

Студії з теорії конгруенцій.

(Studien aus der Kongruenzentheorie).

НАПИСАВ

Др. Микола Чайковський.

Опираючись на класичній теорії конгруенцій, даній Gauss'ом в „Disquisitiones arithmeticae“¹⁾, можемо розв'язувати тільки такі конгруенції, які мають самі дійсні корінї. Щоби одначе перевести розв'язку конгруенцій вповні, треба за почином Galois²⁾ ввести рід мнимих величин, які тут гратимуть подібну роль, що звичайні мнимі числа $a + bi$ ($i^2 = -1$) в теорії рівнянь. Отсю думку перевели новіші математики (головно Американці: Cole, Moore і Dickson³⁾), будуючи теорію „поля Galois“; вона відповідає подекуди теорії алгебраїчних тіл.

На тій основі переведена тут теорія конгруенцій третього й четвертого степеня з первочисельним модулем. Тим предметом займав ся вже Cauchy⁴⁾, але тільки в тіснім обсягу дійсних розв'язок. Щоби одначе могли тут перевести повну теорію згаданих конгруенцій, подаємо в першій частині 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 всі числа природного ряду

$$0, 1, 2, 3, \quad m-1, m, m+1, \quad (1)$$

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 модуля m на m клас; кожда з них містить в собі безконечно багато чисел, пристайних поміж собою ($\text{mod. } m$), так що замість всім числами природного ряду, можемо в деяких проблемах математики оперувати класами неприємних поміж собою чисел

$$K_0, K_1, K_2, \dots, K_{m-1} \quad (2)$$

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

$$0, 1, 2, \dots, m-1, \quad (2a)$$

то називаємо їх числами модуля m або системою найменших остаників модуля m і пишемо се так: $[\text{mod. } m]$. До класи K_0 належать всі многократно модуля.

2. Визначну роль в теорії чисел грає повна система остаників первочисельного модуля p :

$$0, 1, 2, \dots, p-1; \quad (2aa)$$

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

Взагалі називаємо полем, тілом або обсягом вимірності систему, яка має ту прикмету, що її елементи, лучені з собою при помочи операцій додавання і множення, дають на вислід опять числа тої системи. Таким полем є система (2aa); вона має ще й ту прикмету, що скількість елементів, які в ній містять ся, є скінчена; се слідує рівно-ж з елементарної теорії чисел. Поле Galois степеня p має отже загалом такі прикмети:

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

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

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

$$((a + b) + c) = (a + (b + c)) \text{ і } ((a b) c) = (a (b c))$$

3) З

$$a + b = d \quad \text{і} \quad a + c = d$$

або

$$a b = e \quad \text{і} \quad a c = e$$

слідує:

$$b = c.$$

4. Обі операції є перемінні, т. є

$$(a + b) = (b + a) \quad \text{і} \quad (a b) = (b a).$$

5) Врешті додавання в полученю з множення є роздільне:

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

Коли за комбінуючу операцію приймемо додавання, то елементи ряду (2аа) творять скінчену групу порядку p ; беручи-ж за основу операцію множення, одержимо з чисел

$$1, 2, 3, \dots, p-1 \quad (2аа^*)$$

рівно-ж скінчену групу порядку $p-1$. Систему (2аа*) назовемо зредукованим полем Galois і зазначимо її $GF[p]^*$. До неї належать всі числа, перві супроти модуля.

В обох разях є поле Galois перемінною групою.

Елемент 0 грає супроти множення особливу роль; іменно, яке-б не було x , в зазвжди:

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

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

З прикмет групи слідує, що до кожного елемента a в $GF[p]$ єствує один і тільки один такий елемент b , який доданий до a дасть число з класу K_0 :

$$a + b \equiv 0 \pmod{p};$$

його значимо

$$b \equiv -a \pmod{p}.$$

Проте в $GF[p]$ можлива до переведення операція віднімання.

Подібно в $GF[p]^*$ зазвжди можлива операція ділення; слідує се з т. зв. теореми Fermat'а. Випишім іменно $GF[p]^*$ і помножимо всі його числа одним з поміж них:

$$1, a, 2, a, \dots, (p-1) \cdot a,$$

то через те зрепродукуємо його, тільки в вишнім порядку. Добуток всіх його чисел в пристайний $\pmod{p}$ до добутка всіх чисел ряду (2аа*), бо в склад обох добутків входять репрезентанти тих самих класів $K_1, K_2, \dots, K_{p-1}$:

$$1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p}$$

або

$$(p-1)! (a^{p-1} - 1) \equiv 0 \pmod{p}.$$

Добуток $(p-1)!$ в супроти модуля p первий, отже мусить бути

$$a^{p-1} \equiv 1 \pmod{p}. \quad (3)$$

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

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

Бо помножимо сю конігруенцію через a^{p-2} , то се дасть:

$$a' \equiv a^{p-2} \pmod{p};$$

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

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

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

4. Прикмети 1) — 5) і вмірець Fermat'a є характеристичні для кожного скінченного поля¹⁾. Поважимо, 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

$$A, B, C, \dots, L \quad (4)$$

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

$$H + A, H + B, H + C, \dots, H + L, \quad (4a)$$

$$A + H, B + H, C + H, \dots, L + H, \quad (4b)$$

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

$$H + I = H,$$

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

$$J + H = H.$$

Звідси слідує:

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

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

(прикмета 2), т. зн.: який би не був елемент M , то в ряді (4) єствує завжди такий елемент I , який доданий до M з правої сторони не змінить його, — і такий елемент J , який доданий до M з лівої сторони рівно-ж не викличе в ній ніякої зміни:

$$M + I = M,$$

$$J + M = M.$$

Врешті після прикмети 3) маємо: для $M = J$ з першого рівняня

$$J + I = J$$

і для $M = I$ з другого:

$$J + I = I,$$

отже

$$J = I.$$

¹⁾ Під „скінченим полем“ розуміємо тут систему, вложену із скінченного числа елементів — у відріжненню від „скінчених алгебраїчних тіл“, де скінченість лежить у тім, що при помочи основи, вложеної із скінченного числа величин, можемо представити кожду величину того тіла. — Пор. Weber, Algebra, I. §. 150, II. §. 80. (endlicher Kongruenzkörper).

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

Єсть проте в ряді (4) один і тільки один такий елемент I , який доданий з лівої або з правої сторони до кожного небудь вишого елемента, не змінить його. Отсей елемент відповідає класі K_0 в $GF[p]$.

Возьмім тепер знова довільний елемент A і творім ряд:

$$A, (A + A), ((A + A) + A), \dots$$

якого числа будемо в скороченню називати:

$$A, 2A, 3A, \dots, mA, \dots; \quad (4в)$$

на основі прикмети 1) містять 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:

$$A + B, 2A + B, 3A + B, \dots, qA + B;$$

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

$$p = kq,$$

а що ми приймали p перше, то $k = 1$, отже $p = q$, т. зн. ряд (4в) вичерпує всі елементи.

Рядом (4в) маємо адефіноване і множене, отже тою дорогою можемо перевести всі дальші аналогії; мусимо ще тільки доказати, що коли модуль m є зложений, то повна система чисел $[\text{mod. } m]$ не творить поля Galois. Бракує тут іменно теореми Fermat'a. Добутки всіх чисел обох рядів

$$1, 2, \dots, m-1, \\ 1a, 2a, \dots, (m-1)a,$$

є — що правда — пристайні до себе $(\text{mod. } m)$, отже:

$$(m-1)! (a^{m-1} - 1) \equiv 0 \pmod{m},$$

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

Нагомість, коли уставио в ряд всі елементи

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

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

$a_0, a_1, \dots, a_{\varphi(m)-1} [a^{\varphi(m)} - 1] \equiv 0 \pmod{m},$
з якого слідує

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \quad (5)$$

бо чинник перед [] є перший супроти m . Це т. зв. узагальнена теорема Фермат'а.

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

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

1) Лінійна конгруенція

$$ax \equiv b \pmod{m} \quad (6)$$

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

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

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

4) Коли $(a, m) = 1$, то конгруенція (6) має тільки одну розв'язку. Бо рівнозначне з нею Діофантове рівняння

$$ax - my = b,$$

не дасть ся ніяк скоротити; воно є рішиме, а вартості на x творять арифметичний поступ з різницею m , т. є всі в поміж собою пристайні $\pmod{m}$.

