NUMERE DE FORMA A^2+AB+B^2 (A, B ÎNTREGI)

DE

EUGEN RUSU

(București)

1. În articolul de față ne ocupăm de inelul numerelor $a + bj$ (a și b întregi raționali ; $j = \frac{1}{2} + i\frac{\sqrt{3}}{2}$; $j^2 = j - 1$).

Vom stabili unicitatea descompunerii în factori primi în acest inel pe o cale directă (independentă de utilizarea algoritmului lui Euclid).

Legat de aceasta, ne ocupăm și de scrierea numerelor naturale în forma $a^2 + ab + b^2$.

2. Unitățile inelului fiind : $1, j, j^2, j^3 = -1, j^4 = -j, j^5 = -j^2$, orice număr din inel are un asociat cu $a > 0$; $b \geqslant 0$ (îl putem înmulți cu o unitate astfel încît produsul să fie în sextanul I, fig. 1).

Norma numărului $\omega = a + bj = a + \frac{1}{2}b + ib\frac{\sqrt{3}}{2}$ este $N(\omega) = a^2 + ab + b^2$; conjugatul lui ω este $\bar{\omega} = a + b - bj = \frac{1}{j}(b + aj)$; $N(\omega) = N(\bar{\omega}) = \omega \cdot \bar{\omega} = a^2 + ab + b^2 = (a + b)^2 - (a + b)b + b^2$.

Dacă γ este divizibil cu α, $\gamma = \alpha \cdot \beta$, atunci $N(\gamma) = N(\alpha) \cdot N(\beta)$, și norma lui γ este un număr divizibil cu norma lui α, nu însă și reciproc. Ne punem problema : ce putem deduce din divizibilitatea normelor ; răspunsul, care urmează, constituie baza studiului de față.

3. TEOREMĂ. *Dacă norma numărului $A + Bj$, $N = A^2 + AB + B^2$ este un număr divizibil cu numărul prim $p = a^2 + ab + b^2 > 3$, iar A (și deci nici B) nu este multiplu de p, atunci $A + Bj$ este divizibil sau cu $a + bj$ sau cu conjugatul lui.*

Demonstrație : Avem

$$\frac{A + Bj}{a + bj} = \frac{(A + Bj)(a + b - bj)}{a^2 + ab + b^2} = \frac{A(a + b) + Bb}{p} + \frac{Ba - Ab}{p}j = \frac{1}{p}(x_1 + y_1 j),$$

$$\frac{A + Bj}{a + b - bj} = \frac{(A + Bj)(a + bj)}{a^2 + ab - b^2} = \frac{Aa - Bb}{p} + \frac{Ab + B(a+b)}{p}j = \frac{1}{p}(x_2 + y_2 j).$$

Însă

$$x_2y_1 = (Aa - Bb)(Ba - Ab) = AB(a^2 + b^2) - ab(A^2 + B^2) = \\ = AB(a^2 + ab + b^2) - ab(A^2 + AB + B^2) = \mathcal{M}p,$$

deci cel puţin unul din numerele x_2, y_1 este $\mathcal{M}p$.

Să arătăm că nu pot fi ambele $\mathcal{M}p$; în adevăr, suma lor, $x_2 + y_1 = (A + B)(a - b) \neq \mathcal{M}p$. Din $A + B = \mathcal{M}p$ şi $N = A(A + B) + B^2 = \mathcal{M}p$, ar rezulta $B = \mathcal{M}p$, contrar ipotezei; din $a - b = \mathcal{M}p$ şi $p = (a - b)^2 + 3ab$ ar rezulta $3ab = \mathcal{M}p$, de asemenea contrar ipotezei.

