Студії з теорії конґруенцій.

(Studien aus der Kongruenzentheorie).

НАПИСАВ

Др. Микола Чайковський.

Опираючись на клясичній теорії конґруенцій, даній Gauss'ом в „Disquisitiones arithmeticae"[1]), можемо розвязувати тільки такі конґруенції, які мають самі дійсні коріні. Щоби одначе перевести розвязку конґруенцій вповні, треба за почином Galois[2]) ввести рід мнимих величин, які тут гратимуть подібну ролю, що звичайні мнимі числа $a+bi$ $(i^2 = -1)$ в теорії рівнань. Отсю думку перевели новійші математики (головно Американці: Cole, Moore і Dickson[3]), будуючи теорію „поля Galois"; вона відповідає подекуди теорії альґебраічних тіл.

На тій основі переведена тут теорія конґруенцій третього й четвертого степеня з первочисельним модулом. Тим предметом займав ся вже Cauchy[4]), але тільки в тіснім обсягу дійсних розвязок. Щоби одначе могти тут перевести повну теорію згаданих конґруенцій, подаємо в першій части нашої розвідки теорію поля Galois в тім виді, як її опісля будемо примінювати до нашої теми.

I. Теорія поля Galois.

§. 1.

1. З елементарної теорії чисел звісно, що всї числа природного ряду

$$0,\ 1,\ 2,\ 3, \qquad m-1,\ m,\ m+1, \tag{1}$$

[1]) Lipsiae 1801, — Werke Bd. I, Leipzig, 1870.

[2]) Sur la théorie des nombres, 1831.

[3]) Dickson, Linear groups with an exposition of the Galois Field theory. Липск, 1901.

[4]) Cauchy, Exercices de Mathématiques, IV. Année, Paris 1829. — Oeuvres, S. II, T. IX. Paris 1891.

розпадають ся після модула m на m кляс; кожда з них містить в собі безконечно богато чисел, пристайних поміж собою (mod. m), так що замість всїми числами природного ряду, можемо в деяких проблємах математики оперувати клясами непристайних поміж собою чисел

$$K_0, K_1, K_2, \quad K_{m-1} \tag{2}$$

згл. їх репрезентантами, т. є системою яких небудь чисел, вибраних довільно по одному з кождої кляси. Коли сю систему становлять числа

$$0, 1, 2, \quad ., m-1, \tag{2a}$$

то називаємо їх числами модула m або системою найменших останків модула m і пишемо се так: [mod. m]. До кляси K_0 належать всї многократи модула.

2. Визначну ролю в теорії чисел грає повна система останків первочисельного модула p:

$$0, 1, 2, \quad ., p-1; \tag{2aa}$$

її назвемо полем Galois степеня p і означимо $GF[p]$.

Взагалї називаємо полем, тїлом або обсягом вимірности систему, яка має ту прикмету, що її елементи, лучені з собою при помочи операцій додаваня і множеня, дають на вислїд опять числа тої системи. Таким полем є система (2aa); вона має ще й ту прикмету, що скількість елементів, які в нїй містять ся, є скінчена; се слїдує рівно-ж з елементарної теорії чисел. Поле Galois степеня p має отже загалом такі прикмети:

1) При помочи операції додаваня одержуємо з кождих двох елементів того поля, a і b, третїй елемент s однозначно; так само при помочи множеня (тут мусимо одначе виключити елемент 0) однозначно елемент m:

$$a + b = s, \qquad a\,b = m.$$

2) Обі операції (додаваня й множеня) є злучні, т. є коли $(a + b)$ є сумою чисел a і b, а $(a\,b)$ їх добутком, то

$$\big((a + b) + c\big) = \big(a + (b + c)\big) \text{ i } \big((a\,b)\,c\big) = \big(a\,(b\,c)\big)$$

3) З

$$a + b = d \qquad \text{i} \qquad a + c = d$$

або

$$a\,b = e \qquad \text{i} \qquad a\,c = e$$

слїдує:

$$b = c.$$

4. Обі операції є перемінні, т. є

$$(a + b) = (b + a) \qquad \text{i} \qquad (a\,b) = (b\,a).$$

5) Врештї додаванє в полученю з множенєм є розділ̈ьне:

$$a\,(b + c) = a\,b + a\,c.$$

Коли за комбінуючу операцію приймемо додаване, то елементи ряду (2aa) творять **скінчену ґрупу** порядку p; беручи-ж за основу операцію множеня, одержимо з чисел

$$1,\ 2,\ 3, \quad .,\ p-1 \qquad (2aa^*)$$

рівно-ж скінчену ґрупу порядку $p-1$. Систему (2aa*) назвемо **зредукованим полем** Galois і зазначимо її $GF[p]^*$. До неї належать всї числа, перві супроти модула.

В обох разах є поле Galois перемінною ґрупою.

Елемент 0 грає супроти множеня особливу ролю; іменно, яке-б не було x, є завсїди:

$$0.\ x = 0 \quad \text{і} \quad x.\ 0 = 0,$$

і навпаки: коли добуток двох чисел належить до кляси K_0, то принайменше один з чинників мусить належати до сеї кляси.

3. З прикмет ґрупи слїдує, що до кождого елемента a в $GF[p]$ єствує один і тільки один такий елемент b, який доданий до a дасть число з кляси K_0:

$$a + b \equiv 0 \ (\text{mod. } p);$$

його значимо

$$b \equiv -a \ (\text{mod. } p).$$

Проте є в $GF[p]$ можлива до переведеня **операція віднимання**.

Подібно є в $GF[p]^*$ завсїди можлива **операція дїленя**; слїдує се з т. зв. **теореми Fermat'a**. Випишім іменно $GF[p]^*$ і помножім всї його числа одним з поміж них:

$$1.\ a,\ 2.\ a, \qquad (p-1).\ a,$$

то через те зрепродукуємо його, тільки в иншім порядку. Добуток всїх його чисел є пристайний (mod. p) до добутка всїх чисел ряду (2aa*), бо в склад обох добутків входять репрезентанти тих самих кляс K_1, K_2, K_{p-1}:

$$1.\ a.\ 2.\ a.\ 3.\ a \qquad (p-1).\ a \equiv 1.\ 2.\ 3 \qquad (p-1) \ (\text{mod. } p)$$

або

$$(p-1)!\ (a^{p-1} \quad 1) \equiv 0 \ (\text{mod. } p).$$

Добуток $(p-1)!$ є супроти модула p первий, отже мусить бути

$$a^{p-1} \equiv 1 \ (\text{mod. } p). \qquad (3)$$

Отсей взірець є характеристичний для $GF[p]^*$. З нього слїдує, що до кождого числа a в $GF[p]^*$ дасть ся дібрати таке число a', що добуток тих обох чисел буде належати до кляси K_1:

$$a\,a' \equiv 1 \ (\text{mod. } p).$$

Бо помножім сю конґруенцію через a^{p-2}, то се дасть:

$$a' \equiv a^{p-2} \ (\text{mod. } p);$$

a є супроти модула p перве, отже і a^{p-2} належить до $GF[p]^*$.

Число a' називаємо **відворотностю** числа a' в $GF[p]^*$ або його **товаришем** (Sozius) і значимо символїчно:

$$a' \equiv \frac{1}{a} \pmod{p}.$$

4. Прикмети 1) — 5) і взорець Fermat'а є характеристичні для кождого **скінченого поля**[1]). Покажемо, що коли система p елементів, де p є перве число, має ті всі прикмети, то вона творить скінчене поле, отже коли скількість елементів поля є первим числом, то його можна вважати полем Galois степеня p.[2])

Нехай будуть

$$A, B, C, \ldots, L \tag{4}$$

даними p елементами. Виберім з поміж них який небудь елемент H і утворім ряди

$$H+A,\ H+B,\ H+C, \qquad H+L, \tag{4a}$$
$$A+H,\ B+H,\ C+H, \qquad L+H, \tag{4б}$$

то вони оба є ідентичні — не вважаючи на порядок членів — з рядом (4) — (прикмета 1). Проте в першім з них мусить містити ся один елемент $H+I$, рівний елементови H з (4),

$$H+I=H,$$

а в другім елемент $J+H$, також рівний H:

$$J+H=H.$$

Звідси слїдує:

$$G+(H+I)=(G+H)+I=G+H$$
$$(J+H)+K=J+(H+K)=H+K$$

(прикмета 2), т. зн.: який би не був елемент M, то в ряді (4) еству завсїди такий елемент I, який доданий до M з правої сторони не змінить його, — і такий елемент J, який доданий до M з лївої сторони рівно-ж не викличе в нїм нїякої зміни:

$$M+I=M,$$
$$J+M=M.$$

Врештї після прикмети 3) маємо: для $M=J$ з першого рівнаня

$$J+I=J$$

і для $M=I$ з другого:

$$J+I=I,$$

отже
$$J=I.$$

---

[1]) Під „скінченим полем" розуміємо тут систему, зложену із **скінченого числа** елементів — у відріжненю від „скінчених альґебраїчних тїл", де скінченість лежить у тім, що при помочи основи, зложеної із скінченого числа величин, можемо представити кожду величину того тїла. — Пор. Weber, Algebra, I. §. 150, II. §. 80. (endlicher Kongruenzkörper).

[2]) Пор. пр. Borel-Drach, Théorie des nombres et l'algèbre supérieure (d'après les conferences par M. J. Tannery), Paris 1895, Note II, стр. 343.

Єствує проте в ряді (4) один і тільки один такий елемент I, який доданай з лівої або з правої сторони до котрого небудь иншого елемента, не змінить його. Огсей елемент відповідає клясі K_0 в $GF[p]$.

Возьмім тепер знова довільний елемент A і творім ряд:

$$A,\ (A+A),\ \big((A+A)+A\big),\ .$$

якого числа будемо в скороченю називати:

$$A,\ 2\,A,\ 3\,A,\qquad .,\ m\,A,\qquad .; \tag{4в}$$

на основі прикмети 1) містить він в собі тільки ті елементи, які є в (4), і є обмежений, отже його елементи будуть повторювати ся. Нехай на $(q+1)$-ім місці стоїть елемент рівний першому; тоді возьмім під розвагу тільки q перших членів. — Коли б ряд (4в) не вичерпував ще всіх елементів (4), то возьмім один з нових елементів B і при його помочи творім новий ряд:

$$A+B,\ 2\,A+B,\ 3\,A+B,\qquad .,\ q\,A+B;$$

на його $(q+1)$-ім місці буде стояти рівно-ж елемент з тої самої кляси, що перший елемент. Всї члени того ряду є відмінні від ряду (4) — (прикмета 3). — Коли ще тепер не зрепродукований цїлий ряд (4), то творимо при помочи нового елемента C третій такий самий ряд, аж врештї вичерпаємо всї елементи з (4); кождий з частинних рядів буде мати таку саму скількість членів, т. є q, отже

$$p=kq,$$

а що ми приймили p перве, то $k=1$, отже $p=q$, т. зн. ряд (4в) вичерпує всї елементи.

Рядом (4в) маємо здефінїоване і множене, отже тою дорогою можемо перевести всї дальші анальоґії; мусимо ще тільки доказати, що коли модул m є зложений, то повна система чисел [mod. m] не творить поля Galois. Бракує тут іменно теореми Fermat'a. Добутки всїх чисел обох рядів

$$1,\ 2,\qquad .,\ m-1,$$
$$1\,a,\ 2\,a,\qquad .,\ (m-1)\,a,$$

є — що правда — пристайні до себе (mod. m), отже:

$$(m-1)!\ (a^{m-1}-1)\equiv 0\ (\text{mod. } m),$$

зате кінцева замітка з уст. 2. не має тут примінення, бо m і $(m-1)!$ мають $HC\Pi>1$, отже модул m можна також представити як добуток двох чисел $<m$.

Натомість, коли уставимо в ряд всї елементи

$$a_0,\ a_1,\ a_2,\qquad .,\ a_{\varphi(m)-1},$$

перві супроти модула m (їх є $\varphi(m)$ — теорема Gauss'a), то при помочи якого небудь з них можемо утворити добуток

$$a_0,\ a_1, \qquad a_{\varphi(m)-1}\ [a^{\varphi(m)} - 1] \equiv 0 \ (\text{mod. } m),$$

з якого слїдує

$$a^{\varphi(m)} \equiv 1 \ (\text{mod. } m), \tag{5}$$

бо чинник перед [ ] є первий супроти m. Се т. зв. **узагальнена теорема Fermat'а.**

Звідси слїдує, що система p елементів, які сповнюють прикмети 1) — 5), є ідентична з $GF[p]$.

5. З огляду на неважність теореми Fermat'а для зложених модулів, мусимо зазначити, що:

1) Лінїйна конґруенція

$$ax \equiv b \ (\text{mod. } m) \tag{6}$$

є тільки тоді рішима, коли $НСП$ чисел a і m містить ся і в b.

2) Коли d є $НСП$ чисел a і b, то конґруенцію можемо скоротити через d, лишаючи модул незмінений.

3) Коли d є $НСП$ чисел a, b і m, то обі сторони конґруенції можемо скоротити через d; модул можемо рівно-ж скоротити або лишити без зміни.

4) Коли $(a, m) = 1$, то конґруенція (6) має тільки одну розвязку. Бо рівнозначне з нею Діофантове рівнане

$$ax - my = b,$$

не дасть ся ніяк скоротити; воно є рішиме, а вартости на x творять аритметичний поступ з ріжницею m, т. є всї є поміж собою пристайні (mod. m).

5) Коли $(a, m) = d$, конґруенція має d ріжних розвязок, бо з конґруенції (6) слїдує

$$\frac{a}{d} x \equiv \frac{b}{d} \left(\text{mod. } \frac{m}{d}\right), \tag{6a}$$

Тут є $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, отже конґруенція має одну розвязку — назвім її z —, а всї її прочі розвязки є $\equiv z \left(\text{mod. } \frac{m}{d}\right)$. Натомість (6) може мати ще й инші розвязки, бо числа, непристайні до себе $\left(\text{mod. } \frac{m}{d}\right)$ не, мусять бути непристайні (mod. m). Отже, коли $x \equiv z \left(\text{mod. } \frac{m}{d}\right)$ є розвязкою конґруенції (6а), то (6) має такі корінї

$$x \equiv z + i \frac{m}{d} \ (\text{mod. } m)$$

$$(i = 0,\ 1, \qquad d - 1),$$

бо вставивши се в (6) одержимо

$$a \left(z + i \frac{m}{d}\right) = az + i \cdot \frac{a}{d} \cdot m \equiv az \equiv b \ (\text{mod. } m).$$

§. 2.

6. До тепер обговорили ми головні прикмети поля Galois степеня p і виказали, що повна система останків модула m творить тільки тоді поле Galois, коли m є первим числом. Тепер займемо ся конструкцією обширнїйших піль Galois і докажемо, що їх степенем може бути тільки **степень первого числа**, p^n.

Альґебраїчний многочлен степеня m, якого сочинники є числами з $GF[p]$:

$$F(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m \pmod{p}, \qquad (1)$$

а a_0 не належить до кляси K_0, називаємо **функцією m-того степеня** в $GF[p]$. За сочинники $a_0, a_1, \ldots, a_m$ можемо приймати всї числа $GF[p]$ з виїмком $a_0 \equiv 0 \pmod{p}$, отже скількість всїх функцій m-ого степеня в $GF[p]$ є $p^m(p-1)$. Коли-ж чинник a_0 добудемо перед скобку і всї функції, що ріжнять ся тільки тим постійним чинником, будемо вважати одною й тою самою функцією, то скількість всїх ріжних функцій є p^m, проте:

В $GF[p]$ є p^m **ріжних функцій m-того степеня.**

7. Функцію $F(x)$ називаємо **зведимою** або **незведимою** в $GF[p]$, відповідно до того, чи можливе або нї розложити її на добуток

$$F(x) \equiv g(x)\, h(x) \pmod{p} \qquad (2)$$

двох инших функцій в $GF[p]$, степенїв низших як степень функції $F(x)$, а висших як 0. — Чинники $g(x)$ і $h(x)$ є зведимі або нї; коли вони оба зведимі, то функція $f(x)$ m-того степеня дасть ся остаточно розложити на m лінїйних чинників:

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_m) \pmod{p} \qquad (3)$$

Коли положимо $x \equiv$ одному з α, тодї буде

$$f(\alpha_i) \equiv 0, \pmod{p},$$

отже $\alpha_1, \alpha_2, \ldots, \alpha_m$ є **корінями конґруенції**

$$f(x) \equiv 0 \pmod{p}. \qquad (4)$$

В елементарній теорії конґруенцій доказують ся такі твердження:

I. (основна теорема): Конґруенція m-того степеня з первим модулом не може мати більше як m ріжних або однакових чинників[1]).

