ПРО ОДНУ ФУНКЦ“Ю, ЗАДАНУ НА ДЕКАРТОВОМУ ДОБУТКУ ТА ЧИСЛА ГІННЕСА

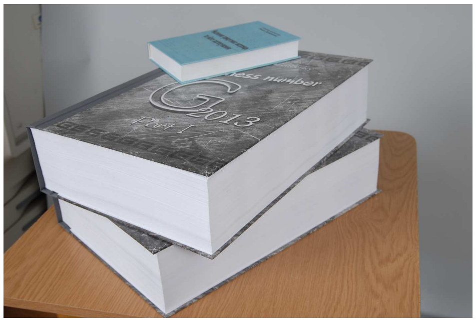
Р.А.ЗАТОРСЬКИЙ

"Наближався 2000-й рік. Розуміючи те, що людство населяючи Землю, своєю "цивілізацією"та "цивілізованістю"вбиває Її і зрештою саме загине, немов бактерії в умираючому людському організмі, я все ж тішився з того, що саме нам судилося пережити рубіж другого та третього тисячоліть. Позаяк моя доля дещо пов'язана з математикою, то у мене з'явилося невимовне бажання мовою математики "звеличити"2000-й рік. Саме тоді появилася, описана нижче, математична ідея, яка у певній мірі дозволяла реалізувати поставлену мету. Я побачив, що число G_{2000} є половинним числом Гіннеса та з певних причин не зміг опублікувати це число. Далі, з аналогічних причин, я пропустив послідовні половинні числа Гіннеса G_{2001}, G_{2006} та G_{2007}. Але наступне половинне число Гіннеса G_{2013} не можу не відзначити, бо не знаю чи доживу до 2031 року, в якому "з'явиться"нове половинне число Гіннеса G_{2031}" — так починається передмова до книги автора "Число Гіннеса G_{2013}". В цій книзі, крім передмови, записане лише одне число, так зване половинне число Гіннеса G_{2013} (див. Рис.1).

У числі Гіннеса G_{2013} 40259996 цифр і воно є найменшим натуральним числом[1], що має наступні нетривіальні властивості: перші чотири цифри числа G_{2013} утворюють число 2013. Якщо видалити ці перші чотири цифри і долучити їх у тому ж порядку вкінці числа G_{2013}, то утворене число зменшиться

[1] 4 квітня 1978 року на засіданні Вченої ради Обчислювального центра АН СРСР при розгляді чергової кандидатської дисертації на ступінь кандидата фізико-математичних наук виникло запитання чи може подана дисертація претендувати на ступінь кандидата фізико-математичних наук чи скоріше кандидата технічних наук. Дисертація не містила жодної теореми, а була лише програма написана на мові ЛІСП, яка дозволяла визначити дії "штучного інтелекту". Погляди присутніх членів ради розділилися. І вирішальним виявилася думка директора інституту А. Дородніцина, який проголосив тезу про те, що *кожна програма може розглядатися як теорема про можливість розв'язання деякої задачі. І якщо програма працює, то можна стверджувати, що теорема доведена.* Ця теза була підтримана А.Марковим, який запропонував дещо уточнити цю тезу: *"Кожна програма є теоремою,*

рівно у 2013 разів. Книга складається із двох частин із сумарним числом сторінок 3655. Кожна сторінка, крім останньої, містить 106 рядків по 104 знаки у кожному.



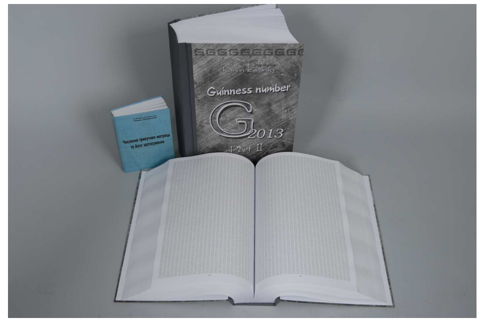


Рис. 1.