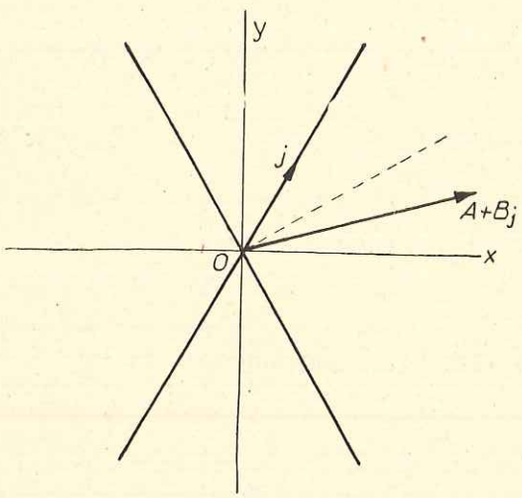

Fig. 1

Dacă $y_1 = \mathcal{M}p$, atunci şi $x_1 = \mathcal{M}p$, căci avem $ax_1 - by_1 = \mathcal{M}p$ iar $a \not\equiv \mathcal{M}p$.

Dacă $x_2 = \mathcal{M}p$, atunci şi $y_2 = \mathcal{M}p$, căci avem $ay_2 - bx_2 = Bp$.

Observaţie: Conjugatul numărului $a + bj$ nu este asociat cu el decît în cazul $a = b$; pentru $a = b = 1$, avem numărul $1 + j$ de normă 3. Dacă $N = A^2 + AB + B^2$ este $\mathcal{M}3$ fără ca A (şi B) să fie, numărul $A + Bj$, este divizibil şi cu $1 + j$ şi cu conjugatul său, care îi este asociat.

Enunţ echivalent. În condiţiile menţionate, sau $(A + Bj) \cdot (a + bj)$, sau $(A + Bj)(a + b - bj)$ are componentele divizibile cu p — prin componentele numărului $A + Bj$ înţelegînd coeficienţii A şi B.

4. Scrierea numerelor naturale prime în forma $a^2 + ab + b^2$.

Numărul $N = A^2 + AB + B^2$, unde A şi B sînt pozitivi şi $(A, B) = 1$, este impar; factorii lui primi sînt de forma $6K + 1$, eventual şi 3.

N are factorul 3, dacă $A - B = \mathcal{M}3$. Fie p un factor prim diferit de 3. Avem

$$A^3 - B^3 = (A - B)(A^2 + AB + B^2) = \mathcal{M}p.$$

Dacă $A \equiv B \pmod p$, nu putem avea $A^3 \equiv B^3 (p)$ de cît dacă $p = 6K + 1$.

Dacă $A \equiv B \pmod p$, $A^2 + AB + B^2 \equiv 3B^2 (p)$, ceea ce nu e posibil pentru că $p > 3$ şi B nu este $\mathcal{M}p$ ($B = \mathcal{M}p$ atrage şi $A = \mathcal{M}p$, ceea ce contrazice condiţia $(A, B) = 1$).

Dacă un număr prim poate fi scris în forma $a^2 + ab + b^2$, el este 3 sau de forma $6K + 1$ (numerele prime de forma $6K - 1$ nu pot fi scrise în forma dată).

TEOREMĂ. *Orice număr prim de forma $p = 6K + 1$ poate fi scris în forma $a^2 + ab + b^2$ cu $a > b > 0$, în mod unic.*

Demonstraţia se face prin inducţie completă. Pentru primele numere, putem verifica propoziţia în mod direct, prin încercări.

Avem $3 = 1^2 + 1 \cdot 1 + 1^2$; $7 = 2^2 + 2 \cdot 1 + 1^2$.

Admitem propoziţia valabilă pentru numerele prime inferioare lui p şi să arătăm că rezultă de aici şi valabilitatea ei pentru însuşi p.

Numărul p fiind de forma $6k + 1$, numerele $1^3, 2^3, \ldots, (p-1)^3$ în împărţirea cu p dau $\frac{p-1}{3}$ resturi, fiecare repetat de 3 ori. Deci putem găsi numerele A şi B, ambele mai mici ca $\frac{p-1}{2}$, astfel ca $A^3 \equiv B^3 \pmod p$. Vom avea

$$A^2 + AB + B^2 = \mathcal{M}p < \frac{3}{4}(p-1)^2 < p^2,$$

adică

$$A^2 + AB + B^2 = p \cdot q \quad \text{cu} \quad q < p.$$

Putem presupune $(A, B) = 1$ căci în caz contrar putem împărţi ambii membri cu d^2, $d = (A, B)$.