II. Ліва сторона конґруенції є (mod. m) ділима кождим „корінevим чинником" $x - \alpha_i$.

III. Сочинники конґруенції є основними симетричними функціями її корінїв.

IV. Многократні корінї конґруенції є заразом корінями її похідних.

[1]) Може їх мати менше як m.

V. Коли функцію $f(x)$ розложити на добуток двох инших (3), і коли (4) має m корінів, то обі конґруенції:

$$g(x) \equiv 0 \text{ і } h(x) \equiv 0 \pmod{p}$$

мають як раз по тільки корінів, кілько виносить їх степень.

VI. Конґруенція

$$x^{p-1} \equiv 1 \pmod{p} \tag{5}$$

має за коріні всі числа $GF[p]$.

З V. і VI. слідує спосіб визначування фактичної скількости корінів даної конґруенції (4): методою Евкліда вишукуємо *НСП* функцій $f(x)$ і $x^{p-1} - 1 \pmod{p}$; він містать в собі всї коріні даної конґруенції, отже його степень подає скількість її корінів. — Отся метода походить від Libri[1].

Із сказаного слідує, що як при рівнанях, так і тут зведимість і рішимість конґруенцій (mod. p) є ідентичні понятя.

Про рішимість (зведимість) конґруенцій можемо рішати на основі таких тверджень:

I. Щоби конґруенція (4) була рішима, є конечне і достаточне, щоби циклїчний визначник Δ степеня $p-1$, утворений із сочинників функції $f(x)$, був $\equiv 0 \pmod{p}$.

II. Конґруенція (4) має точно r ріжних корінів, коли ряд визначника Δ є r.[2]).

III. Виріжник незведимої в $GF[p]$ функції є $\equiv (-1)^{n-1} \pmod{p}$; коли $f(x)$ розпадаєть ся на r незведимих (mod. p) чинників, є її виріжник $\equiv (-1)^{n-r} \pmod{p}$[3]).

8. Займаючи ся квадратними функціями в $GF[p]$, приходимо до понятя квадратних останків і не-останків.

Скількість всїх квадратних функцій в $GF[p]$ є p^2, бо в

$$f(x) = x^2 + a\,x + b \tag{6}$$

можуть a і b приймати всї вартости з $GF[p]$.

Повну квадратну конґруенцію

$$x^2 + a\,x + b \equiv 0 \pmod{p} \tag{6a}$$

---

[1]) Mémoires de Mathématiques, I. p. 164.

[2]) Коли даний визначник Δ степеня k і всї його підвизначники степенїв 1, 2, 3, . . . l мають вартість 0 згл. $\equiv 0 \pmod{p}$, а бодай один з підвизначників ряду $l+1$ є $\equiv 0$ згл. $= 0$, тодї кажемо, що Δ має ряд (Rang) $k - l$ (Kronecker, Frobenius).

[3]) Теореми I—II: Rados, Zur Theorie der Kongruenzen höheren Grades, Crelle's Journ. 89. (1886), p. 258—260; Kronecker, ibid. p. 320; Gegenbauer, Wiener Ber. 95. 2 (1887), p. 165—169, 610—617. — Теорема III. Stickelberger, Verhandlungen des I. intern. math. Kongresses in Zürich, 1897, p. 186; Voronoï, Verh. des III. int. math. Kongr. in Heidelberg, 1904, p. 186.

розвязуємо подібно як квадратне рівнанє. Сочинник a можемо заступити яким небудь парнистим числом, що належить до тої самої кляси: $a \equiv 2a'$ (mod. p), отже напишемо:

$$(x + a')^2 \equiv a'^2 - b \pmod{p}, \tag{6б}$$

проте повну конґруенцію зводимо на двочленну

$$y^2 \equiv s \pmod{p}. \tag{7}$$

Вона може бути рішима або ні; в першім разї називаємо s **квадратним останком**, в другім **квадратним не-останком** модула p; коли-б було $s \equiv 0$, то конґруенція мала би один подвійний корінь $y \equiv 0$. Виключивши се, бачимо, що теорема Fermat'а наводить нас на такі крітерії рішимости конґруенції (7): коли

$$s^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{8а}$$

то конґруенція є рішима; вона є нерішима, коли

$$s^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{8б}$$

Кожде число $GF[p]^*$ мусить сповнювати (для $p > 2$) **одну і тільки одну** з тих двох формулок; їх називаємо **крітеріями Euler'а**. Їх заступив **Legendre** символом $\left(\frac{s}{p}\right)$, іменно є:

$$\left(\frac{s}{p}\right) \equiv s^{\frac{p-1}{2}} \pmod{p}, \tag{9}$$

отже: 1) коли s є кв. останком, маємо

$$\left(\frac{s}{p}\right) = +1;$$

2) в разї не-останка:

$$\left(\frac{s}{p}\right) = -1.$$

3) Коли-ж для повности допустимо і $s \equiv 0$, то

$$\left(\frac{s}{p}\right) = 0.$$

Вартість символа $\left(\frac{s}{p}\right)$ називаємо **квадратним характером** числа s супроти модула p, отже: $\left.\begin{matrix}\text{останки}\\ \text{не-останки}\end{matrix}\right\}$ мають кв. характер ± 1, числа кляси K_0 характер 0.

Скількість останків і не-останків кождого модула є однакова і виносить по $\frac{p-1}{2}$. Добуток двох останків або двох й не-останків є останком, добуток останка й не-останка не-останком, бо

$$\left(\frac{s}{p}\right) \cdot \left(\frac{t}{p}\right) = \left(\frac{st}{p}\right). \tag{9а}$$

В дальшім будемо потрібувати крітерій для кв. характеру чисел ± 1, ± 2, ± 3; вони є:
$+1$ є завсїди останком; -1 останком для первочисельних модулів $p \equiv 1 \pmod{4}$, не-останком для $p \equiv -1 \pmod{4}$, т. зн.

$$\left(\frac{+1}{p}\right) = +1, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{9б}$$

Для ± 2:

$p =$	$8n+1$	$8n+3$	$8n+5$	$8n+7$
$\left(\frac{2}{p}\right) =$	$+1$	-1	-1	$+1$
$\left(\frac{-2}{p}\right) =$	$+1$	$+1$	-1	-1

Для ± 3:

$p =$	$12n+1$	$12n+5$	$12n+7$	$12n+11$
$\left(\frac{3}{p}\right) =$	$+1$	-1	-1	$+1$
$\left(\frac{-3}{p}\right) =$	$+1$	-1	$+1$	-1

9. Анальоґічно до квадратних останків і не-останків дефінїюємо останки й не-останки всїх инших степенів. Іменно, коли двочленна конґруенція

$$y^n \equiv s \pmod{p} \tag{10}$$

є рішима, s є n-тим (степенним) останком; коли вона нерішима, s є n-тим (степенним) не-останком. (Приймаємо, що s не є многократю модула).

Коли s належить до кляси K_1, маємо т. зв. одиничну конґруенцію (Einheitskongruenz):

$$x^n \equiv 1 \pmod{p}; \; (n \geqq 3) \tag{11}$$

вона є анальоґічна до рівнань подїлу кола. Її розвязки будемо називати n-тими коріннями одиницї (mod. p).

Коли r є найменшим виложником, для якого є $z^r \equiv 1 \pmod{p}$, тодї кажемо, що z належить (mod. p) до виложника r. Коли $r = p-1$, z є первісним n-тим коренем одиницї (mod. p); коли $r < n$, корінь називаємо непервісним. В такім разї є $n = k \cdot r$.

Нехай буде $n = p - 1$; тодї — на основі теореми Fermat'a — є всї числа $GF[p]$ n-тими коріннями одиницї, та не всї вони належать до виложника $p-1$; пр. квадратні останки належать до виложника $\frac{p-1}{2}$. Коли нїяка низша степень числа g, аж щойно $(p-1)$-ша, є $\equiv 1 \pmod{p}$, тодї називаємо g первісним коренем конґруенції (12) або первісним коренем числа p.

Всї корінї, спільні обом конґруенціям

$$x^{\alpha} \equiv 1 \text{ і } x^{\beta} \equiv 1 \pmod{p} \tag{11a}$$

є корінями конґруенції

$$x^{\delta} \equiv 1 \pmod{p}, \tag{11б}$$

де $\delta = (\alpha, \beta)$.[1] Отже, коли α і β є перві супроти себе, то обі конґруенції (11а) не мають спільних корінїв крім $x \equiv 1$.

Виложники, до яких належать (mod. p) числа $GF[p]^*$, є подільниками числа $p-1$.

До кождого подільника d числа $p-1$ належить (mod. p) $\varphi(d)$ чисел з $GF[p]^*$. До виложника $p-1$ належить (mod. p) $\varphi(p-1)$ чисел, т. зн. кожде число p має $\varphi(p-1)$ первісних корінїв.

Коли g є одним із первісних корінїв числа p, то ряд

$$1, g, g_2, \ldots, g^{p-2} \tag{12}$$

є ідентичний — не вважаючи на порядок чисел — з $GF[p]^*$, отже всї ті числа є поміж собою ріжні. Отже до кождого числа з $GF[p]^*$ належить одна із $p-1$ перших степенеий числа g, т. зн. один із виложників від 0 до $p-2$. Коли знайдемо, що

$$s \equiv g^{\sigma} \pmod{p}, \tag{13}$$

то σ називаємо показчиком числа p (при основі g):

$$\sigma \equiv \operatorname{ind}_g s$$

згл.

$$\sigma \equiv \operatorname{ind}_g s \pmod{p-1}, \tag{14}$$

бо виложники повторюють ся що $p-2$.

Теорія показчиків є анальоґічна з теорією льоґаритмів; вона дуже придатна до розвязки двочленних конґруенцій.

Конґруенція (10) є рішима, коли

$$s^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \tag{15}$$

де $d = (p-1, n)$; вона має тодї d корінїв. Назвім $y_0 \equiv g^{\eta_0}$ один з її корінїв, то прочі корінї будуть

$$y_0, \alpha y_0, \alpha^2 y_0, \ldots, \alpha^{d-1} y^0,$$

де $\alpha \equiv g^{\frac{p-1}{d}}$ Формулка (15) є анальоґічна до крітерії Euler'а; вона висказує, що a є n-тим останком числа p. Символ, анальоґічний до Legendre'ового, є;

$$\left(\frac{s}{p}\right)_n = 1. \tag{16}$$

10. Примінення. 1) $n = 2$; тодї є $p-1$ паристе, отже $d = (p-1, 2) = 1$. Крітерія Euler'а звучить, як знаємо: $s^{\frac{p-1}{2}} \equiv +1 \pmod{p}$;

[1]) Знаком (m, n) зазначуємо $НСП$ чисел m і n.

маємо по $\frac{p-1}{2}$ останків і не-останків. Первісні другі корінї з одиниції (mod. p) є: $+1$ і -1.

2) В разї $n=3$ маємо дві можливости: а) $p\equiv 1$ (mod. 6), б) $p\equiv -1$ (mod. 6); числа всїх инших форм не є перві.

а) Коли $p\equiv 1$ (mod. 6), то $d=3$, отже одинична конґруенція $z^3\equiv 1$ (mod. p) має три розвязки: $1, \alpha, \alpha^2$, де $\alpha\equiv g^{\frac{p-1}{3}}$ Двочленна конґруенція (10) є рішима, коли $s^{\frac{p-1}{3}}\equiv 1$ (mod. p), нерішима, коли $s^{\frac{p-1}{3}}\equiv\alpha$ або α^2, отже коли один її корінь є r, то два другі є αr і $\alpha^2 r$. Єствує проте $\frac{p-1}{2}$ кубових останків, а $2.\frac{p-1}{3}$ не-останків; всї кляси чисел $GF[p]$ дїлять ся на три громади так, що кожде число i тої громади є $\equiv\alpha^i$ (mod. p) ($i=0, 1, 2$). Кубовий характер числа s значимо так:

$$\left[\frac{s}{p}\right]\equiv s^{\frac{p-1}{3}} \text{ (mod. } p). \tag{17}$$

б) $p\equiv -1$ (mod. 6); тодї є $p-1=6m-2$, отже $d=(6m-2, 3)=1$, проте крітерія звучить $s^{p-1}\equiv 1$ (mod. p). В такім разї всї числа $GF[p]^*$ є кубовими останками, отже двочленна конґруенція (10) є завсїди рішима, зате одинична конґруенція має тільки одну розвязку, $x\equiv 1$.

3) $n=4$. Тут мусимо розріжнити рівно-ж дві можливости: а) $p\equiv -1$ (mod. 4), б) $p\equiv +1$ (mod. 4).

а) Коли p має форму $4m-1$, то $p-1=4m-2$, отже $d=2$; одинична конґруенція $x^4\equiv 1$ (mod. p) може мати очивидно тільки дві розвязки: $+1$ і -1. Крітерія для двоквадратного характеру числа s є проте ідентична з Euler'овою для квадратних останків; отже кождий квадратний $\begin{Bmatrix}\text{останок}\\ \text{не-останок}\end{Bmatrix}$ є в тім разї і двократним $\begin{Bmatrix}\text{останком}\\ \text{не-останком}\end{Bmatrix}$ того самого числа — і навпаки.

б) В разї $p\equiv 1$ (mod. 4) є $p-1=4m$, отже $d=4$. Одинична конґруенція має чотири розвязки; $1, \alpha, \alpha^2, \alpha^3$, де $\alpha\equiv g^{\frac{p-1}{4}}$ З огляду на те, що $\alpha^2\equiv g^{\frac{p-1}{2}}$, а g є первісним коренем, отже належить до виложника $p-1$, є $\alpha^2\equiv -1$, а дальше $\alpha^3\equiv -\alpha$, проте корінї згаданої конґруенції можна написати також так: $1, \alpha, -1, -\alpha$.

Крітерією рішимости для $y^4\equiv s$ (mod. p) є тут $s^{\frac{p-1}{4}}\equiv 1$ (mod. p), а корінї тої конґруенції мають вартости $r, r\alpha, -r, -r\alpha$, де

$r^4 \equiv s$ (mod. p). Величина $s^{\frac{p-1}{4}}$ може приймати (mod. p) такі чотири вартости: ± 1, $\pm \alpha$; супроти того всї числа $GF[p]^*$ розпадають ся на чотири кляси, відповідно до того, до котрого з первісних четвертих корінїв одиницї (mod. p) є пристайна його $\frac{p-1}{4}$-ша степень.

Теорію двоквадратних останків перевів Gauss[1]), розширивши обсяг дїйсних чисел на числа форми $a + b\,i$, де i є коренем рівнаня $x^2 + 1 = 0$, а a і b належать до $GF[p]$; він дав тим чином початок теориї альґебраїчних чисел. Подібно ужив Eisenstein[2]) коріня рівнаня $x^3 = 1$, т. є величини $\varrho = \frac{-1 + i\sqrt{3}}{3}$, до збудованя теориї кубових останків.

§. 3.

