$$\frac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5}.$$

Łatwo zauważyć, że z równań (3) i (4) podobną drogą można otrzymać tożsamościowy układ z układem (8) dla ilości $A_{2,i}$, $A_{2,k}$, $A_{2,l}$, $A_{2,m}$, $A_{2,r}$, z którego podobnie wypływa

$$A_{2,i} : A_{2,k} : A_{2,l} : A_{2,m} : A_{2,r} = \Delta_1 : \Delta_2 : \Delta_3 : \Delta_4 : \Delta_5 . \tag{10}$$

Przez porównanie związków (9) i (10) otrzymujemy

$$A_{1,i} : A_{1,k} : A_{1,l} : A_{1,m} : A_{1,r} = A_{2,i} : A_{2,k} : A_{2,l} : A_{2,m} : A_{2,r} ,$$

co jest, wogóle, niemożliwem. Wniosek stąd, że koniecznie muszą zachodzić następujące równania:

$$\Delta_1 = \Delta_2 = \Delta_3 = \Delta_4 = \Delta_5 = 0 \tag{11}$$

czyli, że układ (8) jest nieoznaczony.

Równania (11) przedstawiają jeden układ warunków całkowalności dla równania (1). Kombinując skaźniki i, k, l, m, r przy różnych ich wartościach $1, 2, \ldots, n$, otrzymamy wszystkie pozostałe układy warunków całkowalności. Sposoby całkowania równania (1), posiadającego dwie całki, wyłożyłem w dodatku do *„Zbioru przykładów i odpowiedzi na kwadratury równań różniczkowych“* [1]).

Płock, w październiku 1892 r.

[1]) Wydanie z zapomogi kasy imienia J. Mianowskiego, Warszawa 1892 r.

O KONGRUENCYI

$x^n + A_1 x^{n-1} + A_2 x^{n-2} + \ldots + A_n \equiv 0 \pmod{p}$ [1]).

NAPISAŁ

E. SNOPEK.

König i Rados z Budapesztu [2]) podali następujący warunek konieczny i dostateczny istnienia pierwiastków kongruencyi

$$a'_0 x^n + a'_1 x^{n-1} + a'_2 x^{n-2} + \ldots + a'_n \equiv 0 \pmod{p} \tag{1}$$

gdzie a'_0, a'_1, a'_2, . . . , a'_n są liczby całkowite (dodatnie i ujemne), a p jest liczbą pierwszą:

I. Kongruencya (1) sprowadzona za pomocą związku $x^{p-1} - 1 \equiv 0 \pmod{p}$ do formy

$$\varphi(x) = b_0 x^{p-2} + b_1 x^{p-3} + \ldots + b_{p-2} \equiv 0 \pmod{p} \tag{2}$$

posiada wtedy przynajmniéj jeden pierwiastek ($< p$), gdy wyznacznik

[1]) Temat téj krótkiéj rozprawki jak również zachętę do jéj opracowania zawdzięczam memu szanownemu Prof. D-rowi J. Puzynie, w którego ćwiczeniach matematycznych w roku szkolnym 1891/92 teoryą liczb się zajmowano.

[2]) Zur Theorie der höheren Congruenzen, Journal für die reine und angewandte Mathematik, XCIX, str. 258—260.

$$B = \begin{vmatrix} b_0, & b_1, & b_2, & \ldots, & b_{p-3}, & b_{p-2} \\ b_1, & b_2, & b_3, & \ldots, & b_{p-2}, & b_0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ b_{p-3}, & b_{p-2}, & b_0, & \ldots, & b_{p-5}, & b_{p-4} \\ b_{p-2}, & b_0, & b_1, & \ldots, & b_{p-4}, & b_{p-3} \end{vmatrix} \equiv 0 \ (\text{mod.}\, p). \qquad (3)$$

W razie $n < p-2$, możemy kongruencyą (1) dopełnić wyrazami o współczynnikach podzielnych przez p (lub $\equiv 0$) aż do stopnia $p-2$, tak, że tylko z kongruencyami stopnia $(p-2)$-go mieć będziemy do czynienia.

