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

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

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

$$x^{\frac{p-1}{2}}\equiv -1 \pmod{p}\,,$$

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

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

t. j. gdy

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

spełniają kryteryum Radosa, $f(x)\equiv 0 \pmod{p}$ posiada także pierwiastki kongruencyi

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

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.

2. *Przemiany kołowe.* Przypadek w którym żaden element nie powtarza się, jest dobrze znany, ale przypomnę go dlatego, bo to da mi możność zastosowania sposobu rozumowania, który doprowadził mnie do rozwiązania pytania ogólnego, będącego przedmiotem niniejszego artykułu.

Niechaj Q_m będzie liczbą przemian kołowych o m elementach bez powtórzeń; Q_{m-1} — takąż liczbą dla przemian o $m-1$ elementach. Jeżeli zastosujemy najprzód metodę używaną dla przemian prostoliniowych bez powtórzeń, znajdziemy

$$Q_m = (m-1)\ Q_{m-1}\,. \tag{1}$$

Wzór ten różni się od znanego wzoru dla przemian prostoliniowych bez powtórzeń

$$P_m = m\ P_{m-1}\,,$$

dlatego, że $m-1$ elementów rozmieszczonych na kole przedstawia tylko $m-1$ miejsc, a w każde z nich można wprowadzić literę m-ą, gdy tymczasem w rozmieszczeniu prostoliniowem takich miejsc jest m.

Z wzoru (1) otrzymujemy

$$Q_m = 1.\ 2.\ 3.\ \ldots\ (m-1) = (m-1)\,!\,,$$

lub

$$Q_m = \frac{P_m}{m}. \tag{2}$$

Metoda ta wzorowana na metodzie przemian prostoliniowych, używanéj w przypadku przemian prostoliniowych, nie nadaje się wtedy, gdy zachodzi powtórzenie jednego lub kilku elementów; należy więc podjąć w tym razie rzecz z innego punktu widzenia.

Wyobraźmy sobie przemianę prostoliniową prostą o m elementach; napiszmy elementy na obwodzie koła w porządku, w jakim je czytamy od strony lewéj ku prawéj; będziemy wtedy mieli przemianę kołową prostą z tych samych złożoną elementów. Jeżeli zamiast rozpoczynać czytanie od pierwszego elementu po stronie lewéj, rozpoczynamy je od elementu któregokolwiek, postępując zawsze od lewéj ku prawéj i powtarzając czytanie od litery pierwszéj od strony lewéj, gdy już dosięgnęliśmy ostatniego elementu po stronie prawéj, znajdziemy zawsze tęż samę przemianę kołową, to — ponieważ czytanie może się rozpocząć od któregokolwiek z m elementów — każda przemiana prostoliniowa prosta daje m razy tęż samę przemianę kołową prostą, skąd

$$P_m = m\ Q_m\,.$$

Jest to związek (2).

3. Poprzednie rozumowanie byłoby błędnem, gdyby czytanie jednéj i téj saméj przemiany prostoliniowéj prostéj, rozpoczęte od dwóch różnych elementów np. od pierwszego i od $(p+1)$-ego, dawało jednę i tęższamę przemianę prostoliniową, ponieważ wtedy użytą by była pewną liczbę razy jedna i ta sama przemiana prostoliniowa; nie byłoby już zatem prawdziwem twierdzenie, że jedna przemiana prostoliniowa, wzięta raz jeden, daje m razy tęż samę przemianę kołową. Ta okoliczność zachodzi mianowicie wtedy, gdy p pierwszych elementów, po przeniesieniu ich w niezmienionem następstwie po za element ostatni, daje tę samą przemianę prostoliniową, t. j. gdy uważana przemiana prostoliniowa może być podzieloną dokładnie na grupy identyczne po p elementów. Wymaga to najprzód, aby p było dzielnikiem liczby m i następnie, aby każdy element powtarzał się przynajmniej m razy. Ta szczególność nie zachodzi dla przemian bez powtórzeń.