11. Займемо ся тепер дальше теорією поля Galois. Ми сказали, що скількість всїх функций m-того степеня в $GF[p]$

$$f(x) = a_0\,x^m + a_1\,x^{m-1} + \qquad + a_m \qquad (1)$$

є $p^m(p-1)$ згл. p^m — відповідно тому, чи функциї, що ріжнять ся постійним чинником, будемо вважати ріжними поміж собою, чи однаковими.

Нехай $F_n(x)$ буде якою небудь незведимою функцією в $GF[p]$ степеня n; тодї конґруенция

$$F_n(x) \equiv 0 \text{ (mod. } p) \qquad (2)$$

не має корінїв в $GF[p]$. Длятого дефінїюємо, подібно як в альґебрі або теориї альґебраїчних чисел, її корінї як нові величини, необняті полем Galois степеня p. Отсї величини називають ся мнимими величинами Galois, бо він перший впровадив їх до теориї конґруенций.[3]) — З огляду на те, що конґруенция n-того степеня не може мати більше як n корінїв (уст. 7), дефінїює нам кожда незведима конґруенция (2) точно n ріжних, мнимих чисел Galois. Проте можемо висказати таку теорему (I), анальоґічну до основної теореми альґебри:

[1]) Theoria residuorum biquadraticorum, Commentatio I. et II., Gottingae 1829/32. — Werke Bd. II. — Пор. рівно-ж Bachmann, Die Lehre von der Kreisteilung, Leipzig 1872, Vorlesung 13—16.

[2]) Crelle's Journ., Bd. 27, 28. Bachmann, op. cit.

[3]) Galois, Sur la théorie des nombres, Bulletin des sciences mathém. de Férussac, 1830. — Oeuvres, p. 17., éd. Liouville 1946. — Abhandlungen über die algebraische Auflösung von Gleichungen, von Abel und Galois, herausg. v. Maser, Berlin 1889, p. 100—107.

Кожда конґруенція n-того степеня з первочисельним модулом має рівно n корінів.

12. Утворім функцію (1) з незвісною x. Коли $m \geq n$, то при помочи конґруенції (2) можна зредукувати всї степені незвісної, висші від $n - 1$, так що зістане нам тільки

$$f(x) = a_0 x^{n-1} + a_1 x^{n-2} + \quad a_{n-1}, \tag{1a}$$

де сочинникови a_0 не накладаємо нїякого обмеженя.

Теорема II. Скількість функцій (1a) є p^n.

Доказ. Що скількість функцій $f(x)$ (степенів 0, 1, 2, . ., n -1), не може бути більша як p^n, слїдує звідси, що кождий з n сочинників може приймати тільки p вартостей. Але вона не може бути менша від p^n, бо коли-б було $f(x) \equiv g(x)$ (mod. p), то звідси слїдувало би

$$(a_0 - b_0) x^{n-1} + (a_1 - b_1) x^{n-2} + \ldots + (a_{n-1} - b_{n-1}) \equiv 0 \pmod{p},$$

де b_i є сочинниками функції $g(x)$. Тому x було би коренем конґруенції степеня низшого нїж n, т. зн. функція $F_n(x)$ мала би з функцією низшого степеня спільний чинник, отже не могла би бути незведима. Отже дві функції $f(x)$ є тільки тодї рівні згл. пристайні, коли їх дотичні сочинники належать (mod. p) до однакових кляс, а такі функції ми вважаємо ідентичними.

13. **Теорема III.** Кожда функція $f(x)$ сповнює конґруенцію

$$X^{p^n} \equiv X \pmod{p}. \tag{3}$$

Доказ. Напишім всї функції $f(x)$ з виїмком тої, якої всї сочинники належать до кляси K_0; їх буде $p^n - 1$:

$$f_1(x), f_2(x), \quad ., f_{p^n-1}(x). \tag{4}$$

Помножім ті всї величини якою небудь з поміж них, X:

$$Xf_1(x), Xf_2(x), \quad Xf_{p^n-1}(x). \tag{4a}$$

Оба ряди, (4) і (4a), складають ся з тих самих величин, тільки в иншім порядку, то-ж і добутки всїх величин кождого ряду є до себе (mod. p) пристайні:

$$f_1 f_2 \quad . f_{p^n-1} \equiv f_1 f_2 \quad f_{p^n-1} X^{p^n-1} \quad \pmod{p}$$

Обі сторони можна скоротити добутком $f_1 f_2 \quad . f_{p^n-1}$, бо нї один його чинник не є пристайний до 0 (mod. p); длятого маємо

$$X^{p^n-1} \equiv 1 \pmod{p} \tag{3a}$$

або

$$X^{p^n} \equiv X \pmod{p}.$$

Отсей взорець є новим узагальненем теореми Fermat'a.

Заключене. 1) Конґруенція (3а) має $p^n - 1$ корінів, обнятих рядом (4). Проте можемо функцію $X^{p^n - 1}$ розложити на добуток

$$X^{p^n} - 1 \equiv \big(X - f_1(x)\big)\,\big(X - f_2(x)\big)\,.\quad \big(X - f_{p^n-1}(x)\big) \pmod{p}.$$

2) Порівнуючи обі сторони тої ідентичної конґруенції і означуючи через σ_1, σ_2, $\quad \sigma_{p^n-1}$ основні симетричні функції величин $f_k(x)$, бачимо, що

$$\sigma_1 \equiv \sigma_2 \equiv \quad \equiv \sigma_{p^n-2} \equiv 0,\ \sigma_{p^n-1} \equiv -1 \pmod{p}.$$

отже
$$\prod_{k=1}^{p^n-1} f_k(x) + 1 \equiv 0 \pmod{p}. \tag{5}$$

Отсе є узагальнене теорема Wilson'a.[1])

3) З окрема зазначімо, що $\sigma_1 \equiv 0 \pmod{p}$, т. зн.

$$\sum_{k=1}^{p^n-1} f_k(x) \equiv 0 \pmod{p}. \tag{6}$$

14. Теорема IV. Загал функцій (1а) або (4) творить поле Galois.

Доказ. Величини (4) репродукують ся через чотири основні операції. Що сума, ріжниця й добуток двох $f(x)$ мають опять ту саму форму, се очивидне; треба тільки ще до ряду (4) дібрати величину 0. Але і квот двох $f(x)$ належить рівно-ж до ряду (4). — Нехай буде дана реляція

$$f(x) \equiv g(x)\,h(x) \pmod{p};$$

тоді при даних $f(x)$ і $g(x)$ можна найти все одну і тільки одну таку функцію $h(x)$, яка сповнюватиме ту реляцію [виключивши $g(x) \equiv$ ідентично $0 \pmod{p}$]. Помножім обі її сторони через $\big[g(x)\big]^{p^n-1}$, то з огляду на (3а) буде

$$h(x) \equiv f(x)\,\big[g(x)\big]^{p^n-2} \pmod{p};$$

отсе оправдує уживати на означене квота символічного взірця

$$h(x) \equiv \frac{f(x)}{g(x)} \pmod{p}.$$

Проте можемо сказати так:

Загал многочленів в $GF[p]$ степеня $(n-1)$-ого[2]) творить поле Galois степеня p^n, коли за змінчиву x прий-

[1]) Теорема Wilson'a звучить: $(p-1)! + 1 \equiv 0 \pmod{p}$; вона є характеристична для первих чисел.

[2]) т. зн. всіх степенів, почавши від 0, до $(n-1)$-ого вкл.

мемо один з инших корінів якоїсь незведимої конґруенції степеня n.

Поле Galois степеня p^n означуємо за Dickson'ом $GF[p^n]$[1]), а коли виключуємо з нього елемент 0, то зазначимо се, подібно, як попередно, $GF[p^n]^*$ і називаємо зредукованим полем Galois.

15. **Теорема V.** Коли в $f(x)$ заступимо x через x^p, то $f(x)$ перемінить ся в свою p-ту степень.

Доказ. Піднесім $f(x)$ (1a) до степені p; се дасть:

$$[f(x)]^p = a_0{}^p (x^p)^{n-1} + a_1{}^p (x^p)^{n-2} + \quad + a_{n-1}^p + g(x),$$

де $g(x)$ є сумою всїх прочих членів, отже членів з многочленними сочинниками (Binomialkoeffizienten), а вони всї є многократями числа p. Примінюючи теорему Fermat'а, $a^p \equiv a$ (mod. p), маємо

$$[f(x)]^p \equiv a_0 (x^p)^{n-1} + a_1 (x^p)^{n-2} + \quad + a_{n-1} \text{ (mod. } p),$$

отже

$$[f(x)]^p \equiv f(x^p) \text{ (mod. } p). \qquad (7)$$

Тому, коли x заступити через x^p, то $f(x)$ перейде в $[f(x)]^p$, т. є кожде X в X^p.

Замітка. Повторюючи сю операцію n разів, одержимо:

$$\left.\begin{aligned} f(x^p) &\equiv [f(x)]^p, \\ f(x^{p^2}) &\equiv [f(x)]^{p^2}, \\ & \\ f\left(x^{p^{n-1}}\right) &\equiv [f(x)]^{p^{n-1}}, \\ f\left(x^{p^n}\right) &\equiv [f(x)]^{p^n} \equiv f(x). \end{aligned}\right\} \text{ (mod. } p),$$

17. Виконаймо отсю субституцію в данїй конґруенції

$$F_n(x) \equiv 0 \text{ (mod. } p); \qquad (2)$$

се дасть:

$$F_n(x^p) \equiv [F_n(x)]^p \equiv 0 \text{ (mod. } p)$$

отже коли x є коренем конґруенції (2), то x^p є її другим коренем. Так само є $F_n\left(x^{p^2}\right) \equiv 0$, $F_n\left(x^{p^3}\right) \equiv 0, \ldots, F_n\left(x^{p^{n-1}}\right) \equiv 0$ (mod. p), отже

Теорема VI. Корінї незведимої конґруенції (2) є

$$x,\ x^p,\ x^{p^2}, \qquad x^{p^{n-1}},$$

де x означує який небудь з її корінів.

---

[1]) Лїтература про поле Galois: Schoenemann, Grundzüge einer allg. Theorie d. höh. Kongr. Crelle's Journal, Bd. 31 (1846) стр. 269—325. Dedekind, Abriss einer Theorie d. höh. Kongr. Crelle, Bd. 54 (1857) стр. 1—26. Dickson, Linear groups etc. стр. 1—71. Scarpis, Exposizione elementare della teoria del campo di Galois, Battaglini Annali, t. XLIV. (1907), p. 153—180.

Отсї величини, се власне мнимі числа, які ввів Galois.

Примір. Конґруенція

$$F_3(x) = x^3 - 3x + 1 = 0 \ (\mathrm{mod.}\ 7)$$

є в $GF[7]$ незведима. Коли x є її коренем, то два другі корінї є x^7 і x^{49}; їх можна зредукувати до многочленів найвисше другого степеня при помочи даної конґруенції. Іменно є $x^3 \equiv 3x - 1$, отже $x^7 = (x^3)^2 . x$, а що $(x^3)^2 \equiv 2x^2 + x + 1$, то $x^7 \equiv 2x^3 + x^2 + x \equiv 2(3x - 1) + x^2 + x \equiv x^2 - 2$; дальше є: $x^{49} = (x^7)^7 \equiv (x^2 - 2)^7 = (x^2 - 2)\ [(x^2 - 2)^3]^2$, а що $(x^2 - 2)^3 \equiv x^6 + x^4 - 2x^2 - 1$, то з огляду на $x^6 + x^4 \equiv - 2x^2 + 1$, маємо $(x^2 - 2)^3 \equiv 3x^2$. Квадрат тої остатньої величини є $9x^4 \equiv - x^2 - 2x$, а помножений через $x^2 - 2$ дає $- x^4 - 2x^3 + 2x^2 - 3x \equiv \quad x^2 - x + 2$, отже коли x є одним коренем даної конґруенції, то оба другі коріеї є $x^7 \equiv x^2 - 2$, $x^{49} \equiv - x^2 - x + 2$. Легко провірити, що $x(x^2 - 2)(\quad x^2 - x + 2) \equiv - 1 \ (\mathrm{mod.}\ 7)$.

17. Напишім ряд степений одної з величин в $GF[p^n]$:

$$1,\ X,\ X^2,\ X^3,\ \ldots;$$

отсей ряд не є безконечний, тільки повторюють ся в періодах що найвисше $(p^n - 1)$-членних, бо $X^{p^{n-1}} \equiv 1 \ (\mathrm{mod.}\ p)$. Але можливе є й таке, що якась низша степень величини X, пр. s-та, буде пристайна до 1. Коли s є найменшим таким виложником, для якого є

$$X^s \equiv 1 \ (\mathrm{mod.}\ p), \tag{8}$$

тодї кажемо, що X належить (mod. p) до виложника s.

Теорема VII. Виложник s, до якого належить яка небудь з величин з $GF[p^n]$, є подїльником числа $p^n - 1$.

Доказ. Нехай s не буде подїльником числа $p^n - 1$; тодї можемо написати так:

$$p^n - 1 = st + r,\ 0 < r < s.$$

Підносячи (6) до степені t, маємо

$$X^{st} \equiv 1 \ (\mathrm{mod.}\ p),$$

а що задля (3a)

$$X^{st+r} \equiv 1 \ (\mathrm{mod.}\ p),$$

то мусїло би бути також $X^r \equiv 1$ (mod. p). Се неможливе, коли $0 < r < s$, бо s є найменшим виложником, для якого сповнюють ся вимога (8). Проте мусить бути $r = 0$, отже

$$s = \frac{p^n - 1}{t}.$$

18. Величину X, яка належить до виложника $p^n - 1$, називаємо первісною величиною в $GF[p^n]$, подібно як число g, яке (mod. p) належить до виложника $p - 1$, назвали ми первісним коренем модула p або первісною величиною в $GF[p]$ (уст. 9).

Теорема VIII. Ціле $GF[p^n]^*$ можна представити рядом степенів котрої небудь первісної величини X того поля.

Доказ. Коли X є первісною величиною в $GF[p^n]$, то ряд

$$1, X, X^2, \ldots, X^{p^n-2} \qquad (9)$$

складаєть ся з $p^n - 1$ поміж собою ріжних величин того поля, бо реляція

$$X^k \equiv X^l \ (\text{mod. } p)$$

можлива тільки тоді, коли $k \equiv l$ (mod. $p^n - 1$); коли-ж k і l є $\leqq p^n - 2$, то се можливе тільки так, що $k = l$, отже два члени з ряду (9) з ріжними виложниками не можуть бути до себе пристайні (mod. p). — Супроти того, що кожде X^k є якоюсь величиною з $GF[p^n]$,

$$X^k \equiv f_k(x) \ (\text{mod. } p),$$

є ряд (9) ідентичний з $GF[p^n]^*$.

§. 4.

19. Незведиму функцію n-того степеня в $GF[p]$, $F_n(x)$, при помочи якої ми конструували $GF[p^n]$, називаємо модуловою функцією (Modularfunktion).

Нехай буде $\Phi(x)$ якоюнебудь функцією в $GF[p]$. Коли її степень r є менший від n, тоді $\Phi(x)$ належить вже прямо до $GF[p^n]$; коли-ж $r \geqq n$, тоді можемо написати її у виді

$$\Phi(x) = f(x) + \varphi(x) F_n(x) + p\,\psi(x), \qquad (1)$$

де $f(x)$ є одною з величин в $GF[p^n]$, $\varphi(x)$ функцією степеня $r - n$, а $\psi(x)$ якоюнебудь функцією в $GF[p]$. В такім разї називаємо — розширюючи понятє пристайности — $\Phi(x)$ пристайним до $f(x)$ з огляду на подвійний модул p, $F_n(x)$ і пишемо

$$\Phi(x) \equiv f(x) \ [\text{modd. } p, F_n(x)]^{1)}. \qquad (1\text{a})$$

Супроти того можемо всї цілі функції з цілочисельними сочинниками подїлити на p^n кляс; кожду з тих кляс будемо характеризувати тою функцією $f(x)$ з $GF[p]$, до котрої вона пристайна [modd. p, $F_n(x)$]. Тих репрезентантів будемо називати, подібно, як в теорії цїлих чисел, повною системою найменших останків подвійного модула p, $F_n(x)$.

