або вищу. У випадку збільшення складності НМ вдається помітно (у 2-3 рази) підвищити точність відтворення інтерполяційних точок за рахунок зниження точності для екстраполяційних.

3. Для НМ ФМТФ існує можливість підвищення екстраполяційних властивостей за рахунок модифікацій передатних функцій нейронів, зокрема шляхом використання апроксимаційних ортогональних поліномів.

1. McCulloch W.S., Pitts W. A logical calculus of ideas immanent in nervous activity// Bull. Mathematical Biophysics. 1943. Vol. 5. P. 115-133.
2. Минский М., Пейперт С. Перцептроны. М., 1971.
3. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. М., 1992.
4. Ткаченко Р.О., Неітераційне навчання штучних нейронних мереж прямого поширення // Технічні вісті. 1999. №1(8), 2(9). С.41-42

УДК 511.217

ПРОСТІ ЧИСЛА КВАДРАТНОГО ПОЛІНОМА І ГІПОТЕЗА А.ШИНЦЕЛЯ

© А. Ковальчук
Національний університет "Львівська політехніка"

Встановлено нескінченність множини простих значень квадратного полінома за умови, що цей поліном має хоч би два різні прості значення і якщо дискримінант такого квадратного полінома – не квадрат цілого числа. Доведено гіпотезу А.Шинцеля.

The infinity of a set of prime numbers of a square polynomial is established, provided that this polynomial has even two different simple significances and if a discriminant of such polynomial - not guadrate of an integer. Is proved A. Schinzel conjecture.

У системі RSA з відкритими ключами при кодуванні інформації необхідно використовувати великі прості числа. Доцільно ці прості числа вибирати не з усього натурального ряду, а в деяких його нескінченних підмножинах, зокрема – в множині всіх значень деякого квадратного полінома.

Нехай a – натуральне, а b – ціле число, $0 \le b < a$. Доведення теореми про те, що в кожній арифметичній прогресії, різниця якої а взаємно проста з першим значенням b, є нескінченна множина простих чисел, тобто конгруенція $p \equiv b(\mathrm{mod}\ a)$ має нескінченну

множину простих розв'язків, отримано Діріхле. За допомогою цієї теореми можна довести твердження: якщо арифметична прогресія $ax + b$, $x = 0, 1, 2, \ldots$ має хоч би два прості значення p і q, $p < q$, то така прогресія має нескінченну множину простих значень.

Для доведення достаньо показати, що числа a і b – взаємно прості і застосувати потім до прогресії згадану теорему.

Дійсно, якщо $p = ax_1 + b$, $q = ax_2 + b$, то припустимо протилежне і нехай $b = rb_r$, $a = ra_r$, $r \neq 1$. Тоді $p = r(a_r x_1 + b_r)$, $q = r(a_r x_2 + b_r)$, звідки, оскільки $a_r x_1 + b_r \neq 1$ і $a_r x_2 + b_r \neq 1$, в силу нерівності $p \neq q$, випливає, що якщо p і q – прості числа, то $r = 1$, що суперечить припущенню.

Отже, простих чисел в арифметичній прогресії – нескінченна множина, якщо простих чисел ця прогресія має хоч би два. Аналогічним твердженням можна встановити нескінченність множини простих значень квадратного полінома, за умови, що цей поліном має хоч би два різні прості значення і якщо дискримінант такого полінома – не квадрат цілого числа.

Нехай на інтервалі $[U, V]$ визначені функції $H(\zeta)$ і $F(\zeta)$.

Означення 1. Якщо для всіх ζ з інтервалу $[\xi, \eta] \subseteq [U, V]$ функції $H(\zeta)$ і $F(\zeta)$ або обидві – спадні, або обидві – зростаючі, або одна з них – зростаюча, а друга – спадна і виконується одна з нерівностей для всіх ζ: або $H(\zeta)$ і $F(\zeta)$, або $H(\zeta) \leq F(\zeta)$, то назвемо $H(\zeta)$ і $F(\zeta)$ одностайно монотонними функціями на інтервалі $[\xi, \eta]$.

Розглянемо квадратний поліном, який має вигляд

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

де $A > 0$, B, C – цілі, x – натуральна змінна.