5) Коли $(a, m) = d$, конгруенція має d різних розв'язок, бо з конгруенції (6) слідує

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \quad (6a)$$

Тут є $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, отже конгруенція має одну розв'язку — назв'їм її

z —, а всі її прочі розв'язки є $\equiv z \pmod{\frac{m}{d}}$. Натомість (6) може

мати ще й інші рсв'язки, бо числа, непристайні до себе $\pmod{\frac{m}{d}}$ не,

мусять бути непристайні $\pmod{m}$. Отже, коли $x \equiv z \pmod{\frac{m}{d}}$ є розв'язкою конгруенції (6a), то (6) має такі корінї

$$x \equiv z + i \frac{m}{d} \pmod{m} \\ (i = 0, 1, \dots, d-1),$$

бо вставивши се в (6) одержимо

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

§. 2.

6. До тепер обговорили ми головні прикмети поля Galois степеня p і вказали, що повна система останків модуля m творить тільки тоді поле Galois, коли m є першим числом. Тепер займемося конструкцією обширніших полів Galois і докажемо, що їх степенем може бути тільки степені першого числа, p^n .

Алгебраїчний многочлен степеня m , якого коефіцієнти є числами з $GF[p]$:

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

а a_0 не належить до класу K_0 , називаємо функцією m -того степеня в $GF[p]$. За коефіцієнти $a_0, a_1, \dots, a_m$ можемо приймати всі числа $GF[p]$ з вимком $a_0 \equiv 0 \pmod{p}$, отже скільки всьх функцій m -ого степеня в $GF[p]$ є $p^m(p-1)$. Коли-ж коефіцієнт a_0 добуємо перед скобку і всі функції, що різняться тільки тим постійним коефіцієнтом, будемо вважати одною й тою самою функцією, то скільки всьх різних функцій є p^m , проте:

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

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

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

двох вищих функцій в $GF[p]$, степенів яких як степені функції $F(x)$, а вищих як 0. — Коефіцієнти $g(x)$ і $h(x)$ є зведимі або ні; коли вони оба зведимі, то функція $f(x)$ m -того степеня дасться остаточно розкласти на m лінійних коефіцієнтів:

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

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

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

отже $\alpha_1, \alpha_2, \dots, \alpha_m$ є коріннями конгруенції

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

В елементарній теорії конгруенцій доказують ся такі твердження:

I. (основна теорема): Конгруенція m -того степеня з першим модулем не може мати більше як m різних або однакових коефіцієнтів¹⁾:

II. Ліва сторона конгруенції в $\pmod{m}$ ділима кождим „корінним коефіцієнтом“ $x - \alpha_i$.

III. Коефіцієнти конгруенції є основними симетричними функціями її корінїв.

IV. Множественні корінї конгруенції є заразом корінями її похідних.

¹⁾ Може їх мати менше як m .

V. Коли функцію $f(x)$ розложити на добуток двох інших (3), і коли (4) має m корінїв, то обі конгруенції:

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

мають як раз по тільки корінїв, кїлько виводить їх степењ.

VI. Конгруенція

$$x^{p-1} \equiv 1 \pmod{p} \quad (5)$$

має за корінї всі числа $GF[p]$.

З V. і VI. слїдує спосїб визначуваня фактичної скїлькості корінїв даної конгруенції (4): методом Евклїда вишукуємо *НСП* функцій $f(x)$ і $x^{p-1} - 1 \pmod{p}$; він містять в собі всі корінї даної конгруенції, отже його степењ подає скїлькїсть її корінїв. — Отся метода походить від Libri¹⁾.

Із сказаного слїдує, що як при рівняннях, так і тут зведимість і рїшимість конгруенцій $\pmod{p}$ є ідентичні понятя.

Про рїшимість (зведимість) конгруенцій можемо рїшати на основї таких тверджень:

I. Щоби конгруенція (4) була рїшима, є konieczне і достаточне, щоби циклічний визначник Δ степењ $p-1$, утворений із сочинників функції $f(x)$, був $\equiv 0 \pmod{p}$.

II. Конгруенція (4) має точно r рїзних корінїв, коли ряд визначника $\Delta \in r. 2)$.

III. Вирїзник незведимої в $GF[p]$ функції $\epsilon \equiv (-1)^{p-1} \pmod{p}$; коли $f(x)$ розпадаєть ся на r незведимих $\pmod{p}$ чинників, є її вирїзник $\equiv (-1)^{p-r} \pmod{p^2}$.

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

Скїлькїсть всіх квадратних функцій в $GF[p]$ є p^2 , бо в

$$f(x) = x^2 + ax + b \quad (6)$$

можуть a і b приймати всі вартості з $GF[p]$.

Повну квадратну конгруенцію

$$x^2 + ax + b \equiv 0 \pmod{p} \quad (6a)$$

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

²⁾ Коли даний визначник Δ степењ k і всі його підвизначники степењів 1, 2, 3, . . . l мають вартість 0 згл. $\equiv 0 \pmod{p}$, а бодей одия з підвизначників ряду $l+1 \equiv 0$ згл. $\neq 0$, тоді маємо, що Δ має ряд (Rang) $k-l$ (Kronecker, Frobenius).

³⁾ Теорема 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; Voronoi, Verh. des III. int. math. Kongr. in Heidelberg, 1904, p. 186.

розв'язуємо подібно як квадратне рівняння. Сочинник a можемо заступити яким небудь парним числом, що належить до тої самої класи: $a \equiv 2a' \pmod{p}$, отже напишемо:

$$(x + a')^2 \equiv a'^2 - b \pmod{p}, \quad (66)$$

проте повну конгруенцію зводимо на двочленну

$$y^2 \equiv s \pmod{p}. \quad (7)$$

Вона може бути рішима або ні; в першій разі називаємо s квадратним останком, в другій квадратним не-останком модуля p ; коли-б було $s \equiv 0$, то конгруенція мала б один подвійний корінь $y \equiv 0$. Виключивши се, бачимо, що теорема Ферма'а наводить нас на такі критерії рішимості конгруенції (7): коли

$$s^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (8a)$$

то конгруенція є рішима; вона є нерішима, коли

$$s^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (86)$$

Кожде число $G F[p]^*$ мусить сповнювати (для $p > 2$) одну і тільки одну з тих двох формул; їх називаємо критеріями

Euler'a. Їх заступив Legendre символом $\left(\frac{s}{p}\right)$, іменно є:

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

отже: 1) коли s є кв. останком, маємо

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

2) в разі 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 модуля p , отже: $\left. \begin{array}{l} \text{останки} \\ \text{не-останки} \end{array} \right\}$ мають кв. характер ± 1 , числа класу K_0 характер 0.

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

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

В дальшій будемо потребувати критерій для кв. характеру чисел $\pm 1, \pm 2, \pm 3$; вони є:
 $+1$ є завжди останком; -1 останком для первочисельних модулів $p \equiv 1 \pmod{4}$, не-останком для $p \equiv -1 \pmod{4}$, т. зв.

$$\left(\frac{+1}{p}\right) = +1, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (96)$$

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. Аналогічно до квадратних останків і не-останків дефініюємо останки й не-останки всіх інших степенів. Іменно, коли двочленна конгруенція

$$y^n \equiv s \pmod{p} \quad (10)$$

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

Коли s належить до класи K_1 , маємо т. зв. одиничну конгруенцію (Einheitskongruenz):

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

вона є аналогічна до рівнянь поділу кола. Її розвязки будемо називати n -тими коріннями одиниці $\pmod{p}$.

Коли r є найменшим виложником, для якого є $z^r \equiv 1 \pmod{p}$, тоді кажемо, що z належить $\pmod{p}$ до виложника r . Коли $r = p - 1$, z є первісним n -тим коренем одиниці $\pmod{p}$; коли $r < n$, корінь називаємо непервісним. В такому разі є $n = k \cdot r$.

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

Всі коріні, спільні обом конгруенціям

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

є коріннями конгруенції

$$x^\delta \equiv 1 \pmod{p}, \quad (11b)$$

де $\delta = (\alpha, \beta)$.¹⁾ Отже, коли α і β є перві супроти себе, то обі конгруенції (11a) не мають спільних корінів крім $x \equiv 1$.

Виложники, до яких належать $\pmod{p}$ числа $GF[p]^*$, є подільниками числа $p - 1$.

