a \neq 0$ належить $\mathbf{Z}_m$, то $m - a$ є оберненим до a за модулем m, а 0 є оберненим до самого себе. Отже, $a +_m (m - a) = 0$ і $0 +_m 0 = 0$.

Комутативність. Якщо a і b належать $\mathbf{Z}_m$, то $a +_m b = b +_m a$.

Множина $\mathbf{Z}_m$ разом з двома операціями $+_m$ і $\cdot_m$ утворює ***комутативне кільце з одиницею***, бо задовольняються такі властивості.

1. Стосовно операції $+_m$ множина $\mathbf{Z}_m$ утворює абелеву групу.

2. Операції множення і додавання пов'язані *дистрибутивними законами*. Якщо a, b і c належать $\mathbf{Z}_m$, то $a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c)$ і $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

3. Для операції множення виконуються такі властивості.

Комутативність: $a \cdot_m b = b \cdot_m a$.

Асоціативність: $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Нейтральний елемент (існування одиниці). Елемент $1 \in \mathbf{Z}_m$ є нейтральним елементом по множенню: $a \cdot_m 1 = 1 \cdot_m a = a$.

Зауваження. Коли працюють з множиною $\mathbf{Z}_m$, часто використовують нотації + і · замість $+_m$ і $\cdot_m$, тобто індекс m не пишуть.

Модулярне піднесення до степеня

У сучасній криптографії важливим є можливість ефективно обчислити $b^n \,\mathbf{mod}\, m$, де b, n та m – великі цілі числа. Непрактично спочатку обчислювати b^n, а потім знаходити остачу від ділення результату на m, бо b^n – велике число. Замість цього ми розглянемо алгоритм, який використовує двійкове подання показника степеня n.

Перед тим, як подати алгоритм, ми проілюструємо головну ідею. Ми пояснимо, як використати двійковий подання n, а саме $n = (a_{k-1} \ldots a_1 a_0)_2$, для обчислення b^n. Спочатку зазначимо, що

$$b^n = b^{a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \cdots b^{a_1 \cdot 2} \cdot b^{a_0}.$$

Це показує, що для обчислення b^n нам потрібно лише обчислити значення b, b^2, $\left(b^2\right)^2 = b^4$, $\left(b^4\right)^2 = b^8$, $\left(b^8\right)^2 = b^{16}$, …, b^{2^k}. Ми перемножуємо лише ті з отриманих термів b^{2^j}, для яких $a_j = 1$. Це дасть b^n.

Наприклад, для обчислення 3^{13} спочатку зазначимо, що $13=(1101)_2$, отже, $3^{13}=3^8 3^4 3^1$. Після послідовних піднесень до квадрату, одержимо $3^2=9$, $3^4=9^2=81$ і $3^8=(81)^2=6561$. Отже, $3^{13}=3^8\cdot 3^4\cdot 3^1=6561\cdot 81\cdot 3=1\,594\,323$.

У разі знаходження $b^n \operatorname{mod} m$ для ефективності обчислень після кожного множення потрібно здійснювати редукцію результату за модулем m. А саме, алгоритм послідовно знаходить $b \,\mathbf{mod}\, m$, $b^2 \,\mathbf{mod}\, m$, $b^4 \,\mathbf{mod}\, m$, $b^8 \,\mathbf{mod}\, m$, $b^{16} \,\mathbf{mod}\, m$, ..., $b^{2^{k-1}} \,\mathbf{mod}\, m$ і перемножує лише ті терми $b^{2^j} \,\mathbf{mod}\, m$, для котрих $a_j=1$, знаходячи після кожного множення залишок від ділення результату на m. Псевдокод для цього алгоритму подано нижче.

Алгоритм 4.1. Модулярне піднесення до степеня.

procedure *modexp*(b: integer, $n=(a_{k-1}a_{k-2}\ldots a_1a_0)_2$, m: positive integer)

```
x := 1
power := b mod m
for i := 0 to k − 1
    if a_i = 1 then x := (x · power) mod m
    power := (power · power) mod m
return x (x equals b^n mod m)
```

Описаний алгоритм був відомий ще до нашої ери в Індії. Його іноді називають *бінарним методом*.