Дискримінант полінома (1) позначимо $D = B^2 - 4AC$; два числа d і δ – взаємно прості, якщо їх найбільший спільний дільник $(d, \delta) = 1$. Якщо над полем цілих чисел розвинення $f(x) = P(x)Q(x)$, де $P(x)$ і $Q(x)$ – поліноми, неможливе, то поліном $f(x)$ – незвідний, в протилежному випадку – звідний.

Якщо поліном (1) – звідний, тобто $f(x) = (Kx + L)(Mx + N)$, то множники $Kx + L$ і $Mx + N$ одностайно монотонні при $x \geq [z]$, де $z = (N - L)/(K - M)$, $[z]$ – ціла частина z, $K \neq M$. Виконавши тоді заміну змінної $x = y + [z]$ з полінома (1), отримаємо інший поліном $g(y) = (Ky + K[z] + L)(My + M[z] + N)$, множники якого – одностайно монотонні при $y \geq 1$. Тому, не зменшуючи загальності, за умови звідності полінома (1) надалі будемо вважати його множники одностайно монотонними функціями при $x \geq 1$.

Лема 1. Якщо поліном (1) має більше двох різних простих додатних значень, то він незвідний.

Доведення. Навпаки, нехай в умовах теореми поліном (1) – звідний. Тоді

$$f(x) = P(x)Q(x), \text{ де } P(x) \text{ і } Q(x) \text{ – одностайно монотонні при } x \geq 1.$$

Виберемо при $n \geq 3$, $1 \leq k \leq n$, $1 \leq l \leq n$, $1 \leq m \leq n$, $k \neq l$, $k \neq m$, $m \neq l$ три довільні прості значення полінома (1) $f(x_k) = p_k < f(x_l) = p_l < f(x_m) = p_m$ при $x_k \geq 1$ і розглянемо зростаючу послідовність

$$a_1 = -p_m,\ a_2 = -p_l,\ a_3 = -p_k,\ a_4 = -1,\ a_5 = 1,\ a_6 = p_k,\ a_7 = p_l,\ a_8 = p_m. \tag{2}$$

Оскільки $f(x) = P(x)\cdot Q(x)$, то в (2) існує зростаюча підпослідовність $a_\nu < a_\lambda < a_\mu$, $1 \le \nu \le 8$, $1 \le \lambda \le 8$, $1 \le \mu \le 8$, $\nu \ne l$, $\mu \ne l$, $\nu \ne \mu$, що $P(x_j) = a_i$, де $j = k, l, m$; $i = \nu, \lambda, \mu$ і тоді

$$a_i Q(x_j) = p_j \tag{3}$$

Але з (3) випливає, що в (2) не існує відповідної підпослідовності $b_i = Q(x_j)$, щоб на проміжку $[x_k, x_m]$ множники $P(x)$ і $Q(x)$ були одностайно монотонними. Суперечність доводить лему 1.

Теорема 1. Якщо $D = t^2$, де $t \ne 0$ – ціле число, і поліном (1) має не менше двох різних простих значень, то цей поліном має тільки два різні прості значення.

Доведення. Якщо $D = t^2$, то поліном (1) – звідний. Нехай при значеннях змінної $x_1 < x_2 < \ldots < x_n$ поліном (1) має прості значення $p_1 < p_2 < \ldots < p_n$. Припустимо, що $n \ge 3$. Тоді в силу леми 1 він незвідний. Суперечність доводить, що поліном не може мати більше двох різних простих значень. В силу умови це означає, що поліном має тільки два різні прості значення. Теорема 1 доведена.

Теорема 2. Якщо поліном (1) має тільки два різні прості значення, то цей поліном – звідний.

Доведення. Нехай $f(1) = p < f(x_0) = q$ – тільки два прості значення полінома (1). Інші значення – складені і, оскільки поліном – квадратний, то для кожного натурального x $f(x) = (Mx + N)(Kx + L)$, де $|Mx + N| \ne 1$, $|Kx + L| \ne 1$, якщо $x \ne 1, x_0$. Знайдемо коефіцієнти M, N, K, L і покажемо, що це – цілі числа. Нехай $p = uv$, $q = \xi\eta$, де u, v, ξ, η – цілі числа. В силу $p < q$ можна прийняти, що $u < \xi$. Тоді мають місце рівності:

$$M + N = u,\ Mx_0 + N = \xi;\ K + L = v,\ Kx_0 + L = \eta,$$

з яких знаходимо:

