6. Пояснити, чому алгоритм 2 закінчиться не більше, ніж за N кроків? (стор. 13).

7. Пояснити, чому алгоритм 2 насправді закінчиться не більше, ніж за $\sqrt{N}$ кроків? (стор. 13).

8. Чому всі складені числа від $p_k + 1$ до $p_k^2 - 1$ вже викреслено на попередніх кроках? (стор. 13).

7. Задачі для самостійної роботи

Задача 1. *Текст, який наведено нижче, зашифровано за допомогою так званого книжкового шифру*:

```
0408 0453 1020 1038 1101 0602 0150 0217 0636 0208 1306 0950
0421 0637 1110 0913 0708 0204 0404 1217 0708 0216 1107 0842
```

Кожне кодове слово складається з двох двозначних чисел. Перше з них вказує на рядок у іншому тексті, а друге — на стовпчик там же. На перетині рядка та стовпчика у тому тексті знаходимо символ оригінального повідомлення. Розшифрувати повідомлення, якщо іншим текстом є початок цієї лекції на сторінці 1.

Задача 2. *У книзі рекордів Гінесса написано, що найбільшим відомим простим числом є* $23021^{377} - 1$. *Довести, що*

a) *це є помилкою*;
b) *вказане число ділиться на 10.*

Задача 3. *Л. Ойлер, геніальний математик XVIII сторіччя, вважав, що значеннями полінома* $P_-(x) = x^2 - x + 41$ *при всіх натуральних* x *є прості числа.*

a) *перевірити його гіпотезу для* $x = 1, 2, \dots, 15$ (*використати решето Ератосфена* 16×16).
b) *чи вірною є гіпотеза Ойлера*? <u>`Вказівка`</u>. Обрати $x = 41$.

Задача 4. *Нехай* $P_+(x) = x^2 + x + 41$.

a) *перевірити, що* $P_+(x)$ *є простим числом для* $x = 1, 2, \dots, 15$;
b) *довести, що серед значень* $P_+(x)$, $x = 1, 2, \dots$, *зустрічаються складені числа.*

Задача 5. *Нехай $p > 2$ — просте число. Довести, що*

a) *обидва числа $p-1$ та $p+1$ є парними;*
b) *одне з чисел $p-1$ або $p+1$ ділиться на 3.*

Задача 6. *Нехай $p \geq 5$ — просте число. Довести, що або $p = 6k+1$, або $p = 6k-1$ для деякого натурального k.*

Задача 7. *Нехай $p \geq 3$ — просте число. Довести, що*

a) *одне з чисел $p-1$ або $p+1$ ділиться на 4;*
b) *невірним є твердження, що одне з чисел $p-1$ або $p+1$ ділиться на 5.*

Задача 8. *Записати слово "*`МОРЗЕ`*" за допомогою азбуки Морзе.*

Задача 9. *Записати слово "*`БРАЙЛЬ`*" за допомогою шифра Брайля.*

Задача 10. a) *Скільки існує перестановочних шифрів для фіксованого параметру n?*

b) *Яким чином дешифруються повідомлення у випадку перестановочного шифру?*

c) *Дешифрувати секретне повідомлення*

емічпо ␣урнка низї␣␣утофбл ␣␣␣у␣␣

якщо ключовим словом є "`динамо`*".*

Задача 11. a) *Скільки існує рандомізованих матричних шифрів з параметром n?*

b) *Дешифрувати секретне повідомлення*

`55 41 25 23 35 64 56 35 52 65 35 61 23`

якщо другий параметр шифру визначається перестановкою (1) на стор. 18.

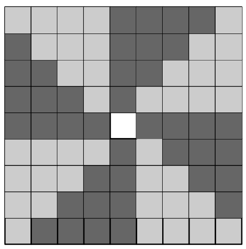
Задача 12. *Число*

$$t_n = \sum_{i=1}^{n} i, \qquad n \geq 1,$$

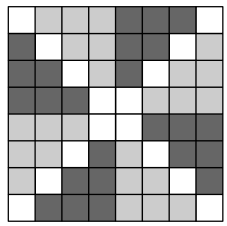
називається n-им трикутним числом.

a) *Пояснити цю назву геометрично.*
b) *Довести рекурентну формулу: $t_n = t_{n-1} + n$, $n \geq 2$.*
c) *Знайти простий вираз для t_n.*

Задача 13. *Пояснити наступне ілюстративне доведення формул Діофанта. Довести їх у загальному випадку*:



$8t_n + 1 = (2n+1)^2$



$8t_{n-1} + 4n = (2n+1)^2$

Задача 14. *Нехай*

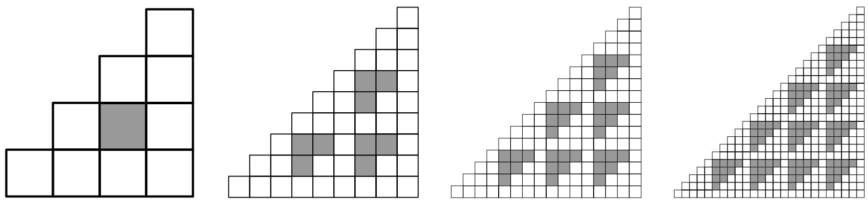
$$\begin{aligned} s_n &= 1, \\ s_n &= s_{n-1} + 2n - 1, \qquad n \geq 2. \end{aligned}$$

Число s_n називається n-м квадратним числом.