Descompunem numărul q în factori primi; ei sînt inferiori lui p şi sînt de forma $6k + 1$ sau 3.

Fie $N = A^2 + AB + B^2 = p \cdot q_1 q_2 \ldots q_h$; $q_i < p$; $(A, B) = 1$. Am admis că $q_1 = a^2 + ab + b^2$.

Conform teoremei de la punctul 3, numărul $A + Bj$ este divizibil cu $a + bj$ sau cu conjugatul acestuia. Cîtul $A_1 + B_1 j$ va avea norma egală cu cîtul normelor, deci cu $p \cdot q_2 \ldots q_h$. Relaţia

$$N_1 = A_1^2 + A_1B_1 + B_1^2 = p\, q_2 \ldots q_h$$

o simplificăm eventual prin $d = (A_1, B_1)$; evident, factorul p nu se simplifică, întrucît nu are exponentul 2; putem presupune A_1 şi B_1 pozitivi, căci în cazul contrar aplicăm identitatea $c^2 - cd + d^2 = (c - d)^2 + (c - d) \cdot d + d^2$. Obţinem o relaţie analogă cu precedenta, însă cu mai puţini factori q. Repetînd procedeul, vom ajunge la o relaţie de forma $a^2 + ab + b^2 = p$, cu $a > b > 0$.

Să demonstrăm acum că scrierea în această formă a lui p este unică.

Dacă $p = A^2 + AB + B^2$ şi totodată $p = a^2 + ab + b^2$, conform teoremei de la pct. 3, $A + Bj$ este divizibil cu $a + bj$ sau cu conjugatul lui; prin împărţire, obţinem un număr cu norma 1, deci o unitate a inelului. Deoarece, conform condiţiilor $A > B > 0$ şi $a > b > 0$, numerele $A + Bj$ şi $a + bj$ sînt ambele în prima jumătate a primului sextan (fig. 1), vectorul corespunzător lui $A + Bj$ formează cu cel al lui $a + bj$, ca şi cu cel al conjugatului lui $a + bj$, un unghi mai mic de 60°. Însă înmulţirea cu j, j^2 etc.

aduce o mărire a argumentului cu $60°$, $2 \cdot 60°$ etc. Rezultă că $A + Bj$ nu poate fi de cît confundat cu $a + bj$.

5. Descompunerea în factori primi în inel. *Numerele prime ale inelului considerat sînt :*

1°. *numerele prime raționale de forma* $6K - 1$ *și* 2 ;

2°. *numerele de forma* $a + bj$ *avînd norma egală cu un număr prim* p *de forma* $6K + 1$, $p = a^2 + ab + b^2$; *conjugatul numărului* $a + bj$ *cu aceeași normă* p, *este un număr prim neasociat cu* $a + bj$;

3°. *numărul* $1 + j$ *de normă* 3, *al cărui conjugat este asociat cu el.*

Demonstrația acestei afirmații se face astfel :

1°. Un număr prim rațional $p = 6k - 1$ nu admite o descompunere în factori raționali. Dacă am avea $p = (a + bj)(c + dj)$, ar rezulta $N(p) = p^2 = (a^2 + ab + b^2)(c^2 + cd + d^2)$, ceea ce nu este posibil.

2°. Un număr prim $p = 6k + 1$ poate fi scris $p = a^2 + ab + b^2 = (a + bj)(a + b - bj)$.

Numărul $a + bj$ este prim, căci din $a + bj = \alpha \cdot \beta$ ar rezulta, egalînd normele, $p = N(\alpha) \cdot N(\beta)$, ceea ce nu este posibil dacă α, β sînt numere distincte de unități.

O afirmație analoagă are loc pentru numărul $1 + j$ de normă 3.

Alte numere prime de cît acestea nu există. În adevăr, fie $N = A + Bj$ un număr prim. Dacă $(A, B) \neq 1$, evident că N nu e prim. Dacă $(A, B) = 1$, considerăm norma numărului N ; dacă aceasta nu ar fi un număr prim rațional, conform teoremei de la punctul 3, am putea descompune pe N în factori.

Unicitatea descompunerii în factori primi se demonstrează observînd că un produs de numere prime nu este divizibil cu un număr prim care nu se află printre factorii lui, eventual înmulțit cu o unitate.