$$M = (\xi - u)/(x_0 - 1),\ N = (ux_0 - \xi)/(x_0 - 1),$$

$$K = (\eta - v)/(x_0 - 1),\ L = (vx_0 - \eta)/(x_0 - 1),$$

$$f(x)(x_0 - 1)^2 = (\xi - u)(\eta - v)x^2 + B_0 x + C_0, \tag{4}$$

де

$$B_0 = (\xi - u)(vx_0 - \eta) - (\eta - v)(ux_0 - \xi),$$

$$C_0 = (ux_0 - \xi)(vx_0 - \eta)$$

Оскільки рівність (4) виконується для кожного x, то існує рівність

$$A(x_0 - 1)^2 = (\xi - u)(\eta - v), \tag{5}$$

або еквівалентна до неї

$$Ax_0^2 - 2Ax_0 + A - (\xi - u)(\eta - v) = 0, \tag{6}$$

яка означає, що відповідне квадратне рівняння має цілий корінь x_0. Тоді

$$A(\xi - u)(\eta - v) = \Delta^2, \tag{7}$$

де $4\Delta^2$ – дискримінант (6).

Нехай $(\xi - u, \eta - v) = r$ – ціле число. Припустимо, що $r > 1$. (Випадок $r < 0$ – неможливий, оскільки з (7) випливає, що існує єдина можливість для множників в цій рівності: $\xi - u > 0$, $\eta - v > 0$). Тоді $\xi - u = \lambda r$, $\lambda < \xi - u$; $\eta - v = \mu r$, $\mu < \eta - v$ і з (7) випливає, що $A\lambda\mu \cdot r^2 = \Delta^2$, тобто $r^2 \mid \Delta^2$, а $r \mid \Delta$. Це означає, що $\Delta = r\delta$, $\delta < \Delta$, а з (7) отримуємо рівність $A\lambda\mu = \delta^2$, яка відповідно до принципу нескінченного спуску не може існувати разом з (7). Отже, припущення невірне і $r = 1$, тобто $(\xi - u, \eta - v) = 1$. Тоді, оскільки $A = MK$, то $[(\xi - u)(\eta - v)]^2/(x_0 - 1)^2 = \Delta^2$. Це означає, що $x_0 - 1$ ділить або $\eta - v$, або $\xi - u$, тобто всі коефіцієнти M, N, K, L – цілі числа, дискримінант полінома (1) – квадрат цілого числа і цей поліном – звідний.

Для завершення доведення покажемо, що якщо $r^2 \mid \Delta^2$, то $r \mid \Delta$. Нехай $\Delta^2 = kR^2$. Якщо k – просте число, то $k \mid \Delta$, $\Delta = k\Delta_1$, і $k\Delta_1^2 = R^2$. Тобто $k \mid R$, $R = kR_1$, і $\Delta_1^2 = kR_1^2$, $\Delta_1 < \Delta$, $R_1 < R$, що відповідно до принципу нескінченного спуску неможливо. Якщо $k = mp$, де p – просте число, тобто $\Delta^2 = mpR^2$, то доведення аналогічне, як в попередньому випадку, коли k – просте число. Отже, якщо $r^2 \mid \Delta^2$, то $r \mid \Delta$. Теорема 2 доведена.

Теорема 3. Якщо поліном (1) має не менше двох різних простих значень $f(1) < f(x_2)$, $x_2 > 1$ і його дискримінант D не квадрат цілого числа, то існує третє просте число $f(x_3)$ таке, що $f(x_3) > f(x_2)$, $x_3 > x_2$.

Доведення. В силу теореми 2 поліном (1) не може мати тільки два різні прості значення. Отже, існує третє просте значення $f(x_3)$, $x_3 \neq x_2$. Якщо $f(x_3) = f(x_2)$, то це означає, що поліном (1) має тільки два прості значення, і в силу теореми 2 цей поліном – звідний, а його дискримінант – квадрат цілого числа, що суперечить умові. Суперечність доводить, що $f(x_3) \neq f(x2)$. Якщо $x_3 > x_2$, то теорема доведена. Якщо $x_3 < x_2$, то впорядковуючи значення змінної по зростанню, за x_3 виберемо більше. Теорема 3 доведена.

