Тома Цюропайлович
(Яворів).

Визначенє повної ґрупи останків числа $a^n \equiv \alpha_n \left(\text{mod. } z = \prod_{i=1}^{i=r} z_i\right)$ для степеня пристайного до періоди ґрупи їх скороченої системи.

Thomas Cjuropajlowytsch
(Jaworiw).

Bestimmung der Gruppe des vollständigen Potenzrestsystems der Zahl $a^n \equiv \alpha_n \left(\text{mod. } z = \prod_{i=1}^{i=r} z_i\right)$ für den der Periode des verkürzten Restsystems kongruenten Grad.

Як звісно, узагальнив Ойлер т. зв. мале Ферматове твердженє, доказуючи, що періодою ґрупи „скороченої“ системи степенних останків числа

$$a^n \equiv \alpha_n \bmod p^\nu \tag{1}$$

є $n = \varphi(p^\nu) = (p-1)p^{\nu-1}$, де p число перве, та що для кождого $(x, z) = 1$ т. є найбільшого спільного подільника чисел x, z рівного 1, сповняють ся

$$x^{\varphi(z)} \equiv 1 \bmod z, \tag{2}$$

де $\varphi(z)$ відома функція з теориї чисел.

Отся розвідка займеть ся визначенєм останків ґрупи їх „повної“ системи для числа (1) о степени пристайнім до періоди ґрупи скороченої системи тих останків після загального модула $z = \prod_1^r p_i^{\alpha_i} = \prod_1^r z_i$, де p число перве, а модулова система $(p_i^{\alpha_i}, p_k^{\alpha_k}) = 1$.

Поперед мале узагальнене Ойлерового узагальненя:

Най $\Phi(z)$ означає найменшу спільну многократь всїх $\varphi(z)$, то очивидно $\Phi(z) = k\varphi(z_i)$, а що для $(x, z) = 1$ і кождого z_i не лише $x^{c\varphi(z)} \equiv 1 \bmod z$ але і $x^{c\varphi(z_i)} \equiv 1 \bmod z_i$,

то із $x^{c\varphi(z_1)} \equiv 1 \bmod z_1$ слїдує також $x^{\Phi(z)} \equiv 1 \bmod z_1$,

„ $x^{c\varphi(z_2)} \equiv 1 \bmod z_2$ $\quad x^{\Phi(z)} \equiv 1 \bmod z_2$,

„ $x^{c\varphi(z_r)} \equiv 1 \bmod z_r$ „ $\quad x^{\Phi(z)} \equiv 1 \bmod z_r$,

т. зн. $x^{\Phi(z)} - 1 = c_1 z_1 = c_2 z_2 = \quad = c_r z_r$,

а се неможливе, коли не сповняють ся

$$x^{\Phi(z)} - 1 = kz \text{ або}$$

$$x^{\Phi(z)} \equiv 1 \bmod z. \tag{3}$$

А що $\Phi(z)$ є подїльником $\varphi(z)$, отже

$$\varphi(z) = t\,\Phi(z), \text{ а } x^{\Phi(z)+i} \equiv x^i \bmod z,$$

то наворотом ґрупи скороченої системи степенних останків числа (2) є вже $\Phi(z)$, так, що $\Phi(z) \leqq \varphi(z)$; очивидно не для кождого x найбільшим, так як і конґруенція (1) має попри первісні також і инші корені.

Коли однак приглянемо ся ґрупі степенних останків числа

$$p^\mu \equiv r_\mu \bmod \xi = \frac{z}{p_\varepsilon^u},$$

де вже $(\xi, p_\varepsilon) = 1$, отже черзї останків

$$r_1,\ r_2,\ r_3 \qquad r_\mu \qquad r_{\Phi(\xi)} \tag{4}$$

то після (3) є

$$p^{\Phi(\xi)} \equiv p^{\Phi(z)} \equiv 1 \bmod \xi, \tag{5}$$

а длятого черга (4) заключує останки всїх чисел p^κ для кождого κ.

Особливо ж, коли p є первісний корінь конґруенції (5), то в черзї (4) є, як звісно, $\Phi(\xi)$ ріжних елементів. Але тодї ξ мусить бути степенею первого числа, а $\Phi(\xi) = \varphi(p^\mu)$. Колиж ξ є зложене, отже $\xi = \prod q_i$, то тодї в наслїдок $(p, \xi) = 1$ в конґруенції

$$p^{\varphi(q_i)} \equiv 1 \bmod q_i \tag{5'}$$

p є первісним коренем або з огляду на всї i, або лиш деякі, або для жадних. Але завсїди в черзї (4) найдуть ся останки всїх степений p^κ для кождого k, причім (r_i, z) не сповняє жадної умови (6).