Нехай X означує якунебудь цїлу функцію з цїлочисельними сочинниками, отже

$$X = f(x) + \varphi(x) F_n(x) + p\,\psi(x);$$

підносїм се рівнанє чергою до степений $p, p^2, \ldots, p^n$. Через се одержимо:

[1]) Означене походить від Serret'a, Algèbre, t. II, стр. 165 (5 вид.).

$$X^{p} = \left[f(x)\right]^{p} + \left[\varphi(x)\right]\left[F_{n}(x)\right]^{p} + p\,\psi_1(x),$$
$$X^{p^2} = \left[f(x)\right]^{p^2} + \left[\varphi(x)\right]^{p^2}\left[F_2(x)\right]^{p^2} + p\,\psi_1(x),$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$X^{p^n} = \left[f(x)\right]^{p^n} + \left[\varphi(x)\right]^{p^n}\left[F_n(x)\right]^{p^n} + p\,\psi_n(x),$$

де функції $\psi_1(x)$, $\psi_2(x)$., близше нас не обходять. Ті рівнаня є рівнозначні з системою конґруенцій

$$\left.\begin{aligned} X^{p} &\equiv f(x^{p}),\\ X^{p^2} &\equiv f\left(x^{p^2}\right),\\ &\ \ \vdots\\ X^{p^n} &\equiv f\left(x^{p^n}\right), \end{aligned}\right\}\ [\text{modd. } p,\ F_n(x)],$$

а що $f\left(x^{p^n}\right) \equiv f(x)$ (mod. p) $\equiv X$ [modd. p, $F_n(x)$], то

$$X^{p^n} \equiv X\ [\text{modd. } p,\ F_n(x)]. \tag{2}$$

Теорема I. Кожда ціла функція з цілочисельними сочинниками сповнює реляцію (2), або иншими словами:

Функція $X^{p^n} - X$ є (mod. p) подільна через модулову функцію $F_n(x)$.

20. Взорець (2) можемо написати ще так:

$$X^{p^n} - X \equiv \varphi(x)\,F_n(x)\ (\text{mod. } p),$$

а що він є важний для кождої величини X в $GF[p^n]$, то можемо підставити також $X = x$, отже будемо мати

$$x^{p^n} - x \equiv \varphi(x)\,F_n(x)\ (\text{mod. } p), \tag{3}$$

тому:

Теорема Ia. Функція $x^{p^n} - x$ є (mod. p) подільна через модулову функцію $F_n(x)$.

Теорема II. Функція $x^{p^m} - x$ є тільки тоді (mod. p) подільна через модулову функцію $F_n(x)$, коли m є многократю виложника n.

Доказ. Коли $m = kn$, то $x^{p^m} - x$ є подільне через $x^{p^m} - x$, отже теорема доказана. Коли-ж m не є многократю n, $m = kn + r$, $0 < r < n$, то з діленя $\left(x^{p^m}\right)$ $\left(x^{p^n}\right)$ випадає останок $x^{p^r} - x$. Отсей многочлен не є подільний через $F_n(x)$, бо $x^{p^n} - x$ і $x^{p^r} - x$ не мають крім x і $x - 1$ ніякого спільного чинника, проте неможлива реляція форми $x^{p^r} - x \equiv \chi(x)\,F_n(x)$ (mod. p) для $0 < r < n$.

21. Отсї теореми дають нам змогу обчислити скількість незведимих (mod. p) в $GF[p]$ функцій n того степеня. Розложім іменно праву сторону конґруенції (3) на незведимі чинники:

$$x^{p^n} - x \equiv x\,F_n(x)\,G(x)\,H(x) \qquad K(x) \ (\mathrm{mod.}\ p).$$

Поміж ними нема двох однакових, бо ліва сторона не має спільного чинника зі своєю похідною.

В ряді

$$x,\ F_n(x),\ G(x),\ H(x), \quad .,\ K(x)$$

містять ся всї незведимі функції n-того степеня, бо ми можемо кожду з них приймити за модулову функцію, а що модулова функція містить ся все в $x^{p^n} - x$, то в згаданім рядї мусять виступати всї такі функції, які можуть грати ролю модулових. — Крім них можуть містити ся в тім рядї незведимі функції тілько таких степенів, які є подїльні через n; слїдує се з теореми II

Проте, коли з $x^{p^n} - x$ виділити добутки всїх незведимих функцій степенїв менших від n, то одержимо добуток всїх незведимих функцій n-того степеня.

Нехай n буде первим числом; тодї з $x^{p^n} - x$ треба усунути добуток всїх лїнійних чинників, проте добуток всїх незведимих (mod. p) функцій первого степеня n є

$$V = \frac{x^{p^n} - x}{x^p - x},$$

а його степень є $p^n - p$. Проте скількість незведимих (mod. p) функцій степеня n є

$$\lambda_n = \frac{1}{n}(p^n - p).$$

Коли n є зложеним числом,

$$n = a^\alpha\, b^\beta \qquad e^\varepsilon,$$

то з $x^{p^n} - x$ мусимо усунути добутки всїх незведимих чинників, яких степенї є подїльниками числа n. Вводячи скорочене

$$x^{p^\lambda} - x = [\lambda],$$

переконаємо ся легко, що бажаний добуток є

$$V = \frac{[n]\,\Pi\left[\frac{n}{d_1 d_2}\right]\Pi\left[\frac{n}{d_1 d_2 d_3 d_4}\right]\cdot\cdot}{\Pi\left[\frac{n}{d}\right]\Pi\left[\frac{n}{d_1 d_3 d_3}\right]},$$

де $d,\ d_1,\ d_2,\ d_3,$ перебігають всї чинники числа n. Степень тої функції є

$$p^n - \sum p^{\frac{n}{d}} + \sum p^{\frac{n}{d_1 d_2}} - \sum p^{\frac{n}{d_1 d_2 d_3}} +$$

отже скількість всїх незведимих функцій n-того степеня є

$$\lambda_n = \frac{1}{n}\left[p^n - \sum p^{\frac{n}{d}} + \sum p^{\frac{n}{d_1 d_2}} - \sum p^{\frac{n}{d_1 d_2 d_3}} + \quad\right]. \quad (4)$$

22. Результати з уст. 16. можна узагальнити при помочи пристайности з подвійним модулом.

1) Кожда функція в $GF[p]$ належить [modd. p, $F_n(x)$] до якогось виложника, що є подільником числа $p^n - 1$; т. зн., коли s є найменшим виложником, для якого

$$X^s \equiv 1 \text{ [modd. } p,\ F_n(x)], \quad (5)$$

то $p^n - 1$ є подільне через s.

2) Коли $s = p^n - 1$, то X називаєть ся первісною величиною в $GF[p^n]$ при подвійнім модулї p, $F_n(x)$. — При помочи степенїв первісної величини X можемо представити цїле $GF[p^n]$.

3) З (5) слїдує безпосередно, що $F_n(x)$ містить ся (mod. p) в $X^s - 1$, отже і в $x^s - 1$.

Дальше докажемо таку

Теорему III. До виложника s належить [modd. p, $F_n(x)$] $\varphi(s)$ ріжних величин з $GF[p^n]$.

Доказ. Коли X належить [modd. p, $F_n(x)$] до виложника s, то в рядї

$$1,\ X,\ X^2, \qquad X^{s-1}$$

є всї величини поміж собою ріжні, а s-та степень кождої з них є $\equiv 1$, бо для кождого $k < s$ є

$$(X^k)^s = (X^s)^k \equiv 1 \text{ [modd. } p,\ F_n(x)].$$

Треба ще тільки найти виложник, до якого належить довільне X^k.

1) Нехай буде $(k, s) = 1$; тодї в рядї k, $2k$, ., $(s-1)k$ нема нї одної многократи числа s, отже нїяке X^{tk} не може бути $\equiv 1$, коли $t < k$, тому X^k належить до виложника s.

2) Коли $(k, s) = d < 1$, то $\left(X^k\right)^{\frac{s}{d}} = \left(X^{\frac{k}{d}}\right)^s \equiv 1 \text{ [modd.} p, F_n(x)]$ а що $\frac{k}{d}$ і s є супроти себе перві, то X^k належить до виложника $\frac{s}{d}$.

Назвім $\psi(d)$ скількість величин X, що належить до виложника d; з огляду на те, що кожде X належить до якогось чинника числа $p^n - 1$ як виложника, маємо

$$\sum_{d/p^n-1} \psi(d) = p^n - 1.$$

З другої сторони є $\Sigma\varphi(d) = p^n - 1$, отже

$$\sum_{d/p^n-1} \psi(d) = \sum_{d/p^n-1} \varphi(d),$$

т. зн. кожде $\psi(d) =$ або 0 або $\varphi(d)$. Перше є виключене, бо тоді було би $\Sigma \psi(d) = 0$, друге дає

$$\psi(d) = \varphi(d),$$

отже наша теорема доказана.

Заключенє. В $GF[p^n]$ є $\varphi(p^n - 1)$ первісних величин $[\text{modd. } p, F_n(x)]$, т. є таких, що належать до виложника $p^n - 1$.

23. **Теорема IV.** Коли X_1 і X_2 належать до виложників s_1 згл. s_2, то $X_1 X_2$ належить до виложника, який є найменшою спільною многократю чисел s_1 і s_2.

Доказ. Після заложеня є

$$X_1^{s_1} \equiv 1, \; X_2^{s_2} \equiv 1 \; [\text{modd. } p \; F_n(x)].$$

Нехай буде v виложником, до якого належить $X_1 X_2$ т. зн. найменшим виложником, для якого є

$$(X_1 X_2)^v \equiv 1 \; [\text{modd. } p, \; F_n(x)];$$

$НСП$ чисел s_1 і s_2 назвім d. Піднесім ту конґруенцію до степени $\frac{s_1}{d}$; се дасть

$$X_1^{\frac{v s_1}{d}} X_2^{\frac{v s_2}{d}} \equiv 1 \; [\text{modd. } p, \; F_n(x)]$$

Тому, що $\left(\frac{s_1}{d}, s_2\right) = 1$, та конґруенція не може бути сповнена инакше, як тільки так, що і $X_1^{\frac{v s_1}{d}} \equiv 1$, і $X_2^{\frac{v s_1}{d}} \equiv 1$. Перша реляція вказує, що v мусить бути подїльне через d, друга, що $\frac{vs_1}{d}$ є многократю числа s_2. Так само побачимо, що $\frac{vs_2}{d}$ є многократю числа s_1, отже v многократю чисел s_1 і s_2; а що v має бути найменшим числом того рода, то наша теорема доказана.

Заключеня. 1) Коли величини $X_1, X_2, \ldots X_k$ належать до виложників $s_1, s_2, \ldots, s_k$, то виложник, до якого належить добуток $X_1 X_2 \ldots X_k$, є найменшою спільною многократю тамтих виложників.

2) Коли $p^n - 1 = a^\alpha b^\beta \ldots$ $(a, b, \ldots$ первi числа), а $X_a, X_b, \ldots$ належать до виложників a^α, b^β, то добуток $X_a X_b \ldots$ є первісною величиною в $GF[p^n]$.

24. **Функцію** $X = f(x)$ з $GF[p]$ називаємо коренем конґруенції

$$\Phi(y) \equiv 0 \; [\text{modd. } p, \; F_n(x)], \tag{6}$$

коли X підставлене в нїй за y, зводить її до виду

$$\Phi(X) = \varphi(x) \; F_n(x) + p \, \psi(x).$$

Теорема V. Конґруенція (6) не може мати більше корінїв, як виносить її степень. Коли степень конґруенції m є рівний n або є подільником того числа, то конґруенція має точно m корінїв.

Доказ. Що конґруенція m-того степеня не може мати більше ріжних корінїв як m, слїдує з елементарної теореми I. в §. 2.

Нехай дальше буде m подільником числа n; тодї всї функції в $GF[p^n]$ є корінями конґруенції

$$X^{p^n} - X \equiv 0 \; [\text{modd. } p, \; F_n(x)]. \qquad (2)$$

З другої сторони є $X^{p^n} - X$ подїльне (mod. p) через кожду величину з $GF[p^n]$, отже і через $\Phi(x)$:

$$X^{p^n} - X \equiv \Phi(X)\, \Psi(X) \; (\text{mod. } p),$$

отже

$$\Phi(X)\, \Psi(X) \equiv 0 \; [\text{modd. } p, \; F_n(x)]$$

має ті самі корінї що (2). Через те розпадають ся всї величини з $GF[p^n]$ на корінї одної з двох конґруенцій

$$\left.\begin{array}{l} \Phi(X) \equiv 0, \\ \Psi(X) \equiv 0 \end{array}\right\} [\text{modd. } p \;\; F_n(x)].$$

Перша з них є степеня m, друга степеня $p^n - m$; коли-б перша мала менше як m корінїв, то друга мусїла-б їх мати більше, нїж виносить її степень.

25. **Теорема VI.** Коли $\Phi(x)$ є функцією m-того степеня в $GF[p]$, то все можна найти таку незведиму (mod. p) функцію $F(x)$ в $GF[p]$, що конґруенція

$$\Phi(X) \equiv 0 \; [\text{modd. } p, \; F(x)]$$

буде мати точно m-корінїв.

Доказ. Розложім $\Phi(X)$ на незведимі (mod. p) чинники з $GF[p]$ степенів $m_1, m_2, \ldots, m_\mu$:

$$\Phi(X) \equiv \Phi_1(X)\, \Phi_2(X) \ldots \Phi_\mu(X) \; (\text{mod. } p);$$

кождий з них буде містити ся (mod. p) в одній з функцій

$$X^{p^{m_1}} - X, \; X^{p^{m_2}} - X, \ldots X^{p^{m_\mu}} - X,$$

а коли n є *нсм*[1]) чисел $m_1, m_2 \ldots m_\mu$, то всї ті функції містять ся знова в $X^{p^n} - X$.

Коли-ж тепер взяти якунебудь незведиму функцію в $GF[p]$ степеня n, то кожда з конґруенцій $\Phi_k(x) \equiv 0$ буде мати при тім самім подвійнім модулї p, $F(x)$ на основі теореми IV. m_k корінїв. Проте добуток тих функцій $\Phi_k(x)$ сповняє вимоги нашої теореми.

[1]) т. є. найменша спільна многократь.

26. **Теорема VII.** Коли X є корінем конґруенції (6), то прочі її коріні є X^p, X^{p^2} ., $X^{p^{n-1}}$

Доказ. Подібно як в уст. 52 знаходимо, що

$$\left[\Phi(X)\right]^{p^k} \equiv \Phi\left(X^{p^k}\right) \equiv 0 \ [\text{modd. } p, F_n(x)]$$

для $k = 0, 1,$ $n-1$, та що дві ріжні степені з повисшого ряду є поміж собою ріжні. Отже теорема доказана.

Заключене. Конґруенція $F_n(x) \equiv 0$ (mod. p) т. зн. $F_n(x) \equiv 0$ [modd. p, $F_n(x)$] має такі коріні: x, x^p, x^{p^2}, $x^{p^{n-1}}$

27. **Теорема VIII.** Поле Galois не залежить від модулової функції.

Доказ. В уст. 21 мали ми такий розклад:

$$x^{p^n} - x \equiv F_n(x)\, G_n(x) \quad . K_n(x)\, L(x) \quad P(x) \ (\text{mod. } p);$$

тут означують $F_n(x)$, $G_n(x)$ $K_n(x)$ незведимі функції степеня n, $L(x)$, ., $P(x)$ функції прочих допустимих степенів. Коли x є елементом з $GF[p^n]$, то

$$x^{p^n} - x \equiv 0 \ (\text{mod. } p),$$

отже

$$F_n(x) \ G_n(x) \qquad K_n(x)\, S(x) \equiv 0 \ (\text{mod. } p),$$

де в $S(x)$ зъединені всї функції низших степенїв, — т. зн., що x може бути коренем одної, і тільки одної, з поміж незведимих конґруенцій

$$\left.\begin{array}{l} F_n(x) \equiv 0, \\ G_n(x) \equiv 0, \\ \\ K_n(x) \equiv 0 \end{array}\right\} \ (\text{mod. } p).$$

Проте можемо за модулову функцію взяти котрунебудь з них, а поле Galois через те не змінить ся.