LEMA 1. *Dacă* $\gamma = a + bj$ *este prim, norma lui fiind* $p = a^2 + ab + b^2$ *și dacă notăm* $\gamma^n = A + Bj$, *atunci* A *și* B *nu sînt divizibili prin* p.

Demonstrația se face prin inducție. 1) pentru $n = 1$, avem $a \not\equiv Mp$, $b \not\equiv Mp$, căci $p = a^2 + ab + b^2$.

2) Admitem că $A \not\equiv Mp$, $B \not\equiv Mp$. Conform teoremei de la pct. 3, sau $(A + Bj)(a + bj)$, sau $(A + Bj)(a + b - bj)$ — nu ambele — au componentele divizibile cu p. Însă în mod imediat al doilea produs are componentele divizibile cu p, deci primul produs nu le are.

LEMA 2. *Dacă modulul lui* $A + Bj$ *este divizibil cu* p, *fără ca* A *și* B *să fie, iar modulul lui* $C + Dj$ *nu este divizibil cu* p, *componentele produsului* $(A + Bj)(C + Dj)$ *nu sînt divizibile cu* p.

Avem $(A + Bj)(C + Dj) = AC - BD + (AD + BC + BD)j$.

Din

$$AC - BD = Mp$$

$$AD + B(C + D) = Mp$$

prin eliminarea lui B ar rezulta

$$A(C^2 + CD + D^2) = Mp,$$

ceea ce nu este posibil conform ipotezei.

TEOREMA. *Un produs de numere prime ale inelului nu poate fi divizibil cu un număr prim diferit de factorii lui, sau neasociat cu niciunul din factorii lui.*

Fie $N = A + Bj$ produsul considerat și fie γ un număr prim al inelului care nu se află printre factorii lui N.

Fie $N = q_1 q_2 \ldots (a_1 + b_1 j)^{k_1} (q_2 + b_2 j)^{k_2} \ldots = A + Bj$, unde q_i sînt numere raționale iar $a_i + b_i j$ numere prime ale inelului, de normă p_i. Norma lui N este $q_1^2 q_2^2 \ldots p_1 p_2 \ldots$. Dacă N este divizibil cu γ, norma lui N este un număr divizibil cu norma lui γ. Dacă γ este rațional el nu poate fi decît unul din numerele q (sau asociat cu acestea).

Să admitem că γ are norma p_1 și nu se află printre factorii lui N ; γ nu poate fi de cît conjugatul numărului $a_1 + b_1 j$. Conform lemelor, A și B nu sînt $\mathcal{M}p$. Conform teoremei de la pct. 3, $A + Bj$ fiind divizibil cu $a_1 + b_1 j$, nu este divizibil cu conjugatul său, ceea ce demonstrează teorema.

Din această teoremă rezultă, după cum se știe, teorema unicității descompunerii în factori primi.

Procedeul de descompunere în factori primi rezultă din teoremele stabilite. Fiind dat numărul $A_1 + B_1 j = C(A + Bj)$, unde $(A, B) = 1$, descompunem pe C în factori primi naturali, iar factorii de forma $p = 6k + 1$ îi scriem sub forma $p = a^2 + ab + b^2$ și îi descompunem la rîndul lor în $p = (a + bj)(a + b - bj)$; numărul $A + Bj$, $(A, B) = 1$, îl descompunem astfel : considerăm norma $N = A^2 + AB + B^2$ și o descompunem în factori primi naturali ; fie $p = a^2 + ab + b^2$ unul din ei ; împărțim pe $A + Bj$ sau la $a + bj$ sau la conjugatul lui, după cum e divizibil sau cu primul sau cu al doilea. Cu cîtul, procedăm în același mod.

Exemplu. Să descompunem numărul $\alpha = 190\ (5 + 41j)$. Avem $190 = 2 \cdot 5 \cdot 19 = 2 \cdot 5(3 + 2j)(5 - 2j)$. Considerăm acum numărul $\beta = 5 + 41j$; $N = 5^2 + 5 \cdot 41 + 41^2 = 1911 = 3 \cdot 7^2 \cdot 13$.