Gdy w wyznaczniku B wszystkie podwyznaczniki pierwsze są $\equiv 0$ (mod. p), to $\varphi(x) \equiv 0$ (mod. p) posiada dwa liniowo od siebie w znaczeniu kongruencyi zależne pierwiastki.

Prócz kryteryum Radosa istnieje jeszcze inne podane przez Schönemanna a mianowicie.

II. Gdy

$$\varphi(1) \,.\, \varphi(2) \ldots \varphi(p-1) \equiv \prod_{h=1,2,\ldots,n} (\varrho_h^{p-1} - 1) \ (\text{mod}\, p), \qquad (4)$$

gdzie $\varphi(1) \,.\, \varphi(2) \ldots \varphi(p-1)$ jest widocznie funkcyą symetryczną liczb $1, 2, \ldots, p-1$, a ϱ_h są pierwiastkami równania $\varphi(x) = 0$, to $\varphi(x) \equiv 0$ (mod. p) posiada pierwiastki.

Gdy $\varphi(x) \equiv 0$ (mod. p) posiada przynajmniéj jeden pierwiastek ($< p$), to w związku (4) po lewéj stronie jeden przynajmniéj z czynników

$$\varphi(\lambda), \ \lambda = 1, 2, \ldots, p-1$$

musi być $\equiv 0$ (mod. p). Wtedy już i cały iloczyn $\varphi(1) . \varphi(2) \ldots \varphi(p-1) \equiv 0$ (mod. p), i prawa strona związku (4) musi być podzielną przez p, a stąd wynika, że kryteryum Schönemanna da się także wyrazić kongruencyą:

$$\prod_{h=1,2,\ldots,n} (\varrho_h^{p-1} - 1) \equiv 0 \ (\text{mod.}\, p) \qquad (5)$$

Mając kryterya I i II udowodnimy, że każde z nich jest tylko inną formą drugiego, czyli inaczéj, że oba kryterya wyrażają jedno i to samo.

Wyznacznik B przedstawił Stern [1]) następującym iloczynem

[1]) Günther, Lehrbuch de Determinantentheorie, str. 84.

$$B = \prod_{\lambda=0}^{p-2} (b_0 + \alpha^{\lambda} b_1 + \alpha^{2\lambda} b_2 + \ldots + \alpha^{\lambda(p-2)} b_{p-2}); \qquad (6)$$

α jest tu pierwiastkiem pierwotnym równania

$$z^{p-1} - 1 = 0.$$

Pomnóżmy kongruencyą $\varphi(x) \equiv 0$ (mod. p) przez takie γ, (co jest możliwe, gdy zakładamy b_0 pierwsze względem p), aby

$$b_0 \gamma \equiv 1 \ (\text{mod.}\, p)$$

i zastąpmy wszystkie $b_k \gamma$ przez reszty najmniejsze (dodatnie), to kongruencya (2) przybierze postać

$$f(x) = x^{p-2} + a_1 x^{p-3} + \ldots + a_{p-2} \equiv 0 \ (\text{mod.}\, p). \qquad (7)$$

Warunek Radosa w zastosowaniu do téj kongruencyi ma postać:

$$D = \begin{vmatrix} 1, & a_1, & a_2, & \ldots, & a_{p-3}, & a_{p-2} \\ a_1, & a_2, & a_3, & \ldots, & a_{p-2}, & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ a_{p-2}, & 1, & a_1, & \ldots, & a_{p-4}, & a_{p-3} \end{vmatrix} \equiv 0 \ (\text{mod.}\, p), \qquad (8)$$

czyli na podstawie (6):

$$D = \prod_{\lambda=0}^{p-2} (1 + \alpha^{\lambda} a_1 + \alpha^{2\lambda} a_2 + \ldots + \alpha^{\lambda(p-2)} a_{p-2}) = \prod_{\lambda=0}^{p-2} g(\alpha^{\lambda}) \equiv 0 \ (\text{mod.}\, p). \qquad (9)$$

gdzie

$$g(\alpha^{\lambda}) = 1 + \alpha^{\lambda} a_1 + \alpha^{2\lambda} a_2 + \ldots + \alpha^{\lambda(p-2)} a_{p-2}.$$