Бо, коли

$$\kappa < \Phi(\xi), \text{ а } \Phi(\xi) = \kappa \,.\, \sigma + s, \tag{7}$$

то ґрупа та прибере для $s = 0$ вид

$$p^{\kappa} \equiv r_{\kappa},\ p^{2\kappa} \equiv r_{2\kappa}, \qquad p^{\kappa\sigma} \equiv p^{\Phi(\xi)} \equiv 1 \bmod \xi,$$

отже в наслїдок (7) заключуєть ся в (4), де після заложеня є написаних (формально) $\Phi(\xi)$ елементів. Колиж $[\kappa, \Phi(\xi)] = 1$, то ґрупа степенних останків знов в наслїдок (7) і $p^{\Phi(\xi)+i} \equiv p^i \bmod \xi$ ріжнить ся від (4) лиш порядком показчиків так, як і повстає з неї через відчислюванє що κ елементів, а се конче доводить до циклю.

Так само є, коли $\kappa > \Phi(\xi)$; бо тодї треба лиш положити $\kappa \equiv \mu' \bmod \Phi(\xi)$, де $\mu' < \Phi(\xi)$, а тодї очивидно для кождого $p^{\kappa} \equiv g \bmod \xi$, навіть тодї, коли саме у наслїдок $\kappa > \Phi(\xi)$ є $(g, z) = 1$, між тим як для $\kappa \leqq \mu$ степень p^{κ} містить ся в $z = \prod p_{\alpha}^{\mu}$, мусить також бути $(g, \xi) = 1$ так, що знову $g^{\Phi(\xi)} \equiv 1 \bmod \xi$, а ґрупа стає ся тотожною з (4).

Завсїди отже останнїй член ґрупи скороченої системи останків $r_{\kappa\Phi(\xi)} \equiv r_{\Phi(\xi)} \equiv 1 \bmod \xi$.

Множім тепер чергу (4) разом із модулом по порядку числами $p, p^2, p^3, \ldots, p^{\nu}$ і покладїм перед кождою ґрупою, що повстане в той спосіб, одиницю, то дістанемо:

$$\begin{array}{r|l|l|l}
 & 1,\ r_1,\ \ r_2, \ldots\ r_{\Phi(\xi)-1}, & r_{\Phi(\xi)}, r_1,\ \ r_2, \ldots & \bmod \xi \\
1, & p,\ r_1 p,\ r_2 p,\ r_{\Phi(\xi)-1} p, & p,\ \ r_1 p,\ r_2 p, & \bmod \xi p \\
1, p, & p^2, r_1 p^2, r_2 p^2, r_{\Phi(\xi)-1} p^2, & p^2,\ \ r_1 p^2, r_2 p^2 & \bmod \xi p^2 \\
. & . \qquad\qquad . & . \qquad . & . \\
. \quad . & . \qquad\qquad . & . \qquad . & . \quad . \\
1, p, p^2, \ldots p^{\nu-1}, & p^{\nu}, r_1 p^{\nu}, r_2 p^{\nu}, r_{\Phi(\xi)-1} p^{\nu}, & p^{\nu},\ \ r_1 p^{\nu}, r_2 p^{\nu}, & \bmod \xi p^{\nu} = z,
\end{array}$$

де будуть повторяти ся лише числа поміж прямовими лїніями так, що в першій ґрупі mod z крім них є еще лиш ν инших елементів, а всї прочі ґрупи чисел о степенях більших від періоди є вже ідентичні. Коли отже відчислимо до тої першої ґрупи $\Phi(z)$ елементів, бачимо на початку елементи $p, p^2, \ldots p^{\nu}$, на кінци $r_{\Phi(\xi)-\nu}\, p^{\nu}$, так, що слїдуюча ґрупа зачинаєть ся вже від $r_{\Phi(\xi)-\nu+1}\, p^{\nu} \equiv\mid p$ і т. д. Бо в першій ґрупі, яка обнимає $\Phi(z)$ елементів, є $\Phi(z) = \Phi(\xi)\ \dfrac{\varphi(p^{\kappa}).\ \Phi(\xi)}{[\varphi(p^{\kappa}),\ \Phi(\xi)]} = t\, \Phi(\xi)$ так, що $\Phi(\xi)$ елементів між прямовими лїніями повторяють ся $(t-1)$ разів. А що в періодї є ще ν елементів $p, p^2, p^3, \ldots, p^{\nu}$, то разом є $(t-1)\,\Phi(\xi) + \nu = \Phi(z) - \Phi(\xi) + \nu$ елементів.