До кожного подільника d числа $p - 1$ належить $\pmod{p}$ $\varphi(d)$ чисел з $GF[p]^*$. До виложника $p - 1$ належить $\pmod{p}$ $\varphi(p - 1)$ чисел, т. зв. кожде число p має $\varphi(p - 1)$ первісних корінів.

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

$$1, g, g^2, \dots, g^{p-2} \quad (12)$$

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

$$s \equiv g^\sigma \pmod{p}, \quad (13)$$

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

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

згл.

$$\sigma \equiv \text{ind}_g s \pmod{p - 1}, \quad (14)$$

бо виложники повторюють ся що $p - 2$.

Теорія показників є аналогічна з теорією логаритмів; вона дуже придатна до розвязки двочленних конгруенцій.

Конгруенція (10) є рішима, коли

$$s^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \quad (15)$$

де $d = (p - 1, n)$; вона має тоді d корінів. Назв'їм $y_0 \equiv g^{\eta_0}$ один з її корінів, то інші коріні будуть

$$y_0, \alpha y_0, \alpha^2 y_0, \dots, \alpha^{d-1} y_0,$$

де $\alpha \equiv g^{\frac{p-1}{d}}$. Формулка (15) є аналогічна до критерію Euler'а; вона вискажує, що α є n -тим останком числа p . Символ, аналогічний до Legendre'ового, є;

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

10. Приміненя. 1) $n = 2$; тоді $p - 1$ паристе, отже $d = (p - 1, 2) = 1$. Критерія Euler'а звучить, як знаємо: $s^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$;

¹⁾ Знаком (m, n) зазначаємо НСП чисел m і n .

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

2) В разі $n=3$ маємо дві можливості: а) $p \equiv 1 \pmod{6}$, б) $p \equiv -1 \pmod{6}$; числа всіх вищих форм не є перві.

а) Коли $p \equiv 1 \pmod{6}$, то $d=3$, отже одинична конгруенція $z^3 \equiv 1 \pmod{p}$ має три розв'язки: $1, \alpha, \alpha^2$, де $\alpha \equiv g^{\frac{p-1}{3}}$. Двочленна конгруенція (10) є рішима, коли $s^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, нерішима, коли $s^{\frac{p-1}{3}} \equiv \alpha$ або α^2 , отже коли один її корінь є r , то два інші є αr і $\alpha^2 r$. Єствує проте $\frac{p-1}{2}$ кубових останків, а $2 \cdot \frac{p-1}{3}$ не-останків; всі класи чисел $GF[p]$ ділять ся на три громади так, що кожне число i тої громади є $\equiv \alpha^i \pmod{p}$ ($i=0, 1, 2$). Кубовий характер числа s значимо так:

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

б) $p \equiv -1 \pmod{6}$; тоді $p-1=6m-2$, отже $d=(6m-2, 3)=1$, проте критерія звучить $z^{p-1} \equiv 1 \pmod{p}$. В таких разі всі числа $GF[p]^*$ є кубовими останками, отже двочленна конгруенція (10) є завжди рішима, зате одинична конгруенція має тільки одну розв'язку, $x \equiv 1$.

3) $n=4$. Тут мусимо розрізнити рівно-ж дві можливості: а) $p \equiv -1 \pmod{4}$, б) $p \equiv +1 \pmod{4}$.

а) Коли p має форму $4m-1$, то $p-1=4m-2$, отже $d=2$; одинична конгруенція $x^4 \equiv 1 \pmod{p}$ може мати очевидно тільки дві розв'язки: $+1$ і -1 . Критерія для двоквадратного характеру числа s є проте ідентична з Euler'овою для квадратних останків; отже кождий квадратний $\left\{ \begin{smallmatrix} \text{останок} \\ \text{не-останок} \end{smallmatrix} \right\}$ є в тім разі і двократним $\left\{ \begin{smallmatrix} \text{останком} \\ \text{не-останком} \end{smallmatrix} \right\}$ того самого числа — і навпаки.

б) В разі $p \equiv 1 \pmod{4}$ є $p-1=4m$, отже $d=4$. Одинична конгруенція має чотири розв'язки; $1, \alpha, \alpha^2, \alpha^3$, 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 виложивка $p-1$, є $\alpha^2 \equiv -1$, а дальше $\alpha^3 \equiv -\alpha$, проте коріні згаданої конгруенції можна написати також так: $1, \alpha, -1, -\alpha$.

Критерією рішимости для $y^4 \equiv s \pmod{p}$ є тут $s^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, а коріні тої конгруенції мають вартости $r, r\alpha, -r, -r\alpha$, де

$r^4 \equiv s \pmod{p}$. Величина $s^{\frac{p-1}{4}}$ може приймати $\pmod{p}$ такі чотири значення: $\pm 1, \pm \alpha$; супроти того всі числа $GF[p]^*$ розпадають на чотири класи, відповідно до того, до якого з перших чотирьох корінїв одиниць $\pmod{p}$ є пристайна його $\frac{p-1}{4}$ -ша степень.

Теорію двоквадратних останків перевів Gauss¹⁾, розширивши обсяг дійсних чисел на числа форми $a + bi$, де i є коренем рівняння $x^2 + 1 = 0$, а a і b належать до $GF[p]$; він дав тим чином початок теорії алгебраїчних чисел. Подібно ужив Eisenstein²⁾ коріння рівняння $x^3 = 1$, т. є величини $\rho = \frac{-1 + i\sqrt{3}}{3}$, до збудовання теорії кубових останків.

§. 3.

11. Займемося тепер далше теорією поля Galois. Ми сказали, що скількість всіх функцій m -того степеня в $GF[p]$

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

є $p^m(p-1)$ згл. p^m — відповідно тому, чи функції, що різняться постійним чинником, будемо вважати різними поміж собою, чи однаковими.

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

$$F_n(x) \equiv 0 \pmod{p} \quad (2)$$

не має корінїв в $GF[p]$. Для того дефініюємо, подібно як в алгебрі або теорії алгебраїчних чисел, її корінї як нові величини, необняті полем Galois степеня p . Отсі величини називають ся миними величинами Galois, бо він перший впровадив їх до теорії конгруенцій.³⁾ — З огляду на те, що конгруенція n -того степеня не може мати більше як n корінїв (уст. 7), дефініює нам кожда незведима конгруенція (2) точно n різних, миних чисел Galois. Проте можемо висказати таку теорему (I), аналогічну до основної теорем алгебри:

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 Ferrussac, 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 конгруенція n -того степеня з первочисельним модулем має рівно n корінів.

12. Утворім функцію (1) з незвідною x . Коли $m \geq n$, то при помочі конгруенції (2) можна зредукувати всі степені незвідної, вищі від $n-1$, так що зістане нам тільки

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

де сочинникови a_0 не накладаємо ніякого обмеження.

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 , слідує звідси, що кождий з n сочинників може приймати тільки p вартостей. Але вона не може бути менша від p^n , бо коли-б було $f(x) \equiv g(x) \pmod{p}$, то звідси слідувало би

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

де b_i є сочинниками функції $g(x)$. Тому x було би коренем конгруенції степеня нижшого ніж n , т. зн. функція $F_n(x)$ мала би з функцією нижшого степеня спільний чинник, отже не могла би бути незведима. Отже дві функції $f(x)$ є тільки тоді рівні згд. пристайні, коли їх дотичні сочинники належать $\pmod{p}$ до однакових класів, а такі функції ми вважаємо ідентичними.

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

$$X^{p^n} \equiv X \pmod{p}. \quad (3)$$

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

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

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

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

Оба ряди, (4) і (4a), складають ся з тих самих величин, тільки в иншій порядку, то-ж і добутки всіх величин кожного ряду є до себе $\pmod{p}$ пристайні:

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

Обі сторони можна скоротити добутком $f_1 f_2 \dots f_{p^n-1}$, бо ні один його чинник не є пристайний до 0 $\pmod{p}$; для того маємо

$$X^{p^n-1} \equiv 1 \pmod{p} \quad (3a)$$

або

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

Отсей взорець є новим узагальненем теореми Fermat'а.

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

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

2) Порівнюючи обі сторони тої ідентичної конгруенції і означаючи через $\sigma_1, \sigma_2, \dots, \sigma_{p^n-1}$ основні симетричні функції величин $f_k(x)$, бачимо, що

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

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

Отсе є узагальнене теорема Wilson'а.¹⁾

3) Зокрема зазначимо, що $\sigma_1 \equiv 0 \pmod{p}$, т. зн.