Примір. В $GF[7]$ є незведимими функціями нпр. $x^3 - 2$ і $x^3 - 3$. Коли приймемо за модулову функцію першу з них, творимо $GF[7^3]$ як загал функцій

$$f(i) = a_0\, i^2 + a_1\, i + a_2 \ (\text{mod. } 7),$$

де i дане конґруенцією $i^3 \equiv 2$ (mod. 7). Коли хочемо представити те саме поле Galois при помочи функції $x^3 - 3$, назвім j корінь кон ґруенції $j^3 \equiv 3$ (mod. 7), тоді $GF[7^3]$ є дане функцією

$$g(j) = b_0\, j^2 + b_1\, j + b_2 \ (\text{mod. } 7),$$

Величини i і j можна виразити одну через другу. Іменно одержуємо через помноженє обох дефініцийних конґруенцій

$$i^3 j^3 \equiv -1 \ (\text{mod. } 7),$$

отже $ij \equiv 3$ або 3α або $3\alpha^2$, де α дане реляцією $\alpha^2 + \alpha + 1 \equiv 0$ (mod. 7), т. зн. $\alpha \equiv 2$. Проте є пр. $ij \equiv 3$. Помножім ту конґруенцію через j^2, то одержимо $i^3 j \equiv 3$, т. зн. $j \equiv -2 i^2$ (mod 7), а дальше $j^2 \equiv i$, т. зн.

$$g(j) \equiv -2 b_1 i^2 + b_0 i + b_2 \pmod{7}.$$

Нпр. величина $g(j) = j^2 - 2j - 3$ відповідає величині $f(i) = 4 i^2 + i - 3$, бо з $j \equiv -2 i^2$ слідує $j^2 \equiv 4 i^4 \equiv 4 i^3 . i \equiv i$.

28. **Теорема IX.** Степенем поля Galois може бути тільки степень первого числа.

Доказ. Ми бачили в уст. 4, що поле Galois найнизшого степеня складаєть ся з p елементів, коли p є первим числом. Нехай x_1 буде одною з величин поля Galois степеня висшого ніж p; тоді формулка $c_1 x_1$, де c_1 належить до $GF[p]$, т. є ряд величин $0 x_1$, $1 x_1$, $2 x_1$, ... $(p-1) x_1$, не вичерпують ще цілого поля. Проте мусить єствувати ще якась инша величина x_2, не обнята тамтим рядом. Утворім всї можливі суми

$$c_1 x_1 + c_2 x_2,$$

де c_1 і c_2 перебігають ціле $GF[p]$; скількість тих сум виносить p^2, бо тільки одна з них є 0, а однакових поміж ними нема. — Ті суми або вичерпують поле Galois, або ні. В першім разї маємо $GF[p^2]$, в другім разї єствує ще нова величина x_3, при помочи якої творимо дальші суми

$$c_1 x_1 + c_2 x_2 + c_3 x_3$$

і т. д. Таким чином бачимо, що степень поля Galois може бути тільки степенню первого числа; отже можна дібрати таких n елементів x_1, x_2, ... x_n, що всї можливі комбінації чисел з $GF[p]$ в сочинниках суми

$$X = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n \pmod{p} \qquad (7)$$

вичерпують ціле $GF[p^n]$. — Таких n елементів називаємо основою поля Galois.

Теорема X. Перших $n-1$ степенів кождої первісної величини з $GF[p^n]$, $1, x, x^2, \ldots, x^{n-1}$ творять основу поля Galois (пор. теорему VIII, уст. 18).

Теорема XI. Поміж величинами (7) є тільки одна ідентично пристайна (mod. p) до зера, або иншими словами: елементи основи поля Galois є лїнїйно незалежні.

Доказ. Кождий з елементів основи $GF[p^n]$ є (mod. p) пристайний до одної з первісних величин x того поля (уст. 18), отже суму X можемо звести до виду

$$X \equiv c'_1 + c'_2 x + c'_3 x^2 + \cdots + c'_n x^{n-1} \pmod{p}.$$

Реляція $X \equiv 0$ можлива тільки так, що всї $c'_k \equiv 0$ (mod. p); коли-б так не було, то первісна величина $GF[p^n]$ сповнювала би конґруенцію степеня низшого як n, а се неможливе, бо x є корінем незведимої конґруенції степеня n. — Отже поміж елементами основи поля Galois не може єствувати ніяка инша лінійна звязь, як тільки та, що всї сочинники є $\equiv 0$ (mod. p), т. зн. ті елементи є лінійно незалежні[1]).

§. 5.

29. Щоби знайти первісні корінї конґруенції

$$X^{p^n} - X \equiv 0 \;[\text{modd. } p,\, F_n(x)], \qquad (1)$$

маємо після уст. 23 (заключене 2) вишукати первісні корінї конґруенцій

$$\left.\begin{aligned} X^{a^\alpha} &\equiv 1, \\ X^{b^\beta} &\equiv 1, \\ &\ldots \end{aligned}\right\} [\text{modd } p,\, F_n(x)],$$

де $a^\alpha\, b^\beta \ldots = p^n - 1$, і утворити їх добуток.

Коли модулова функція $F_n(x)$ належить (mod. p) до виложника $p^n - 1$, то всї її корінї є первісними величинами в $GF[p^n]$.

30. Коли знайдемо одну з незведимих (mod. p) функцій степеня n в $GF[p]$, $F_n(x)$, шукаємо при її помочи первісного кореня конґруенції (1). Тодї можемо розложити лїву сторону тої конґруенції на незведимі чинники.

Нехай X буде первісним корінем конґруенції (1); його k-та степень буде сповнювати якусь незведиму в $GF[p]$ конґруенцію

$$\Phi(x) \equiv 0 \;[\text{modd } p,\, F_n(x)] \qquad (2)$$

степеня $m = n$ або $\frac{n}{d}$; корінї тої конґруенції будуть

$$X^k,\; X^{kp},\; X^{kp^2},\; \ldots\; X^{kp^{m-1}},$$

отже будемо мати

$$\Phi(u) \equiv (u - X^k)(u - X^{kp})\left(u - X^{kp^2}\right) \ldots \left(u - X^{kp^{m-1}}\right) \;[\text{modd. } p,\, F_n(x)],$$

Тому, що $X^{kp^m} \equiv X^k$, отже $X^{k\,(p^m-1)} \equiv 1$ [modd. p, $F_n(x)$], мусить бути виложник $k(p^m - 1)$ многократю числа $p^n - 1$, отже m мусить бути таким найменшим числом, для якого $p^m - 1$ є подїльне через n; се висказуєть ся так, що X відповідає (passt) виложникови m.[2])

Коли X^k належить до виложника s, то ks є подїльне через $p^n - 1$, отже s є многократю числа n, а що отся конґруенція спов-

---

[1]) Пор. анальоґічну теорему в теорії альґебраїчних чисел. Гл. пр. Weber, Algebra, Bd. II (2 Aufl.), §. 161.

[2]) Encyklopädie der math. Wiss. Bd. I. 1, p. 575.

нюєть ся для $n = s$, то X^k належить до виложника n. Але і $\Phi(X)$ належить до того самого виложника, як се легко провірити; проте коли хочемо найти всї незведимі конґруенції степеня n і всїх инших допустимих степенів, беремо за k якунебудь многократь числа m, перву супроти n.

31. Galois пояснює свою теорію на такім примірі: знайти незведиму конґруенцію, від якої залежать первісні корінї двочленної конґруенції

$$X^{7^3} \equiv X \pmod{7}. \qquad (*)$$

Тут є $p = 7$, $n = 3$. Одною з незведимих (mod. 7) функцій третього степеня є $x^3 - 2$, отже творимо $GF[7^3]$ з функцій

$$f(x) = a_0 x^2 + a_1 x + a_2 \ [\text{modd. } 7,\ x^3 - 2].$$

Нашою задачею є, знайти таку величину $X = f(x)$, якої всї степени, від зерової до $(7^3 - 1)$-ої включно, мають вичерпати всї корінї конґруенції

$$X^{7^3-1} - 1 \equiv X^{2.3^2.19} - 1 \equiv 0 \pmod{7}.$$

Після уст. 81. маємо помножити через себе первісні корінї таких трех конґруенцій

$$\left.\begin{array}{l} X^2 \equiv 1 \\ X^{3^2} \equiv 1 \\ X^{19} \equiv 1 \end{array}\right\} \pmod{7}. \qquad (**)$$

Перша з них має первісний корінь -1, лїву сторону другої можна розложити на добуток $(X^3 - 1)(X^3 - 2)(X^3 + 3) \pmod{7}$, отже її первісні корінї містять ся в конґруенціях

$$X^3 - 2 \equiv 0 \text{ і } X^3 + 3 \equiv 0 \pmod{7}.$$

Назвім корінь першої з них x, то x є первісним коренем середньої конґруенції в системи (**).

Врештї шукаємо первісного коріня третьої конґруенції. Galois робить се так, що пробує, чи функція $f(x) = ax + b$ її не сповнить, т. зн., як треба дібрати a і b, щоби було сповнене

$$(ax + b)^{19} \equiv 1 \pmod{7}.$$

З двочленного розвиненя слїдують такі вартости: $a \equiv 1$, $b \equiv -1$, отже $f(x) \equiv x - 1$ є тим первісним коренем. Помножім через себе ті три знайдені первісні корінї, то одержимо первісний корінь конґруенції (*):

$$X \equiv -1 \,.\, x \,.\, (x - 1) = -x^2 + x \pmod{7}. \qquad (***)$$

Елїмінуючи x з (***) і $x^3 - 2 \equiv 0 \pmod{7}$, одержимо конґруенцію, від якої залежить X:

$$X^3 - X + 2 \equiv 0 \pmod{7}.$$

II. Конґруенції третього і четвертого степеня.

§. 6.

Конґруенції третього степеня.

32. Нехай буде дана конґруенція третього степеня в $GF[p]$

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3 \equiv 0 \pmod{p} \qquad (1)$$

Метода, яку примінює Cauchy, полягає на зведеню повної конґруенції до двочленної; є вона зовсім аналоґічна до методи Lagrange'а при рівнанях третього степеня. Cauchy розвязує в тій цїли одну двочленну конґруенцію третього степеня і дві квадратні.

33. **Двочленні конґруенції.** Спеціяльна (одинична) конґруенція

$$z^3 \equiv 1 \pmod{p} \qquad (2)$$

має завсїди один дїйсний корінь 1 і ще два инші, γ і γ^2, звязані реляцією

$$\gamma^2 + \gamma + 1 \equiv 0 \pmod{p};$$

ми назвали їх первісними третими коріннями одиницї (mod. p). Розвязуючи ту квадратну конґруенцію, або примінюючи результати уст. 10, бачимо, що коли $p \equiv 1$ (mod. 6), то γ і γ^2 є дїйсні, а саме

$$\gamma \equiv g^{\frac{p-1}{3}} \pmod{p};$$

означимо їх через α і α^2. В разї $p \equiv -1$ (mod. 6) належать вони до $GF[p^2]$; коли первісну величину того поля означимо через ε, одержимо

$$\gamma \equiv \frac{p-1}{2}(1-\varepsilon), \quad \gamma^2 \equiv \frac{p-1}{2}(1+\varepsilon), \quad \varepsilon^2 \equiv -3 \pmod{p}.$$

34. **Загальна двочленна конґруенція**

$$x^3 \equiv A \pmod{p} \qquad (3)$$

зводить ся до попередньої. Нехай r буде одним з її корінїв, тодї два инші корінї є, як знаємо, $r\gamma$ і $r\gamma^2$.

Крітерією рішимости для (3) в $GF[p]$ є

$$A^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

де $d = (p-1, 3)$, отже коли $p \equiv 1$ (mod. 6), то $d = 3$, проте крітерія звучить

$$A^{\frac{p-1}{3}} \equiv 1 \pmod{p}. \qquad (4)$$

Коли вона сповнена, то конґруенція має три дїйсні корінї:

$$r, \ \alpha r, \ \alpha^2 r.$$

В противнім разї назвім j одну з первісних величин в $GF[p^3]$; тодї три корінї є

$$j,\ \alpha j,\ \alpha^2 j.$$

Коли $p \equiv -1$ (mod. 6), то A є все третїм степенним останком, отже конґруенція (3) має все один дїйсний корінь r. Зате два инші корінї належать до $GF[p^2]$, отже (3) має такі три корінї

$$r,\ \frac{p-1}{2}(1 - \varepsilon)\,r,\ \frac{p-1}{2}(1+\varepsilon)\,r.$$

35. Повну конґруенцію третього степеня (1) множимо числом a_0', стоваришеним (mod. p) з числом a_0, і при помочи лїнїйного підставленя усуваємо член з квадратом незвісної; через те одержимо зредуковану конґруенцію

$$y^3 - 3Ay - 2B \equiv 0 \text{ (mod. } p). \qquad (4)$$

Назвім її корінї y_1, y_2, y_3 і утворім при їх помочи такі двіресольвенти:

$$27\,v_1 = (3\,t_1)^3 \equiv (y_1 + \gamma y_2 + \gamma^2 y_3)^3,$$
$$27\,v_2 = (3\,t_2)^3 \equiv (y_1 + \gamma^2 y_2 + \gamma y_3)^3,$$

де $\gamma^2 + \gamma + 1 \equiv 0$ (mod. p). З огляду на те, що

$$27\,(v_1 + v_2) = 2\,\sigma_1^3 - 9\,\sigma_1\,\sigma_2 + 27\,\sigma_3,$$
$$27^2\,v_1\,v_2 = (\sigma_1^2 - 3\,\sigma_2)^3,$$

а у нас є $\sigma_1 = 0$, $\sigma_2 = -3\,A$, $\sigma_3 = 2\,B$ (основні симетричні функції корінів), маємо

$$v_1 + v_2 = 2\,B,\ v_1\,v_2 = A^3,$$

отже квадратна конґруенція для v_1 і v_2 є

$$v^2 - 2\,B\,v + A^3 \equiv 0 \text{ (mod. } p). \qquad (5)$$

Вріжник тої конґруенції, а заразом і конґруенції (3), є

$$D \equiv B^2 - A^3 \text{ (mod. } p). \qquad (6)$$

Нехай буде $D \equiv \beta^2$ (β може бути дїйсне або належати до $GF[p^2]$), отже маємо

$$v \equiv B \pm \beta,$$

проте зістає ще до розвязки конґруенція

$$t^3 \equiv v. \qquad (7)$$

Коли се стало ся і $t \equiv t_1$ є її розвязкою для $v \equiv v_1$, то для $v \equiv v_2$ одержимо $t \equiv t_2$, обмежуючи ся в виборі корінїв конґруенції (7), подібно як при формулї Cardan'а, реляцією

$$t_1\,t_2 \equiv A \text{ (mod. } p)$$

(бо $v_1\,v_2 \equiv A^3$). Маємо тому:

$$y_1 + y_2 + y_3 \equiv 0,$$
$$y_1 + \gamma y_2 + \gamma^2 y_3 \equiv 3\,t_1,$$
$$y_1 + \gamma^2 y_2 + \gamma y_3 \equiv 3\,t_2,$$

а звідси:

$$\left.\begin{aligned} y_1 &\equiv t_1 + t_2, \\ y_2 &\equiv \gamma^2 t_1 + \gamma t_2, \\ y_3 &\equiv \gamma t_1 + \gamma^2 t_2, \end{aligned}\right\} \text{ (mod. } p).$$

Бачимо отже, що розвязка даної конґруенції (4) зводить ся до трьох инших:

1) квадратної для v: $v^2 - 2Bv + A^3 \equiv 0$,

2) квадратної для γ: $\gamma^2 + \gamma + 1 \equiv 0$,

3) двочленної третього степеня $t^3 \equiv B + \beta \equiv C$, всї (mod. p).