a) *Пояснити назву геометрично.*
b) *Знайти просту формулу для s_n.*

Задача 15. *В 1775 році Л. Ойлер довів, що якщо n є трикутним числом, то $9n+1$, $25n+3$ та $49n+6$ також є трикутними числами. Перевірити це.*

Задача 16. *Нижче наведено ілюстрацію до доведення властивості трикутних чисел для чотирьох значень n. Знайти формулу, яка описує цю властивість, і довести її у загальному випадку.*



$t_1^2 + t_2^2 = t_4$ $\quad$ $t_2^2 + t_3^2 = t_9$ $\quad$ $t_3^2 + t_4^2 = t_{16}$ $\quad$ $t_4^2 + t_5^2 = t_{25}$

Задача 17. *Довести, що існує $\left[\frac{a}{b}\right]$ натуральних чисел, які не перевищують a і діляться на b.*

Задача 18. *Високосний рік — це такий, кількість днів у якому становить 366 — на одну добу більше, ніж у звичайному (невисокосному) році. У такий рік місяць лютий має не 28, а 29 днів. Високосні роки визначаються за наступним правилом: рік є високосним, якщо з нього починається сторіччя і його порядковий номер ділиться на 400, або з нього сторіччя не починається, але його порядковий номер ділиться на 4. Скільки високосних років до 2016 було після 1600?*

Задача 19. *У древньому Єгипті використовували своєрідний метод множення чисел, який ми продемонструємо на прикладі множення 23 на 45. Перш за все, запишемо перше з цих чисел у вигляді суми степенів двійки*: $23 = 1 + 2 + 4 + 16 = 2^0 + 2^1 + 2^2 + 2^4$. *Тоді*

$$23 \cdot 45 = 1 \cdot 45 + 2 \cdot 45 + 4 \cdot 45 + 16 \cdot 45.$$

Тепер побудуємо таблицю:

1	2	4	8	16
45✓	90✓	180✓	360	720✓

Перший рядок містить всі степені двійки, *які не перевищують 23*; *елементи другого дорівнюють добутку 45 та відповідного степеня* *двійки у тому ж стовпчику (легше обчислювати, якщо помітити, що кожний наступний елемент це подвоєний попередній). Знаком* ✓ *відмічено ті елементи другого стовпчика, які відповідають двійковому розкладу 23. Потрібний результат дорівнює сумі елементів з символом* ✓:

$$23 \cdot 45 = 45 + 90 + 180 + 720 = 1035.$$

Використовуючи египетський метод множення, перемножити 25 та 33.

Задача 20. *Так званий "селянський" метод множення двох чисел схожий на египетський. Для ілюстрації цього методу перемножимо 24 та 43. Спочатку складемо таблицю:*

24	12	6	3	1
43	86	172	344✓	688✓

Перший її рядок починається з 24, а кожний наступний елемент є часткою від ділення попереднього на 2. Другий рядок починається з 43, а кожний наступний елемент вдвічи більший за попередній. Ми позначили знаком ✓ *ті елементи другого рядка, які відповідають непарним числам у першому рядку. Результат множення є сума елементів з символом* ✓*:*

$$24 \cdot 43 = 344 + 688 = 1032.$$

Довести "селянський" метод множення натуральних чисел.

Задача 21. *Нескладно підрахувати, що* $123 \cdot 7 \cdot 11 \cdot 13 = 123123$*. Довести, що* $(abc)_{10} \cdot 7 \cdot 11 \cdot 13 = (abcabc)_{10}$*, де* a, b, c *— довільні цифри, а* $(xyz\ldots)_{10}$ *означає десяткове число, складене з цифр* $x, y, z, \ldots$ *.*

Задача 22. *Репьюнітом (repeated unit, англ.) називається число, всі десяткові цифри якого дорівнюють одиниці. Якщо репюніт складається з* n *одиниць, то він позначається* R_n*. Довести, що якщо* R_n *є простим, то* n *також є простим.*

Задача 23. *Нехай n є простим числом. Чи обов'язково репюніт R_n є простим?*

Задача 24. *Довести, що сума двух послідовних непарних чисел є добутком принаймні трьох (не обов'язково різних) простих чисел.*

Задача 25. *Довести, що квадрат будь-якого непарного числа $n > 1$ можна записати у вигляді $8m + 1$ для деякого натурального числа m.*

Задача 26. *Числами Фібоначчі називають члени послідовності $F_1 = 1$, $F_2 = 1$,*

$$F_n = F_{n-1} + F_{n-2}, \qquad n \geq 3.$$

Довести, що F_n є парним тоді і тільки тоді, коли n ділиться на 3.

Задача 27. *Нехай $\{F_n\}$ — це послідовність чисел Фібоначчі (задача 26). Знайти $\sum_{i=1}^{n} F_i$.*

Задача 28. *Довести, що якщо $2^m - 1$ є простим, то й m є простим.*

Задача 29. *Числами Ферма називають члени послідовності*

$$f_n = 2^{2^n} + 1, \qquad n \geq 1.$$

Довести, що

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2, \qquad n \geq 2.$$

Задача 30. *Нехай $\{f_n\}$ — це послідовність чисел Ферма (задача 29). Нескладно підрахувати, що $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$. Можна також продовжити цей ланцюжок:*

$$f_5 = 4294967297, \qquad f_6 = 18446644033331951617.$$

Таким чином, кожне число Ферма F_n, $2 \leq n \leq 6$, закінчується на 7. Довести це твердження для всіх $n \geq 2$ (використайте задачу 29).

Задача 31. *Довести, що C_{2n}^n є парним числом.*