Щоби їх доповнити до числа $\Phi(z)$, треба дочислити ще $\Phi(\xi) - \nu$ елементів. Отже дійсно $r_{\Phi(\xi)-\nu} p^\nu$ є останній елемент всїх пазваних ґруп, т. зн.,

$$p^{\lambda\Phi(z)} \equiv p^{\Phi(z)} \equiv r_{\Phi(\xi)-\nu} p^\nu. \tag{8}$$

З того знову читаємо, що і кождий ступінь числа p лишає для $n \equiv o \bmod \Phi(z)$ на степенний останок $\bmod z$ число $r_{\Phi(\xi)-\nu} p^\nu$, а так само кожде число, подільне числом p, яке крім p не заключує жадних инших чинників числа z, отже має вид $u p^\lambda$, де $(u, z) = 1$, а λ довільне.

Бо тоді $u^{\Phi(z)} \equiv 1$, $p^{\lambda\Phi(z)} \equiv \varrho \bmod z$, отже і $(u p^\lambda)^{r\Phi(z)} \equiv \varrho \bmod z$.

Коли однак $r_{\Phi(\xi)-\nu} p^\nu \equiv \varrho$, а $r_{\Phi(\xi)-\nu} \equiv \beta \bmod \xi$, то по помноженю сеї останньої конґруенції числом $p^\nu \equiv r_\nu \bmod \xi$ одержимо $r_{\Phi(\xi)} \equiv \beta r_\nu \bmod \xi$; але $r_{\Phi(\xi)} \equiv 1$, отже і

$$\beta r_\nu \equiv 1 \bmod \xi; \tag{9}$$

при тім треба вважати, що r_ν є степенний останок кождого найвисшого ступіня числа p, який є заключений в модулї z так, що для $p^\nu < z$, $r_\nu = p_\nu$, а (9) переходить в

$$\varrho = p^\nu \beta \equiv 1 \bmod \xi. \tag{10}$$

Але тому, що (4) важне для кождого показчика i із p_i та **й для їх добутків, тому (8) буде важне не лише для** p^λ при **довільнім λ, але й для кождого иншого подільника a** числа $z = a z'$, **хочби a не заключало самих найвисших ступінїв** $p_i^{\alpha_i}$, отже $a = \prod p_i^{\kappa_i}$, де $\kappa_i \leqq \alpha_i$. Завсїди мусимо дістати на основі (8) і їх добутків

$$a^{\Phi(z)} \equiv R \prod_{i=1}^{i=\nu} r_i\, [\Phi(\xi_i) - \alpha_i]\, p_i^{\alpha_i}, \tag{8'}$$

де $R\prod$ означає останок добутка $\equiv$ добуткови останків, α_i найвисші викладпики первих чинників числа a, заключені в z, а показчик i при p жадає, щоби всї p_i були зглядно перві т. зн. $(p_\iota, p_{\iota\iota}) = 1$.

Бо в противнім разї (8) не могли би сповняти ся для довільного λ.

З того однак слїдує дальше, що в ґрупі степенних останків т. зв. „повної“ їх системи для $n = c\,\Phi(z)$ добуток двох ріжних останків мусить $\equiv$ останкови тої самої ґрупи так, як і всї числа цїлі взагалї можуть бути супроти модула перві, або мати з ним якийсь спільний подільник, не виключаючи його самого. В першім разї $\Phi(z)$ — тим останком є одиниця, в другім добуток з неї і иншої якоїсь решти після (8).

Реасумуючи бачимо, що $\Phi(z)$-тий степенний останок **для якого небудь** числа a, заключеного в z, є тотожний **із** $\Phi(z)$-тим степенним останком того подільника d **числа** $z = d\,\xi_d$, $d = \prod p_i^{\alpha_i}$, що заключує в собі **ті самі** первi числа, що і a, лише всї піднесені до **тих** ступінїв, які є для даного p_i в модулї z найвисші. **так**, що коли число має r зглядно первих чинників p_i, то і скількість $\Phi(z)$-тих ступінних останків крім одиниці і зера є сумою комбінацій без повтореня r елементів 1., 2, 3., ., $(r-1)$. кляси, отже

$$\chi(\Phi) = \binom{r}{1} + \binom{r}{2} + \binom{r}{3} + \ldots + \binom{r}{r-1} + \binom{r}{r-2} = 2^r - 2,$$

а з одиницею і зером очивидно 2^r так, що се число є клясою названої ґрупи „повної“ системи степенних останків.