36. **Дискусія розвязки.** 1) Конґруенція для v є зведима або нї, відповідно до того, чи

$$\left(\frac{D}{p}\right) = +1 \text{ чи } -1.$$

2) Конґруенція для γ є при $p = 6n + 1$ зведима, при $p = 6n - 1$ незведима.

3) Конґруенція $t^3 \equiv C$ є при $p = 6n + 1$ зведима або нї, відповідно тому, чи

$$\left[\frac{C}{p}\right] = 1 \text{ чи } \neq 1;$$

при $p = 6n - 1$ є вона все зведима.

Займемо ся перше дискусією виріжника D

I. $D \equiv 0$ (mod. p); тодї є $v_1 \equiv v_2 \equiv B$, отже $t_1 = t_2 = t$; t є дїйсне, бо тодї $t^2 \equiv A$, а що $A^3 \equiv B^2$, то $\left(\frac{A}{p}\right) = \left(\frac{A^3}{p}\right) = \left(\frac{B^2}{p}\right) = +1$. Тодї є $y_1 = 2t$, $y_2 = y_3 = (\gamma + \gamma^2)t \equiv -t$. Отже коли чисельна вартість виріжника є многократю модула, то конґруенція має одну двократну розвязку. — Щоби розвязка була трикратна, мусить ще бути $2t \equiv -t$, т. зн. $t \equiv 0$ (mod. p), отже і $A \equiv B \equiv 0$ (mod. p). Тодї трикратна розвязка є $y \equiv 0$, отже коли від y перейдемо до x через лінійну субституцію, то трикратна розвязка буде $x \equiv c$, т. зн. дана конґруенція звучить: $(x - c)^3 \equiv 0$ (mod. p).

II. $\left(\frac{D}{p}\right) = +1$; в такім разї заложім $r^2 \equiv D$, отже буде r дїйсне, $v \equiv B \pm r \equiv C$ дїйсне. Тепер розвязуємо

$$t^3 \equiv C \text{ (mod. } p). \tag{7a}$$

1) Коли $p \equiv 1$ (mod. 6), тодї є такі можливости:

$$\text{а) } \left[\frac{C}{p}\right] = 1, \text{ б) } \left[\frac{C}{p}\right] \neq 1.$$

а) Коли C є кубовим останком, то t є дїйсне $= \tau$, а що і γ є дїйсне $= \alpha$, то маємо

$$\left.\begin{aligned} y_1 &\equiv \tau_1 + \tau_2, \\ y_2 &\equiv \alpha^2 \tau_1 + \alpha \tau_2, \\ y^3 &\equiv \alpha \tau_1 + \alpha^2 \tau_2, \\ \alpha^2 &+ \alpha + 1 \equiv 0 \end{aligned}\right\} \text{ (mod. } p).$$

Всї три розвязки є дїйсні, ріжні поміж собою.

б) Коли C є не-останком, то t належить до $GF[p^3]$, отже $t=j$, і

$$\left.\begin{aligned} y_1 &\equiv j_1 + j_2, \\ y_2 &\equiv \alpha^2 j_1 + \alpha j_2, \\ y_3 &\equiv \alpha j_1 + \alpha^2 j_2, \\ j^3 &\equiv C,\ j_1 j_2 \equiv A. \end{aligned}\right\} \pmod{p}.$$

Можемо ще одначе усунути один із елементів j, так що в розвязці буде приходити тільки одна j. Іменно є $j_1{}^3 j_2 \equiv A j_1{}^2$; помножім $MC \equiv A$, то $j_2 \equiv M j_1{}^2$, отже коли напишемо j за j_1, а Mj^2 за j_2, то:

$$\left.\begin{aligned} y_1 &\equiv j\ (1 + Mj), \\ y_2 &\equiv j\ (\alpha^2 + \alpha Mj), \\ y_3 &\equiv j\ (\alpha + \alpha^2 Mj), \end{aligned}\right\} \pmod{p}.$$

В тім разі є всі три розвязки величинами в $GF[p^3]$, а наша розвязка лежала в тім, що ми виразили всі три y при помочи корінь можливо найпростїйшої модулової функції $j^3 - C \equiv 0 \pmod{p}$.

3) $p = 6n - 1$, тоді C є завсїди останком, а γ належить до $GF[p^2]$, отже маємо

$$\left.\begin{aligned} y_1 &\equiv \tau_1 + \tau_2 \\ y_2 &\equiv \frac{p-1}{2}\left[(\tau_1 + \tau_2) + \varepsilon(\tau_1 - \tau_2)\right] \\ y_3 &\equiv \frac{p-1}{2}\left[(\tau_1 + \tau_2) - \varepsilon(\tau_1 - \tau_2)\right] \\ &\tau_1 \tau_2 \equiv A,\ \varepsilon^2 \equiv -3 \end{aligned}\right\} \pmod{p}.$$

В тім разі є y_1 дїйсне, а y_2 і y_3 є спряжені в $GF[p^2]$.

III $\left(\frac{D}{p}\right) = -1$. Тоді конґруенція $D \equiv \beta^2$ є незведима, отже β належить до $GF[p^2]$. Положім $\beta = i$, то се дасть $v \equiv B \pm i$, і

$$t^3 \equiv B + i.$$

Заложім

$$t_1 \equiv a + b\,i,$$

де a і b є величинами з $GF[p]$ або $GF[p^3]$, то злучена з t_1 величина t_2 має форму

$$t_2 \equiv a - b\,i.$$

Порівнане сочинників при $t^3 \equiv B + i$ і $t_1{}^3 \equiv (a + b\,i)^3$ дає такі дві реляції:

$$a(a^2 + 3b^2 D) \equiv B,\ b(3a^2 + b^2 D) \equiv 1 \pmod{p}.$$

Коли дана конґруенція є рішима, то обі ті реляції є рівночасно рішимі в дїйсних числах, отже маємо

$$\left.\begin{aligned} y_1 &\equiv t_1 + t_2 \equiv 2a \\ y_2 &\equiv \gamma^2(a + bi) + \gamma(a - bi) \equiv -a + (\gamma^2 - \gamma)\,b\,i \\ y_3 &\equiv \gamma(a + b\,i) + \gamma^2(a - b\,i) \equiv -a - (\gamma^2 - \gamma)\,b\,i \end{aligned}\right\} \pmod{p}.$$

а) Коли $p = 6n + 1$, то $\gamma^2 - \gamma \equiv \alpha^2$ α є дійсне; положім ще $m \equiv b^2(\alpha^2 - \alpha)$, то $m^2 \equiv$ $3b^2$, отже

$$\left.\begin{aligned} y_1 &\equiv 2a \\ y_2 &\equiv -a + mi \\ y_3 &\equiv -a - mi \\ m^2 &\equiv -3b^2,\ i^2 \equiv D \end{aligned}\right\} \pmod{p}.$$

Отже одна розвязка є дійсна, дві инші з $GF[p^2]$.

б) Коли $p = 6n - 1$, то $\gamma^2 - \gamma \equiv -1$; положім $\varepsilon i \equiv \omega$, то се є дійсне число, бо коли $\varepsilon^2 \equiv -3$, $i^2 \equiv D$, то $(\varepsilon i)^3 \equiv -3D$, а коли $\left(\frac{D}{p}\right) = -1$, то $\left(\frac{-3D}{p}\right) = +1$. Отже маємо

$$\left.\begin{aligned} y_1 &\equiv 2a \\ y_2 &\equiv -a - b\omega \\ y_3 &\equiv -a + b\omega \\ \omega^2 &\equiv -3D \end{aligned}\right\} \pmod{p}$$

Проте в тім разї маємо три дїйсні розвязки; тут маємо повну анальоґію до casus irreducibilis рівнань третього степеня.

Примір

$$y^3 + 5y + 4 \equiv 0 \pmod{11}.$$

Маємо тут $A \equiv 2$, $B \equiv -2$, отже $D \equiv -4$, а що $\left(\frac{-4}{11}\right) = \left(\frac{-1}{11}\right) = -1$, то можемо положити $i^2 \equiv -4 \pmod{11}$, або коли за i впровадити величину $\vartheta = 5i$, т. зн. $\vartheta^2 \equiv -1 \pmod{11}$ отже ϑ буде мати вартість звичайного Gauss-ового символа i. Супроти того квадратна ресольвента прийме вид

$$v^2 + 5v - 3 \equiv 0 \pmod{11},$$

а її розвязка є $v \equiv -2 \pm 2\vartheta \pmod{11}$, отже

$$t^3 \equiv -2 + 2\vartheta.$$

Положім $t = a + b\vartheta$, то одержимо дві конґруенції

$$\left.\begin{aligned} a^3 - 3ab^2 &\equiv -2 \\ 3ab - b^3 &\equiv 2 \end{aligned}\right\} \pmod{11}$$

яких розвязкою є $a \equiv 1$, $b \equiv 1$, отже $t_1 \equiv 1 + \vartheta$, $t_2 = 1 - \vartheta$. З $\varepsilon^2 \equiv -3$, $\vartheta^2 \equiv -1$ слїдує $(\varepsilon\vartheta)^2 \equiv 3$, т. зн. $\varepsilon\vartheta \equiv \omega \equiv 5 \pmod{11}$, отже

$$\left.\begin{aligned} y_1 &\equiv 2 \\ y_2 &\equiv -1 - 5 \equiv -6 \\ y_2 &\equiv -1 + 5 \equiv 4 \end{aligned}\right\} \pmod{11}.$$

IV. Коли-ж дана конґруенція є незведима, то всї три розвязки належать до $GF[p^3]$, а модулова функція не дасть ся в тім разї звести до двочленної. Назвім один корінь даної конґруенції j, то два инші корінї є j^p і j^{p^2}

37. **Зіставлене.** Рішимість конґруенції залежить від того, чи циклічний визначник Δ степеня $p-1$, утворений з її сочинників, є $\equiv 0 \pmod{p}$, чи ні.

I. $\Delta \equiv 0 \pmod{p}$; тоді маємо:

1) коли $\left(\frac{D}{p}\right) = +1$, а) для $p = 6n+1$ 3 корінї;
б) для $p = 6n-1$ 1 корінь;

2) коли $\left(\frac{D}{p}\right) = -1$, а) для $p = 6n+1$ 1 корінь;
б) для $p = 6n-1$ 3 корінї.

Щоби усунути ріжницю поміж обома формами числа p, положім за Міріма новим[1])

$$R \equiv -3D \pmod{p},$$

то $\left(\frac{R}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{D}{p}\right)$, а що $\left(\frac{-3}{p}\right) = \pm 1$ для $p = 6n \pm 1$, то маємо

1. а) $\left(\frac{D}{p}\right) = +1$, $\left(\frac{-3}{p}\right) = +1$, отже $\left(\frac{R}{p}\right) = +1$,

1. б) $\left(\frac{D}{p}\right) = +1$, $\left(\frac{-3}{p}\right) = -1$, отже $\left(\frac{R}{p}\right) = -1$;

2. а) $\left(\frac{D}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = +1$, отже $\left(\frac{R}{p}\right) = -1$,

2. б) $\left(\frac{D}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = -1$, отже $\left(\frac{R}{p}\right) = +1$.

Проте можемо сказати коротко: конґруенція має три дійсні корінї, коли $\left(\frac{R}{p}\right) = +1$, один дійсний корінь, коли $\left(\frac{R}{p}\right) = -1$.

II. Коли $\Delta \not\equiv 0 \pmod{p}$, то конґруенція є нерішима.

Конґруенції четвертого степеня.

38. Двочленна одинична конґруенція

$$z^4 \equiv 1 \pmod{p} \tag{8}$$

має все два дїйсні корінї $+1$ і -1; її первісні корінї залежать від

$$z^2 + 1 \equiv 0 \pmod{p}. \tag{8a}$$

Коли $p \equiv 1 \pmod{4}$, то $\left(\frac{-1}{p}\right) = +1$. отже (8а) має два дїйсні корінї $\alpha \equiv g^{\frac{p-1}{4}} \pmod{p}$ і $\alpha^3 \equiv -\alpha$, так що всї корінї конґруенції (8) є

[1]) D. Mirimanoff, Sur les congruences du troisième dégré, Enseignement mathématique, t. IX. (1907), p. 381—384.

$$1,\ \alpha,\ -1,\ -\alpha.$$

В разї $p \equiv -1 \pmod{4}$ є $\left(\frac{-1}{p}\right) = -1$, отже оба коріні конґруенції (8а) є в $GF[p^2]$. Назвім одну з величин в $GF[p^2]$ γ, тодї маємо такі коріні конґруенції (8):

$$1,\ \gamma,\ -1,\ -\gamma.$$

39. **Для загальної двочленної конґруенції**

$$x^4 \equiv A \pmod{p} \qquad (9)$$

є крітерією рішимости $A^{\frac{p-1}{d}} \equiv 1 \pmod{p}$; в разї $p \equiv 1 \pmod{4}$ мусить отже бути A двоквадратним, в разї $p \equiv -1 \pmod{4}$ квадратним останком. Проте в першім разї має конґруенція (9) 4 або 0 дїйсних корінів,

$$r,\ \alpha r,\ -r,\ -\alpha r,$$

в другім разї 2 або 0 дїйсних

$$r,\ \gamma r,\ -r,\ -\gamma r.$$

Коли крітерія рішимости несповнена, тодї дефінїює дана конґруенція $GF[p^4]$.

40. **Повну конґруенцію четвертого степеня**

$$F(x) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \equiv 0 \pmod{p} \qquad (10)$$

зводимо до зредукованої форми

$$f(y) = y^4 - 6Ly^2 - 4My - 3N \equiv 0 \pmod{p}. \qquad (11)$$

Нехай її коріні будуть y_1, y_2, y_3, y_4, то їх основні симетричні функції є $\sigma_1 \equiv 0$, $\sigma_2 \equiv -6L$, $\sigma_3 \equiv 4M$, $\sigma_4 \equiv -3N$.