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

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

Доказ. Величини (4) репродукують ся через чотири основні операції. Що сума, різниця й добуток двох $f(x)$ мають опять ту саму форму, се очевидне; 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 $[g(x)]^{p^n-1}$,

то з огляду на (3а) буде

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

отсе оправдує уживати на означенє квота символічного взірця

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

Проте можемо сказати так:

Загал многочленів в $GF[p]$ степеня $(n-1)$ -ого²⁾ творить поле Galois степеня p^n , коли заамінчиву x прий-

¹⁾ Теорема Wilson'а 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.

немо один з інших корінїв якоїсь незведимої конгруенції 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:

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

де $g(x)$ є сумою всіх прочих членів, отже членів з многочленними сочинниками (Binomialkoeffizienten), а вони всі є многократями числа p . Примінюючи теорему Fermat'a, $a^p \equiv a \pmod{p}$, маємо

$$[f(x)]^p \equiv a_0 (x^p)^{n-1} + a_1 (x^p)^{n-2} + \dots + a_{n-1} \pmod{p},$$

отже

$$[f(x)]^p \equiv f(x^p) \pmod{p}. \quad (7)$$

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:

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

17. Виконаймо отсю субституцію в давній конгруенції

$$F_n(x) \equiv 0 \pmod{p}; \quad (2)$$

се дасть:

$$F_n(x^p) \equiv [F_n(x)]^p \equiv 0 \pmod{p}$$

отже коли x є коренем конгруенції (2), то x^p є її другим коренем.

Так само є $F_n(x^{p^2}) \equiv 0$, $F_n(x^{p^3}) \equiv 0, \dots, F_n(x^{p^{n-1}}) \equiv 0 \pmod{p}$,

отже

Теорема VI. Корінї незведимої конгруенції (2) є

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

де x означає який небудь з її корінїв.

¹⁾ Література 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.

Осєї величини, се власне мнимої числа, які ввів Galois.

Примір. Конґруенція

$$F_3(x) = x^3 - 3x + 1 \equiv 0 \pmod{7}$$

є в $GF[7]$ незведима. Коли x є її коренем, то два другі коріні є x^7 і x^{49} ; їх можна зредувати до многочленів найвище другого степеня при помочи даної конґруенції. Іменно є $x^3 \equiv 3x - 1$, отже $x^7 = (x^3)^2 \cdot x$, а що $(x^3)^2 \equiv 2x^3 + x + 1$, то $x^7 \equiv 2x^3 + x^2 + x \equiv 2(3x - 1) + x^2 + x \equiv x^2 - 2$; далше 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 $-x^4 - 2x^3 + 2x^2 - 3x \equiv x^2 - x + 2$, отже коли x є одним коренем даної конґруенції, то оба другі коріні є $x^7 \equiv x^2 - 2$, $x^{49} \equiv -x^2 - x + 2$. Легко перевірити, що $x(x^2 - 2)(-x^2 - x + 2) \equiv -1 \pmod{7}$.

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

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

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

$$X^s \equiv 1 \pmod{p}, \quad (8)$$

тоді кажемо, що X належить $\pmod{p}$ до виложника s .

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

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

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

Підносячи (6) до степені t , маємо

$$X^{st} \equiv 1 \pmod{p},$$

а що задля (3а)

$$X^{st+r} \equiv 1 \pmod{p},$$

то мусіло би бути також $X^r \equiv 1 \pmod{p}$. Се неможливе, коли $0 < r < s$, бо s є найменшим виложником, для якого сновнюєть 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 $\pmod{p}$ належить до виложника $p - 1$, назвали ми первісним коренем модуля 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

$$1, X, X^2, \dots, X^{p^n-2} \quad (9)$$

складається з $p^n - 1$ поміж собою різних величин того поля, бо реляція

$$X^k \equiv X^l \pmod{p}$$

можлива тільки тоді, коли $k \equiv l \pmod{p^n - 1}$; коли-ж k і l є $\leq p^n - 2$, то це можливе тільки так, що $k = l$, отже два члени з ряду (9) з різними вложниками не можуть бути до себе пристайні $\pmod{p}$. — Супроти того, що кожне X^k є якоюсь величиною з $GF[p^n]$,

$$X^k \equiv f_k(x) \pmod{p},$$

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

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

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

$$\Phi(x) \equiv f(x) \pmod{p, F_n(x)}^1. \quad (1a)$$

Супроти того можемо всі цілі функції з цілочисельними сочинниками поділити на p^n класів; кождо з тих класів будемо характеризувати тою функцією $f(x)$ з $GF[p]$, до котрої вона пристайна $\pmod{p, F_n(x)}$. Тих репрезентантів будемо називати, подібно, як в теорії цілих чисел, повною системою найменших останків подвійного модуля $p, F_n(x)$.

Нехай X означує якогонебудь цілу функцію з цілочисельними сочинниками, отже

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

підносім се рівняне чергою до степенів $p, p^2, \dots, p^n$. Через се одержимо:

¹⁾ Означенє походить від Serret'a, *Algèbre*, t. II, стр. 165 (5 вид.).

$$\begin{aligned} X^p &= [f(x)]^p + [\varphi(x)] [F_n(x)]^p + p \psi_1(x), \\ X^{p^2} &= [f(x)]^{p^2} + [\varphi(x)]^{p^2} [F_n(x)]^{p^2} + p \psi_1(x), \end{aligned}$$

$$X^{p^n} = [f(x)]^{p^n} + [\varphi(x)]^{p^n} [F_n(x)]^{p^n} + p \psi_n(x),$$

де функції $\psi_1(x)$, $\psi_2(x)$..., ближше нас не обходять. Ті рівняння є рівнозначні з системою конгруенцій

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

а що $f(x^{p^n}) \equiv f(x) \pmod{p} \equiv X \pmod{p, F_n(x)}$, то

$$X^{p^n} \equiv X \pmod{p, F_n(x)}. \quad (2)$$

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

Функція $X^{p^n} - X \pmod{p}$ подільна через модульову функцію $F_n(x)$.

20. Взявши (2) можемо написати ще так:

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

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

$$x^{p^n} - x \equiv \varphi(x) F_n(x) \pmod{p}, \quad (3)$$

тому:

Теорема Ia. Функція $x^{p^n} - x \pmod{p}$ подільна через модульову функцію $F_n(x)$.

Теорема II. Функція $x^{p^m} - x \pmod{p}$ подільна через модульову функцію $F_n(x)$, коли m є мною кратю виложника n .

Доказ. Коли $m = kn$, то $x^{p^m} - x$ є подільне через $x^{p^n} - x$, отже теорема доказана. Коли-ж m не є мною кратю n , $m = kn + r$, $0 < r < n$, то з ділення $(x^{p^m}) : (x^{p^n})$ випадає остачок $x^{p^r} - x$. 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 $x^{p^r} - x \equiv \chi(x) F_n(x) \pmod{p}$ для $0 < r < n$.

21. Отже теорема дають нам змогу обчислити скільки незведених $\pmod{p}$ в $GF[p]$ функцій n того степеня. Розложимо іменно праву сторону конгруенції (3) на невідомі чинники:

$$x^{p^n} - x \equiv x F_n(x) G(x) H(x) K(x) \pmod{p}.$$

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

В ряді

$$x, F_n(x), G(x), H(x), \dots, K(x)$$

містять ся всі незведимі функції n -того степеня, бо ми можемо кождо з них приймати за модулову функцію, а що модулова функція містить ся все в $x^{p^n} - x$, то в згаданім ряді мусять виступати всі такі функції, які можуть грати ролю модулових. — Крім них можуть містити ся в тім ряді незведимі функції тільки таких степенів, які є подільні через n ; слідує се з теореми II

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

Нехай n буде першим числом; тоді з $x^{p^n} - x$ треба усунути добуток всіх лінійних чинників, проте добуток всіх незведимих $(\text{mod. } p)$ функцій першого степеня n є

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

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

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

Коли n є зложеним числом,

$$n = a^\alpha b^\beta \dots e^\epsilon,$$

то з $x^{p^n} - x$ мусимо усунути добутки всіх незведимих чинників, яких степені є подільниками числа n . Вводячи скорочене

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

переконаємо ся легко, що бажаний добуток є

$$V = \frac{[n] \prod \left[\frac{n}{d_1 d_2} \right] \prod \left[\frac{n}{d_1 d_2 d_3 d_4} \right] \dots}{\prod \left[\frac{n}{d} \right] \prod \left[\frac{n}{d_1 d_3 d_5} \right]},$$

де $d, d_1, d_2, d_3, \dots$ перебігають всі 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 всіх незведимих функцій n -того степеня є

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

22. Результати з уст. 16. можна узагальнити при помочі пристайності з подвійним модулем.

