FORMULE PENTRU REZOLVAREA CONGRUENȚEI $x^2 \equiv a \pmod{P}$ ÎN CAZURI PÎNĂ ACUM NECUNOSCUTE ȘI APLICAREA LOR PENTRU A DETERMINA DIRECT RĂDĂCINILE PRIMITIVE ALE UNOR NUMERE PRIME

DE

IOAN SCHÖNHEIM

Comunicare prezentată în ședința din 22 octombrie 1955 a Filialei Cluj a Academiei R.P.R.

I.

1. Nu se cunoaște pînă în prezent o formulă care să ne dea soluțiile congruenței

$$x^2 \equiv a \pmod{P} \tag{1}$$

unde am notat cu a un reziduu patratic al numărului prim P.

Rezultatele care ne sînt cunoscute sînt următoarele:

A. Dacă, P este de forma $4k + 3$, congruența (1) are soluția

$$x \equiv \pm a^{k+1} \pmod{P}.$$

B. a) Dacă P nu este de forma $4k + 3$, deci e de forma $4k + 1$, congruența (1) s-a putut rezolva numai pentru $a \equiv -1 \pmod{P}$, atunci $x \equiv \pm (2k)!$, în restul cazurilor s-au indicat procedee implicînd un număr de încercări care depinde de numărul, de cîte ori conține k pe 2 ca factor. Anume

b) Dacă k este fără soț deci P e de forma $8k' + 5$, soluția congruenței (1) este $x \equiv \pm a^{k+1} 2^{(k'+1)s}$, unde se alege pentru s valoarea convenabilă dintre numere 0 ; 1.

Cazurile A, B.a și B.b au fost citate ca singurele cunoscute în anul 1922 de M. Kraitchik [1].

c) Dacă k admite o singură dată pe 2 ca factor, deci P e de forma $16k' + 9$, soluția congruenței (1) se alege, după L. E. Dickson [2] din următoarele trei posibilități

$$x \equiv \pm a^{\frac{k'+1}{2}}; \quad x \equiv \pm a^{\frac{k'+1}{2}} N^{2k'}; \quad x \equiv \pm 4k' N^{k'} (N^{2k'} - 1)\, a^{\frac{k'+1}{2}} (a^{k'} - 1) \pmod{P}$$

după cum

$$a^{k'} \equiv 1;\ a^{k'} \equiv -1;\ a^{2k'} \equiv -1 \pmod P$$

aci am notat cu N un nonreziduu pătratic al lui P.

d) Dacă în general k admite de $\alpha - 2$ ori pe 2 ca factor, deci $P = 2^\alpha h + 1$, $\alpha > 1$, h impar, I. M. Vinogradov [3] indică un procedeu simplu, prin care putem determina prin α încercări numărul s din formula de rezolvare $x \equiv \pm a^{\frac{h+1}{2}} N^s \pmod P$, unde N are aceeași semnificație ca mai sus.

2. Se înțelege că în considerațiuni teoretice și cite odată chiar în calcularea efectivă a soluțiilor, o formulă este preferabilă unui procedeu. Ori, cum am arătat la punctul 1. B, dacă $P = 2^\alpha h + 1$, $\alpha > 1$, singurul reziduu pentru care s-a putut determina direct soluția congruenței (1) este $a \equiv -1 \pmod P$, sau ținînd seamă de forma lui P, $a \equiv 2^\alpha h \pmod P$.

Noi am putut stabilii o formulă, care ne permite rezolvarea congruenței (1) pentru un modul de aceeași formă, aplicabilă pentru reziduul $a \equiv (-1)^{\frac{p_i - 1}{2}} p_i$, p_i fiind un divizor prim al lui h. Rezultatul acesta se enunță riguros în felul următor:

Dacă $e > 1$ este factorul fără soț al exponentului la care aparține 2 față de modulul prim $P = 2^\alpha h + 1, \alpha > 2$, h impar > 1 și e_i $(i = 1, 2, \ldots, l)$ sînt cîturile obținute prin împărțirea lui e cu factorii săi primi p_i, deci $e_i = \frac{e}{p_i}$, congruențele

$$x^2 \equiv (-1)^{\frac{p_i - 1}{2}} p_i \pmod P \tag{2}$$

admit respectiv soluțiile

$$x \equiv \pm \left(1 + 2 \sum_{\mu_i} 2^{2^{\alpha-1} \mu_i}\right) \tag{3}$$

unde μ_i parcurge reziduurile pătratice ale lui p_i.

Înainte de a trece la demonstrația acestei afirmații vom face asupra ei cîteva observații.