Зауваження. Якщо $f(x_0)$ – просте число і $x_0 \neq 1$, то замінивши x на $z + x0 - 1$, отримаємо поліном $F(z)$ степеня 2, у якого значення $F(1)$, $F(x_1 + x_0 - 1)$ – прості числа.

Теорема 4. Якщо поліном (1) має два різні прості значення $f(1) < f(x_1)$ і його дискримінант D – не квадрат цілого числа, то такий поліном має нескінченну підмножину простих значень.

Доведення. Нехай $f(1) = p_1 < f(x_1) = p_2$ – прості значення і для всякого цілого t дискримінант $D \neq t^2$. В силу теореми 3 існує третє просте значення $f(x_2) > f(x_1)$, $x_2 > x_1$. Побудуємо квадратний поліном $h_1 = Ay^2 + B_1y + C_1$, для якого виконуються умови

$$h_1(1) = f(x_1),\ h_1(y_{2,1}) = f(x_2), \tag{8}$$

де $y_{2,1} = x_2 - x_1 + 1$. З (8) тоді отримаємо лінійні рівняння відносно B_1 і C_1, звідки $B_1 = 2A(x_1 - 1) + B$, $C_1 = f(x_1 - 1)$. Легко переконатися, що дискримінант полінома $h_1(y)$ $D_1 = B_1^2 - 4AC_1 = D$. Тому за теоремою 3 існує третє просте значення полінома $h_1(y)$: $h_1(y_{3,1}) = Ay + B_1y + C_1$.

Оскільки $B_1 > B$, $C_1 > C$, то $h_1(y_{3,1}) > f(x_2)$ і $y_{3,1} > y_{2,1}$. Легко перевірити, що $h_1(y_{3,1}) = f(x_3)$, де $x_3 = y_{3,1} + x_2 - 1$. Отже, поліном (1) має не менше, ніж чотири прості значення.

Припустимо, що при $n \geq 4$ $f(1) < f(x_1) < \ldots < f(x_{n-2}) < f(x_{n-1})$ – прості значення полінома (1), причому просте $f(x_{n-1})$ – значення полінома $h_{n-3}(y) = Ay^2 + B_{n-3}y + C_{n-3}$, де $B_{n-3} = 2A(x_{n-3} - 1) + B$, $C_{n-3} = f(x_{n-3} - 1)$.

Побудуємо поліном $h_{n-2}(y) = Ay + B_{n-2}y + C_{n-2}$ за умови $h_{n-2}(1) = f(x_{n-2})$, $h_{n-2}(y_{2,n-2}) =$

$f(x_{n-1})$, $y_{2,n-2} = x_{n-1} - x_{n-2} + 1$.

За теоремою 3 поліном $h_{n-2}(y)$ дискримінанта $D_{n-2} = B_{2,n-2}^2 - 4AC_{n-2} = D$ має третє просте значення $f(x_n) = h_{n-2}(y_{3,n-2})$, $x_n = y_{3,n-2} + x_{n-1} - 1$, $y_{3,n-2} > y_{2,n-2}$, $x_n > x_{n-1}$, де числа B_{n-2} і C_{n-2} мають вигляд $B_{n-2} = 2A(x_{n-2} - 1)$, $C_{n-2} = f(x_{n-2} - 1)$ і можуть бути знайдені з таких рівнянь: $B_{n-2} + C_{n-2} = f(x_{n-2}) - A$, $y_{2,n-2}B_{n-2} + C_{n-2} = f(x_{n-2}) - Ay$. Причому, оскільки $B_{n-2} > B_{n-3}$ і $C_{n-2} > C_{n-3}$, то $h_{n-2}(y_{3,n-2}) > f(x_{n-1})$. Теорема 4 доведена, оскільки при всякому $n \geq 4$ в множині всіх значень полінома (1) існують прості значення

$$f(1) < f(x_1) < \ldots < f(x_{n-1}) < f(x_n) < \ldots$$

Лема 2. Якщо

$$A\beta - B\alpha = 0 \tag{9}$$

і ціле число $g(x) = \alpha x^2 + \beta x + \gamma$ ділить ціле число $f(x) = Ax^2 + Bx + C$, $A\alpha \neq 0$, то

$$C\alpha - A\gamma = 0, \tag{10}$$

$$C\beta - B\gamma = 0. \tag{11}$$

Доведення. Якщо ціле число $g(x)$ ділить ціле число $f(x)$, то залишок від ділення $(A\beta - B\alpha)x - (C\alpha - A\gamma) = 0$, і в силу (9) тоді виконується (10), а в силу (9) і (10) має місце (11). Лема 2 доведена.