Роботу алгоритму 1 проілюстровано наступним прикладом.

Приклад. Використаємо алгоритм 1 для знаходження $3^{644}\,\mathbf{mod}\,645$.

Знаходимо $(644)_{10} = (1010000100)_2$.

Послідовно обчислюємо.

$i = 0$. Оскільки $a_0 = 0$, то $x = 1$ і $power = 3^2\,\mathbf{mod}\,645 = 9\,\mathbf{mod}\,645 = 9$.

$i = 1$. Оскільки $a_1 = 0$, то $x = 1$ і $power = 9^2\,\mathbf{mod}\,645 = 81\,\mathbf{mod}\,645 = 81$.

$i = 2$. Оскільки $a_2 = 1$, то $x = (1 \cdot 81)\,\mathbf{mod}\,645 = 81$ і $power = 81^2\,\mathbf{mod}\,645 = 111$.

$i = 3$. Оскільки $a_3 = 0$, то $x = 81$ і $power = 111^2\,\mathbf{mod}\,645 = 12321\,\mathbf{mod}\,645 = 66$.

$i = 4$. Оскільки $a_4 = 0$, то $x = 81$ і $power = 66^2\,\mathbf{mod}\,645 = 4356\,\mathbf{mod}\,645 = 486$.

$i = 5$. Оскільки $a_5 = 0$, то $x = 81$ і $power = 486^2\,\mathbf{mod}\,645 = 236196\,\mathbf{mod}\,645 = 126$.

$i = 6$. Оскільки $a_6 = 0$, то $x = 81$ і $power = 126^2\,\mathbf{mod}\,645 = 15876\,\mathbf{mod}\,645 = 396$.

$i = 7$. Оскільки $a_7 = 1$, то $x = (81 \cdot 396)\,\mathbf{mod}\,645 = 471$ і $power = 396^2\,\mathbf{mod}\,645 = 81$.

$i = 8$. Оскільки $a_8 = 0$, то $x = 471$ і $power = 81^2\,\mathbf{mod}\,645 = 6561\,\mathbf{mod}\,645 = 111$.

$i = 9$. Оскільки $a_9 = 1$, то знаходимо $x = (471 \cdot 111)\,\mathbf{mod}\,645 = 36$.

Отже, за алгоритмом 1 ми одержали результат $3^{644}\,\mathbf{mod}\,645 = 36$.

Прості числа

Просте число — це додатне ціле число, більше від одиниці, яке має рівно два різних натуральних дільники (лише 1 і саме число). Решту чисел, окрім одиниці, називають *складеними*. Таким чином, всі натуральні числа, більші від одиниці, розбивають на прості й складені. Теорія чисел вивчає властивості простих чисел.

Ось усі прості числа, що не більші 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Теорема 3.6 (основна теорема арифметики). Кожне натуральне число, яке більше одиниці, можна представити як добуток простих чисел, причому, в єдиний спосіб з точністю до порядку множників.

Таким чином, прості числа – це елементарні «будівельні блоки» натуральних чисел.

Представлення натурального числа у вигляді добутку простих називають *розкладом на прості* або *факторизацією* числа. Нині невідомі поліноміальні алгоритми факторизації чисел, хоча й не доведено, що таких алгоритмів не існує (тут мова йде про поліноміальну залежність часу роботи алгоритму від логарифма розміру числа, тобто від кількості його цифр). На припущенні про високу обчислювальну складність задачі факторизації ґрунтується криптосистема RSA.

Приклад. Факторизацію чисел 100, 641, 999 та 1024 подано нижче:

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$;

$641 = 641$;

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$;

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$.

Деякі цікаві властивості простих чисел.

- Натуральне $p > 1$ є простим тоді й тільки тоді, коли $(p-1)! + 1$ ділиться на p.

- Якщо $n > 1$ – натуральне, то існує просте p, таке, що $n < p < 2n$.

- Будь-яке просте число більше 3 можна представити у вигляді $6k + 1$, або у вигляді $6k - 1$, де k – якесь натуральне число.