На цьому фото зображено книгу "Число Гіннеса G_{2013}", яка складається з двох частин. Для порівняння обєму цієї книги поряд з нею лежить стандартних розмірів книга автора, в якій 508 сторінок.

Нижче дамо означення цілого та половинного чисел Гіннеса та спеціальної функції f_n, при допомозі якої можна згенерувати ці числа. Вкінці замітки сформулюємо кілька запитань на які мені не вдалося знайти відповіді та наведемо деякі корисні застосування функції f_n.

1. Операція f_n та числа Гіннеса

Називаймо числа іменами Людей.
Поки є люди, вони пам'ятатимуть про числа.
Якщо людей не стане, про них "пам'ятатимуть"числа.

Нехай маємо деяке натуральне k-цифрове число n. Кожному такому натуральному числу поставимо у відповідність декартів добуток

$$\Omega_n = \{0, 1, 2, \dots, 10^k - 1\} \times \{0, 1, 2, \dots, n - 1\}.$$

Цей декартів добуток можна графічно зобразити на координатній площині у вигляді прямокутника цілих точок (точок з цілочисельними координатами) з головною діагоналлю, що сполучає початок координат із точкою $(10^k-1, n-1)$.

справедливість якої доведена для тих випадків, для яких програма дає правильну відповідь." Так от доведення того факту, що це число є найменшим натуральним числом, із описаними вище властивостями, полягає у складанні простої програми та роботи комп'ютера, який дає очікуваний результат.

Означення 1.1. *Нехай функція $f_n : \Omega_n \to \Omega_n$ довільній точці $(x, y) \in \Omega_n$ ставить у відповідність точку $(x', y') \in \Omega_n$, тобто $f_n(x, y) = (x', y')$, причому виконується рівність*

$$nx + y = x' + 10^k y'.$$

Оберненою функцією до функції f_n назвемо таку функцію f_n^{-1}, що рівність $f_n^{-1}(x', y') = (x, y)$ виконується тоді і лише тоді, коли виконується рівність $f_n(x, y) = (x', y')$.

Легко доводиться твердження про те, що обидві, означені вище, функції є бієктивними відображеннями множини Ω_n в себе. Точку (x, y) назвемо *нерухомою точкою функції* f_n, якщо виконується рівність $f_n(x, y) = (x, y)$. Неважко довести, що координати нерухомих точок функції f_n задовольняють рівність

$$(n - 1)x = (10^k - 1)y,$$

а самі точки лежать на головній діагоналі декартового прямокутника Ω_n , причому при довільному натуральному n функція f_n має принаймні дві нерухомі точки $(0, 0)$ і $(10^k - 1, n - 1)$.

Приклад 1. Всі нерухомі точки функції f_{34} у множині Ω_{34} визначаються при допомозі рівняння

$$x = 3y.$$

Ними є 34 точки: $(3i, i),\ i = 0, 1, \ldots, 33$.

Позаяк множина Ω_n скінченна і складається лише з нерухомих та рухомих точок, то можна стверджувати, що функція f_n, при допомозі деякої початкової точки (x, y), яку назвемо *твірною точкою*, згенерує *орбіту*

$$O_n(x, y) = \{(x, y), f_n(x, y), f_n^2(x, y), \ldots, f_n^{r-1}\}$$

довжини r, де r — найменше натуральне число, для якого виконується рівність $f_n^r(x, y) = (x, y)$.

Нижче серед всіх твірних точок (x, y) орбіти $O_n(x, y)$, згенерованої функцією f_n, особливу роль відіграватиме точка $(n, 0)$, яку назвемо *стандартною твірною точкою* множини Ω_n.

Означення 1.2. *Точку* $\overline{(x, y)} = (\overline{x}, \overline{y})$ назвемо *спряженою точкою* до точки (x, y), якщо виконуються рівності

$$\overline{x} = 10^k - 1 - x,\ \overline{y} = n - 1 - y. \tag{1.1}$$

Неважко переконатися в тому, що спряжені точки симетричні відносно точки, що є центром симетрії квадрата Ω_n.