Означення 2. Натуральне число n назвемо псевдопростим в деякій підмножині $\mathfrak{N}$ натурального ряду, якщо в цій підмножині це число має своїми дільниками тільки одиницю і число n.

Зауважимо, що кожне просте в натуральному ряду є псевдопростим в підмножині $\mathfrak{N}$.

Запишемо довільне значення $f(x)$ полінома (1) у вигляді добутку

$$f(x) = f_1 \cdot f_2 \cdot \ldots \cdot f_l. \tag{12}$$

Теорема 5. Якщо розвинення числа $f(x)$ має вигляд (12), то кожний псевдопростий дільник f_i, $i = 1, \ldots, l$ або є значення полінома (1), або є значення деякого іншого квадратного полінома.

Доведення. Побудуємо поліном $g_i(x) = A_i x^2 + B_i x + C_i$, для якого виконуються умови

$$g_i(x_i) = A_i x_i^2 + B_i x_i + C_i = f_i, \tag{13}$$

$$AB_i - BA_i = 0. \tag{14}$$

Нехай $f(x_i) = Ax_i^2 + Bx_i + C$, $1 \leq i \leq l$, $f(x_i) \neq f(x_j)$, $x_i \neq x_j$. В силу леми 2 тоді

$$CB_i - BC_i = 0, \tag{15}$$

а з (13) і (15) знайдемо, що:

$$B_i[f(x_i) - Ax_i^2] = B(f_i - A_i x_i^2), \tag{16}$$

звідки в силу (14) випливає рівність

$$Bf_i = B_i f(x_i). \tag{17}$$

З (14) і (15) в силу (16) ще знаходимо:

$$Af_i = A_i f(x_i) \tag{18}$$

$$Cf_i = C_i f(x_i) \tag{19}$$

Домноживши рівності (17), (18), (19) відповідно на цілі числа μ_i, ν_i, λ_i, додамо результати. Тоді отримаємо

$$T_i f_i = T_{i,i} f(x_i), \tag{20}$$

де $T_i = \nu_i A + \mu_i B + \lambda_i C$, $T_{i,i} = \nu_i A_i + \mu_i B_i + \lambda_i C_i$.

Цілі числа $\mu_i > 0$, $\nu_i > 0$, $\lambda_i > 0$ завжди можна вибрати такими, щоб число T_i не було дільником числа $f(x_i)$, наприклад, $\mu_i = x_i^2$, $\nu_i = x_i$, $\lambda_i = 2$. Тоді в (20) T_i ділитиме $T_{i,i}$, $T_{i,i} = k_i T_i$, і з (20) випливає, що

$$f_i = k_i f(x_i). \tag{21}$$

Якщо тепер в розвиненні (12) дільник f_i – псевдопростий, то в силу (21) і леми 3, або $f_i = f(x_i)$, або $f_i = k_i$. Теорема 5 доведена, оскільки кожне натуральне число k_i є значенням деякого квадратного полінома.

В розвиненні числа $f(x)$ на псевдопрості множники деякі можуть повторюватися. Позначивши $f_1 < f_2 < \ldots < f_k$ різні псевдопрості множники – значення полінома (1) в цьому розвиненні, через $\alpha_1, \alpha_2, \ldots \alpha_k$ – відповідну їхню кратність, отримаємо розвинення

$$f(x) = f_1^{\alpha_1} \cdot f_2^{\alpha_2} \cdot \ldots \cdot f_k^{\alpha_k} \cdot g_1^{\beta_1} \cdot g_2^{\beta_2} \cdot \ldots \cdot g_m^{\beta_m}, \tag{F}$$

де $g_1, g_2, \ldots, g_m$ – різні псевдопрості, які не є значеннями полінома, а $\beta_1, \beta_2, \ldots, \beta_m$ – їхні кратності.

Теорема 6. Кожне значення $f(x)$ полінома (1) може мати не більше одного псевдопростого дільника, який не є значенням полінома (1).