Утворім такі триресольвенти:

$$\left.\begin{aligned} 4v_1 &\equiv (y_1 + y_2 - y_3 - y_4)^2 - 16L \\ 4v_2 &\equiv (y_1 - y_2 + y_3 - y_4)^2 - 16L \\ 4v_3 &\equiv (y_1 - y_2 - y_3 + y_4)^2 - 16L \end{aligned}\right\} \pmod{p}, \qquad (12)$$

або коли положимо для скороченя

$$\begin{aligned} a &= (y_1 + y_2 - y_3 - y_4)^2, \\ b &= (y_1 - y_2 + y_3 - y_4)^2, \\ c &= (y_1 - y_2 - y_3 - y_4)^2, \end{aligned}$$

то будемо мати

$$\left.\begin{aligned} 4v_1 &\equiv a - 16L \\ 4v_2 &\equiv b - 16L \\ 4v_3 &\equiv c - 16L \end{aligned}\right\} \pmod{p}.$$

Щоби найти конґруенцію, від якої залежать v_1, v_2, v_3, творимо основні симетричні функції

$$\begin{aligned} 4(v_1 + v_2 + v_3) &= \tau_1 - 48L, \\ 16(v_1 v_2 + v_2 v_3 + v_3 v_1) &= \tau_2 - 32\tau_1 L + 3.16^2 L^2, \\ 64 v_1 v_2 v_3 &= \tau_3 - 16\tau_2 L + 16^2 \tau_1 L^2 - 16^3 L^3, \end{aligned}$$

де $\tau_1 = a + b + c$, $\tau_2 = a\,b + b\,c + c\,a$, $\tau_3 = a\,b\,c$. Ті три остатні величини легко обчислити; вони є

$$\tau_1 = 3\,\sigma_1{}^2 - 8\,\sigma_2.$$
$$\tau^2 = (3\,\sigma_1{}^3 - 16\,\sigma_1\,\sigma_2 + 16\,\sigma_3)\,\sigma_1 + 16\,\sigma_2{}^2 - 64\,\sigma_4,$$
$$\tau_3 = (\sigma_1{}^3 - 4\,\sigma_1\,\sigma_2 + 8\,\sigma_3)^2,$$

а з огляду на вартости функцій σ маємо

$$\tau_1 = 48\,L,$$
$$\tau_2 = 16.12\,(3\,L^2 + N),$$
$$\tau_3 = 64.16\,M^2.$$

Звідси слїдує передовсїм

$$4\,(v_1 + v_2 + v_3) = \tau_1 - 48\,L \equiv 0,$$

а проте можемо обі прочі функції написати так:

$$16\,(v_1\,v_2 + v_2\,v_3 + v_3\,v_1) = \tau_2 - 16\,\tau_1\,L,$$
$$64\,v_1\,v_2\,v_2 = \tau^3 - 16\,\tau_2\,L + 2.16^3\,L^3,$$

отже врешті є

$$v_1\,v_1 + v_2\,v_3 + v_3\,v_1 = -\,12\,(L^2 - N),$$
$$v_1\,v_2\,v_3 = 16\,(M^2 - 3\,L\,N - L^2).$$

Проте конґруенція для v (ресольвента третього степеня) є

$$\varphi(v) = v_2 - 12\,(L^2 - N)\,v - 16\,(M^2 - 3\,L\,N - L^3) \equiv 0 \pmod{p}. \quad (13)$$

Знайшовши її три корінї, v_1, v_2, v_3, творимо

$$a \equiv 4\,v_1 + 16\,L,$$
$$b \equiv 4\,v_2 + 16\,L,$$
$$c \equiv 4\,v_3 + 16\,L$$

і розвязуємо три квадратні конґруенції

$$\left.\begin{aligned} 16\,X^2 &\equiv a \\ 16\,Y^2 &\equiv b \\ 16\,Z^2 &\equiv c \end{aligned}\right\} \pmod{p}. \quad (14)$$

Коли маємо їх корінї, находимо корінї даної конґруенції (11) з

$$\left.\begin{aligned} y_1 + y_2 + y_3 + y_4 &\equiv 0 \\ y_1 + y_2 - y_3 - y_4 &\equiv 4\,X \\ y_1 - y_2 + y_3 - y_4 &\equiv 4\,Y \\ y_1 - y_2 - y_3 + y_4 &\equiv 4\,Z \end{aligned}\right\} \pmod{p}.$$

Вони є

$$\left.\begin{aligned} y_1 &\equiv X + Y + Z \\ y_2 &\equiv X - Y - Z \\ y_3 &\equiv -X + Y - Z \\ y_4 &\equiv -X - Y + Z \end{aligned}\right\} \pmod{p}. \quad (15)$$

З конґруенцій (14) одержуємо по дві вартости на X, Y, Z; в розвязці (15) треба їх так комбінувати, щоби було

$$4\,X\,Y\,Z \equiv M \pmod{p}, \quad (16)$$

отже, коли заложимо, що M є (mod. p) додатне, т. зн. $< \frac{p-1}{2}$, то скількість відємних (mod. p) величин, т. є X, Y, $Z > \frac{p-1}{2}$, буде 0 або 2. Можна також так поступити, що знайшовши дві з них, третю виначодимо з реляції (16).

41. **Дискусія.** Конґруенція (11) і її ресольвента (13)[1]) мають однаковий виріжник

$$D \equiv 64\,[(M^2 - 3\,L\,N - L^3)^2 - (L^2 - N)^3]. \qquad (17)$$

Від нього залежить якість розвязки.

I. Коли $D \equiv 0$ (mod. p), то $\varphi(v) \equiv 0$ має один многократний корінь, який може бути: 1) трикратний, 2) двократний.

1) Коли (13) має трикратний корінь $v_1 = v_2 = v_3$, то він є $\equiv 0$ (mod. p), проте ресольвента є

$$\varphi(v) = v^3 \equiv 0 \text{ (mod. } p).$$

В такім разі є оба инші сочинники в $\varphi(v)$ пристайні до зера:

$$L^2 - N \equiv 0,\ M^2 - 3\,L\,N - L^3 \equiv 0 \text{ (mod. } p),$$

тому панують поміж ними такі звязи:

$$N \equiv L^2,\ M^2 \equiv 4\,L^3 \text{ (mod. } p),$$

отже L мусить бути квадратним останком для p.

Звідси слідує дальше: $a = b = c \equiv 16\,L$, проте $16\,X^2 \equiv 16\,L$ або

$$X^2 \equiv L \text{ (mod. } p),$$

а що $\left(\frac{L}{p}\right) = +1$, то ся конґруенція є рішима, отже X дійсне. Назвім її корінь X, тоді є $Y \equiv Z \equiv X$, проте

$$z_1 \equiv 3\,X,\ y_2 \equiv y_3 \equiv y_4 \equiv -X.$$

Конґруенція четвертого степеня, якої ресольвента (13) має потрійний корінь, виглядає так:

$$f(y) = (y - 3\,X)\,(y + X)^3 \equiv 0 \text{ (mod. } p),$$

отже вона має один однократний, один трикратний корінь.

Замітка. Коли $X \equiv 0$, тоді $f(y)$ має чотирократний корінь; тоді є $L \equiv 0$, отже і $M \equiv 0$, $N \equiv 0$, а конґруенція звучить $f(y) = y^4 \equiv 0$ (mod. p).

2) Коли ресольвента має один двократний дійсний корінь $v_2 = v_3$, то кладучи $v_1 \equiv 2\,z$, (z дійсне) маємо $v_2 = v_3 \equiv -z$, отже

$$\varphi(v) = v^3 - 3\,z^2\,v - 2\,z^3 \equiv 0 \text{ (mod. } p).$$

---

[1]) Ресольвентами називаємо і функції, яких уживаємо до розвязки рівнаня (чи конґруенції), і рівнане (конґруенцію), від якого вона залежить. Непорозумілня нема тут чого побоювати ся.

Для визначеня z маємо реляцію $z^2 \equiv 4(L^2 - N)$; вона є завсіди рішима, бо з огляду $D \equiv 0$ є $(M^2 - 3LN - L^3)^2 \equiv (L^2 - N)^3$, отже $\left(\frac{L^2 - N}{p}\right) = +1$. Тоді є

$$a \equiv 4(4L + 2z),$$
$$b = c \equiv 4(4L - z).$$

Дальше розвязуємо

$$\left.\begin{array}{l} 16X^2 \equiv 4(4L + 2z) \\ 16Y^2 = 16Z^2 \equiv 4(4L - z) \end{array}\right\} (\mathrm{mod.}\ p) \qquad (18)$$

і маємо врешті

$$\left.\begin{array}{l} y_1 \equiv X + 2X \\ y_2 \equiv X - 2Y \\ y_3 = y_4 \equiv -X \end{array}\right\} (\mathrm{mod.}\ p),$$

отже один двократний корінь. Другий корінь є лише тоді двократний, коли $Y \equiv 0$ (mod. p).

а) $Y \not\equiv 0$ (mod. p). В такім разї (11) виглядає так:

$$f(y) = y^4 - 2(X^2 - 2Y^2)y^2 - 8XY^2 + X^2(X^2 - 4Y^2) \equiv 0\ (\mathrm{mod.}\ p). \ (11a)$$

Чи X і Y можуть належати до иншого поля, як до $GF[p]$? Сочинники конґруенції (11a) мусять бути дїйсні; коли отже положимо $X = \alpha + \beta i$, $Y = \gamma + \delta i$, де i належить до $GF[p^2]$, то се доведе до таких реляцій:

$$\left.\begin{array}{l} 2\gamma\delta \equiv \alpha\beta \\ (2\alpha^2 + \gamma^2 + \delta^2 i^2)\beta \equiv 0 \\ (\alpha\beta - 2\gamma\delta)(\alpha^2 + \beta^3 i^2) \equiv 2\alpha\beta(\gamma^2 + \delta^2 i^2) \end{array}\right\} (\mathrm{mod.}\ p).$$

Супроти першої реляції зводить ся третя до

$$(\gamma^2 + \delta^2 i^2)\alpha\beta \equiv 0,$$

а в злуці з другою дає $\alpha^3\beta \equiv 0$. Звідси слїдує, що мусить бути $\alpha \equiv 0$ або $\beta \equiv 0$, а проте і одна з величин γ і δ рівно-ж $\equiv 0$.

Нехай буде перше $\alpha \not\equiv 0$, $\beta \equiv 0$; се не накладає на γ і δ нїякого иншого обмеженя, як тільки те, що одна з них є $\equiv 0$, т. зн. Y^2 є дїйсне. Коли-ж $\alpha \equiv 0$, $\beta \not\equiv 0$, тодї з другої реляції слїдує $\gamma \equiv \delta \equiv 0$; отже коли в X дїйсна часть є $\equiv 0$, тодї є або $X \equiv 0$, або $Y \equiv 0$ (mod. p). Проте всї сочинники конґруенції (11a) є дїйсні, і корінї або всї дїйсні, або двократний дїйсний, а два прочі належать до $GF[p^2]$.

б) $Y \equiv 0$ (mod. p) потягає за собою $z \equiv 4L$, т. зн. $3L^2 + N \equiv 0$ (mod. p). Се вимагає, щоби було $\left(\frac{-3N}{p}\right) = +1$ і дальше, з огляду на $D \equiv 0$, $M^2(M^2 + 16L^3) \equiv 0$ (mod. p). Тут мусить бути $M \equiv 0$, бо

$M^2 \equiv -16 L^3$ веде до $L \equiv 0$, отже рівно-ж і тодї було би $M \equiv 0$. Проте дана конґруенція виглядає так:

$$f(y) = (y^2 - X^2)^2 \equiv 0 \pmod{p},$$

а її корінї є $y_1 = y_2 \equiv X$, $y_3 = y_4 \equiv -X$.

42. Коли циклїчний визначник Δ, степеня $p-1$, утворений з сочинників ресольвенти $\varphi(v)$, є пристайний до 0 (mod. p), тодї $\varphi(v) \equiv 0$ має три або один дїйсний корінь, відповідно до квадратного характеру величини $R \equiv -3D$.

II. $\left(\frac{R}{p}\right) = +1$; v_1, v_2, v_3 є дїйсні, ріжні поміж собою. Утворім a, b, c і означім характери символів $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{c}{p}\right)$. З поміж усїх можливих їх комбінацій є допустимі такі:

α) один з поміж тих символів є $= 0$;

β) два або три символи є $= 0$;

γ) всї три символи мають вартість $+1$;

δ) один символ є $+1$, два -1.

Евентуальности, щоби один або три символи були -1, є недопустимі, бо abc є квадратом.

α) Коли одна з величин a, b, c є $\equiv 0$, тодї мусить бути одно $v \equiv -4L$; коли подїлимо $\varphi(v)$ через $v + 4L$, одержимо як вимогу подїльности $M \equiv 0$, отже ресольвента має такі корінї:

$$\begin{aligned} v_1 &\equiv -4L, \\ v_2 &\equiv 2L + 2T, \\ v_3 &\equiv 2L - 2T, \end{aligned}$$

де T залежить від $T^2 \equiv 3N$, а $X \equiv 0$. Проте корінї даної конґруенції є

$$\left.\begin{aligned} y_1 &\equiv -y_2 \equiv Y + Z \\ y_3 &\equiv -y_3 \equiv Y - Z \end{aligned}\right\} \pmod{p}.$$

α_1) Коли $\left(\frac{3N}{p}\right) = +1$, то v_2 і v_3 є дїйсні, а Y і Z дїйсні або мнимі, відповідно до характерів величин $6L \pm 2T$.

α_2) Коли $\left(\frac{3N}{p}\right) = -1$, то v_2 і v_3 належать до $GF[p^2]$, отже маємо

$$\left.\begin{aligned} 4Y^2 &\equiv 6L + 2i \\ 4Z^2 &\equiv 6L - 2i \\ i^2 &= 3N \end{aligned}\right\} \pmod{p},$$

т. зн. Y і Z є спряжені в $GF[p^2]$. Положім $Y = \alpha + \beta i$, $Z = \alpha - \beta i$, то α і β находимо з

$$\left.\begin{aligned} 4\alpha\beta &\equiv 1 \\ 2(\alpha^2+\beta^2 i^2) &\equiv 3L \end{aligned}\right\} \pmod{p}.$$

Елімінуючи з другої конґруенції $\beta \equiv \frac{1}{4\alpha}$, одержимо

$$16\alpha^4 + 24L\alpha^2 + 3N \equiv 0 \pmod{p}. \qquad (18)$$

При помочи α виразимо коріні y так:

$$\left.\begin{aligned} y_1 \equiv -y_2 &\equiv 2\alpha \\ y_3 \equiv -y_4 &\equiv 2\beta i \end{aligned}\right\} \pmod{p},$$

де 2β є (mod. p) товаришем величини 2α.

Конґруенція для α (18) є рівнозначна з

$$(4\alpha^2 + 3L)^2 \equiv 9L^2 - 3N \pmod{p}. \qquad (18a)$$

Займім ся її правою стороною. Вона не може бути $\equiv 0$, бо тоді було би $N \equiv 3L^2$, т. зн. $4\alpha^2 \equiv -3L$, отже мусїло би бути $\left(\frac{9L^2}{p}\right) = -1$, а се недорічність. Отже можливе тільки таке, що $\left(\frac{9L^2-3N}{p}\right) = +1$ або -1.

В першім разї, $\left(\frac{9L^2-3N}{p}\right) = +1$, положім $9L^2 - 3N = U^2$; се дасть

$$4\alpha^2 \equiv -3L \pm U;$$

тут знова може бути $\left(\frac{-3L \pm U}{p}\right) = \pm 1$. В разї $+1$ є α дїйсне, отже y_1 і y_2 дійсні, а y_3 і y_4 належать до $GF[p^2]$; в разї -1 дієть ся навпаки. Тому, коли $\left(\frac{9L^2-3N}{p}\right) = +1$, маємо два коріні дїйсні, противних знаків, а два другі чисто мнимі спряжені в $GF[p^2]$.

Коли-ж врешті $\left(\frac{9L^2-3N}{p}\right) = -1$, то положім $9L^2 - 3N \equiv j^2$, де j належить до $GF[p^2]$, отже є

$$4\alpha^2 \equiv -3L \pm j.$$

Положім ще $\alpha = \mu + \nu j$, то се доведе до конґруенції

$$(8\mu^2 + 3L)^2 \equiv 3N \pmod{p},$$

яка є, з огляду на $\left(\frac{3N}{p}\right) = -1$, нерішима в $GF[p]$. Проте конґруенція (18) є нерішима в $GF[p^2]$, отже мусимо за α приймити якусь величину з $GF[p^4]$; тодї j дасть ся виразити через α:

$$j \equiv 4\alpha^2 + 3L,$$

отже шукана розвязка звучить:

$$\left.\begin{aligned} y_1 \equiv -y_2 &\equiv 2\alpha \\ y_3 \equiv -y_4 &\equiv 2\beta(4\alpha^2 + 3L) \\ 4\alpha\beta &\equiv 1 \end{aligned}\right\} \pmod{p}.$$

β) Коли ще другий з символів $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{c}{p}\right)$ є 0, то через дальше ділене дійдемо до вимоги $3N \equiv 7L^2$, т. зн.

$$f(y) = y^4 - 6Ly^2 - 7L^2 \equiv 0 \pmod{p};$$

квадратами її корінів є

$$y^2 \equiv 7L \text{ і } -L.$$

Одержуємо проте дві пари корінїв рівних, з протвними знаками; вони можуть або бути дїйсні, або належати до $GF[p^2]$.