Твердження 1.1. *Для довільної точки* $(x,y)\in\Omega_n$ *із рівності*

$$f_n(x,y)=\overline{(x,y)} \tag{1.2}$$

випливає рівність

$$f_n\overline{(x,y)}=(x,y) \tag{1.3}$$

і навпаки.

Отже, інколи спряжені точки утворюють орбіту довжини 2.

Приклад 2. У множині Ω_n, де n — одноцифрове чи двоцифрове число, самоспряжені орбіти довжини 2 відсутні; у множині Ω_{103} існує 6 різних самоспряжених орбіт довжини 2 :

$$(76,95)\leftrightarrow(923,7),(153,87)\leftrightarrow(846,15),(230,79)\leftrightarrow(769,23),$$

$$(307,71)\leftrightarrow(692,31),(384,63)\leftrightarrow(615,39),(461,55)\leftrightarrow(538,47),$$

а у множині Ω_{142} — їх налічується аж 71.

Твердження 1.2. *Нехай задано дві не спряжені точки* $(x,y),(x',y')$ *множини* Ω_n. *Тоді із справедливості рівності*

$$f_n(x,y)=(x',y'),$$

випливає справедливість рівності

$$f_n\overline{(x,y)}=\overline{(x',y')}.$$

Доведення. Перша рівність цього твердження рівносильна рівності

$$nx+y=10^ky'+x'.$$

Враховуючи її, маємо рівності

$$n(10^k-1-x)+n-1-y=10^kn-1-(nx+y)=10^k(n-1-y')+(10^k-1-x'),$$

які рівносильні другій рівності цього твердження. □

Таким чином, якщо серед точок орбіти $O_n(x,y)$, згенерованої функцією f_n, не існує жодної пари спряжених точок, то у декартовій множині Ω_n існує ще одна орбіта $O_n(\overline{x},\overline{y})$, яку назвемо спряженою орбітою до орбіти $O_n(x,y)$, причому графічно ці орбіти симетричні відносно центра симетрії прямокутника Ω_n. Існують також самоспряжені орбіти, до складу яких входять лише взаємно спряжені точки. Графічно такі орбіти є центрально симетричними.

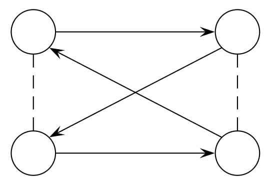


Рис. 2.

На цьому рисунку штрихові відрізки з'єднують пари спряжених точок, а $(x,y) \to (x',y')$ означає $f_{37}(x,y) = (x',y')$. У множині Ω_{37} налічується 34 орбіти з такою структурою, а у множині Ω_{46} — їх є 18.

Означення 1.3. *Цілим числом Гіннеса назвемо число G_n, згенероване функцією f_n при допомозі стандартної твірної точки $(n,0)$, якщо довжина відповідної орбіти $O_n(n,0)$ дорівнює $|\Omega_n| - 2$.*

Аналогічно дається означення половинного числа Гіннеса.

Означення 1.4. *Половинним числом Гіннеса, згенерованим функцією f_n при допомозі твірної точки $(n,0)$, назвемо число G_n, довжина відповідної орбіти якого дорівнює $\frac{1}{2}|\Omega_n| - 1$.*

Наведемо програму на Maple-мові n := 2013: k := 4: x := 2013: y := 0: i := 0: z := x: t := y: m := n*z+t:t := floor(m/10^k) $: z := m - 10^k * t : i := i + 1 : while`or`(x <> z, y <> t) do m := n * z + t : t := floor(m/10^k) : z := m - 10^k * t : i := i + 1 end do : print(i)$

В цій програмі на вході маємо $k = 4$-цифрове число $n = 2013$ та стандартну твірну точку $(n,0) = (2013,0)$, а на виході — довжину орбіти $O_{2013}(2013,0) = i$. За цією програмою ЕОМ після не більше як 5-хвилинної роботи дає число 10064999. Позаяк всі перші компоненти кожної пари орбіти є чотирицифровими числами, то половинне число Гіннеса G_{2013} містить всього

$$10064999 \cdot 4 = 40259996$$

цифр.