- Якщо $p > 3$ – просте, то $p^2 - 1$ кратне 24.

Відкриті проблеми щодо простих чисел.

Перераховані Едмундом Ландау на П’ятому міжнародному математичному конгресі (1912 р., Кембридж, Велика Британія, де він був обраний головою). Жодна з цих проблем не розв’язана донині.

- Проблема Гольдбаха (*перша проблема Ландау*): довести або спростувати, що кожне парне число, більше двох, може бути представлено у вигляді суми двох простих чисел.

- *Друга проблема Ландау*: чи нескінченна множина «простих близнюків» – простих чисел, різниця між якими дорівнює 2?

- Гіпотеза Лежандра (*третя проблема Ландау*): чи правильно, що між n^2 і $(n+1)^2$ завжди знайдеться просте число?

- *Четверта проблема Ландау*: чи нескінченна множина простих чисел виду n^2+1?

Відкритою проблемою є також існування нескінченної кількості простих чисел у багатьох цілочисельних послідовностях, наприклад, у послідовності чисел Фібоначчі.

Пробне ділення.

Часто важливо показати, що задане ціле число – просте. Наприклад, у криптології великі прості числа використовують для шифрування повідомлень. Один метод перевірки числа на простоту грунтується на такій теоремі.

Теорема 3.7. Якщо n – складене число, то n має простий дільник, який не більший ніж $\sqrt{n}$.

Наслідок. Якщо ціле число m не ділиться на жодне просте число, яке не більше ніж $\sqrt{m}$, то число m – просте.

На цій теоремі засновано метод перевірки цілих чисел на простоту «в лоб», за допомогою алгоритму, відомого як **пробне ділення**.

Приклад. Покажемо, що число 107 – просте. Прості, які не більші ніж $\sqrt{107}$, такі: 2, 3, 5, 7. Тому що жодне з цих чисел не ділить 107, то число 107 – просте.

Цю теорему можна використати й для факторизації складених чисел. Алгоритм тут такий. Починаємо з простого числа 2. Якщо n число складене, то за теоремою 3.7 простий множник p, який не перевищує $\sqrt{n}$, буде знайдено. Коли простий множник p знайдено, продовжуємо факторизацію n/p. Зазначимо, що n/p не має простих множників, менших p. На наступному кроці, якщо n/p не має простих множників більших або рівних p і менших $\sqrt{n/p}$, то число n/p просте. Інакше, якщо воно має простий множник q, і ми продовжимо факторизацію $n/(pq)$. Процедура завершиться, коли на якомусь кроці одержимо просте число.

Приклад. Знайдемо факторизацію числа 7007. Жодне з простих чисел 2, 3 та 5 не ділить 7007. Проте, 7 ділить 7007, причому $7007/7 = 1001$. Тепер пробуємо ділити 1001 на прості, починаючи з 7. Маємо одразу $1001/7 = 143$. Продовжуємо кроки алгоритму, використовуючи пробне ділення 143 на послідовні прості числа, починаючи з 7. Одержимо $143/11 = 13$. Оскільки 13 – число просте, то алгоритм зупиняється. Результат: $7007 = 7^2 \cdot 11 \cdot 13$.

Решето Ератосфена.

Це метод побудови всіх простих чисел, які не більші заданого числа n. Такі числа мають прості множники, не більші ніж $\sqrt{n}$. Нехай потрібно знайти всі прості числа не більші 60. Ці число має прості множники, не більші $\sqrt{60}$. Очевидно, це тільки 2, 3, 5 і 7.

Для початку процесу викреслюємо числа (окрім 2), які діляться на 2 (це кожне друге число).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Наступне просте число 3. Викреслюємо всі числа (окрім 3), які діляться на 3 (це кожне третє число).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Наступне просте число 5. Викреслюємо всі числа (окрім 5), які діляться на 5 (це кожне п’яте число).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Останнє просте число 7. Викреслюємо всі числа (окрім 7), які діляться на 7 (це кожне сьоме число).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

У результаті отримали послідовність простих чисел, не більших ніж 60.