Доведення. Скористаємося рівністю (21) з доведення теореми 5, припустивши протилежне, а саме, що для $x \geq 1$ кожне значення $f(x)$ полінома (1) має більше одного псевдопростого дільника, який не є його значенням. В силу (21) тоді існують значення індекса $i = n$, $i = m$, що $f_n = k_n$, $f_m = k_m$ – псевдопрості, які не є значеннями полінома (1), і тоді отримуємо $f(x_i) = f(x_j) = 1$ при $x_i \neq x_j$, що суперечить тому, що якщо $x \geq 1$ і $x_i \neq x_j$, то $f(x_i) \neq f(x_j)$. Суперечність доводить теорему 6.

Для таких поліномів в силу теореми 6 їх розвинення (F) має вигляд:

$$F(x) = f_1^{\alpha_1} \cdot f_2^{\alpha_2} \cdot \ldots \cdot f_k^{\alpha_k} \cdot g^{\gamma}, \tag{G}$$

де g – псевдопросте, яке не є значенням полінома (1), γ – його кратність.

Теорема 7. Кожне значення $f(x)$ полінома (1) має не менше одного псевдопростого дільника, який є значенням полінома (1).

Доведення. Припустимо протилежне. Тоді деяке значення $f(x_0)$ полінома (1) має псевдопростими дільниками тільки числа, що не є значеннями полінома (1). За

теоремою 6 таких дільників не може бути більше одного. Це означає, що значення $f(x_0)$ полінома (1) не є значенням полінома (1). Отримана суперечність доводить теорему 7.

Теорема 8 (А.Шинцель, [1]). Якщо t – натуральне число, $f_1(x)$, ..., $f_t(x)$ – квадратні поліноми з цілими коефіцієнтами і додатними старшими, незвідні, для яких виконується умова: не існує натурального числа $d > 1$, яке було б дільником добутку $f_1(x)\cdot\ldots\cdot f_t(x)$ для кожного цілого значення x, то існує нескінченна множина натуральних чисел x, що кожне з чисел $f_1(x)$, ..., $f_t(x)$ є простим числом.

Доведення. Нехай $f_1(x)$, ..., $f_t(x)$ – вказані квадратні поліноми, серед яких множина простих значень полінома $f_i(x)$ – скінченна, $1 \le i \le t$. Тоді ця множина не може містити більше одного простого числа, оскільки в протилежному випадку за теоремою 4 ця множина була б нескінченною. Отже, поліном $f_i(x)$ має єдине просте значення $p \ge 2$, яке за теоремою 8 є дільником кожного значення $f_i(x)$. Але це означає, що добуток $f_1(x)\cdot\ldots\cdot f_t(x)$ ділиться на p для кожного значення x, що суперечить умові. Отримана суперечність доводить теоерему 8.

Теорема 9. Якщо $k \ne 1$, то кожне парне число $2k$ нескінченним числом способів може бути подане різницею двох різних простих чисел.

Доведення. Розглянемо поліноми $f(x) = x^2 - k$ і $g(x) = x^2 + k$. Тоді $f(1)g(1) = 1 - k^2$, $f(0)g(0) = -k^2$. З умовою $k > 1$. Тому не існує натурального числа $d > 1$, що $d \mid f(x)g(x)$ для кожного цілого числа x, оскільки тоді $d \mid k^2$ і $d \mid (k^2 - 1)$, що неможливо для $k \ne 1$. Отже, за теоремою 8 існує нескінченна множина натуральних чисел x, що кожне з чисел $f(x)$, $g(x)$ є відповідно простим p, q і $q - p = 2k$. Теорема 9 доведена.

Теорема 10 (Х.Гольдбах, [2]). Кожне парне натуральне число, починаючи з 6, може бути подане сумою двох простих чисел.

Доведення. За теоремою 10 довільне парне число $a \ne 2$ можна подати у вигляді: $a = p - q$, де p і q – деякі прості числа. Виберемо парні натуральні числа $b = q + r$, де r – довільне непарне просте число. Тоді для довільного парного числа $c = a + b$ виконується рівність $c = p + r$. Теорема 10 доведена.

Теорема 11 (Постулат Бертрана). Для всякого натурального $n>2$ між n і $2n$ існує хоч би одне просте число $p \ge 3$.

Доведення. Оскільки в силу теореми 10 для кожного парного числа $2n = p + q$, де p, q – прості, то існує просте (нехай це буде p), що $p < 2n$. Причому, або $p > n$, і доведення закінчене, або $p \le n$. Припустимо, що $p \le n$. Тоді p або не ділить, або ділить n.