4. Uważajmy teraz przemiany prostoliniowe z powtórzeniem. Niechaj elementy

$$a,\ b,\ c,\ \ldots\ l$$

powtarzają się odpowiednio razy

$$\alpha,\ \beta,\ \gamma\ \ldots\ \lambda\,,$$

niechaj

$$\alpha + \beta + \gamma + \ldots + \lambda = m\,.$$

Liczba przemian jest, jak wiadomo, równa

$$\frac{1.\ 2.\ 3.\ \ldots\ m}{1.\ 2.\ 3.\ \ldots\ \alpha.\ 1.\ 2.\ 3.\ \ldots\ \beta.\ \ldots\ \text{i}\ 1.\ 2.\ 3.\ \ldots\ \lambda}$$

lub

$$\frac{m\,!}{\alpha\,!\ \beta\,!\ \ldots\ \lambda\,!}$$

Zbadajmy najprzód przypadek, w którym $\alpha, \beta, \gamma \ldots \lambda$ nie mają innego wspólnego dzielnika prócz jedności. Wtedy, jak w przypadku przemian prostych, jest rzeczą niemożliwą, aby przemiana prostoliniowa podzieliła się na grupy identyczne, co by być mogło tylko wtedy, gdyby każdy element w każdéj grupie mógł powtarzać się jednakową liczbą razy, a to wymagałoby warunku, aby $\alpha, \beta\ \gamma \ldots$ były podzielne wszystkie przez liczbę całkowitą różną od jedności, co sprzeciwia się założeniu. Wynika więc stąd, że w tym przypadku liczba przemian kołowych z temi samemi powtórzeniami równa się m razy zmniejszonéj liczbie przemian prostoliniowych, t. j. liczbie

$$\frac{(m-1)\,!}{\alpha\,!\ \beta\,!\ \gamma\,!\ \ldots\ \lambda\,!}\,.$$

5. Załóżmy, że $\alpha, \beta, \gamma \ldots \lambda$ mają tylko jeden dzielnik wspólny d, który jest liczbą pierwszą; liczba ta jest oczywiście dzielnikiem i sumy m. Niechaj

$$\alpha=\alpha_1 d,\ \beta=\beta_1 d,\ \gamma=\gamma_1 d, \ldots, \lambda=\lambda_1 d,\ m=m_1 d.$$

Ogół przemian prostoliniowych daje się tu podzielić na dwie i tylko na dwie kategorye. Do pierwszéj należą przemiany prostoliniowe, nie dające się podzielić na grupy identyczne po m_1 elementów, do drugiej te, dla których ten podział jest możliwy. Niechaj Q będzie liczbą pierwszych, Q_1 — liczbą drugich, wtedy oczywiście

$$Q+Q_1=\frac{m!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!}.$$

Dla otrzymania wszystkich przemian prostoliniowych drugiéj kategoryi dość uważać te, które stanowią jednę z grup, a więc

$$Q_1=\frac{m_1!}{\alpha_1!\,\beta_1!\,\gamma_1!\ldots\lambda_1!}.$$

Te dwa związki dają Q i Q_1. Każda z Q przemian prostoliniowych pierwszéj kategoryi daje m razy też samą przemianę kołową, a każda z Q_1 przemian drugiéj kategoryi daje m_1 razy też samą przemianę; liczba więc szukana przemian kołowych z powtórzeniami będzie

$$\frac{Q}{m}+\frac{Q_1}{m_1}.$$

Każda z części składowych téj sumy musi być oczywiście liczbą całkowitą.

6. Dajmy, że $\alpha, \beta, \ldots \lambda$ mają dwa czynniki wspólne d i d_1, będące liczbami pierwszemi. Niechaj

$$\alpha=\alpha_1 d,\quad \beta=\beta_1 d, \ldots\ldots \lambda=\lambda_1 d,\quad m=m_1 d$$
$$\alpha=\alpha_2 d_1,\quad \beta=\beta_2 d_1, \ldots, \lambda=\lambda_2 d_1,\quad m=m_2 d_1$$
$$\alpha=\alpha_3 dd_1,\ \beta=\beta_3 dd_1, \ldots, \lambda=\lambda_3 dd_1,\ m=m_3 dd_1.$$

Ogół przemian prostoliniowych składać się będzie z czterech kategoryj:

1) przemiany, nie dające się podzielić na grupy identyczne ani o m_1, ani o m_2, ani o m_3 elementach; ich liczba niechaj będzie Q;

2) przemiany, dające się podzielić na grupy identyczne po m_1 elementów i nie mniej; oznaczmy ich liczbę przez Q_1;

3) przemiany, dające się podzielić na grupy identyczne po m_2 elementów i nie mniej; liczbę ich oznaczmy przez Q_2;

4) wreszcie takie przemiany, które dają się podzielić na grupy identyczne po m_3 elementów i nie mniej; liczbę ich oznaczmy przez Q_3.