Avem $3 = (1 + j)(2 - j)$; β este divizibil și cu $1 + j$ și cu $2 - j$ (care sînt asociate).

Să-l împărțim, de exemplu, cu $1 + j$; obținem $\beta = (1 + j)\ (17 + 12j)$. Cîtul $17 + 12j$ îl împărțim printr-un număr de normă 7. Avem $7 = (2 + j) \times (3 - j)$. Constatăm că $17 + 12j$ este divizibil cu $2 + j$ (nu cu conjugatul lui). Am putea împărți cu $2 + j$, iar cîtul din nou cu $2 + j$. Norma avînd ca factor pe 7^2, putem împărți dintr-odată cu $(2 + j)^2 = 3 + 5j$.

$$\frac{17 + 12j}{3 + 5j} = \frac{(17 + 12j)(8 - 5j)}{7^2} = 4 - j.$$

Cîtul $4 = j$ este număr prim avînd norma 13. Obținem deci :

$$\alpha = 2 \cdot 5 \cdot (3 + 2j)(5 - 2j)(1 + j)(2 + j)^2(4 - j).$$

6. Scrierea numerelor naturale în forma $a^2 + ab + b^2$, $a > b > 0$. Conform pct. 4, numerele prime de forma $6k + 1$ pot fi scrise în mod unic în această formă.

Să considerăm un număr $N = p_1^{k_1} \dots p_m^{k_m}$, unde orice p este de forma $6k + 1$. Putem scrie :

$$N = (a_1 + b_1 j)^{k_1} (a_1 + b_1 - b_1 j)^{k_1} (a_2 + b_2 j)^{k_2} (\quad)^{k_2} \dots,$$

unde într-o paranteză goală subînțelegem numărul conjugat celui din paranteza care o precede.

Dacă asociem un factor cu exponentul k_1, altul cu exponentul k_2, ..., altul cu exponentul k_m, de o parte, și factorii rămași pe de altă parte, obținem pe N sub forma

$$N = (A + Bj)(\quad) = A^2 + AB + B^2.$$

Dacă A și B nu sînt pozitivi, vom folosi identitatea

$$A^2 - AB + B^2 = (A - B)^2 + (A - B) \cdot B + B^2.$$

Această asociere o putem face în 2^{m-1} moduri.

Conform pct. 5, $(A, B) = 1$.

Putem face și alte asocieri de forma $(A + Bj)(\quad)$ grupînd în expresia factorului $A + Bj$ pe $(a_1 + b_1 j)^{k_1 - \lambda}$. $(\quad)^{\lambda} \dots$; în acest caz însă A și B nu vor fi primi între ei, ci vor avea ca divizor comun pe $p_1^{\lambda} \dots$

Reciproc, să presupunem că avem dat $N = A^2 + AB + B^2$ cu $(A, B) = 1$. Vom putea scrie $N = (A + Bj)(\quad)$. Numărul $A + Bj$ îl descompunem în factori primi. N avînd factorul $p_1^{k_1}$, numărul $A + Bj$ este divizibil sau cu $a_1 + b_1 j$, sau cu conjugatul lui — nu cu ambii — pentru că $(A, B) = 1$.

Rezultă că orice scriere $N = A^2 + AB + B^2$ conduce la o anumită asociere a factorilor din (1). Prin urmare cele 2^{m-1} moduri de scriere a lui N în forma dată, sînt singurele posibile.

Aceste moduri sînt distincte între ele.

Concluzie. *Un număr* $N = p_1^{k_1}, \dots, p_k^{k_m}$ $(p = 6k + 1)$ *poate fi scris în* 2^{m-1} *moduri în forma* $N = A^2 + AB + B^2$ *cu* $(A, B) = 1, A > B > 0$.

Dacă $N = 3^k p_1^{k_1} \dots p_m^{k_m}$ $(p = 6k + 1)$, *el poate fi scris tot în* 2^{m-1} *moduri în forma dată, din cauză că numărul prim de modul* 3, $1 + j$ *este asociat cu el însuși.*

$$N = (1 + j)^k (A + Bj)[(2 - j)^k (A + B - Bj)].$$

Asocierea $[(1 + j)^k (A + Bj)][\quad]$ *sau* $[(1 + j)^k (A + B - Bj)][\quad]$ *dă aceeași scriere a lui* N.