Pierwiastkami równania $f(x) = 0$ niech będą

$$\varrho_1, \varrho_2, \ldots, \varrho_{p-2}.$$

Ponieważ

$$\begin{aligned} a_1 &= -\Sigma \varrho_1, \\ a_2 &= \Sigma \varrho_1 \varrho_2, \\ &\vdots \\ a_{p-2} &= -\varrho_1 \varrho_2 \ldots \varrho_{p-2}, \end{aligned}$$

przeto

$$1 + \alpha^{\lambda} a_1 + \alpha^{2\lambda} a_2 + \ldots + \alpha^{\lambda(p-2)} a_{p-2} = 1 - \alpha^{\lambda} \Sigma \varrho_1 + \alpha^{2\lambda} \Sigma \varrho_1 \varrho_2 - \ldots$$
$$\ldots - \alpha^{\lambda(p-2)} \varrho_1 \varrho_2 \ldots \varrho_{p-2} = \prod_{h=1}^{p-2} (1 - \alpha^{\lambda} \varrho_h) .$$

Stąd, uwzględniając (9), mieć będziemy:

$$D = \prod_{\lambda=0}^{p-2} \prod_{h=1}^{p-2} (1 - \alpha^{\lambda} \varrho_h) \equiv 0 \text{ (mod. } p).$$

Mnożąc D przez $(-1)^{p-1}$ i zmieniając wzajemnie h i λ, otrzymamy:

$$D = \prod_{h=1}^{p-2} \prod_{\lambda=0}^{p-2} (\alpha^{\lambda} \varrho_h - 1) \equiv 0 \text{ (mod. } p) ;$$
$$D = \prod_{h=1}^{p-2} (\varrho_h^{\,p-1} - 1) \equiv 0 \text{ (mod. } p); \tag{10}$$

że zaś ta kongruencya jest identyczną z (5), więc twierdzenie nasze jest udowodnione.

Przyjmijmy, że z naszych poszukiwań wyłączamy pierwiastki o wartościach $+1$ lub -1, których istnienie odrazu poznać można. Gdy bowiem $f(x) \equiv 0$ (mod. p) posiada pierwiastek $\equiv +1$ (mod. p), to widocznie być musi

$$1 + a_1 + a_2 + \ldots + a_{p-2} \equiv 0 \text{ (mod. } p),$$

a pierwiastek $\equiv -1$ (mod. p) wskazuje kongruencya

$$1 - a_1 + a_2 - a_3 + \ldots - a_{p-2} \equiv 0 \text{ (mod. } p) .$$

Do kryteryum zatem, wskazującego pierwiastki różne od $+1$ i od -1, dojdziemy w ten sposób:

W wyznaczniku (8) dodajmy elementy wszystkich wierszy do wiersza ostatniego i odejmijmy każdy pion następny od poprzedniego, to otrzymamy

$$D = (1 + a_1 + \ldots + a_{p-2}) \begin{vmatrix} (1-a_1), & (a_1-a_2), & (a_2-a_3), \ldots, & (a_{p-3}-a_{p-2}), & a_{p-2} \\ (a_1-a_2), & (a_2-a_3), & (a_3-a_4), \ldots, & (a_{p-2}-1), & 1 \\ (a_2-a_3), & (a_3-a_4), & (a_4-a_5), \ldots, & (1-a_1), & a_1 \\ \vdots & & & & \\ (a_{p-3}-a_{p-2}), & (a_{p-2}-1), & (1-a_1), \ldots, & (a_{p-5}-a_{p-4}), & a_{p-4} \\ 0, & 0, & 0, \ldots, & 0, & 1 \end{vmatrix}$$