Розглянемо перший випадок. Тоді $n - p = a$, $2n - p = q$. Віднявши і додавши ці дві рівності, отримаємо, що $n = q - a$, $3n - 2p = q + a$, звідки випливає, що $a^2 = q^2 + 2pn - 3n^2$. Остання рівність виконується при кожному n. А оскільки ліва її частина – повний квадрат, то дискримінант правої її частини $4(p^2 + 3q^2) = 0$, що неможливо, оскільки $p \ne 0$, $q \ne 0$. Отже, якщо $p \le n$, то p ділить n, $n = mp$. Тоді $2mp = p + q$, тобто $p(2m - 1) = q$, що неможливо, оскільки q – просте число. Отримані суперечності доводять, що нерівність $p \le n$ неможлива. Теорема 11 доведена.

Теорема 12. Для довільного $n > 2$ і цілого k, $0 \le k < n/2$, між n і $2(n - k)$ існує хоча б одне просте число $p \ge 3$.

Доведення. Оскільки за теоремою 10 для будь-якого парного числа $2(n - k)$ виконується рівність $2(n - k) = p + q$, де p і q – непарні прості, то існує просте число

(нехай це буде p) , що $p < 2(n - k)$. Причому, або $p > n$, і доведення закінчене, або $p \le n$. Припустимо, що $p \le n$. Тоді або p не ділить n, або p ділить n. Розглянемо перший випадок. Тоді $n - p = a$, $2n - p = q + 2k$. Віднявши і додавши ці дві рівності, знайдемо, що $n = q - a + 2k$, а також $3n - 2p = q + a + 2k$. Звідси випливає, що виконується рівність $-a^2 = 3n^2 - 2(p + 4k)n + 4k(p + k) - q^2$ при кожному натуральному n. Ліва частина останньої рівності – повний квадрат для кожного n. Тоді дискримінант правої її частини дорівнює нулеві. Це означає, що має місце наступна рівність: $(p - 2k)^2 + 3q^2 = 0$, що неможливо, оскільки $p \ne 0$ і $q \ne 0$. Отже, якщо $p \le n$, то p ділить n. Нехай $n = mp$. Тоді виконується рівність $(2m - 1)p - 2k = q$, звідки в силу того, що $q > 2$ – просте, випливає що $(p, k) = 1$. Нехай $p \le n/2$. Тоді $n - 2p = a$, $2n - p = q + 2k$. З цих рівностей знайдемо, що $n + p = q + 2k - a$, а також, що $3n - 3p = q + 2k + a$. Звідси випливає, що при кожному натуральному n виконується: $-a^2 = 3n^2 - [3p^2 + (q + 2k)^2]$. Ліва частина останньої рівності – повний квадрат для кожного n. Тоді дискримінант правої її частини дорівнює нулеві. Це означає, що має місце наступна рівність: $(q + 2k)^2 + 3p^2 = 0$, що неможливо, оскільки $p \ne 0$ і $q > 0$. Отже, $p \ge n/2$, тобто $n \le 2p$. Розділивши останню нерівність на p, отримаємо, що $m \le 2$. При $m = 1$ $p - q = 2k$, $n = p$ і теорема 12 доведена. А оскільки $4p - 2k < 4p - 2n/2 = 2p$, тобто $p < k < n/2$, що суперечить припущенню, то випадок $m = 2n = 2p$ неможливий. Отримані суперечності доводять, що нерівність $p \le n$ неможлива. Теорема 12 доведена.

1. *Sierpin'ski W.* Elementary theory of numbers. Warsawa, 1964, Pan'stwowe wydawnictwo naukowe, C.335.
2. *Прахар К.* Распределение простых чисел. М., 1967

УДК 681. 513

РЕАЛІЗАЦІЯ СТРУКТУРНОГО АЛГОРИТМУ РОЗПІЗНАВАННЯ ОБРАЗІВ НА ОДНОРІДНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

© А. Худий
Державний науково-дослідний інститут інформаційної інфраструктури

Запропоновано реалізацію структурного алгоритму розпізнавання образів на ООС (однорідних обчислювальних системах) на прикладі зображення у вигляді матриці розмірністю 256×256.

A reduced realization of structure algorithm of recognition of images on the homogenous calculus systems.