Exemple. 1°. Fie $N = 13^2 \cdot 19 = 3211$. Avem :

$13 = (3 + j)(4 - j)$; $13^2 = (3 + j)^2(\quad) = (8 + 7j)(\quad)$; $19 = (3 + 2j)(5 - 2j)$.

$$N = (8 + 7j)(\quad)(3 + 2j)(\quad).$$

1) $N = [(8 + 7j)(3 + 2j)][\quad] = (10 + 51j)(\quad)$.

$N = 10^2 + 10 \cdot 51 + 51^2 = 51^2 + 51 \cdot 10 + 10^2$.

2) $N = [(8 + 7j)(5 - 2j)][\quad] = (54 + 5j)(\quad)$.

$N = 54^2 + 54 \cdot 5 + 5^2$.

2°. Fie $N = 3 \cdot 13^2 \cdot 19$. Avem :

$$N = (1 + j)(\quad)(10 + 51j)(\quad)$$

1) $N = [(1 + j)(10 + 51j)][\quad] = (-41 + 112j)(\quad)$.

$N = 71^2 + 71 \cdot 41 + 41^2$.

2) $N = [(1 + j)(61 - 51j)] \cdot [(2 - j)(10 + 51j)] = (112 - 41j)(71 + 41j)$,

ceea ce dă aceeași scriere a lui N.

Luînd $N = (1 + j)(\quad)(54 + 5j)(\quad)$, obținem

$$N = 64^2 + 64 \cdot 49 + 49^2.$$

Primit la 12. III. 1962.

ЧИСЛА ВИДА $A^2 + AB + B^2$ (A, B, ЦЕЛЫЕ)

КРАТКОЕ СОДЕРЖАНИЕ

Рассматривается кольцо чисел $a + bj$, a и b целые, $j = \frac{1}{2} + \frac{i\sqrt{3}}{2}$.

Доказывается теорема:

Если число $N = A^2 + AB + B^2$ (Норма числа $A + Bj$) *делимо на простое число* $p = a^2 + ab + b^2 > 3$, *без того чтобы* A и B *были таковыми, то* $A + Bj$ *делимо или на* $a + bj$, *или на его сопряженное число.*

На этой основе доказывается единственность разложения на простые множители рассматриваемого кольца, непосредственно (без применения алгорифма Евклида) и описывается приём разложения.

В связи с этим, показывается что любое простое число вида $p = 6k + 1$ представляется единственным образом в виде $p = a^2 + ab + b^2$, $a > b > 0$, а число N, имеющее m простых множителей вида $6k + 1$, каждый определённой степени, представляется в 2^{m-1} различных образов в виде $a^2 + ab + b^2$ с $a > b > 0$.

NOMBRES DE LA FORME $A^2 + AB + B^2$ (A, B, ENTIERS)

RÉSUMÉ

On considère l'anneau des nombres $a + bj$, a et b entiers, $j = \frac{1}{2} + \frac{\sqrt{3}}{2}$.

On démontre le théorème :

Si le nombre $N = A^2 + AB + B^2$ (la norme du nombre $A + Bj$) *est divisible par le nombre premier* $p = a^2 + ab + b^2 > 3$, *sans que* A *et* B *le soient, alors* $A + Bj$ *est divisible soit par* $a + bj$, *soit par le conjugué de celui-ci.*

Cela dit, on démontre l'uncité de la décomposition en facteurs premiers dans l'anneau considéré, de manière directe (sans faire appel à l'algorithme d'Euclide), et on décrit le procédé de décomposition.

Concurremment, on montre que tout nombre premier de la forme $p = 6k + 1$ s'écrit de maniére unique sous la forme $p = a^2 + ab + b^2$ avec $a > b > 0$, et qu'un nombre N ayant m facteurs premiers de la forme $6k + 1$, chacun à un puissance quelconque, s'écrit de 2^{m-1} manières sous la forme $a^2 + ab + b^2$ avec $a > b > 0$.