A. p_i va fi un divizor al lui h, căci *e* trebuind să fie un factor al lui $P - 1$, divide pe h.

B. Formula (3) este aplicabilă și dacă $\alpha < 3$. Întocmai dacă $\alpha = 1$ și $h \equiv 3 \pmod 4$, în celelalte cazuri $\alpha - 1$ trebuie înlocuit cu α.

C. Ținînd seama de observația precedentă putem afirma că prin formulele (2) și (3) am găsit soluția congruenței (1) cel puțin pentru o valoare a reziduului *a*, oricare ar fi modulul prim $P = 4k + 1$, cu excepția divizorilor numerelor lui Fermat, căci pentru aceștia $e = 1$.

D. Un caz particular important ar fi $h = p$ număr prim. Atunci congruența

$$x^2 \equiv (-1)^{\frac{p-1}{2}} p \pmod P$$

are soluția

$$x \equiv \pm \left(1 + 2 \sum_{\mu} 2^{2^{\alpha-1} \mu}\right)$$

căci $e_i = 1$. În acest caz nu trebuie cercetat e, dacă știm că P nu este divizorul unui număr de al lui Fermat.

E. Exponentul la care aparține 2 față de un modul prim $P = 2^\alpha h + 1$ se menționează de obicei în tabelele cuprinzînd astfel de numere prime [4].

F. Rezultatele noastre pot fi aplicate și în cazul dacă nu se cunoaște valoarea lui *e*, chiar și dacă h e compus. Sîntem atunci conduși la un procedeu (vezi 3. B) principial deosebit de procedeul 1. B. d, căci pe cînd acesta presupune α încercări, al nostru cel mult un număr de încercări egal cu numărul factorilor lui h. Procedeul nostru va fi deci utilizabil și practic dacă h conține un număr mic de factori, cu toate că α e mare.

3. Pentru a demonstra rezultatele din punctul precedent vom porni de la expresia

$$S = 1 + 2 \sum_{\mu} r^\mu \tag{4}$$

în care μ parcurge reziduurile patratice ale unui număr prim p. Precum se știe [5], dacă r este rădăcina ecuației

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0 \tag{5}$$

expresia (4) satisface relația

$$S^2 = (-1)^{\frac{p-1}{2}} p \tag{6}$$

care poate servi la determinarea după Gauss a perioadelor de cîte $\frac{p-1}{2}$ rădăcini ale ecuației (5).

Dacă înlocuim în (4) și (5) relația de egalitate cu congruența modulo P, număr prim și modificăm corespunzător demonstrația care conduce la egalitatea (6), ajungem la congruența

$$S^2 \equiv (-1)^{\frac{p-1}{2}} p \pmod P$$

ceea ce arată că

$$x \equiv \pm (1 + 2 \sum_{\mu} r^\mu) \pmod P$$

este soluția congruenței

$$x^2 \equiv (-1)^{\frac{p-1}{2}} p \pmod P$$

r fiind o rădăcină a congruenței

$$x^{p-1} + \ldots + 1 \equiv 0 \pmod P \tag{7}$$

și μ avînd aceeași semnificație ca mai sus.

Acest rezultat se poate obține [6] și folosind imaginarele lui Gallois, cum se face la a 7-a demonstrație a legii reciprocității după Gauss.

Rămîne să determinăm o rădăcină a congruenței (7).

A. În ipoteza că factorul fără soț al exponentului la care aparține 2 față de modulul $P = 2^{\alpha}h + 1$ este e, are loc congruența

$$2^{2^{\alpha} e} \equiv 1 \pmod{P} \tag{8}$$

și chiar

$$2^{2^{\alpha-1} e} \equiv 1 \pmod{P}$$

dacă $\alpha > 2$, căci atunci 2 este reziduu pătratic al lui P. Rezultă, dacă p este un divizor prim al lui e, descompunerea

$$\left(2^{2^{\alpha-1} \cdot \frac{e}{p}} - 1\right)\left(2^{2^{\alpha-1} \frac{e}{p}(p-1)} + 2^{2^{\alpha-1} \frac{e}{p}(p-2)} + \ldots + 1\right) \equiv 0 \pmod{P}$$

sau o descompunere analoagă pentru (8), dacă $\alpha < 3$. Deoarece primul factor nu poate fi divizibil cu P, rezultă că $r \equiv 2^{2^{\alpha-1} \frac{e}{p}}$ resp. $2^{2^{\alpha} \frac{e}{p}} \pmod{P}$ este rădăcina congruenței (7).