Коли-ж всї три символї є $= 0$, то звідси слїдує $L = 0$, отже маємо чотирократний корінь $y = 0$.

γ) Коли всї три символи, $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{c}{p}\right)$, є $= +1$, то X, Y, Z є дїйсні; дана конґруенція має чотири ріжні, дїйсні розвязки.

δ) Нехай врештї буде $\left(\frac{b}{p}\right) = \left(\frac{c}{p}\right) = -1$, $\left(\frac{a}{p}\right) = +1$; тодї є X дійсне, Y і Z мнимі. Заложім $Y = \alpha + \beta i$, $Z = \gamma + \delta i$, тодї мусить бути $\gamma \equiv \pm \alpha$, $\delta \equiv \mp \beta \pmod{p}$, бо $4XYZ \equiv M$ є дійсне. Величини α і β визначуємо з конґруенцій

$$\left.\begin{aligned} X^2 + 2(\alpha^2 + \beta^2 i^2) &\equiv 3L \\ 4X(\alpha^2 - \beta^2 i^2) &\equiv M \end{aligned}\right\} \pmod{p},$$

а маючи їх, одержуємо такі корінї конґруенції (11):

$$\left.\begin{aligned} y_1 &\equiv X + 2\alpha \\ y_2 &\equiv X - 2\alpha \\ y_3 &\equiv -X + 2\beta i \\ y_4 &\equiv -X - 2\beta i \end{aligned}\right\} \pmod{p},$$

отже y_1, y_2 і y_3, y_4 творять дві пари розвязок: одну дійсну, другу спряжену в $GF[p^2]$.

43. В разї, коли III $\left(\frac{R}{p}\right) = -1$, ресольвента має один дійсний корінь, а два инші спряжені в $GF[p^2]$:

$$\left.\begin{aligned} v_1 &\equiv -2\alpha \\ v_2 &\equiv \alpha + \beta i \\ v_3 &\equiv \alpha - \beta i \end{aligned}\right\} \pmod{p},$$

отже ресольвента є

$$\varphi(v) = v^3 - (3\alpha^2 + \beta^2 i^2)v + 2\alpha(\alpha^2 - \beta^2 i^2) \equiv 0 \pmod{p},$$

а величини a, b, c мають рівно-ж форму $A + Bi$. В тім разї належать корінї y або до $GF[p^2]$, або до $GF[p^4]$, подібно як попередно.

IV. Коли ресольвента $\varphi(v) \equiv 0 \pmod{p}$ є незведима, то X, Y, Z, які залежать від її корінів, є величинами, спряженими в $GF[p^3]$. Отже $X+Y+Z$ є дійсне, т. зн. y_1 є дїйсне, а три прочі корінї належать до $GF[p^3]$.

44. Як виконувати операції на величинах поля Galois, покажемо на слїдуючім примірі:

$$f(y) = y^4 - 5y^2 + 7y - 5 \equiv 0 \pmod{19}.$$

Тут є $L \equiv 4$, $M \equiv 3$, $N \equiv 8 \pmod{19}$, отже ресольвента звучить:

$$\varphi(v) = v^3 - v + 3 \equiv 0 \pmod{19}.$$

Її виріжник є $D \equiv -5$, а що $\left(\frac{-5}{19}\right) = -1$, то вона має один дійсний корінь -4 і два инші $2(1 \pm i)$, де i дане реляцією

$$i^2 \equiv 2 \pmod{19}. \qquad (*)$$

Тому є

$$\left.\begin{array}{l} 16X^2 \equiv a \equiv -9 \\ 16Y^2 \equiv b \equiv -4+8i \\ 16Z^2 \equiv c \equiv -4-8i \end{array}\right\} \pmod{19}.$$

Перша зводить ся до

$$X^2 \equiv 3 \pmod{19}, \qquad (**)$$

а що $\left(\frac{3}{19}\right) = -1$, то X належить до $GF[p^2]$; проте можемо його виразити через i. Робимо се так: множимо з собою (*) і (**), се дає $(Xi)^2 \equiv 6 \equiv 5^2$, $Xi \equiv \pm 5$, $Xi^2 \equiv 2X^2 \equiv \pm 5i$, отже

$$X \equiv \pm 7i;$$

нам вистарчить знати одну вартість, пр. $X \equiv 7i$.

Опісля находимо Y і Z, так що положимо

$$Y = \alpha + \beta i, \; Z = \alpha - \beta i;$$

се дає з огляду на $a + b + c \equiv 16(X^2 + Y^2 + Z^2) \equiv 2$

$$\left.\begin{array}{r} \alpha^2 + 2\beta^2 \equiv -5 \\ \alpha\beta \equiv 5 \end{array}\right\} \pmod{19}.$$

Звідси елїмінуємо β і одержуємо

$$\alpha^4 + 5\alpha^2 - 7 \equiv 0 \pmod{19} \qquad (***)$$

або

$$(\alpha^2 - 7)^2 \equiv -1 \pmod{19}.$$

-1 є знова не-останком для 19, отже треба корінь конґруенції $z^2 \equiv -1 \pmod{19}$ виразити через i; легко знайти, що $z \equiv 3i$, бо $z^2 \equiv 9i^2$. Отже є

$$\alpha^2 \equiv 7 + 3i \pmod{19}, \qquad (\dagger)$$

коли знова обмежимо ся до одного тільки знака.

Величина α, дана конґруенцією (***), дефінїює $GF[p^4]$; при помочи реляції (†) можемо представити $GF[p^2]$, т. зн. i, через α:

$$i \equiv -5\alpha^2 + 4 \pmod{19}. \qquad (\dagger\dagger)$$

Остаточно треба ще виразити β згл. βi через α. 3 $\alpha\beta \equiv 5$ (mod. 19) слїдує $\alpha^3 \beta i \equiv 5 \alpha i$, т. зн.

$$(7 + 3 i) \beta i \equiv 5 \alpha i.$$

Розширюючи обі сторони спряженою величиною $7 - 3 i$, одержимо з огляду на $(7 + 3 i)(7 - 3 i) = 49 - 9 i^2 \equiv -3 + 1 \equiv 12$,

$$12 \beta i \equiv 5 \alpha i (7 - 3 i) \equiv -3 \alpha i + 4 \alpha i^2,$$

отже дальше

$$12 \beta i \equiv -\alpha(\alpha^2 - 7) + 8 \alpha \equiv -\alpha^3 - 4 \alpha,$$

т. зн.

$$\beta i \equiv -8 \alpha^3 + 6 \alpha.$$

Маємо отже

$$\left.\begin{aligned} X &\equiv -4 \alpha^2 + 9 \\ Y &\equiv -8 \alpha^3 + 7 \alpha \\ Z &\equiv 8 \alpha^3 - 5 \alpha \end{aligned}\right\} \text{(mod. 19).}$$

Звідси слїдують корінї даної конґруенції, виражені при помочи корінів простїйшої конґруенції (***):

$$\left.\begin{aligned} y_1 &\equiv -4 \alpha^2 + 2 \alpha + 9 \\ y_2 &\equiv -4 \alpha^2 - 2 \alpha + 9 \\ y_3 &\equiv 3 \alpha^3 + 4 \alpha^2 - 7 \alpha - 9 \\ y_4 &\equiv -3 \alpha^3 + 4 \alpha^2 + 7 \alpha - 9 \end{aligned}\right\} \text{(mod. 19).}$$

45. Як примір, в якімресольвента 3. степеня є незведима, отже приходить ся розвязувати квадратні конґруенції в $GF[p^3]$, розвяжемо таку конґруенцію:

$$f(y) = y^4 + y^2 - 2 y + 3 \equiv 0 \text{ (mod. 7).}$$

Тут є: $L \equiv 1$, $M \equiv -3$, $N \equiv -1$, отже

$$\varphi(v) = v^3 - 3 v + 1 \equiv 0 \text{ (mod. 7).}$$

Отся ресольвента є незведима; назвім один її корінь $v_1 \equiv j$, то два другі корінї є $v_2 \equiv j^2 - 2$, $v_3 \equiv -j^2 - j + 2$, (гл. уст. 16), отже

$$\left.\begin{aligned} a &\equiv -3 j + 2 \\ b &\equiv -3 j^2 + 1 \\ c &\equiv 3 j^2 + 3 j + 3 \end{aligned}\right\} \text{(mod. 7),}$$

а квадратні конґруенції для X, Y, Y зводять ся до

$$\left.\begin{aligned} X^2 &\equiv 2 j + 1 \\ Y^2 &\equiv 2 j^2 - 3 \\ Z^2 &\equiv -2 j^2 - 2 j - 2 \end{aligned}\right\} \text{(mod. 7).}$$

Першу з них розвязуємо так, що покладимо $X \equiv \alpha j^2 + \beta j + \gamma$, і визначуємо α, β, γ з

$$\left.\begin{aligned} 3 \alpha^2 + 2 \alpha \gamma + \beta^2 &\equiv 0 \\ \alpha^2 + \alpha \beta - 2 \beta \gamma &\equiv -2 \\ \gamma^2 \quad 2 \alpha \beta &\equiv 1 \end{aligned}\right\} \text{(mod. 7);}$$

се дає $\alpha \equiv 3$, $\beta \equiv 1$, $\gamma \equiv 0$, отже

$$X \equiv 3j^2 + j \pmod{7}.$$

Подібно знаходимо

$$Y \equiv -2j^2 - 3j + 3 \pmod{7},$$

а Z можемо обчислити зі звязи

$$4XYZ \equiv M \pmod{p},$$

т. є

$$XYZ \equiv 1 \pmod{7}.$$

Добуток XY є $\equiv \vartheta \equiv 2j^2 - 3j - 3$, отже

$$\vartheta Z \equiv 1 \pmod{7}.$$

Коли ϑ належить до виложника s, т. зн. $\vartheta^s \equiv 1 \pmod{7}$, то

$$Z \equiv \vartheta^{s-1} \pmod{7}.$$

Треба проте знайти виложник s; він мусить містити ся в $7^3 - 1 = 342 = 2 . 3^2 . 19$. Піднесім ϑ до степенів 2, 3, 6, ..., то найдемо $\vartheta^{57} \equiv 2$, отже

$$\vartheta^{57} Z \equiv 2Z \equiv \vartheta^{56} \pmod{7},$$

т. зн.

$$Z \equiv -3\vartheta^{56} \pmod{7},$$

а що $\vartheta^{56} \equiv 3j^2 + j - 3$, то

$$Z \equiv -2j^2 - 3j + 2 \pmod{7}.$$

Отже корінї даної конґруенції є

$$\left.\begin{array}{ll} y_1 \equiv & -j^2 + 2j - 2 \\ y_2 \equiv & 2 \\ y_3 \equiv & -3j^2 - j + 1 \\ y_4 \equiv & -3j^2 - j - 1 \end{array}\right\} \pmod{7}.$$

Берлїн, май — червень 1913.

Résumé.

Gegenstand der vorliegenden Abhandlung bildet die Untersuchung der kubischen und der biquadratischen Kongruenzen mit Primzahlmodul im Galois'schen Felde. Dem eigentlichen Gegenstande geht ein Abriß der Theorie der Kongruenzen auf Grund der Eigenschaften des Galois'schen Feldes voran.

Mit den in Rede stehenden Kongruenzen hat sich schon Cauchy (1829) beschäftigt, ging aber über die Untersuchung der reduziblen Fälle nicht hinaus. Seine Methode ist der Lagrange'schen (für die kubischen bzw. biquadratischen Gleichungen) analog.

I. Die allgemeine kubische Kongruenz, auf die Form

$$f(y) = y^3 - 3Ay - 2B \equiv 0 \pmod{p}$$

reduziert, wird mit Hilfe der Resolventen gelöst:

$$\left.\begin{aligned} 27 v_1 &= (3t_1)^3 \equiv (y_1 + \gamma y_2 + \gamma^2 y_3)^3 \\ 27 v_2 &= (3t_2)^3 \equiv (y_1 + \gamma^2 y_2 + \gamma y_3)^3 \end{aligned}\right\} \pmod{p},$$

worin y_1, y_2, y_3 die Wurzeln von $f(y) \equiv 0$ sind, und γ durch

$$\gamma^2 + \gamma + 1 \equiv 0 \pmod{p}$$

gegeben wird; v_1 und v_2 hängen vor der Kongruenz ab

$$\varphi(v) = v^2 - 2Bv + A^2 \equiv 0 \pmod{p},$$

deren Diskriminante $D = B^2 - A^3$ zugleich Diskriminante von $f(y)$ ist.

Die Diskussion der Lösung führt zu folgenden Ergebnissen:

1) Ist $D \equiv 0 \pmod{p}$, so hat $f(y) \equiv 0$ eine doppelte, bzw. dreifache Wurzel; 2) ist $\left(\frac{-3D}{p}\right) = +1$, so hat die Kongruenz 3, ist 3) $\left(\frac{-D}{p}\right) = -1$, so hat sie nur eine reelle Wurzel, — vorausgesetzt, daß sie überhaupt lösbar ist. — Das Lösbarkeitskriterium lautet: es soll die zyklische aus den Koeffizienten der Kongruenz gebildete Determinante $(p-1)$ ter Ordnung $\equiv 0 \pmod{p}$ sein (König-Kronecker).

II. Die biquadratische Kongruenz reduziert man auf

$$f(y) = y^4 - 6Ly^2 - 4My - 3N \equiv 0 \pmod{p}$$

und führt als Resolventen ein

$$\left.\begin{aligned} 4v_1 &\equiv (y_1 + y_2 - y_3 - y_4)^2 - 16L \\ 4v_2 &\equiv (y_1 - y_2 + y_3 - y_4)^2 - 16L \\ 4v_2 &\equiv (y_1 - y_2 - y_3 + y_4)^2 - 16L \end{aligned}\right\} \pmod{p}$$

die von

$$\varphi\,((y) \equiv v^3 - 12\,(L^2 - N)\,v - 16\,(M^2 - 3\,L\,N - L^3) \equiv 0 \pmod{p}$$

abhängen. Hat $\varphi\,(y) \equiv 0$ (die Resolventenkongruenz oder kurz: die Resolvente) eine Doppelwurzel, so hat auch die gegebene Kongruenz mehrfache Wurzeln, aber nur in diesem Falle.

Ist die Resolvente vollständig lösbar, also sind ihre Wurzeln v_1, v_2, v_3 reell,dann löst man die drei quadratischen Kongruenzen

$$\left.\begin{aligned} (y_1 + y_2 - y_3 - y_4)^2 &\equiv 4\,v_1 + 16\,L \\ (y_1 - y_2 + y_3 - y_4)^2 &\equiv 4\,v_2 + 16\,L \\ (y_1 - y_2 - y_3 + y_4)^2 &\equiv 4\,v_3 + 16\,L \end{aligned}\right\} \pmod{p};$$

nennt man ihre Lösungen $4\,X$, $4\,Y$, $4\,Z$, dann hat man:

$$\left.\begin{aligned} y_1 &\equiv X + Y + Z \\ y_2 &\equiv X - Y - Z \\ y_3 &\equiv -X + Y - Z \\ y^4 &\equiv -X - Y - Z \end{aligned}\right\} \pmod{p}.$$

Je nachdem die obigen quadratischen Kongruenzen alle lösbar sind oder nicht, bekommt man für die y entweder reelle Zahlen, oder Größen des Galois'schen Feldes der Ordnungen p^2 bzw. p^4.

Enthält die Resolvente einen irreduziblen quadratischen Faktor, so sind zwei von den v imaginär, d. h. konjugiert komplex im Galois'schen Felde der Ordnung p^2. Dann gehören die y dem Galois'schen Felde der Ordnungen p^2 oder p^4.

Ist schließlich die Resolvente irreduzibel, so hat die gegebene Kongruenz eine reelle Wurzel, und die drei übrigen gehören dem Galois'schen Felde der Ordnung p^3 an.