Będzie oczywiście:

$$Q+Q_1+Q_2+Q_3=\frac{m!}{\alpha!\,\beta!\ldots\lambda!}$$

Jeżeli zamiast $\alpha, \beta, \ldots \lambda$ weźmiemy $\alpha_1, \beta_1, \ldots, \lambda_1$, następnie $\alpha_2, \beta_2, \ldots, \lambda_2$, wreszcie $\alpha_3, \beta_3, \ldots, \lambda_3$, i powtórzymy to samo rozumowanie, znajdziemy

$$Q_1+Q_3=\frac{m_1!}{\alpha_1!\,\beta_1!\ldots\lambda_1!},$$

$$Q_2+Q_3=\frac{m_1!}{\alpha_2!\,\beta_2!\ldots\lambda_2!},$$

$$Q_3=\frac{m_3!}{\alpha_3!\,\beta_3!\ldots\lambda_3!}.$$

Te cztery związki określają liczby Q, Q_1, Q_2, Q_3, a szukana liczba przemian kołowych z temi samemi powtórzeniami będzie:

$$\frac{Q}{m}+\frac{Q_1}{m_1}+\frac{Q_2}{m_2}+\frac{Q_3}{m_3}.$$

7. To, co powiedziano wyżéj, wystarcza do zrozumienia metody, przechodzę zatem do przypadku najogólniejszego. Niechaj d_n będzie największym wspólnym dzielnikiem liczb $\alpha, \beta, \gamma, \ldots \lambda$ i niechaj $\lambda, d, d_2, \ldots$ $\ldots, d_p, \ldots, d_n$ będą wszystkie dzielniki liczby d_n, t. j. dzielniki wspólne liczb $\alpha, \beta, \ldots \lambda$. Połóżmy

$$\alpha=\alpha_p\, d_p,\quad \beta=\beta_p\, d_p, \ldots, \lambda=\lambda_p\, d_p,\quad m=m_p\, d_p.$$

Można zawsze dzielniki liczby d_n uporządkować w ten sposób, aby liczba d_p nie miała już żadnego dzielnika w szeregu dzielników liczby d_n o skaźniku wyższym od p; wiemy nadto, że nie może mieć dzielników po za tym szeregiem, skąd wynika, że wszystkie dzielniki liczby $\frac{d_n}{d_p}$ znajdują się pomiędzy temi dzielnikami liczby d_n, których skaźnik jest równy p lub od p wyższy.

Przy takiem założeniu można ogół przemian prostoliniowych podzielić na tyle kategoryj, ile jest dzielników liczby d_n; a każda kategorya charakteryzuje się tem, że przemiana prostoliniowa do niéj należąca może być podzielona na d_p grup identycznych o m_p elementach i nie mniej. Niechaj Q_p będzie liczba przemian téj kategoryi. Dla oznaczenia $n+1$ liczb Q_p, będziemy tedy mieli układ $n+1$ równań następujących:

$$Q+Q_1+Q_2+\ldots+Q_p+\ldots+Q_n=\frac{m!}{\alpha!\,\beta!\ldots\lambda!},$$

$$Q_1+\ldots+Q_i+\ldots+Q_n=\frac{m_1!}{\alpha_1!\,\beta_1!\ldots\lambda_1!},$$

$$Q_2+\ldots+Q_j+\ldots+Q_n=\frac{m_2!}{\alpha_2!\,\beta_2\ldots\lambda_2!},$$

. . . .

$$Q_n=\frac{m_n!}{\alpha_n!\,\beta_n!\ldots\lambda_n!};$$

d_i jest jednym którymkolwiek z dzielników liczby $\frac{d_n}{d_1}$, d_j jednym którymkolwiek z dzielników liczby $\frac{d_n}{d_2}$, i t. d.