B. Dacă nu cunoaștem exponentul la care aparține 2 față de P putem porni de la egalitatea dată de teorema lui Fermat $2^{2^{\alpha} h} \equiv 1 \pmod{P}$ sau chiar, ca și mai înainte

$$2^{2^{\alpha-1} h} \equiv 1 \pmod{P}. \tag{9}$$

Fie descompunerea în factori primi egali sau diferiți a lui h

$$h = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_j \quad j \geqslant l$$

atunci congruența (9) se va descompune astfel

$$\left(2^{2^{\alpha-1}} - 1\right)\left(\sum_{i_1=0}^{p_1-1} 2^{2^{\alpha-1} \cdot i_1}\right)\left(\sum_{i_2=0}^{p_2-1} 2^{2^{\alpha-1} p_1 i_2}\right) \ldots \left(\sum_{i_j=0}^{p_j-1} 2^{2^{\alpha-1} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{j-1} \cdot i_j}\right) \equiv 0 \pmod{P}$$

Dacă mai departe P nu divide vreun număr de al lui Fermat, una dintre paranteze, afară de prima, trebuie să fie divizibilă cu P, fie aceea în care indicele este i_n, atunci congruența

$$x^2 \equiv (-1)^{\frac{p_n - 1}{2}} p_n \pmod{P}$$

are soluția

$$x \equiv \pm\left(1 + 2 \sum_{\mu_n} 2^{2^{\alpha-1} p_1 p_2 \ldots p_{n-1} \mu_n}\right) \pmod{P}$$

Cu aceasta, toate afirmațiile din punctul 2 sînt complect demonstrate.

II.

1. Nu se cunoaște o formulă, care permite calcularea unei rădăcini primitive a numărului prim P în general.

Folosind rezultatele din cap. I. vom putea stabili o astfel de formulă aplicabilă pentru o categorie destul de largă de numere prime. Anume vom demonstra următoarea teoremă:

Dacă $P = 2^{\alpha}h + 1$ este un număr prim, $\alpha \geqq 3$, h impar > 1, α și $2h$ prime între ele, și dacă 2 este un reziduu patratic primitiv al lui P atunci soluțiile congruenței

$$x^2 \equiv (-1)^s h \pmod{P} \tag{10}$$

s fiind numărul factorilor primi de forma $4k + 3$ ai lui h, — reprezintă cîte o rădăcină primitivă ρ a lui P și sînt date de formula

$$\rho = x \equiv \pm \prod_{p_i} \left(1 + 2 \sum_{\mu_i} 2^{2^{\alpha-1} \frac{h}{p_i} \cdot \mu_i}\right) \pmod{P} \tag{11}$$

unde p_i parcurge divizorii primi egali sau diferiți din descompunerea lui h iar μ_i reziduurile patratice ale lui p_i.

Prin reziduu patratic primitiv se înțelege aci o rădăcină primitivă a congruenței $x^{2^{\alpha-1} \cdot h} \equiv 1 \pmod{P}$, care prin urmare nu satisface o congruență analoagă de grad mai mic.

Pentru a stabili teorema vom demonstra cîteva leme.

A. Dacă b este un reziduu pătratic primitiv al numărului prim $P = 2^{\alpha}h + 1$, $\alpha > 2$, h impar, ρ o rădăcină primitivă al lui P, așa că $b \equiv \rho^{2k} \pmod{P}$, atunci numerele k și 2h vor fi prime între ele.

Ca să vedem aceasta e destul să observăm că în caz contrar b ar fi $\equiv 1 \pmod{P}$ pentru un exponent mai mic decît cel presupus.

B. În aceleași ipoteze soluțiile congruenței

$$x^2 \equiv b \ (\equiv \rho^{2k}) \pmod{P} \tag{12}$$

se dovedesc a fi rădăcini primitive ale lui P.

Aceasta rezultă din faptul că k și 2h sînt prime între ele cum s-a arătat în lema A, în consecință k și $P - 1$ sînt deasemenea prime între ele, așa că ρ^k rădăcina congruenței (12) este rădăcina primitivă a lui P odată cu ρ; același lucru rezultă și pentru $-\rho^k$ dacă ținem seama de ipoteza făcută în legătură cu α.

C. Dacă mai presupunem că și α cu 2h sînt prime între ele, din ipoteza că 2 este un reziduu patratic primitiv al lui P rezultă același lucru și pentru $\pm h$.

Într-adevăr, din $2^{\alpha}h \equiv -1 \pmod{P}$ rezultă $h^{2^{\alpha-1} h} \equiv 1 \pmod{P}$, congruență ce nu poate fi satisfăcută de un exponent mai mic g, altfel ar rezulta $2^{\alpha g} \equiv 1 \pmod{P}$ și $2^{g} \equiv 1 \pmod{P}$, contrar ipotezei.