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

$$X^s \equiv 1 \pmod{p, F_n(x)}, \quad (5)$$

то $p^n - 1$ є подільне через s .

2) Коли $s = p^n - 1$, то X називається первісною величиною в $GF[p^n]$ при подвійнім модулі $p, F_n(x)$. — При помочі степенів первісної величини X можемо представити ціле $GF[p^n]$.

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

Дальше докажемо таку

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

Доказ. Коли X належить $[\text{modd. } p, F_n(x)]$ до виложника s , то в ряді

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

всі величини поміж собою різні, а s -та степе́нь ко́ждої з них є $\equiv 1$, бо для кожного $k < s$ є

$$(X^k)^s = (X^s)^k \equiv 1 \pmod{p, F_n(x)}.$$

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

1) Нехай буде $(k, s) = 1$; тоді в ряді $k, 2k, \dots, (s-1)k$ немає одної множкрати числа s , отже ніяке X^{ik} не може бути $\equiv 1$, коли $t < k$, тому X^k належить до виложника s .

$$2) \text{ Коли } (k, s) = d < 1, \text{ то } (X^k)^{\frac{s}{d}} = (X^{\frac{k}{d}})^s \equiv 1 \pmod{p, F_n(x)}$$

а що $\frac{k}{d}$ і s є супроти себе перві, то X^k належить до виложника $\frac{s}{d}$.

Назв'їм $\psi(d)$ 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

$$\sum \psi(d) = p^n - 1.$$

$$d/p^n - 1$$

З другої сторони є $\sum \varphi(d) = p^n - 1$, 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 $\sum \psi(d) = 0$, друге дає

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

отже наша теорема доведена.

Заключене. 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 мноюкратю чисел s_1 і s_2 .

Доказ. Після заложення є

$$X_1^{s_1} \equiv 1, X_2^{s_2} \equiv 1 \pmod{p, F_n(x)}.$$

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

$$(X_1 X_2)^v \equiv 1 \pmod{p, F_n(x)};$$

НСП чисел s_1 і s_2 назовім d . Піднесім ту конгруенцію до степені $\frac{s_1}{d}$; се дасть

$$X_1^{\frac{v s_1}{d}} X_2^{\frac{v s_2}{d}} \equiv 1 \pmod{p, F_n(x)}$$

Тому, що $\left(\frac{s_1}{d}, s_2\right) = 1$, та конгруенція не може бути сповнена

иначе, 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 подільне через d , друга, що $\frac{v s_1}{d}$ є мноюкратю числа s_2 . Так само побачимо, що $\frac{v s_2}{d}$ є мноюкратю числа s_1 , отже v мноюкратю чисел s_1 і s_2 ; а що v має бути найменшим числом того рода, то наша теорема доведена.

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

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

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

$$\Phi(y) \equiv 0 \pmod{p, F_n(x)}, \quad (6)$$

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

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

Теорема V. Конгруенція (6) не може мати більше корінїв, як виносить її степеень. Коли степеень конгруенції m є рівний n або є подільником того числа, то конгруенція має точно m корінїв.

Докаа. Що конгруенція 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 ; тоді всі функції в $GF[p^n]$ є корінями конгруенції

$$X^{p^n} - X \equiv 0 \pmod{p, F_n(x)}. \quad (2)$$

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

$$X^{p^n} - X \equiv \Phi(X) \Psi(X) \pmod{p},$$

отже

$$\Phi(X) \Psi(X) \equiv 0 \pmod{p, F_n(x)}$$

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

$$\left. \begin{aligned} \Phi(X) &\equiv 0, \\ \Psi(X) &\equiv 0 \end{aligned} \right\} \pmod{p, F_n(x)}.$$

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, ніж виносить її степеень.

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

$$\Phi(X) \equiv 0 \pmod{p, F(x)}$$

буде мати точно m корінїв.

Доказ. Розложім $\Phi(X)$ на незведимі $(\text{mod. } p)$ чинники з $GF[p]$ степенїв $m_1, m_2, \dots, m_\mu$:

$$\Phi(X) \equiv \Phi_1(X) \Phi_2(X) \dots \Phi_\mu(X) \pmod{p};$$

кождий з них буде містити ся $(\text{mod. } p)$ в одній з функцій

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

а коли n є н.с.м¹⁾ чисел $m_1, m_2, \dots, m_\mu$, то всі 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 конгруенцій $\Phi_k(x) \equiv 0$ буде мати при тім самим подвійнім модулі $p, F(x)$ на основі теореми IV. m_k корінїв. Проте добуток тих функцій $\Phi_k(x)$ словнює вимоги нашої теореми.

¹⁾ т. є. найменша спільна кратність.

26. Теорема VII. Коли X є корінем конгруенції (6), то інші її коріні є $X^p, X^{p^2}, \dots, X^{p^{n-1}}$.

Доказ. Подібно як в уст. 52 знаходимо, що

$$[\Phi(X)]^{p^k} \equiv \Phi(X^{p^k}) \equiv 0 \pmod{p, F_n(x)}$$

для $k=0, 1, \dots, n-1$, та що дві різні степені з пов'язаного ряду є поміж собою різні. Отже теорема доказана.

Заклучене. Конгруенція $F_n(x) \equiv 0 \pmod{p}$ т. зн. $F_n(x) \equiv 0 \pmod{p, F_n(x)}$ має такі коріні: $x, x^p, x^{p^2}, \dots, x^{p^{n-1}}$.

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

Доказ. В уст. 21 мали ми такий розклад:

$x^{p^n} - x \equiv F_n(x) G_n(x) \dots K_n(x) L(x) P(x) \pmod{p}$;
тут означають $F_n(x), G_n(x), \dots, K_n(x)$ незведимі функції степеня n , $L(x), \dots, P(x)$ функції прочих допустимих степенів. Коли x є елементом з $GF[p^n]$, то

$$x^{p^n} - x \equiv 0 \pmod{p},$$

отже

$$F_n(x) G_n(x) \dots K_n(x) S(x) \equiv 0 \pmod{p},$$

де в $S(x)$ з'єднані всі функції нижчих степенів, — т. зн., що x може бути коренем одної, і тільки одної, з поміж незведимих конгруенцій

$$\left. \begin{aligned} F_n(x) &\equiv 0, \\ G_n(x) &\equiv 0, \\ K_n(x) &\equiv 0 \end{aligned} \right\} \pmod{p}.$$

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

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

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

де i дане конгруенцією $i^3 \equiv 2 \pmod{7}$. Коли хочемо представити те саме поле Galois при помочі функції $x^3 - 3$, назовім j корінь конгруенції $j^3 \equiv 3 \pmod{7}$, тоді $GF[7^3]$ є дане функцією

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

Величини i і j можна виразити одну через другу. Іменно одержуємо через помноження обох дефініційних конгруенцій

$$i^3 j^3 \equiv -1 \pmod{7},$$

отже $ij \equiv 3$ або 3α або $3\alpha^2$, де α дане реляцією $\alpha^2 + \alpha + 1 \equiv 0 \pmod{7}$, т. зн. $\alpha \equiv 2$. Проте є пр. $ij \equiv 3$. Помножім ту конгру-

енцію через j^2 , то одержимо $i^3 j \equiv 3$, т. зн. $j \equiv -2i^2 \pmod{7}$, а даліше $j^2 \equiv i$, т. зн.

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

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

28. Теорема IX. Степенем поля Galois може бути тільки степені першого числа.