Легко переконатися в тому, що серед одноцифрових чисел половинним числом Гіннеса є число 9, а цілими числами Гіннеса - числа $2, 3$ та 6.

Наведемо всі двоцифрові половинні числа Гіннеса:

$$14, \mathbf{20,\ 21}, 24, 27, 30, 33, 41, 48, 51, 54, 62, 66, 69, 75, 77, 87, 90, 92.$$

А ось всі трицифрові половинні числа Гіннеса:

$$102, 105, 108, 135, 144, 162, 165, 183, 189, 192, 204, 213, 222, 231, 240, 261,$$
$$267, 273, 276, 291, 294, 303, 306, 309, 327, 330, 339, 357, 372, 378, 390, 420,$$
$$444, 456, 465, 474, 498, 507, 513, 522, 525, 534, 537, 543, 564, 567, 585, 588,$$
$$600, 603, 609, 612, 621, 639, 645, 660, 663, 669, 672, 696, 705, 726, 732, 738,$$
$$765, 774, 789, 795, 807, 819, 822, 834, 840, 855, 873, 885, 891, 894, 906, 921,$$
$$933, 936, 942, 957, 975, 981, 990.$$

Означення 1.5. *Два половинні числа Гіннеса G_n та G_{n+1} називатимемо **половинними числами-близнюками Гіннеса**.*

Серед двоцифрових чисел є тільки одна пара половинних чисел–близнюків Гіннеса. Серед трицифрових чисел немає жодної такої пари. Наведемо кілька перших пар чотирицифрових половинних чисел–близнюків Гіннеса:

$$(1085, 1086),\ (1091, 1092),\ (1109, 1110),\ (1160, 1161),\ (1187, 1188),\ (1208, 1209),$$
$$(1316, 1317),\ (1337, 1338),\ (1370, 1371),\ (1553, 1554),\ (1658, 1659),\ (1742, 1743),$$
$$(1775, 1776),\ (1796, 1797),\ (1889, 1890),\ (1922, 1923),\ (2000, 2001),\ (2006, 2007),$$
$$(2174, 2175), \ldots.$$

Якщо функція f_n у множині Ω_n генерує m_1 орбіт довжини r_1, m_2 орбіт довжини r_2 і т.д. m_s орбіт довжини r_s, то цей факт позначатимемо через

$$\Omega_n \sim \{r_1^{m_1}, r_2^{m_2}, \ldots, r_s^{m_s}\},$$

причому виконується рівність $|\Omega_n| = \sum_{i=1}^{s} r_i m_i$.

Таким чином, розклад декартової множини Ω_n, пов'язаної з натуральним числом n, на орбіти у великій мірі, нагадує факторизацію натуральних чисел.

$$\Omega_{10} \sim \{1^{10}, 3^{330}\},\ \Omega_{11} \sim \{1^2, 3^2, 39^{28}\},\ \Omega_{12} \sim \{1^{12}, 54^{22}\},\ \Omega_{13} \sim \{1^4, 216^6\}$$
$$\Omega_{14} \sim \{1^2, 699^2\},\ \Omega_{15} \sim \{1^2, 107^{14}\},\ \Omega_{16} \sim \{1^4, 3^{12}, 5^{24}, 15^{96}\},\ \Omega_{17} \sim \{1^2, 283^6\}$$
$$\Omega_{18} \sim \{1^2, 3^2, 128^2, 384^4\},\ \Omega_{19} \sim \{1^{10}, 15^{126}\},\ \Omega_{20} \sim \{1^2, 999^2\},\ \Omega_{21} \sim \{1^2, 1049^2\}.$$

У зв'язку з цим природно виникають наступні запитання.