Pentru a demonstra acum teorema, observăm conform cu lema C, că h este un reziduu pătratic primitiv al lui P, deci cum am arătat în lema

B. rădăcinile congruenței (10) sînt rădăcini primitive ale lui P. Acestea sînt într-adevăr date de formula (11), căci dacă congruențele

$$x^2 \equiv a_1,\ x^2 \equiv a_2,\ \ldots,\ x^2 \equiv a_m \pmod{P}$$

admit respectiv soluțiile

$$x \equiv \pm b_1,\ x \equiv b_2,\ \ldots,\ x \equiv \pm b_m \pmod{P}$$

atunci congruența

$$x^2 \equiv a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_m \pmod{P}$$

are soluția

$$x \equiv \pm b_1 \cdot b_2 \cdot \ldots \cdot b_m \pmod{P},$$

ori în cap. I. am stabilit formula (3), care se poate aplica în ipotezele teoremei la toți divizorii lui h.

Menționăm aci că în tabelele de numere prime se găsește deobicei și valoarea $\tau = \frac{P-1}{x}$, x fiind exponentul la care aparține 2 modulo P. Numerele prime p pentru care 2 este un reziduu patratic primitiv, sînt deci acelea pentru care $\tau = 2$.

III.

Vom ilustra prin cîteva exemple aplicabilitatea formulelor stabilite.

1. Să se rezolve congruența $x^2 \equiv 5 \pmod{521}$. Aci $P = 521 = 2^3 . 5.13 + 1$ exp $2 = 2^2 . 5.13$. Formula (3) ne dă soluția

$$x \equiv \pm \left(1 + 2 \sum_{(\mu=1,4)} 2^{2^2 \cdot 13 \cdot \mu}\right) \equiv \pm 199 \pmod{521}.$$

2. Să se determine două rădăcini primitive ale numărului 521. Formula (11) ne dă rădăcinile cerute, căci aci $h = 5.13$ este prim cu $\alpha = 3$ și 2 este reziduu pătratic primitiv al lui 521. Așa că

$$\rho \equiv \pm \left(1 + 2 \sum_{\mu=1,4} 2^{2^2 \cdot 13 \cdot \mu}\right)\left(1 + 2 \sum_{(\mu=1,3,4,5,10,12)} 2^{2^2 \cdot 5 \cdot \mu}\right) \equiv \pm 199 \cdot 137 \equiv \pm 171 \pmod{521}.$$

3. Să se rezolve congruența $x^2 \equiv -3 \pmod{2^\alpha \cdot 3 + 1}$ unde α este astfel ales ca $2^\alpha \cdot 3 + 1$ să fie prim și să nu fie un divizor al vreunui număr de al lui Fermat. Aci $h = 3$, număr prim, deci fără să cunoaștem exp 2 față de $2^\alpha 3 + 1$, soluția este

$$x \equiv \pm \left(1 + 2^{2^{\alpha-1}+1}\right)^r \pmod{P}.$$

BIBLIOGRAFIE

1. M. Kraitchik, *Théorie des nombres*, Paris, 1922, t. I. p. 85.
2. L. E. Dikson, *Introduction to the theory of numbers*. Cap. III, exerc. IX, 6, ed. germ. Leipzig-Berlin 1931.
3. I. M. Vinogradov, *Bazele teoriei numerelor*. Cap. V. exerc. 2, c.
4. M. Kraitchik, *Recherches sur la théorie des nombres*, Paris, 1924, tabela I, pag. 131.
5. P. Bachmann, *Die Lehre von der Kreisteilung*, ed. 1927, pag. 87, 105.
6. P. Bachmann, *Niedere Zahlentheorie*, Leipzig 1902, pag. 398.

КРАТКОЕ СОДЕРЖАНИЕ

Формулы для разрешения сравнений $x^2 \equiv a \pmod{P}$ в случаях до сих пор неизвестных и их применение для прямого определения первообразных корней некоторых простых чисел

И. ШЁНХЕЙМ

В единственных двух случаях: A) P простое число формы $4k + 3$, a некоторый квадратный вычет P и B) $P = 2^\alpha h + 1$, $\alpha \geqq 2$, $a \equiv -1 \equiv 2^\alpha h \pmod{P}$, в которых сравнение (1) могло быть прямо разрешено, в настоящей работе добавляется прямое разрешение сравнения (1) если $a \equiv (-1)^{\frac{p-1}{2}} p \pmod{P}$, p будучи одним из простых делителей h.

