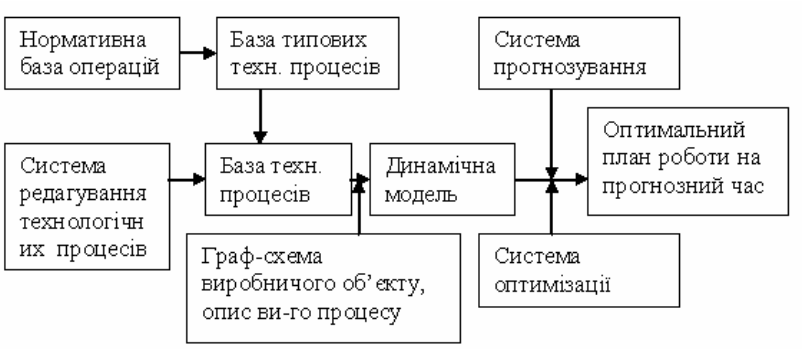

Рис. 2. Система автоматизації процесу побудови моделі об'єкта та моделювання його виробничого процесу

Висновки

Запропоноване і обґрунтоване в роботі представлення технологічного процесу у вигляді теоретико-графових об'єктів забезпечує однозначну інтерпретацію довільного абстрактного технологічного процесу і тому його без додаткових застережень можна використати для побудови довільного існуючого виробничого процесу.

Результати роботи дали можливість побудувати динамічну модель роботи станції та сформулювати задачі на максимальну переробну і пропускну її спроможність.

1. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ, 2-е изд.: Пер. с англ. – М.: Издательский дом "Вильямс", 2005. – 1296 с.: ил. – Парал. тит. англ. ISBN 5-8459-0857-4 (рус.) 2. Майника Э. Алгоритмы оптимизации на сетях и графах. – М.: Мир, 1981. – 324 с.

УДК 681.84.087.4

А. Ковальчук
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ПРО ДЕЯКІ НЕСКІНЧЕННІ МНОЖИНИ ПРОСТИХ ЧИСЕЛ ДЛЯ ВИКОРИСТАННЯ В СИСТЕМІ RSA

Для квадратного полінома з цілими коефіцієнтами і від натуральної змінної розв'язана задача про потужність підмножини простих значень такого полінома. На підставі отриманого результату обгрунтовується можливість побудови алгоритмів вибору простих чисел для криптографічних систем з відкритими ключами.

For the quadratic polinomial with integer coefficients and at the natural variable the solving of the problem of the infinity sets of the prime values of this polynomial is presented. With a foundation on the recived result the possibility of the construction of the prime numbers for the kryptographic systems with open keys are based.

Вступ

При побудові криптоалгоритмів для генерування системи ключів в системі RSA необхідно випадково вибирати прості числа для генерування відкритого ключа $N = p \cdot q$, від випадковості

факторизації якого залежить стійкість побудованої криптографічної системи. Наслідком такого вибору простих чисел є можливість використання їх в асиметричних криптосистемах, причому множина $\boldsymbol{A}$, з якої вибираються прості числа, має бути рівнопотужною множині натуральних чисел, тобто – нескінченною.

Використовуючи теорему, доведену в цій статті, і застосовуючи відомі [1] тести перевірки чисел на простоту (наприклад, тест Адлемана перевіряє простоту числа $\boldsymbol{n}$ за $\boldsymbol{O}((\log \boldsymbol{n})^{c \log\log\log \boldsymbol{n}})$ кроків, де $\boldsymbol{c}$ – абсолютна константа [1]), можна конструювати алгоритми генерування простих чисел. А саме, множиною $\boldsymbol{A}$ може бути множина всіх простих значень квадратного полінома, кожне значення якого має вигляд $\boldsymbol{a^2 + Kb^2}$.

Означення і терміни

Розглянемо квадратний поліном вигляду

$$f(x) = Ax^2 + Bx + C \ , \tag{1}$$

де $A > 0$, B, C – цілі числа, x – натуральна змінна. Найбільший спільний дільник натуральних чисел d і δ позначимо (d, δ), дискримінант полінома (1) позначимо $D = B^2 - 4AC$.

Нехай нескінченна підпослідовність значень змінної x визначена так:

$$x = \mathrm{U}(y_1, \ldots, y_k) \tag{2}$$

де кожна змінна y_j, $j = 1, \ldots, k$, змінюється на деякій нескінченній підмножині натурального ряду, а функція U набуває натуральні значення.

Означення. Значення полінома (1)

$$f(x) = A\{\mathrm{U}\}^2 + B\{\mathrm{U}\} + C \ , \tag{3}$$

де символом $\{\mathrm{U}\}$ позначено праву частину (2), назвемо значенням заданого вигляду.