Równania te określają zupełnie niewiadome, ponieważ wyznacznik układu redukuje się do przekątnéj główněj i jest równy $+1$.

Znając te liczby, znajdziemy bezpośrednio szukaną liczbę przemian kołowych z temi samemi powtórzeniami, mianowicie:

$$\frac{Q}{m}+\frac{Q_1}{m_1}+\frac{Q_2}{m_2}+\ldots+\frac{Q_p}{m_p}+\ldots+\frac{Q_n}{m_n};$$

gdzie każda z części składowych sumy jest oczywiście liczbą całkowitą.

Pytanie nasze jest zatem zupełnie rozwiązane; zobaczymy niżéj, jak otrzymamy rezultat daje się wyrazić za pomocą prostego wzoru

8. *Waryacye kołowe z powtórzeniami.* Uważam najprzód waryacye prostoliniowe, t. j. grupy o m elementach, dające się utworzyć z p elementów $a, b, c, \ldots, l$, rozmieszczonych na prostéj, z których każdy może być powtórzony aż do m razy. Tu każde dwie grupy różnią się, albo porządkiem, albo wyborem elementów. Te waryacye można rozłożyć na przemiany z powtórzeniami o m elementach.

W tym celu rozważmy wszystkie układy rozwiązań całkowitych dodatnich i równych zeru równania

$$\alpha+\beta+\gamma+\ldots+\lambda=m$$

gdzie liczb $\alpha, \beta, \gamma\ldots\lambda$ jest p. Rozwiązania te nazwijmy *skaźnikami.*

Przyjmujemy za rozwiązania tylko układy różne t. j. takie, które nie dają się otrzymać jedne z drugich przez prostą przemianę skaźników.

Niechaj $k\leqq p$ będzie liczba skaźników jednego układu, nierównych zeru. Biorę k liczb z pomiędzy p liczb $a, b, c\ldots l$ i tworzę wszystkie przemiany z powtórzeniami tych k elementów, z których pierwszy powtarza się α razy, drugi β razy i t. d. Powtarzam to samo działanie z tym samym układem skaźników dla wszystkich waryacyj prostych, jakie mogę otrzymać z p liter, biorąc je po k, i otrzymuję w ten sposób wszystkie przemiany, odpowiadające temu samemu układowi skaźników; są one różnemi tylko wtedy, gdy wszystkie skaźniki uważanego układu są różne.

W tym przypadku całkowita liczba przemian tak utworzonych, odpowiadających temu samemu układowi skaźników, jest

$$p\,(p-1)\ldots(p-k+1)\cdot\frac{m!}{\alpha!\,\beta!\ldots\lambda!}.$$

Lecz gdy skaźniki układu dzielą się na q grup, a mianowicie na $i_1, i_2, \ldots, i_q$ grup równych, tak, że

$$i_1+i_2+\ldots+i_q=k,$$

wtedy, dla otrzymania całkowitéj liczby przemian kołowych różnych odpowiadających układowi skaźników, trzeba podzielić liczbę poprzednio znalezioną przez iloczyn $i_1!\,i_2!\ldots i_q!$, co doprowadza do wyrażenia

$$\frac{p\,(p-1)\ldots(p-k+1)}{i_1!\,i_2!\ldots i_q!}\cdot\frac{m!}{\alpha!\,\beta!\ldots\lambda!}.$$

Obliczając to wyrażenie dla każdego z różnych układów skaźników i dodając otrzymane liczby, znajdziemy liczbę waryacyj prostoliniowych z powtórzeniami t. j. waryacyj zupełnych z p elementów wziętych po m.

Łatwo to sprawdzić. Wiemy, że ta liczba jest p^m. Jeżeli rozwiniemy potęgę

$$(a+b+c+\ldots+l)^m$$

to suma poprzednio utworzona jest sumą wyrazów tego rozwinięcia przy założeniu

$$a=b=c=\ldots=l=1,$$

albowiem wszystkie wyrazy stają się równemi 1, rozwinięcie sprowadza się do liczby wyrazów różnych a wyrażenie nierozwinięte do p^m.