До їх визначеня служить або взорець (8) враз із тим, що $r_{\Phi(\ )} \equiv 1 \bmod \xi$, де треба би по порядку розвязувати згл. редукувати модулові системи $(r_r\,x - 1, \xi)$, $(r_r\,x_1 - x, \xi)$, $(r_r\,x_2 - x, \xi)$ і т. д. ν разів, або, що скорше доводить до цїли, взорець (9), якого розвязка при помочи редукції модулової системи $(r_r\,\beta - 1, \xi)$ згл. при $d \equiv r_d \bmod \xi_d = \frac{z}{d}$, $(r_d\,\beta - 1, \xi_d)$ дуже скоро дає β; то число треба після (10) помножити числом p_κ^{ν} згл. d, т. є названим уже подільником числа z, рівним добуткови первих чисел p_i, піднесених до найвисших ступінїв ν_1, які приходять в z, щоби дістати $\Phi(z)$-тий степенний останок т. є $a^{\Phi(z)} \equiv \varrho \bmod z$.

Ті останки мають цікаву прикмету, спільну з одиницею, а іменно ту, що всї належать питомо до викладника 1, т. зн., що їх степенні останки є однакові для кождого n так, що для $a^{\Phi(\ )} \equiv \varrho \bmod z$ сповняють ся $\varrho^n \equiv \varrho \bmod z$ для кождого n.

Бо із $r_d\,\beta \equiv 1 \bmod \xi_d$ слїдує

$$\varrho \equiv d\,\beta \equiv \bmod \xi_d,\ d^2\beta \equiv d,\ d^2\beta^2 \equiv d\,\beta \bmod z,$$

отже $\varrho^2 \equiv \varrho \bmod z$, а за тим і

$$\varrho^n \equiv \varrho^{n-1} \equiv \varrho^{n-2} \equiv \qquad \equiv \varrho^3 \equiv \varrho^2 \equiv \varrho \bmod z.$$

Приміром для $z = 5^2.3^3.7$, $a = 5.3 = 15$ є $\varphi(5^2) = 20$, $\varphi(3^3) = 18$, $\varphi(7) = 6$, $\Phi(z) = м(20, 18, 6) = 180$, між тим як $\varphi(z) = 1080$. Для кождого числа u, що сповняє умову $(u, z) = 1$, є $u^{\Phi(z)} = u^{180} \equiv 1 \bmod z$, а для кождого a', подільного через 15, неподільного через 7, є $a'^{180} \equiv 3375 \bmod z = 4725$, при чім $3375^n \equiv 3375 \bmod z$ для кождого n.

Бо $5^2.3^3 = 675 \equiv 3 \bmod 7$, а модулова система

$$(3\beta - 1,\ 7) = (7\beta - 6\beta + 2,\ 7) = (\beta + 2,\ 7) = (\beta - 5,\ 7)$$

дає $\beta \equiv 5 \bmod 7$, у нас $\beta = 5$, отже після (10) $p^{\nu} \beta = 5.675 = 3375$, т. зн.

$$15^{\Phi(z)} \equiv 3375 \bmod z,$$

а з того для кождого u і $(u, z) = 1$ також

$$(15\, u)^{\Phi(z)} \equiv 3375 \bmod z, \tag{11}$$

$$\text{бо } u^{\Phi(z)} \equiv 1 \bmod z.$$

А що $(25\,\beta - 1, \xi_d = 189) = (189\,\beta - 100\,\beta + 4, 189) = (89\,\beta + 4, 189) = (189\,\beta - 187\,\beta + 136) = (2\,\beta + 136, 189) = (\beta + 68, 189) = (\beta - 121, 189)$, то для $d = 25$ є $\beta = 121$, а

$$(5\,\lambda)^{\Phi(z)} \equiv (25)^{\Phi(z)} \equiv 25.121 = 3025 \bmod z.$$

Се помножене конґруенцією (11), дає:

$$(15.5\,\lambda\, u)^{\Phi(z)} \equiv 3375.3025 = 10\ 209\ 375 \equiv 3375 \bmod z,$$

як після теорії.