Принцип нескінченного спуску [3]. Якщо з припущення про те, що деяке ціле додатне число має задану множину властивостей, випливає, що існує менше додатнє ціле число з тією ж множиною властивостей, то жодне додатне число не може мати цю множину властивостей.

Основна частина

Теорема 1. Якщо не менше, ніж три прості числа вигляду (3) мають вигляд $f_n = a_n^2 + K_n b_n^2$, $n = 1, \ldots, L$, $L \geq 3$ і $K_n \neq 0$ – ціле, a_n, b_n – цілі числа, то в множині всіх значень полінома (1) міститься нескінченна підмножина простих чисел вказаного вигляду.

Доведення. Розглянемо всі прості значення вказаного вигляду полінома (1), за зростанням $f_1 < \ldots < f_n < \ldots$, $n \geq 3$, $x_1 < \ldots < x_n < \ldots, f_n = f(x_n) = Ax_n^2 + Bx_n + C$ і припустимо, що множина всіх таких простих значень – скінченна.

Нехай для довільного значення полінома (1) $f(x_0)$ виконується нерівність $f(x_0) > P$, де $P = f(X)$ – найбільше його просте значення вказаного вигляду, $x_0 > X$, x_0 – довільне раціональне число, $x_0 = s_0 / z_0$, s_0, z_0 – довільні натуральні числа, $s_0 > Xz_0$. Тоді для x_0 і кожного x_n існує раціональне число $\alpha_{n,0}$, що виконуються рівності

$$x_0 = x_n + \alpha_{n,0} \ , \tag{4}$$

$$f(x_0) = f_n + t_{n,0} \ , \tag{5}$$

де

$$A\alpha_{n,0}^2 + (2Ax_n + B)\alpha_{n,0} + C - t_{n,0} = 0. \tag{6}$$

Рівність (6) означає, що $\alpha_{n,0}$ є раціональним коренем квадратного рівняння:

$$Az^2 + (2Ax_n + B)z + C - t_{n,0} = 0 \ , \tag{7}$$

в силу чого існує раціональне число $u_{n,0}$, $u_{n,0}^2$ – дискримінант рівняння (7).

Взявши до уваги тотожність

$$(a^2 + Kb^2)(\boldsymbol{T}^2 + K\boldsymbol{R}^2) = (a\boldsymbol{T} - Kb\boldsymbol{R})^2 + K(a\boldsymbol{R} + b\boldsymbol{T})^2,$$

де $a^2 + Kb^2 \neq 0$, $K \neq 0$ – ціле число, розглянемо лінійну відносно $\boldsymbol{T}$ і $\boldsymbol{R}$ систему:

$$\begin{cases} a\boldsymbol{T} - Kb\boldsymbol{R} = \gamma \\ b\boldsymbol{T} + \ a\boldsymbol{R} \ = b \end{cases} \tag{8}$$

де γ – довільне раціональне число.

Визначник системи (8) $\Delta = a^2 + Kb^2 \neq 0$ і, отже, ця система має єдиний ненульовий розв'язок і виконуються рівності:

$$\Delta\boldsymbol{T} = \gamma a + Kb^2, \ \Delta\boldsymbol{R} = (a \ - \gamma)b \ . \tag{9}$$

В силу довільності в (9) числа γ, вибираючи $\gamma = a_{\text{n}} t_{n,0} - K_{\text{n}} u_{n,0}, b_{\text{n}}$, $b = b_{\text{n}}$, $a = a_{\text{n}}$, $K = K_{\text{n}}$ і враховуючи (9), з другої рівності (8) отримаємо

$$u_{n,0}\, a_{\text{n}} = - (t_{n,0} \ -1) b_{\text{n}} \ . \tag{10}$$

Після піднесення до квадрата обох частин (10) і тотожних перетворень отримаємо:

$$u_{n,0}^2 f_{\text{n}} = [(t_{n,0} \ -1)^2 + K_{\text{n}} u_{n,0}^2 \,] \, b_n^2 \ . \tag{11}$$

Легко переконатися, що $u_{n,0}^2 = (2Ax_{\text{n}} + B) + 4A\, t_{n,0}^2 = (\ 2Ax_0 + B)^2$. Оскільки раціональне число $x_0 = s_0 / z_0$, то $u_{n,0} = (2As_0 + Bz_0) / z_0$. Нехай $(t_{n,0} \ - 1)^2 + K_{\text{n}} u_{n,0}^2 = \xi_{n,0} / \eta_{n,0}$, де $\xi_{n,0}, \eta_{n,0}$ – цілі числа, $(\xi_{n,0}, \eta_{n,0}) = 1$. Тоді (11) набуває вигляду

$$(2As_0 + Bz_0)^2 \eta_{n,0} f_{\text{n}} = z_0^2 \ \xi_{n,0} \ b_n^2 \ . \tag{12}$$