Przy tem założeniu możemy dla danego układu skaźników przejść od przemian prostoliniowych, utworzonych z k elementów wziętych z pomiędzy p danych, do przemian kołowych z tych samych elementów, z temi samemi powtórzeniami i oznaczyć ich liczbę. Mnożąc tę liczbę przez

$$\frac{p(p-1)\ldots(p-k+1)}{i_1!\, i_2! \ldots i_q!},$$

będziemy mieli liczbę przemian kołowych o tych samych skaźnikach utworzonych ze wszystkiemi elementami; dodając nakoniec rezultaty odpowiadające wszystkim różnym układom skaźników sprawdzającym równanie

$$\alpha + \beta + \ldots + {}_2 = m,$$

znajdziemy całkowitą liczbę waryacyj kołowych zupełnych.

II.

Wzory ogólne.

Niechaj $\alpha, \beta, \ldots, \lambda$ będą skaźniki pewnéj przemiany, D ich największy wspólny dzielnik. Położmy

$$\alpha = \alpha' D, \quad \beta = \beta' D, \ \ldots, \ \lambda = \lambda' D,$$

gdzie liczby $\alpha', \beta', \ldots, \lambda'$ są względnie pierwsze, oraz

$$\alpha + \beta + \ldots + \lambda = m = m' D.$$

Położmy dla każdego n:

$$P(n) = \frac{(m' n)!}{(\alpha' n)!\,(\beta' n)! \ldots (\lambda' n)!}$$

Widzieliśmy w I, że gdy d_p jest jednym z dzielników liczby D i gdy oznaczymy przez $Q\left(\frac{D}{d_p}\right)$ liczbę przemian prostoliniowych o skaźnikach $\alpha, \beta, \ldots, \lambda$, dających się podzielić na d_p grup identycznych i nie więcej niż o $\left(m' \frac{D}{d_p}\right)$ elementach, to:

$$\sum_1^D Q\left(\frac{D}{d_p}\right) = P(D)$$

gdzie suma po lewéj rozciąga się na wszystkie dzielniki liczby D, wliczając w nie 1 i D. Ogólniéj, gdy n jest jakimkolwiek z dzielników liczby D, będzie

$$\sum_1^n Q\left(\frac{n}{d_p}\right) = P(n), \qquad (\alpha)$$

gdzie suma rozciąga się na wszystkie dzielniki d_p liczby D, będące zarazem dzielnikami liczby n, wliczając w nie 1 i n.

Liczba przemian kołowych o skaźnikach $\alpha, \beta, \ldots \lambda$ jest

$$\sum_1^D \frac{Q\left(\frac{D}{d_p}\right)}{m_p};$$

ponieważ $m_p = \frac{m}{d_p}$, przeto ta suma równa się

$$\frac{1}{m} \sum_1^D Q\left(\frac{D}{d_p}\right) d_p$$

gdzie suma rozciąga się na wszystkie dzielniki d_p liczby D, włączając w nie 1 i D.

9. Pan C. Jordan wskazał mi użytek, jaki dla rozwiązania tego pytania, które poniżéj jeszcze uogólniam, można wyciągnąć z następnego ogólnego twierdzenia z teoryi liczb.

Jeżeli przez $a, b, c \ldots l$ oznaczymy wszystkie dzielniki pierwsze i różne od siebie liczby całkowitéj n i jeżeli

$$\sum_1^n R(d_p) = S(n),$$

gdzie suma rozciąga się na wszystkie dzielniki d_p liczby n, włączając w nie 1 i n, i także

$$\sum_1^d R(d_q) = S(d)$$

gdzie d jest jednym z dzielników liczby n, d_q zaś jednym z dzielników liczby n, które są zarazem dzielnikami liczby d, to będzie:

$$R(n) = S(n) - \sum S\left(\frac{n}{a}\right) + \sum S\left(\frac{n}{ab}\right) - \sum S\left(\frac{n}{abc}\right) + \ldots,$$

gdzie sumy rozciągają się na kombinacye pojedyńcze, podwójne i t. d. liczb $a, b, c, \ldots, l$.