$$= (1 + a_1 + \ldots + a_{p-2}) \begin{vmatrix} (1-a_1), & (a_1-a_2), & (a_2-a_3), & \ldots, (a_{p-4}-a_{p-3}), & (a_{p-3}-a_{p-2}) \\ (a_1-a_2), & (a_2-a_3), & (a_3-a_4), & \ldots, (a_{p-3}-a_{p-2}), & (a_{p-2}-1) \\ (a_2-a_3), & (a_3-a_4), & (a_4-a_5), & \ldots, (a_{p-2}-1), & (1-a_1) \\ \vdots & & & & \\ (a_{p-4}-a_{p-3}), & (a_{p-3}-a_{p-2}), & (a_{p-2}-1), & \ldots, (a_{p-7}-a_{p-6}), & (a_{p-6}-a_{p-5}) \\ (a_{p-3}-a_{p-2}), & (a_{p-2}-1), & (1-a_1), & \ldots, (a_{p-6}-a_{p-5}), & (a_{p-5}-a_{p-4}) \end{vmatrix} .$$

Dodajmy elementy wiersza 1, 3, 5, . . . , $(p-4)$-go do wiersza ostatniego, to:

$$D = (1 + a_1 + a_2 + \ldots + a_{p-2}) (1 - a_1 + a_2 - \ldots - a_{p-2})$$
$$\times \begin{vmatrix} (1-a_1), & (a_1-a_2), & (a_2-a_3), \ldots, & (a_{p-4}-a_{p-3}), & (a_{p-3}-a_{p-2}) \\ (a_1-a_2), & (a_2-a_3), & (a_3-a_4), \ldots, & (a_{p-3}-a_{p-2}), & (a_{p-2}-1) \\ \vdots & & & & \\ (a_{p-4}-a_{p-3}), & (a_{p-3}-a_{p-2}), & \ldots\ldots\ldots, & (a_{p-7}-a_{p-6}), & (a_{p-6}-a_{p-5}) \\ 1, & -1, & \ldots\ldots\ldots, & -1, & 1 \end{vmatrix} .$$

Dodajmy każdy pion do poprzedniego, a następnie zredukujmy ten wyznacznik na niższy o jeden stopień, to będzie:

$$D = (1 + a_1 + a_2 + \ldots + a_{p-2}) (1 - a_1 + a_2 - \ldots - a_{p-2})$$
$$\times \begin{vmatrix} (1-a_2), & (a_1-a_3), & (a_2-a_4), & \ldots, (a_{p-5}-a_{p-3}), & (a_{p-4}-a_{p-2}) \\ (a_1-a_3), & (a_2-a_4), & (a_3-a_5), & \ldots, (a_{p-4}-a_{p-2}), & (a_{p-3}-1) \\ (a_2-a_4), & (a_3-a_5), & (a_4-a_6), & \ldots, (a_{p-3}-1), & (a_{p-2}-a_1) \\ \vdots & & & & \\ (a_{p-5}-a_{p-3}), & (a_{p-4}-a_{p-2}), & (a_{p-3}-1), & \ldots, (a_{p-9}-a_{p-7}), & (a_{p-8}-a_{p-6}) \\ (a_{p-4}-a_{p-2}), & (a_{p-3}-1), & (a_{p-2}-a_1), & \ldots, (a_{p-8}-a_{p-6}), & (a_{p-7}-a_{p-5}) \end{vmatrix} \tag{11}$$

czyli

$$D = (1 + a_1 + a_2 + \ldots + a_{p-2}) (1 - a_1 + a_2 - \ldots - a_{p-2}) \, \Delta ,$$

jeżeli przez Δ oznaczymy wyznacznik prawéj strony związku (11). Dwa pierwsze czynniki tego związku wskazują możliwość istnienia pierwiastków $+1$ lub -1, a gdy się o nie nie troszczymy, to warunek konieczny i dostateczny istnienia pierwiastków różnych od $+1$ i od -1 przedstawia kongruencya:

A.) $$\Delta \equiv 0 \pmod{p}$$

albo, — co wynika z (9) — kongruencya

B.) $$\prod_{\lambda=1,2,\ldots,\frac{p-3}{2},\frac{p+1}{2},\ldots,p-2} g(\alpha^{\lambda}) \equiv 0 \pmod{p},$$

gdyż

$$g(1) = g(\alpha^0),\quad g(-1) = g(\alpha^{\frac{p-1}{2}}).$$

Przyjmijmy np., że kongruencya (A) zachodzi w ten sposób, że w wyznaczniku Δ wszystkie wyrazy jednego wiersza (lub pionu) są $\equiv 0 \pmod{p}$ a więc, że

$$a_r \equiv a_{r+2} \pmod{p}$$

$$r = s,\ s+1,\ s+2, \ldots, s+p-4,\ s \leqq p-4.$$

Za a_0 bierzemy 1, a za $r > (p-2)$ stawiamy $r - p + 1$. W wypadku tym zachodzą między współczynnikami związki

$$\left.\begin{aligned} 1 &\equiv a_2 \equiv a_4 \equiv \ldots \equiv a_{p-3} \\ a_1 &\equiv a_3 \equiv a_5 \equiv \ldots \equiv a_{p-2} \equiv a. \end{aligned}\right\} \pmod{p}$$

Uwzględniając te związki w kongruencyi $f(x) \equiv 0 \pmod{p}$, otrzymamy

$$f(x) = x^{p-2} + a\,x^{p-3} + x^{p-4} + a\,x^{p-5} + \ldots + a \equiv 0 \pmod{p},$$

czyli

$$\begin{aligned} f(x) &= x^{p-2} + x^{p-4} + \ldots + x + a\,(x^{p-3} + x^{p-5} + \ldots + 1) \\ &= x\,(x^{p-3} + x^{p-5} + \ldots + 1) + a\,(x^{p-3} + x^{p-5} + \ldots + 1) \\ &= (x+a)\,(x^{p-3} + x^{p-5} + \ldots + 1) \equiv 0 \pmod{p}. \end{aligned}$$

Ponieważ

$$x^{p-3} + x^{p-5} + \ldots + 1 = \frac{x^{p-1} - 1}{x^2 - 1}$$

a

$$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\ldots(x-p+1),$$

przeto kongruencya $f(x) \equiv 0 \pmod{p}$ posiada pierwiastki

$$2, 3, 4, \ldots, p-2,$$

a prócz tego pierwiastek $-a$, który może przybierać wartość $+1$, lub -1.

Iloczyn $\Pi\, g(\alpha^{\lambda})$ składa się z $(p-3)$ czynników. Jeżeli s czynników pomnożonych przez siebie daje na iloczyn liczbę całkowitą, to iloczyn pozostałych $(p-3-s)$ czynników musi być także liczbą całkowitą, gdyż $\Pi\, g(\alpha^{\lambda})$ jest liczbą całkowitą. Jeżeli $\Pi\, g(\alpha^{\lambda})$ ma być $\equiv 0 \pmod{p}$, to przynajmniéj jedna z grup o s lub o $(p-3-s)$ czynnikach musi być $\equiv 0 \pmod{p}$. W ten sposób otrzymamy pewne związki, którym muszą czynić zadość współczynniki.

Dla przykładu rozważmy jeden przypadek.

$$\prod_{\lambda=1,2,\ldots,\frac{p-3}{2},\frac{p+1}{2},\ldots,p-2} (1 + \alpha^{\lambda} a_1 + \alpha^{2\lambda} a_2 + \ldots + \alpha^{\lambda(p-2)} a_{p-2})$$

$$= \prod_{\lambda=1,2,\ldots,\frac{p-3}{2},\frac{p+1}{2},\ldots,p-2} \left[(1-a_{\frac{p-1}{2}}) + (a_1 - a_{\frac{p+1}{2}})\alpha^{\lambda} + (a_2 - a_{\frac{p+3}{2}})\alpha^{2\lambda} + \ldots + (a_{\frac{p-3}{2}} - a_{p-2})\alpha^{\lambda\frac{p-3}{2}}\right],$$

gdyż każde

$$\alpha^{\lambda r} = -\,\alpha^{\left(\lambda r + \frac{p-1}{2}\right)},\qquad r = 0, 1, 2, \ldots, \frac{p-3}{2}.$$