I. Если $e > 1$ нечётный сомножитель показателя степени, которому принадлежит 2 по простому модулю $P = 2^\alpha h + 1$, $\alpha > 2$, h нечетный > 1 и $e_i = \frac{e}{p_i}$ $(i = 1, 2 \ldots\ldots e)$, где p_i простые сомножители e, сравнения (2) допускают соответственно решения (3) где μ_i проходит квадратные вычеты p_i.

Формула (3) может быть использована и для $\alpha < 3$, если ставится α вместо $\alpha - 1$.

Демонстрация делается, принимая во внимание известный корень сравнения деления круга и составляя периоды по $\frac{p-1}{2}$, которые удовлетворяют определённое сравнение второй степени.

Определяя как примитивный квадратный вычет P число b которое удовлетворяет сравнение $b^{\frac{p-1}{2}} \equiv 1 \pmod{P}$ без того, чтобы его удовлетворить для меньшего показателя степени и употребляя предыдущий результат, устанавливается формула для прямого определения первоначальных корней для довольно широкой категории простых чисел.

II. Если $P = 2^\alpha h + 1$ простое число, $\alpha \geqq 3$, h нечётное > 1, α и $2h$ взаимно простые и если 2 примитивный квадратный вычет P, а s число простых сомножителей h формы $4k + 3$ то решения сравнения (10) представляют по одному первообразному корню P и даны формулой (11), где p_i проходит все равные и разные делители h, а μ_i квадратный вычет p_i.

Содержание лемм, применённых в демонстрации, следующее:

A) Если b примитивный квадратный вычет и ρ примитивный корень P, следовательно $b \equiv \rho^{2k}$, то k и $2h$ взаимно простые.

В ρ^k, следовательно, первообразный корень P.

B) Если α и $2h$ взаимно простые и 2 примитивный квадратный вычет P, то $\pm h$ является таким же вычетом.

Несколько примеров иллюстрируют применяемость формул.

RÉSUMÉ

Formules pour résoudre la congruence $x^2 \equiv a \pmod P$ dans des cas encore inconnus et leur application pour déterminer directement des racines primitives de certains nombres premiers.

par

I. SCHÖNHEIM

Aux seuls cas: A. P nombre premier de la forme $4k+3$, a résidu quadratique de P et B. $P = 2^\alpha h + 1$, $\alpha \geq 2$, $a \equiv -1 \equiv 2^\alpha h \pmod P$ dans lesquels la congruence (1) a pu être résolue directement, s'ajoute ici la détermination directe des solutions de la congruence (1) si $a \equiv (-1)^{\frac{p-1}{2}} p \pmod P$, p étant un des certains diviseurs premiers de h:

I. *Si $e > 1$ est le facteur impair de l'exposant auquel appartient 2 pour le modul premier $P = 2^\alpha h + 1$, $\alpha > 2$, h impair > 1 et $e_i = \frac{e}{p_i}$, p_i étant les facteurs premiers de e — les congruences (2) admettent respectivement les solutions (3) où μ_i parcourt les résidus quadratiques de p_i.*

La formule (3) sera utilisable aussi quand $\alpha < 3$, en y mettant α au lieu de $\alpha - 1$.

Pour démontrer I. on considère une racine connue de la congruence de la division du cercle et on construit les périodes de $\frac{p-1}{2}$ lesquelles, doivent satisfaire à une certaine congruence de second degré.

En définissant comme résidu quadratique primitif de P un nombre b tel que $b^{\frac{p-1}{2}} \equiv 1 \pmod P$, sans l'être pour un exposant moindre — et en utilisant le résultat précédent, on établit une formule qui permet de déterminer directement des racines primitives d'une catégorie assez large de nombres premiers.

II. *Si $P = 2^\alpha h + 1$ est premier, $\alpha \geq 3$, h impair > 1, et α et $2h$ premiers entres eux, si encore 2 est un résidu quadratique primitif de P, s le nombre des facteurs premiers de la forme $4k+3$ de h — les solutions de la congruence (10) sont des racines primitives de P et sont données par la formule (11) où p_i parcourt tous les diviseurs premiers égaux ou différents de h et μ_i les résidus quadratiques de p_i.*

Les lemmes utilisés pour la démonstration continnent les faits suivants:

A. Si b est un résidu quadratique primitif et ρ une racine primitive de P, donc $b \equiv \rho^k$, k et $2h$ sont premiers entres eux.

B. Donc ρ^k est une racine primitive de P.

C. Si α et $2h$ sont premiers entre eux et 2 est un résidu quadratique primitif de P, $\pm h$ est un résidu de la même nature.

L'applicabilité des formules énoncées est ensuite illustrée par quelques exemples numériques.