Szukajmy funkcyi R takiéj, aby było $S(n) = n$; a więc

$$R(n) = n - \sum \frac{n}{a} + \sum \frac{n}{ab} - \sum \frac{n}{abc} + \ldots,$$

lub

$$R(n) = n\left(1 - \sum \frac{1}{a} + \sum \frac{1}{ab} - \sum \frac{1}{abc} + \ldots\right),$$

lub

$$R(n) = n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \ldots \left(1 - \frac{1}{l}\right),$$

$$R(n) = \varphi(n)$$

gdzie $\varphi(n)$ jest funkcyą dobrze znaną, wyrażającą, ile jest liczb względnie pierwszych z liczbą n i od niéj mniejszych.

Mamy więc.

$$\sum_1^n \varphi(d_p) = n$$

i także

$$\sum_1^{d_p} \varphi(d') = d_p,$$

gdzie d' jest jakimkolwiek z dzielników liczby d_p.

10. Przy takiem założeniu szukana liczba przemian kołowych może być napisana pod postacią

$$\frac{1}{m} \sum_1^D \left[Q\left(\frac{D}{d_p}\right) \sum_1^{d_p} \varphi(d')\right]$$

gdzie d' jest jednym którymkolwiek z dzielników liczby d_p, d_p zaś którymkolwiek z dzielników liczby D. Liczba d' może przyjmować wszystkie wartości dzielników liczby D i można uporządkować wyrazy téj sumy według wartości, jakie przyjmuje $\varphi(d')$. Szukajmy grupy wyrazów, odpowiadających oznaczonéj wartości liczby d'. Ponieważ d_p jest wielokrotnością liczby d', połóżmy więc:

$$d_p = \varepsilon d',$$

gdzie ε jest liczbą całkowitą; liczba całkowita $\frac{D}{d_p}$ staje się tedy równą

$$\frac{D}{d'} \frac{1}{\varepsilon}$$

a więc ε jest dzielnikiem liczby całkowitéj $\frac{D}{d}$, którą oznaczymy przez δ'. Odwrotnie każdemu dzielnikowi ε liczby δ' odpowiada wyraz mający $\varphi(d')$ za czynnik. Suma takich wyrazów jest tedy

$$\varphi(d') \sum_1^{\delta'} Q\left(\frac{\delta'}{\varepsilon}\right),$$

przy uwzględnieniu zaś związku (α):

$$\varphi(d')\ P(d'). \qquad (d'\delta = D)$$

Wynika stąd następujące proste wyrażenie liczby szukanéj:

$$\frac{1}{m} \sum_1^D P(\delta)\, \varphi(d) \qquad (d\delta = D)$$

gdzie suma rozciąga się na wszystkie dzielniki d liczby D, włączając w nie 1 i D i pamiętając, że $\varphi(1) = 1$. Stąd mamy

Twierdzenie. Liczba przemian kołowych elementów różnych, powtarzających się odpowiednio $\alpha, \beta, \ldots, \lambda$ razy, jest

$$\frac{1}{m} \sum_1^D P\left(\frac{D}{d}\right) \varphi(d), \qquad \varphi(1) = 1,$$

gdzie $m = \alpha + \beta + \ldots + \lambda$; D jest największym wspólnym dzielnikiem liczb $\alpha, \beta, \ldots \lambda$; d jednym z dzielników liczby D, włączając w nie 1 i D. Wreszcie $P\left(\frac{D}{d}\right)$ jest liczbą przemian prostoliniowych tych samych elementów o skaźnikach

$$\frac{\alpha}{d},\ \frac{\beta}{d},\ \ldots,\ \frac{\lambda}{d}.$$

Wynika stąd bezpośrednio dla waryacyj kołowych p-éj klasy z m elementów różnych.

Twierdzenie. Liczba waryacyj kołowych zupełnych p-éj klasy o m elementach różnych jest:

$$\frac{1}{m}\, S\, \frac{p\,(p-1)\ldots(p-k+1)}{i_1!\, i_2!\ldots i_q!} \sum_1^n P\left(\frac{n}{d}\right) \varphi\,(d), \qquad \varphi\,(1)=1$$

gdzie suma S rozciąga się na wszystkie różne układy rozwiązań całkowitych dodatnich równania

$$\alpha+\beta+\ldots+\lambda=m;$$

k oznacza liczbę skaźników nierównych zeru w jednym układzie, n — największy wspólny dzielnik skaźników tego samego układu; wreszcie liczby $i_1, i_2, \ldots, i_q$, których suma jest k, oznaczają, ile jest w tym samym układzie skaźników o wartościach równych.