Проблема 1. *Чи існують цілі числа Гіннеса G_n для багатоцифрових чисел n?*

Проблема 2. *Дослідити потужність множини половинних чисел Гіннеса.*

Проблема 3. *Дослідити закон розподілу натуральних чисел n у натуральному ряді, для яких числа G_n є половинними числами Гіннеса.*

Проблема 4. *Дослідити потужність множини чисел-близнюків Гіннеса.*

2. Операція f_n і добуток багатозначних чисел

"Зовнішнє подібне до внутрішнього; мале таке ж, як і велике; закон один для всього... "(Гермес)

Для однозначних натуральних чисел n, операція f_n зустрічається в кожному алгоритмі множення багатозначних чисел.

Приклад 3. *Нехай необхідно перемножити одноцифрове число* $n = 2$ *на деяке натуральне число* $\overline{x_4x_3x_2x_1x_0} = 72389$. *Добуток цих чисел можна отримати при допомозі операції* f_2, *яка послідовно застосовується до пар*

$$(x_0, y_0) = (9, 0),\ (x_1, y_1) = (8, 1),\ (x_2, y_2) = (3, 1),\ (x_3, y_3) = (2, 0),\ (x_4, y_4) = (7, 0).$$

При цьому ми отримаємо відповідні пари:

$$(x'_0, y'_0) = (8, 1),\ (x'_1, y'_1) = (7, 1),\ (x'_2, y'_2) = (7, 0),\ (x'_3, y'_3) = (4, 0),\ (x'_4, y'_4) = (4, 1).$$

Зауважимо, що згідно з алгоритмом множення, ми відправлялися від нульового значення y_0, *а всі інші значення* y_i, $i = 1, 2, 3, 4$ *були вибрані згідно з рівностями* $y_i = y'_{i-1}$, $i = 1, 2, 3, 4$. *Результатом добутку є число*

$$\overline{y'_4x'_4x'_3x'_2x'_1x'_0}.$$

Операція f_n узагальнює алгоритм множення одноцифрового числа на довільне натуральне k-цифрове число. Нехай задано деяке багатоцифрове число m і k–цифрове число n. Для того, щоб знайти добуток mn необхідно розбити число m починаючи з його кінця на s груп по k цифр у кожній, а дальше поступати так як у попередньому прикладі.

Приклад 4. *Якщо, наприклад,* $m = 2345678$ *і* $n = 23$, *то, у цьому випадку операція* f_{23} *послідовно застосовується до пар*

$$(x_0, y_0) = (78, 0),\ (x_1, y_1) = (56, 17),\ (x_2, y_2) = (34, 13),\ (x_3, y_3) = (2, 7).$$

При цьому отримаємо відповідні пари

$$(x'_0, y'_0) = (94, 17),\ (x'_1, y'_1) = (05, 13),\ (x'_2, y'_2) = (95, 7),\ (x'_3, y'_3) = (53, 0)$$

і результатом добутку є число $\overline{0'53'95'05'94}$.

Таким чином, нами отримано алгоритм множення багатозначних чисел.

Тепер побудова чисел Гіннеса, породжених k–цифровим натуральним числом n та стандартною твірною точкою $(n, 0)$ стає очевидною. Для побудови такого числа, згідно із описаним вище алгоритмом множення багатоцифрових чисел, достатньо виписати з права наліво вряд перші компоненти орбіти $O_n(n, 0)$.

3. Операція f_n і паркети

Числа, як і люди, мають своє "обличчя" і "характер".

Позаяк операція f_n при деяких n розбиває множину Ω_n на парне число взаємно спряжених орбіт та певне число самоспряжених орбіт, то при допомозі цієї операції можна побудувати прямокутний паркет із центром симетрії в точці перетину діагоналей цього прямокутника. Для цього слід об'єднати точки взаємно спряжених орбіт та зафарбувати їх у певний колір.

Приклад 5. f_8–операция розбиває множину Ω_8 на шість орбіт довжиною 13 і дві нерухомі точки. Об'єднуючи множини пар взаємно спряжених орбіт в одну множину, отримаємо три групи по 26 точок в кожній та одну групу, що складається із двох нерухомих точок. Тепер співставимо кожній групі точок певний колір, а кожній парі цих множин — одиничний квадрат на координатній площині. Таким чином, дістанемо розмальований прямокутник. Склеємо кілька отриманих кольорових прямокутників і отримаємо центрально симетричний паркет, який задається натуральним числом 8.