Доказ. Ми бачили в уст. 4, що поле Galois найвищого степеня складається з p елементів, коли p є першим числом. Нехай x_1 буде одною з величин поля Galois степеня вищого ніж p ; тоді формулка $c_1 x_1$, де c_1 належить до $GF[p]$, т. є ряд величин $0x_1, 1x_1, 2x_1, \dots, (p-1)x_1$, не вичерпують ще цілого поля. Проте можуть виступати ще якась інша величина x_2 , не обнята тамтим рядом. Утворім всі можливі суми

$$c_1 x_1 + c_2 x_2.$$

де c_1 і c_2 перебігають ціле $GF[p]$; скількисть тих сум виводить p^2 , бо тільки одна з них є 0, а однакових поміж ними нема. — Ті суми або вичерпують поле Galois, або ні. В першому разі маємо $GF[p^2]$, в другому разі виступає ще нова величина x_3 , при помочі якої творимо даліші суми

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

і т. д. Таким чином бачимо, що степені поля Galois може бути тільки степені першого числа; отже можна дібрати таких n елементів $x_1, x_2, \dots, x_n$, що всі можливі комбінації чисел з $GF[p]$ в сочавниках суми

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

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

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

Теорема XI. Поміж величинами (7) є тільки одна ідентично пристайна $\pmod{p}$ до зера, або вишшиє словами: елементи основи поля Galois є лінійно незалежні.

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

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

Реляція $X \equiv 0$ можлива тільки так, що всі $c'_k \equiv 0 \pmod{p}$; коли-б так не було, то первісна величина $GF[p^n]$ сповнювала би конгру-

енцію степеня нижшого як n , а се неможливе, бо x є корінем незведимої конгруенції степеня n . — Отже поміж елементами основи поля Galois не може вступувати ніяка вища лінійна зв'язь, як тільки та, що всі сочинники $\varepsilon \equiv 0 \pmod{p}$, т. зн. ті елементи є лінійно незалежні¹⁾.

§. 5.

29. Щоби знайти первісні коріні конгруенції

$$X^{p^n} - X \equiv 0 \pmod{p, F_n(x)}, \quad (1)$$

маємо після уст. 23 (заключення 2) вишукати первісні коріні конгруенцій

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

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

Коли модулова функція $F_n(x)$ належать $\pmod{p}$ до виложника $p^n - 1$, то всі її коріні є первісними величинами в $GF[p^n]$.

30. Коли знайдемо одну з незведених $\pmod{p}$ функцій степеня n в $GF[p]$, $F_n(x)$, шукаємо при її помочи первісного коріня конгруенції (1). Тоді можемо розложити ліву сторону тої конгруенції на незведимі чинники.

Нехай X буде первісним корінем конгруенції (1); його k -та степеня буде сповнювати якусь незведиму в $GF[p]$ конгруенцію

$$\Phi(x) \equiv 0 \pmod{p, F_n(x)} \quad (2)$$

степеня $m = n$ або $\frac{n}{d}$; коріні тої конгруенції будуть

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

отже будемо мати

$$\Phi(u) \equiv (u - X^k)(u - X^{kp}) \dots (u - X^{kp^{m-1}}) \pmod{p, F_n(x)},$$

Тому, що $X^{kp^m} \equiv X^k$, отже $X^{k(p^m-1)} \equiv 1 \pmod{p, F_n(x)}$, мусить бути виложник $k(p^m - 1)$ многократно числа $p^n - 1$, отже m мусить бути таким найменшим числом, для якого $p^m - 1$ є подільне через n ; се висказується так, що X відповідає (passt) виложникови m .²⁾

Коли X^k належить до виложника s , то ks є подільне через $p^n - 1$, отже s є многократно числа n , а що ота конгруенція спов-

¹⁾ Пор. аналогічну теорему з теорії алгебраїчних чисел. Гл. пр. Weber, Algebra, Bd. II (2 Aufl.), §. 161.

²⁾ Encyclopädie der math. Wiss. Bd. I. 1, p. 575.

нують ся для $n = s$, то X^k належить до виложника n . Але і $\Phi(X)$ належить до того самого виложника, як се легко перевірити; проте коли хочемо знайти всі незведимі конгруенції степеня n і всіх інших допустимих степенів, беремо за k якунебудь многократно числа n , першу супроти n .

31. Galois пояснює свою теорію на такім прикладі: знайти незведиму конгруенцію, від якої залежать первісні корені двочленної конгруенції

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

Тут є $p = 7$, $n = 3$. Одною з незведимих $\pmod{7}$ функцій третього степеня є $x^3 - 2$, отже творимо $GF[7^3]$ з функцій

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

Нашою задачею є, знайти таку величину $X = f(x)$, якої всі степені, від аерової до $(7^3 - 1)$ -ої включно, мають вичерпати всі корені конгруенції

$$X^{7^3-1} - 1 \equiv X^{2 \cdot 3 \cdot 19} - 1 \equiv 0 \pmod{7}.$$

Після уст. 81. маємо помножити через себе первісні корені таких трьох конгруенцій

$$\left. \begin{aligned} X^2 &\equiv 1 \\ X^{3^2} &\equiv 1 \\ X^{19} &\equiv 1 \end{aligned} \right\} \pmod{7}. \quad (**)$$

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

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

Назв'їм корінь першої з них x , то x є первісним коренем середньої конгруенції в системі (**).

Врешті шукаємо первісного кореня третьої конгруенції. 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 розвинення слідуєть такі вартости: $a \equiv 1$, $b \equiv -1$, отже $f(x) \equiv x - 1$ є тим первісним коренем. Помнож'їм через себе ті три знайдені первісні корені, то одержимо первісний корінь конгруенції (*):

$$X \equiv -1 \cdot x \cdot (x - 1) \equiv -x^2 + x \pmod{7}. \quad (***)$$

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

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

II. Конгруєнції третього і четвертого степеня.

§. 6.

Конгруєнції третього степеня.

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

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

Метода, яку примінює Саусху, полягає на зведенню повної конгруєнції до двочленної; в вона зовсім аналогічна до методи Lagrange'а при рівняннях третього степеня. Саусху розв'язує в тій цілі одну двочленну конгруєнцію третього степеня і дві квадратні.

33. Двочленні конгруєнції. Спеціальна (однична) конгруєнція

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

має завжди один дійсний корінь 1 і ще два інші, γ і γ^2 , зв'язані реляцією

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

ми назвали їх первісними третими коріннями одніці $\pmod{p}$. Розв'язуючи ту квадратну конгруєнцію, або примінюючи результати уст. 10, бачимо, що коли $p \equiv 1 \pmod{6}$, то γ і γ^2 є дійсні, а саме

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

означимо їх через α і α^2 . В разі $p \equiv -1 \pmod{6}$ 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 конгруєнція

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

зводиться до попередньої. Нехай r буде одним з її корінїв, тоді два інші корінї є, як знаємо, $r\gamma$ і $r\gamma^2$.

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

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

де $d = (p-1, 3)$, отже коли $p \equiv 1 \pmod{6}$, то $d = 3$, проте критерій звучить

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

Коли вона сповнена, то конгруєнція має три дійсні корінї:

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

В противнім разі назв'їм j одну з первісних величин в $GF[p^2]$; тоді три корінї є

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

Коли $p \equiv -1 \pmod{6}$, то A є все третім степенним останком, отже конгруенція (3) має все один дійсний корінь r . Зате два інші коріні належать до $GF[p^3]$, отже (3) має такі три коріні

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

35. Повну конгруенцію третього степеня (1) множимо числом α_0' , стоваришеним $\pmod{p}$ з числом α_0 , і при помочі лінійного підставлення усуваємо член з квадратом невідомої; через те одержимо зредукowaną конгруенцію

$$y^3 - 3Ay - 2B \equiv 0 \pmod{p}. \quad (4)$$

Назв'їм її коріні y_1, y_2, y_3 і утворім при їх помочі такі дві резольвенти:

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

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

де $\gamma^2 + \gamma + 1 \equiv 0 \pmod{p}$. 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 $\sigma_1 = 0$, $\sigma_2 = -3A$, $\sigma_3 = 2B$ (основні симетричні функції корінів), маємо

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

отже квадратна конгруенція для v_1 і v_2 є

$$v^2 - 2Bv + A^3 \equiv 0 \pmod{p}. \quad (5)$$

Виріжник тої конгруенції, а заразом і конгруенції (3), є

$$D \equiv B^2 - A^3 \pmod{p}. \quad (6)$$

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

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

проте зістає ще до розв'язки конгруенція

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

Коли се стало ся і $t \equiv t_1$ є її розв'язкою для $v \equiv v_1$, то для $v \equiv v_2$ одержимо $t \equiv t_2$, обмежуючи ся в виборі корінів конгруенції (7), подібно як при формулці Cardan'a, реляцією

$$t_1 t_2 \equiv A \pmod{p}$$

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

$$y_1 + y_2 + y_3 \equiv 0,$$

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

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

а звідси:

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

Бачимо отже, що розв'язка даної конгруенції (4) зводиться до трьох інших:

- 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 $t^3 \equiv B + \beta \equiv C$, всі (mod. p).