W przypadku szczególnym waryacyj kołowych prostych mamy

$$k=m,\quad i_1=i_2=\ldots=i_{q-1}=0,\quad i_q=m,\quad n=1,$$

a więc liczba waryacyj kołowych prostych p-éj klasy z m elementów jest

$$\frac{1}{m}\, p\,(p-1)\ldots(p-m+1) \quad \text{lub} \quad \frac{1}{m} A_p^m$$

gdzie A_p^m przedstawia liczbę waryacyj prostoliniowych prostych, co łatwo sprawdzić bezpośrednio.

12. ***Uogólnienia.*** Połóżmy w ogólności

$$(\beta) \qquad \sum_1^n Q\left(\frac{n}{d}\right) = P\,(n),$$

gdzie d jest jednym z dzielników liczby n, która sama jest jednym z dzielników liczby D. Liczby $Q\left(\frac{D}{d}\right)$ nie mają już znaczenia specyalnego, wyżéj im nadanego, a są poddane tylko warunkowi, aby były oznaczone dla każdéj wartości liczby d. Co się tyczy liczb $P\,(n)$, są one określone za pomocą równości (β)

Dajmy, że chcemy obliczyć wyrażenie

$$\sum_1^D Q\left(\frac{D}{d}\right) d^t,$$

gdzie t jest liczbą zupełnie dowolną.

Szukajmy najprzód Q takiego, aby było

$$\sum_1^n Q\left(\frac{n}{d}\right) = n^t \qquad (d \text{ jest dzielnikiem liczby } n)$$

Stosując powyższe twierdzenie ogólne z teoryi liczb, znajdziemy

$$Q\,(n) = n^t\left(1-\frac{1}{a^t}\right)\left(1-\frac{1}{b^t}\right)\ldots\left(1-\frac{1}{l^t}\right),$$

gdzie $a, b, c \ldots l$ są dzielnikami pierwszemi liczby n różnemi od siebie. Oznaczmy liczbę po prawéj przez $\varphi_t(n)$. Dla $t=1$ znajdujemy $\varphi_1(n)=\varphi\,(n)$, dla $t=0$ przy $n=1$ będzie $\varphi_0\,(n)=0$, lecz dla $n=1$, należy przyjąć zawsze $\varphi_t(1)=1$ dla t dowolnego. Przy takiem założeniu znajdziemy, jak wyżéj,

$$\sum_1^D Q\left(\frac{D}{d}\right) d^t = \sum_1^D P\left(\frac{D}{d}\right) \varphi_t\,(d). \qquad (\gamma)$$

Dowolność w wyborze funkcyi Q pozwala z téj równości ogólnéj wyprowadzić mnóstwo związków, z których zbadamy niektóre.

13. Postarajmy się najprzód znaleść związki pomiędzy funkcyami $\varphi_t(n)$. Połóżmy w tym celu

$$Q'\left(\frac{n}{d}\right) = Q\left(\frac{n}{d}\right)\cdot\left(\frac{n}{d}\right)^\theta,$$

gdzie θ jest dowolne. Będzie

$$\sum_1^D Q'\left(\frac{D}{d}\right) d^t = \sum_1^D Q\left(\frac{D}{d}\right) D^\theta\, d^{t-\theta} = D^\theta \sum_1^D Q\left(\frac{D}{d}\right) d^{t-\theta}$$

lub

$$\sum_{1}^{D} Q'\left(\frac{D}{d}\right) d^t = D^\theta \sum_{1}^{D} P\left(\frac{D}{d}\right) \varphi_{t-\theta}\,(d)$$