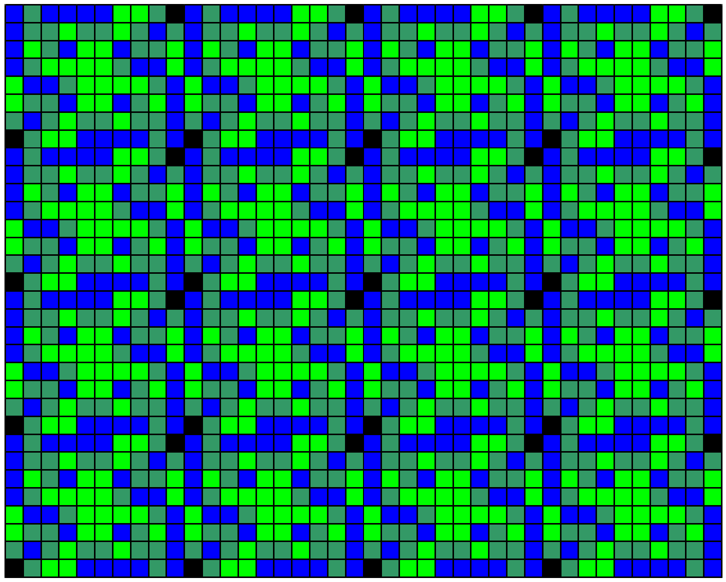


Рис. 3.

Зауважимо, що зображенню на координатній площині точок, що відповідають орбітам $O_n(n,0)$, відповідає характерний структурований малюнок. Таким чином, кожне натуральне число має своє "обличчя" та "характер". Нижче, на рис.4 та 5 відповідно зображено точки орбіт $O_9(9,0)$ і $O_7(7,0)$.

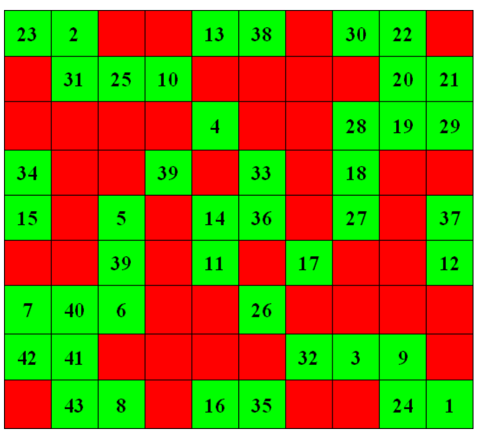


Рис. 4.

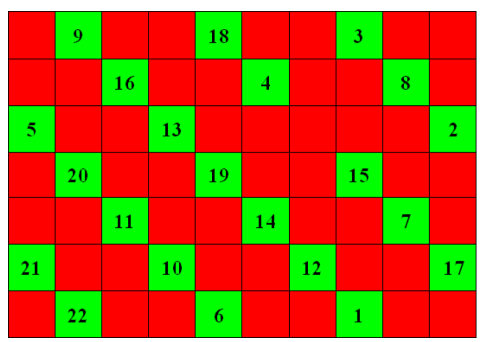


Рис. 5.

4. Числа Гіннеса та генератори псевдовипадкових чисел

"Генерація випадкових чисел — занадто важлива справа,
щоб залишати її на волю випадку."(Роберт Р. Кавъю)

Під одновимірним генератором псевдовипадкових чисел (ГПВЧ)[1] - розуміють алгоритм, який генерує послідовність чисел, елементи якої майже незалежні один від одного і рівномірно розподілені на деякому відрізку.

ГПВЧ знаходять свої застосування в найрізноманітніших галузях людських знань: в ЕОМ, програмуванні, методі Монте-Карло [2], криптографії [3] тощо.