Jeżeli zatem

$$1 \equiv a_{\frac{p-1}{2}} \pmod{p},\ a_1 = a_{\frac{p+1}{2}},\ a_2 = a_{\frac{p+3}{2}}, \ldots, a_{\frac{p-3}{2}} = a_{p-2},$$

to

$$\prod_{\lambda=1,2,\ldots,\frac{p-3}{2},\frac{p+1}{2},\ldots,p-2} g(\alpha^{\lambda}) \equiv 0 \pmod{p} \tag{12}$$

Wstawiając wartości (12) w kongruencyą, otrzymamy

$$f(x) = x^{p-2} + a_1 x^{p-3} + \ldots + x^{\frac{p-3}{2}} + a_1 x^{\frac{p-5}{2}} + \ldots + a_{\frac{p-3}{2}} \equiv 0 \pmod{p},$$

czyli

$$f(x) = (x^{p-2} + x^{\frac{p-3}{2}}) + a_1\,(x^{p-3} + x^{\frac{p-5}{2}}) + \ldots + a_{p-3}\,(x^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Wyjmijmy z każdego wyrazu czynnik $(x^{\frac{p-1}{2}}+1)$, to

$$f(x)=(x^{\frac{p-1}{2}}+1)(x^{\frac{p-3}{2}}+a_1 x^{\frac{p-5}{2}}+\ldots+a_{\frac{p-3}{2}})\equiv 0 \ (\mathrm{mod.}\ p).$$

Stąd okazuje się, że kongruencya $f(x)$, o współczynnikach (12) posiada zawsze pierwiastki kongruencyi

$$x^{\frac{p-1}{2}}\equiv -1 \ (\mathrm{mod.}\ p),$$

a w wypadku, gdy prócz (12) zachodzi między współczynnikami związek

$$\begin{vmatrix} 0, & 0, 0, \ldots, 1, & a_1, a_2, \ldots, a_{\frac{p-3}{2}} \\ 0, & 0, 0, \ldots, a_1, & a_2, a_3, \ldots, a_{\frac{p-5}{2}} \\ \vdots & & \\ a_{\frac{p-3}{2}}, & 0, 0, \ldots, & \ldots\ldots\ldots, a_{\frac{p-5}{2}} \end{vmatrix}\equiv 0 \ (\mathrm{mod.}\ p),$$

t. j. gdy

$$1, a_1, a_2, \ldots, a_{\frac{p-3}{2}},$$

spełniają kryterym Radosa, $f(x)\equiv 0$ (mod. p) posiada także pierwiastki kongruencyi

$$x^{\frac{p-3}{2}}+a_1 x^{\frac{p-5}{2}}+\ldots+a_{\frac{p-5}{2}}\equiv 0 \ (\mathrm{mod.}\ p).$$

Lwów w sierpniu 1892.

TEORYA PRZEMIAN I WARYACYJ KOŁOWYCH ZUPEŁNYCH.

PRZEZ

E. JABŁOŃSKIEGO.

I.

Metoda oznaczenia liczby przemian i waryacyj kołowych z powtórzeniami.

1. Teorya przemian i waryacyj z powtórzeniami lub bez powtórzeń jest zupełnie znaną dla przypadku, w którym wszystkie elementy (litery) składające uważa się za rozmieszczone na linii prostéj lub ogólniej wzdłuż jakiéjkolwiek linii niezamkniętéj; takie przemiany lub waryacye nazywamy prostoliniowemi. Gdy zaś przypuścimy, że elementy są wypisane na obwodzie koła lub na jakiéjkolwiek linii zamkniętéj, wtedy przemiany i waryacye nazywają się *kołowemi*. Pytanie oznaczenia liczby tych przemian i waryacyj nie było dotąd, o ile wiem, rozwiązane, wyjąwszy dla przypadku, w którym nie zachodzi powtórzenie jednego lub kilku elementów. Podam tu metodę elementarną rozwiązania ogólnego tego pytania, zajmę się przemianami, a potem waryacyami kołowemi — porządek taki jest tu konieczny; w drugiej zaś części pokażę, jak można otrzymane rezultaty wyrazić we wzorach ogólnych.

[1]) Autor podał treść téj prscy w Comptes Rendus Akademii paryskiej (kwiecień 1892) i ogłosił ją w Journal de Mathématiques, VIII, 1892.