Щоби се і в инший спосіб провірити, утворім $\xi_{5^2} = 3^3.7 = 189 = \xi_1$, $\xi_2 = \xi_{5^3} = 175$, $\xi_3 = 225$, $\Phi(\xi_1) = м\,(18,6) = 18$, $\Phi(\xi_2) = м\,(20,6) = 60$, $\Phi(\xi_3) = м\,(20,18) = 180$, а тоді дістанемо після (3):

$$5^{18} \equiv 1 \bmod \xi_1,\quad 3^{60} \equiv 1 \bmod \xi_2,\quad 7^{180} \equiv 1 \bmod \xi_3,$$

$$5^{180} \equiv 1 \qquad 3^{180} \equiv 1 \quad „ \qquad 7^{180} \equiv 1 \quad „$$

$$(5\,x - 1, 189) = (189\,x - 190\,x + 38, 189) = (x - 38, 189),$$

$$(3\,x - 1, 175) = (x - 117, 175),\ 117 : 3 = \underline{39},\ 39 : 3 = \underline{13},\ \text{т. зн.}$$

$$5^{179} \equiv 38 \bmod \xi_1,\ 3^{179} \equiv 117 \bmod \xi_2, \text{ а так само із}$$

$$(5\,x_1 - 38, 189) = (x_1 - 121, 189) \text{ т. зн.}$$

$$5^{178} \equiv 121 \bmod \xi_1.\ 3^{178} \equiv \underline{39},\ 3^{177} \equiv \underline{13} \bmod \xi_2,$$

отже

$$5^{180} \equiv 3025 \bmod z$$

$$\underline{3^{180} \equiv 351 \bmod z}$$

$$15^{180} \equiv 3375 \bmod z,\ q.\ e.\ d.$$

А що і $(3\,\lambda)^{180} \equiv 351 \bmod z$, то

$(15.3\,\lambda\, u)^{\Phi(z)} \equiv 351\,.\,3375 = 1\ 184\ 625 = 250\,z + 3375 \equiv 3375 \bmod z$, т. зн. дійсно також $(3\,\lambda\,.\,15\,u)^{\Phi(z)} \equiv 3375 \bmod z$.

А що $(7\,x - 1,\ 225) = (x + 32,\ 225) = (x - 193,\ 225)$, то $7^{\Phi(z)} \equiv 7.193 = 1351 \bmod z$, так, що ціла ґрупа степенних останків їх „повної" системи для $n = c\,\Phi(z)$ обіймає $2^3 = 8$ елементів т. є 0, 1, 351, 3025, 1351 і їх добутки $\underline{3375}$, $1351\,.\,351 = 474201 = 100\,z + \underline{1701}$ і $1351\,.\,3025 = 4086775 = 864\,z + \underline{4375}$. Останню решту можемо дістати також і після (8): $d = 25.7 = 175$, $\xi_d = 27$; $(175\,x - 1,\ 27) = (13\,x - 1,\ 27) = (x + 2,\ 27) = (x - \underline{25},\ 27)$, отже $a^{\Phi(z)} \equiv 175\,.\,25 = 4375 \bmod z$.

Так само і прочі останки.

Яворів, у червни 1917.

INHALTSANGABE.

Ist $z = \prod z_i$ in lauter gegen einander relativ prime Faktoren z_i zerlegt, so ist die Periode der verkürzten Restgruppe das kleinste gemeinschaftliche Vielfache aller $\varphi(z_i)$ (die bekannte zahlentheoretische Funktion), d. h. $\Phi(z)$. Dann ist:

$$a^{\Phi(z)} \equiv R \prod r_i^{[\Phi(\xi_i) - \alpha_i]} \, p_i^{\alpha_i}, \tag{8'}$$

wo a irgend eine (ganze) Zahl, $R\prod$ den Rest des Produktes, r_i den Rest desjenigen Teilers $d = \prod_{i=1}^{i=\kappa} p_i^{\alpha_i}$ von z bedeutet, welcher mit a dieselben Primzahlen zu gemeinsamen Faktoren hat, jede aber zu der in z vorkommenden höchsten Potenz α_i erhoben und $\xi_i = \dfrac{z}{d}$ bedeutet. Gibt es r verschiedene Primzahlen in z, so ist die Klasse der Gruppe 2^r und das Produkt der Elemente der Gruppe bildet wiederum ein Element der Gruppe, welches immer die merkwürdige Eigenschaft hat, zum Exponenten 1 eigentümlich zu gehören.