36. Дискусія розв'язки. 1) Конгруенція для v є зведима або ні, відповідно до того, чи

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

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

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

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

при $p = 6n - 1$ є вона все зведима.

Займемося перше дискусією вирізняка D

I. $D \equiv 0 \pmod{p}$; тоді є $v_1 \equiv v_2 \equiv B$, отже $t_1 = t_2 = t$; t є дійсне, бо тоді $t^2 \equiv A$, а що $A^3 \equiv B^2$, то $\left(\frac{A}{p}\right) = \left(\frac{A^3}{p}\right) = \left(\frac{B^2}{p}\right) = +1$.
Тоді є $y_1 = 2t$, $y_2 = y_3 = (\gamma + \gamma^2)t \equiv -t$. Отже коли чисельна вартість вирізняка є многократною модуля, то конгруенція має одну двократну розв'язку. — Щоби розв'язка була трикратна, мусять ще бути $2t \equiv -t$, т. зв. $t \equiv 0 \pmod{p}$, отже і $A \equiv B \equiv 0 \pmod{p}$. Тоді трикратна розв'язка є $y \equiv 0$, отже коли від y перейдемо до x через лінійну субституцію, то трикратна розв'язка буде $x \equiv c$, т. зв. дава конгруенція звучить: $(x - c)^3 \equiv 0 \pmod{p}$.

II. $\left(\frac{D}{p}\right) = +1$; в такому разі зложім $r^2 \equiv D$, отже буде r дійсне, $v \equiv B \pm r \equiv C$ дійсне. Тепер розв'язуємо

$$t^3 \equiv C \pmod{p}. \quad (7a)$$

1) Коли $p \equiv 1 \pmod{6}$, тоді є такі можливості:

$$a) \left[\frac{C}{p}\right] = 1, \quad b) \left[\frac{C}{p}\right] \neq 1.$$

a) Коли C є кубовим остатком, то t є дійсне $= \tau$, а що і γ є дійсне $= \alpha$, то маємо

$$\left. \begin{aligned} y_1 &\equiv \tau_1 + \tau_2, \\ y_2 &\equiv \alpha^2 \tau_1 + \alpha \tau_2, \\ y_3 &\equiv \alpha \tau_1 + \alpha^2 \tau_2, \\ \alpha^2 + \alpha + 1 &\equiv 0 \end{aligned} \right\} \pmod{p}.$$

Всі три розв'язки є дійсні, різні поміж собою.

6) Коли C є не-останком, то t належить до $GF[p^3]$, отже $t \equiv j$, 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 розв'язці буде приходити тільки одна j . Іменно в $j_1^3 j_2 \equiv A j_1^2$; помножимо $M C \equiv A$, то $j_2 \equiv M j_1^2$, отже коли напишемо j за j_1 , а $M j^2$ за j_2 , то:

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

В тім разі є всі три розв'язки величинами в $GF[p^3]$, а наша розв'язка лежала в тім, що ми виразили всі три y при помочі коріння можливо найпростішої модулової функції $j^3 - C \equiv 0 \pmod{p}$.

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

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

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

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

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

Заложимо

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

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

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

Порівняння 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 конгруенція є рішима, то обі ті реляції є рівночасно рішимами в дійсних числах, отже маємо

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

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

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

Отже одна розв'язка є дійсна, дві інші 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 $(\varepsilon i)^2 \equiv -3D$, а коли $\left(\frac{D}{p}\right) = -1$, то $\left(\frac{-3D}{p}\right) = +1$. Отже маємо

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

Проте в тім разі маємо три дійсні розв'язки; тут маємо повну аналогію до casus irreducibilis рівнянь 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 $\vartheta \equiv 5i$, т. зн. $\vartheta^2 \equiv -1 \pmod{11}$ отже ϑ буде мати вартість звичайного Gauss-ового символу i . Супроти того квадратна ресольвента прийме вид

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

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

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

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

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

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

$$\left. \begin{aligned} y_1 &\equiv 2 \\ y_2 &\equiv -1 - 5 \equiv -6 \\ y_3 &\equiv -1 + 5 \equiv 4 \end{aligned} \right\} \pmod{11}.$$

IV. Коли ж дана конгруенція є незведима, то всі три розв'язки належать до $GF[p^3]$, а модулова функція не дасть ся в тім разі звести до двоиченної. Назв'їм один корінь даної конгруенції j , то два інші коріні є j^p і j^{p^2} .

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

В разі $p \equiv -1 \pmod{4}$ є $\left(\frac{-1}{p}\right) = -1$, отже оба корінні конгруєнції (8а) є в $GF[p^2]$. Назв'ємо одну з величин в $GF[p^2]$ γ , тоді маємо такі корінні конгруєнції (8):

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

39. Для загальної двочленної конгруєнції

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

є критерієм рішимості $A^{\frac{p-1}{4}} \equiv 1 \pmod{p}$; в разі $p \equiv 1 \pmod{4}$ мусить отже бути A двоквадратним, в разі $p \equiv -1 \pmod{4}$ квадратним останком. Проте в першій разі має конгруєнція (9) 4 або 0 дійсних коріннів,

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

в другій разі 2 або 0 дійсних

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

Коли критерій рішимості несповнена, тоді дефініює дана конгруєнція $GF[p^4]$.

40. Повну конгруєнцію четвертого степеня

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

зводимо до зредукованої форми

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

Нехай її корінні 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 три ресольвенти:

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

або коли положимо для скорочення

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

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 конгруєнцію, від якої залежать v_1, v_2, v_3 , творимо основні симетричні функції

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

де $\tau_1 = a + b + c$, $\tau_2 = ab + bc + ca$, $\tau_3 = abc$. 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 вартості функцій σ маємо

$$\tau_1 = 48L,$$

$$\tau_2 = 16.12(3L^2 + N),$$

$$\tau_3 = 64.16M^2.$$

Звідси слідує передовсім

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

а проте можемо обі інші функції написати так:

$$16(v_1v_2 + v_2v_3 + v_3v_1) = \tau_2 - 16\tau_1L,$$

$$64v_1v_2v_3 = \tau_3 - 16\tau_2L + 2.16^3L^3,$$

отже врешті є

$$v_1v_1 + v_2v_3 + v_3v_1 = -12(L^2 - N),$$

$$v_1v_2v_3 = 16(M^2 - 3LN - L^3).$$

Проте конгруенція для v (решовента третього степеня) є

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

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

$$a \equiv 4v_1 + 16L,$$

$$b \equiv 4v_2 + 16L,$$

$$c \equiv 4v_3 + 16L$$

і розв'язуємо три квадратні конгруенції

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

Коли маємо їх коріні, знаходимо коріні даної конгруенції (11) з

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

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 конгруенцій (14) одержуємо по дві вартості на X, Y, Z ; в розв'язці (15) треба їх так комбінувати, щоби було

$$4XYZ \equiv M \pmod{p}, \quad (16)$$

отже, коли заложимо, що $M \not\equiv 0 \pmod{p}$ додатне, т. зн. $< \frac{p-1}{2}$, то скількість відємних $\pmod{p}$ величин, т. є $X, Y, Z > \frac{p-1}{2}$, буде 0 або 2. Можна також так поступити, що знайшовши дві з них, третю винаходимо з реляції (16).

41. Дискусія. Конгруенція (11) і її резольвента (13)¹⁾ мають однаковий вирішник

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

Від нього залежить якість розв'язки.

1. Коли $D \equiv 0 \pmod{p}$, 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 $\equiv 0 \pmod{p}$, проте резольвента є

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

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

$$L^2 - N \equiv 0, \quad M^2 - 3LN - L^3 \equiv 0 \pmod{p},$$

тому панують поміж ними такі зв'язи:

$$N \equiv L^2, \quad M^2 \equiv 4L^3 \pmod{p},$$

отже L мусить бути квадратним останком для p .