Перший алгоритм для побудови псевдовипадкових чисел було запропоновано американським математиком, одним із творців ЕОМ, Джоном фон Нейманом. Його алгоритм відомий також як метод середини квадратів. Він полягає в тому, що вибирають довільне 4–значне число $a = 0, a_1a_2a_3a_4$. Підносять його до квадрата $a^2 = 0, a'_1a'_2a'_3a'_4a'_5a'_6a'_7a'_8$ і переходять до нового 4–значного числа $0, a'_3a'_4a'_5a'_6$ і т.д.

Головною перевагою цього арифметичного алгоритму є його простота, а недоліком — те, що він генерує не більше як 10000 різних чисел.

В [4], першим автором цієї статті, запропоновано двовимірний арифметичний генератор псевдовипадкових чисел, який базується на операції f_n. Цей ГПВЧ дещо подібний до арифметичного генератора Джона фон Неймана. Другим автором статті [4] запропонований генератор було апробовано у системі дистанційного контролю знань, а третім автором було проведено його тестування при допомозі загальноприйнятих критеріїв: рівномірності, інтервалів, "максимуму–t"і покер–критерію.

В цій статті послідовність псевдовипадкових чисел задається першими та другими компонентами орбіти $O_n(n, 0)$. При цьому натуральне число n підбирається так, щоб число G_n було цілим або половинним числом Гіннеса. Наприклад, при допомозі половинного числа Гіннеса G_{200000} можна побудувати орбіту, що є двовимірним випадковим масивом з періодом 99999999999. Незважаючи на висловлення Джона фон Неймана: "кожен, хто прихильний до арифметичних методів генерування випадкових чисел, без сумніву грішний,"наведений вище генератор має величезний період та успішно витримав всі тестування.

Якщо, наприклад, відкладати всі точки орбіти $O_{2000}(2000, 0)$ на площині листка формату А4, то вони цю площину покриватимуть так, що листок, у різні проміжки часу, буде однотонно сірим. Звідси випливає придатність наведеного вище ГПВЧ і до методу Монте–Карло.

Одним із найбільш поширених алгоритмів генерування псевдовипадкових чисел $x_n,\ n = 0, 1, 2, \ldots, L$ є алгоритм, який запропонував американський математик Д.Н. Лемер. Цей алгоритм задається наступними рівностями:

$$m_{n+1} \equiv 5^{17} m_n (mod\, 2^{40}),\ n = 0, 1, 2, \ldots, L,\ m_0 = 1,$$

$$x_n = 2^{-40} m_n.$$

Серед сучасних ГПВЧ широке застосування має Mersenne twister. Цей генератор запропонований в 1997 році Мацумото і Нішімурою. Його позитивною якістю є величезний період $(2^{19937} - 1)$ та рівномірний розподіл в 623–х вимірах. Однак цей генератор не придатний для застосувань в криптографії, бо існує алгоритм, який розпізнає послідовність, породжену при допомозі Mersenne twister, як невипадкову.

Вкажемо на ще одне застосування функції f_n. Кожній твірній точці (x, y) функція f_n при достатньо великих значеннях n ставить у відповідність деякий масив чисел, або його фрагмент, за яким важко відтворити самі числа (n, x, y). Тобто функція f_n є важко оборотною функцією і може використовуватися при генеруванні ключових слів для методу одноразового блокнота шифрування інформації.

Проблема 5. *Побудувати при допомозі функції f_n криптосистему з відкритим ключем.*

Автор сподівається, що у майбутньому функція f_n знайде нові плідні застосування і їй буде виділене достойне місце у теорії чисел.

Література

[1] *А.Зубинсъкий* У пошуках випадковості. (рос.) Компьютерное Обозрение, 29 (2003).

[2] *И.М.Соболь* Метод Монте–Карло.—М.:Наука, 1985.— 80 с.

[3] *О.В.Вербіцький* Вступ до криптології, ВНТЛ.—Львів, 1998.

[4] *Р.А.Заторський, П.І.Федорук, Н.М.Дяків* Генератор випадкових чисел у системі дистанційного контролю знань.//Математичні машини і системи. — 2004. — №4. — С. 98–107.