Якщо в (12) просте f_{n} ділить $\xi_{n,0}$, тобто $\xi_{n,0} = Z_{n,0} f_{\text{n}}$, де в силу $(\xi_{n,0}, \eta_{n,0}) = 1$ має місце умова $(Z_{n,0}, \eta_{n,0}) = 1$, то (12) набуває вигляду

$$(2As_0 + Bz_0)^2 \eta_{n,0} \ = z_0^2 \ Z_{n,0} \ b_n^2 \ . \tag{13}$$

Нехай p – простий дільник числа $Z_{n,0}$. Тоді просте число p ділить число $2As_0 + Bz_0$, тобто $2As_0 + Bz_0 = p\, L_{n,0}$, $L_{n,0} < 2As_0 + Bz_0$, $Z_{n,0} = p\, C_{n,0}$, $C_{n,0} < Z_{n,0}$, а (13) набуває вигляду

$$L_{n,0}^2 \ \eta_{n,0} \ p = z_0^2 \ C_{n,0} \ b_n^2 \ . \tag{14}$$

Отже, разом з рівністю (12) має місце рівність (14), де $C_{n,0} < \xi_{n,0}$ і $L_{n,0}^2 < (2As_0 + Bz_0)^2$, що відповідно до принципу нескінченного спуску неможливо, тобто просте f_{n} не ділить $\xi_{n,0}$.

У (12) просте f_{n} не може ділити b_n^2, оскільки у протилежному випадку з $f_{\text{n}} = a_{\text{n}}^2 + K_{\text{n}} b_{\text{n}}^2$ випливало б, що якщо $b_{\text{n}} = f_{\text{n}} B_{\text{n}}$, то $a_{\text{n}} = f_{\text{n}} A_{\text{n}}$, що при простому f_{n} приводить до існування неможливої рівності $1 = f_{\text{n}}(A_n^2 + K_{\text{n}} B_n^2)$, де B_{n} і A_{n} – деякі цілі числа.

Отже, в (12) кожне просте f_{n} ділить z_0^2, тобто f_{n} ділить кожне z_0. Тобто, всі прості f_{n} є дільниками кожного цілого числа z_0, що суперечить тому, що число z_0 – довільне. Отримана суперечність доводить теорему 1.

Результати

Наслідок 1. У множині значень полінома $f(x) = x^2 + 3x + 1$ містяться нескінченні підмножини простих чисел вигляду $a^2 + 2b^2$ і $a^2 + 3b^2$.

Доведення. Запишемо $f(x)$ у вигляді: $f(x) = (\ x + 1)^2 + x$. Виконавши заміну $x = 2y^2$, маємо: $f(2y^2) = (2y^2 + 1)^2 + 2y^2$ і для $y = 1, 2, 3$ числа $f(2y^2) = 11, 89, 379$ – прості . Тоді за теоремою 1 простих чисел вигляду $(2y^2 + 1)^2 + 2y^2$ у множині всіх значень заданого полінома – нескінченна множина.

Якщо виконати заміну $x = 3y^2$, то $f(3y^2) = (3y^2 + 1)^2 + 3y^2$, а при $y = 1, 3, 5$ числа $f(3y^2) = 17, 127, 5851$ – прості, тобто простих вигляду $(3y^2 + 1)^2 + 3y^2$ – також нескінченна множина.

Наслідок 2. Простих чисел Ферма $F_{\text{k}} = 2^{2^k} + 1$ – нескінченна множина.

Розглянемо квадратний поліном $f(x) = x^2 + 1$ і виконаємо заміну $x = 2^{2^{k-1}}$, $k = 1, 2, 3, \ldots$ Тоді $f(2^{2^{k-1}}+1) = 2^{2^k} + 1$, тобто всі числа F_k є значеннями полінома $f(x)$. Окрім того, для $k = 1, 2, 3$ маємо $x = 2, 4, 16$ і $f(2) = 5$, $f(4) = 17$, $f(16) = 257$. За теоремою 1 на нескінченній підмножині значень змінної x поліном $f(x)$ набуває простих значень вигляду $F_k = f(2^{2^{k-1}}+1)$, оскільки $f(x) = 1^2 + 1 \cdot x^2$.

Означення 2. Натуральні числа вигляду $F_{k,m} = 2^{2^k} + m$, де $k = 0, 1, 2, 3, \ldots, m$ – непарне число, назвемо узагальненими числами Ферма.

Означення 3. Натуральні числа вигляду $M_{n,l} = 2^n - l$, де $n = 1, 2, 3, \ldots, l$ – непарне число, назвемо узагальненими числами Мерсенна.

Наслідок 4. Всі три множини узагальнених чисел Ферма $F_{k,1}$, $F_{k,3}$, $F_{k,7}$ таких, що

$$F_{k,3} - F_{k,1} = 2,\ F_{k,7} - F_{k,3} = 4,\ F_{k,7} - F_{k,1} = 6, \qquad (15)$$

– нескінченні.