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

$$X^2 \equiv L \pmod{p},$$

а що $\left(\frac{L}{p}\right) = +1$, то ця конгруенція є рішима, отже X дійсне. Назв'їм її корінь X , тоді є $Y \equiv Z \equiv X$, проте

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

Конгруенція четвертого степеня, якої резольвента (13) має потрійний корінь, виглядає так:

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

отже вона має один однократний, один трикратний корінь.

Замітка. Коли $X \equiv 0$, тоді $f(y)$ має чотирикратний корінь; тоді є $L \equiv 0$, отже і $M \equiv 0$, $N \equiv 0$, а конгруенція звучить $f(y) = y^4 \equiv 0 \pmod{p}$.

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

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

¹⁾ Резольвентами називаємо і функції, яких уживаємо до розв'язки рівняня (чи конгруенції), і рівняня (конгруенцію), від якого вона залежить. Непорозуміння нема тут чого побоювати ся.

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

$$\begin{aligned} \alpha &\equiv 4(4L + 2z), \\ b = c &\equiv 4(4L - z). \end{aligned}$$

Дальше розв'язуємо

$$\left. \begin{aligned} 16X^2 &\equiv 4(4L + 2z) \\ 16Y^2 &\equiv 16Z^2 \equiv 4(4L - z) \end{aligned} \right\} \pmod{p} \quad (18)$$

і маємо в решті

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

отже один двократний корінь. Другий корінь є лише тоді двократний, коли $Y \equiv 0 \pmod{p}$.

а) $Y \not\equiv 0 \pmod{p}$. В таких разі (11) виглядає так:

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

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

$$\left. \begin{aligned} 2\gamma\delta &\equiv \alpha\beta \\ (2\alpha^2 + \gamma^2 + \delta^2 i^2)\beta &\equiv 0 \\ (\alpha\beta - 2\gamma\delta)(\alpha^2 + \beta^2 i^2) &\equiv 2\alpha\beta(\gamma^2 + \delta^2 i^2) \end{aligned} \right\} \pmod{p}.$$

Супроти першої реляції зводить ся третя до

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

а в злучі з другою дає $\alpha^3\beta \equiv 0$. Звідси слідує, що мусять 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 ніякого зовнішнього обмеження, як тільки те, що одна з них $\equiv 0$, т. зн. Y^2 є дійсне. Коли-ж $\alpha \equiv 0$, $\beta \not\equiv 0$, тоді з другої реляції слідує $\gamma \equiv \delta \equiv 0$; отже коли в X дійсна частина $\equiv 0$, тоді ϵ або $X \equiv 0$, або $Y \equiv 0 \pmod{p}$. Проте всі сочинники конгруенції (11a) є дійсні, і корінь або всі дійсні, або двократний дійсний, а два прочі належать до $GF[p^2]$.

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

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

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

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

42. Коли циклічний визначник Δ , степеня $p-1$, утворений з сочинників ресольвенти $\varphi(v)$, є пристайний до $0 \pmod{p}$, тоді $\varphi(v) \equiv 0$ має три або один дійсний корінь, відповідно до квадратного характеру величини $R \equiv -3D$.

II. $\left(\frac{R}{p}\right) = +1$; v_1, v_2, v_3 є дійсні, різні поміж собою. Утво-

рім a, b, c і означім характери символів $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{c}{p}\right)$. З поміж усіх можливих їх комбінацій є допустимі такі:

а) один з поміж тих символів $\equiv 0$;

б) два або три символи $\equiv 0$;

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

δ) один символ $\equiv +1$, два -1 .

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

а) Коли одна з величин $a, b, c \equiv 0$, тоді мусять бути одно $v \equiv -4L$; коли поділимо $\varphi(v)$ через $v + 4L$, одержимо як вимогу подільності $M \equiv 0$, отже ресольвента має такі коріні:

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

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

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

α₁) Коли $\left(\frac{3N}{p}\right) = +1$, то v_2 і v_3 є дійсні, а Y і Z дійсні або мнимі, відповідно до характерів величин $6L \pm 2T$.

α₂) Коли $\left(\frac{3N}{p}\right) = -1$, то v_2 і v_3 належать до $GF[p^2]$,

отже маємо

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

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

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

Елімінуємо з другої конгруенції $\beta \equiv \frac{1}{4\alpha}$, одержимо

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

При помочи α виразимо коріні y так:

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

де $2\beta \in \pmod{p}$ товаришем величини 2α .

Конгруенція для α (18) є рівнозначна з

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

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

В першій разі, $\left(\frac{9L^2 - 3N}{p}\right) = +1$, 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 разі $+1$ є α дійсне, отже y_1 і y_2 дійсні, а y_3 і y_4 належать до $GF[p^2]$; в разі -1 дієть ся навпаки. Тому, коли $\left(\frac{9L^2 - 3N}{p}\right) = +1$, маємо два коріні дійсні, протилежних 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 конгруенції

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

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

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

отже шукана розвязка звучить:

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

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

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

$$y^2 \equiv 7L \text{ і } -L.$$

Одержуємо проте дві пари коріння рівних, з протилежними знаками;
вони можуть або бути дійсними, або належати до $GF[p^2]$.

Коли-ж всі три символи $\epsilon \equiv 0$, то звідси слідує $L \equiv 0$, отже
маємо чотирократний корінь $y \equiv 0$.

γ) Коли всі три символи, $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{c}{p}\right), \epsilon \equiv +1$, то X, Y, Z
є дійсними; дана конгруенція має чотири різні, дійсні розв'язки.

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

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

а маючи їх, одержуємо такі коріння конгруенції (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 розв'язок: одну дійсну, другу
спряжену в $GF[p^2]$.

43. В разі, коли III $\left(\frac{R}{p}\right) = -1$, ресольвента має один дій-
сний корінь, а два інші 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 α, β, ϵ мають рівно-ж форму $A + Bi$. В тім разі нале-
жать коріння y або до $GF[p^2]$, або до $GF[p^4]$, подібно як по-
передно.

IV. Коли ресольвента $\varphi(v) \equiv 0 \pmod{p}$ є незведима, то
 X, Y, Z , які залежать від її коріння, є величинами, спряженими

в $GF[p^3]$. Отже $X + Y + Z$ є дійсне, т. зн. y_1 є дійсне, а три інші корені належать до $GF[p^3]$.

44. Як виконувати операції на величинах поля Galois, покажемо на наступному прикладі:

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

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

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

Тому є

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

Перша зводиться до

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

а що $\left(\frac{3}{19}\right) = -1$, то X належить до $GF[p^2]$; проте можемо його виразити через i . Робимо це 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

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

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

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

Звідси елімінуємо β і одержуємо

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

або

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

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

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

коли знова обмежимося до одного тільки знака.

Величина α , дана конгруенцією (***), дефініює $GF[p^4]$; при помочі реляції ($\dagger$) можемо представити $GF[p^2]$, т. зн. i , через α :

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

Остаточно треба ще виразити βi згл. βi через α . З $\alpha\beta \equiv 5 \pmod{19}$ слідує $\alpha^3\beta i \equiv 5\alpha i$, т. зн.

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

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

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

отже даліше

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

т. зн.

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

Маємо отже

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

Звідси слідує коріні даної конгруенції, виражені при помочі корінів простішої конгруенції (**):

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

45. Як примір, в якім ресольвента 3. степеня є незведима, отже приходить ся розв'язувати квадратні конгруенції в $GF[p^3]$, розв'яжемо таку конгруенцію:

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

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

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

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

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

а квадратні конгруенції для X , Y , Z зводять ся до

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

Першу з них розв'яжемо так, що покладемо $X \equiv \alpha j^2 + \beta j + \gamma$, і визначуємо α , β , γ з

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

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 зв'язи

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

т. є

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

Добуток XY є $\vartheta \equiv 2j^2 - 3j - 3$, 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 $7^3 - 1 = 342 = 2 \cdot 3^2 \cdot 19$. Піднесім ϑ до степеней 2, 3, 6, ..., то знайдемо $\vartheta^{57} \equiv 2$, отже

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

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 конгруенції є

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

Берлін, май — червень 1913.

R é s u m é.

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

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

reduziert, wird mit Hilfe der Resolventen gelöst:

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

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 von 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

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

die von

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

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

nennt man ihre Lösungen $4X, 4Y, 4Z$, 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.