Розглянувши квадратні поліноми $f(x) = x^2 + 1$, $g(x) = x^2 + 3$, $h(x) = x^2 + 7$ і виконавши заміну $x = 2^{2^{k-1}}$, $k = 1, 2, 3, \ldots$ отримаємо: $f(2^{2^{k-1}}) = F_{k,1}$, $g(2^{2^{k-1}}) = F_{k,3}$, $h(2^{2^{k-1}}) = F_{k,7}$. Для $k = 1, 2, 4$ маємо $x = 2,4,256$, $f(2) = 5$, $f(4) = 17$, $f(256) = 65537$; $g(2) = 7$, $g(4) = 19$, $g(256) = 65539$; $h(2) = 11$, $h(4) = 23$, $h(256) = 65543$ – прості. А оскільки $f(x) = x^2 + 1 \cdot 1^2$, $g(x) = x^2 + 3 \cdot 1^2$, $h(x) = x^2 + 7 \cdot 1^2$, то за теоремою 1 простих $f(x)$, $g(x)$, $h(x)$ – нескінченні множини, а також за теоремою 1 нескінченними є три множини пар узагальнених простих чисел Ферма у відповідних рівняннях (15).

Наслідок 5. Множини $M_{n,3}$ і $M_{n,19}$ узагальнених простих чисел Мерсенна – обидві нескінченні.

Для доведення з використанням теореми 1 розглянемо квадратні поліноми: $g(x) = 2x^2 - 3$ і $h(x) = 2x^2 - 19$. Після заміни $x = 2^{(n-1)/2}$, $n = 3, 5, 7, \ldots$маємо: $g(2^{(n-1)/2}) = 2^n - 3$, $h(2^{(n-1)/2}) = 2^n - 19$ і для чисел $n = 3,5,9$; $x = 2,4,16$: $g(2) = 5 = 2^2 + 1 \cdot 1^2$, $g(4) = 29 = 5^2 + 1 \cdot 4^2$, $g(16) = 509 = 5^2 + 1 \cdot 22^2$. Для $h(x)$: $n = 5,7,11$; $x = 4,8, 32$ – $h(4) = 13 = 3^2 + 1 \cdot 2^2$, $h(8) = 109 = 3^2 + 1 \cdot 10^2$, $h(32) = 2029 = 2^2 + 1 \cdot 45^2$.

Зауваження 1.

Розглянувши поліном $f(x) = 2x^2 - 1$, можна аналогічно довести, що множина простих чисел Мерсенна $M_n = 2^n - 1$ – нескінченна.

Наслідок 6. Множина пар простих чисел p і q, для яких виконується рівність $2p - 1 = q^2$ – нескінченна.

Доведення. Розглянемо поліноми: $f(x) = 2x^2 + 2x + 1$, $g(x) = 4x^2 + 4x + 1$. Тоді $2f(x) - 1 = g(x)$, або $2f(x) - 1 = (2x + 1)^2$. За теоремою Діріхле простих чисел $q = 2x + 1$ – нескінченна множина. Виділимо в множині всіх значень полінома $f(x)$ такі, що q – просте число. Тоді для $x = 1, 2, 5$ $q = 3, 5, 11$ і $f(x) = 5,13,61$ і доведення наслідку 6 за теоремою 1 закінчене, оскільки $f(x) = (x+1)^2 + 1 \cdot x^2$.

Наслідок 7. Множина простих чисел вигляду $p = 4^m + 3$, де натуральне число $m \geq 2$ – нескінченна.

Розглянемо поліном $f(x) = x^2 + 3$, виконаємо заміну $x = 4^{m/2}$, $m = 2,6,8, \ldots$ Тоді $f(4^{m/2}) = 4^m + 3$ і для $m = 2, 6, 8, \ldots$ $x = 4, 64, 256, \ldots$, $f(x) = 19, 4099, 65539\ldots$ Окрім того, $f(x) = x^2 + 3 \cdot 1^2$ і за теоремою 1 наслідок 7 доведено.

Зауваження 2. Перевірка, чи конкретні натуральні числа є простими, здійснювалася за таблицями простих чисел [2].

Висновок. Отже, випадковий вибір простих чисел p і q, про які згадувалося у вступі, можна здійснювати з якої-небудь нескінченної конкретної множини простих чисел, приведених в наслідках. Це дає можливість отримувати відносно стійкі RSA-криптосистеми, користуючись при цьому будь-яким тестом перевірки натурального числа на простоту.

1. Василенко О.Н. Современные способы проверки простоты чисел // Кибернетический сборник. – 1988. – №25. – С. 162 – 187. 2. Леммер Д.Н. Таблицы простых чисел от 2 до 10006721. – М., 1967. 3. Эдвардс Г. Последняя теорема Ферма. – М.: Мир, 1980.