Z drugiéj strony, kładąc

$$P'(n) = \sum_{1}^{n} Q'\left(\frac{n}{d}\right),$$

będziemy mieli

$$\sum_{1}^{D} Q'\left(\frac{D}{d}\right) d^t = \sum_{1}^{D} P'\left(\frac{D}{d}\right) \varphi_t\,(d) = D^\theta \sum_{1}^{D} P\left(\frac{D}{d}\right) \varphi_{t-\theta}\,(d),$$

lub

$$\sum_{1}^{D} P'(\delta)\,\varphi_t\,(d) = D^\theta \sum_{1}^{D} P(\delta)\,\varphi_{t-\theta}\,(d). \qquad (d\,\delta = D)$$

Lecz mamy także

$$P'(\delta) = \sum_{1}^{\delta} Q'\left(\frac{\delta}{d'}\right), \qquad (d' \text{ jest dzielnikiem liczby } \delta \text{, która jest dzielnikiem liczby } D)$$

lub

$$P'(\delta) = \sum_{1}^{\delta} Q\left(\frac{\delta}{d'}\right)\left(\frac{\delta}{d'}\right)^\theta = \delta^\theta \sum_{1}^{\delta} Q\left(\frac{\delta}{d'}\right) d'^{t-\theta}$$

lub przez wzgląd na (γ):

$$P'(\delta) = \delta^\theta \sum_{1}^{\delta} P\left(\frac{\delta}{d'}\right) \varphi_{-\theta}\,(d').$$

Otrzymamy więc równość zasadniczą

$$D^\theta \sum_{1}^{D} P(\delta)\,\varphi_{t-\theta}\,(d) = \sum_{1}^{D}\left[\delta_1^\theta \sum_{1}^{D} P(\delta')\,\varphi_{-\theta}\,(d')\right]\varphi_t\,(d_1)$$

$$(d\,\delta = d_1\,\delta_1 = D \ \text{ i } \ d'\,\delta' = \delta_1)$$

Uporządkujmy stronę drugą według wartości $P(\delta')$, gdy δ' przyjmuje wszystkie wartości dzielników liczby D. Jeżeli uczynimy

$$\delta' = \delta, \quad \delta_1 = d'\,\delta,$$

będzie

$$d_1 = \frac{D}{\delta}\,\frac{1}{d'} = \frac{d}{d'};$$

więc d' jest dzielnikiem liczby d, i odwrotnie każdemu dzielnikowi d' liczby d odpowiada po drugiéj stronie wyraz w $P(\delta)$; będzie zatem

$$D^\theta \sum_{1}^{D} P(\delta)\,\varphi_{t-\theta}\,(d) = \sum_{1}^{D}\left[P(\delta) \sum_{1}^{D} \delta^\theta\, d'^\theta\, \varphi_{-\theta}\,(d')\,\varphi_t\left(\frac{d}{d'}\right)\right]$$

Równość ta ma miejsce nietylko dla liczby D, ale i dla jéj wszystkich dzielników, wnosimy stąd, że

$$D^\theta\,\varphi_{t-\theta}\,(d) = \sum_{1}^{d} \delta^\theta\, d'^\theta\, \varphi_\theta\,(d')\,\varphi_t\left(\frac{d}{d'}\right), \qquad (d' \text{ jest dzielnikiem liczby } d)$$

lub

$$\varphi_{t-\theta}\,(d) = \sum_{1}^{d} \left(\frac{d'}{d}\right)^\theta \varphi_{-\theta}\,(d')\,\varphi_t\left(\frac{d}{d'}\right).$$

Lecz $\frac{d}{d'}$ jest także jednym którymkolwiek z dzielników liczby d, a więc nakoniec

$$\varphi_{t-\theta}\,(n) = \sum_{1}^{n} \varepsilon^{-\theta}\,\varphi_t\,(\varepsilon)\,\varphi_{-t}\left(\frac{n}{\varepsilon}\right),$$

gdzie suma rozciąga się na wszystkie dzielniki ε liczby całkowitéj n, włączając w nie 1 i n.

Skaźniki t i θ są dowolne, lecz należy pamiętać, że dla $t = 0$ lub $\theta = 0$ $\varphi_0\,(\varepsilon)$ jest zerem, wyjąwszy dla $\varepsilon = 1$, w którym to przypadku jest jednością.

Dla $\theta = -1$ mamy

$$\varphi_{t+1}\,(n) = \sum_{1}^{n} \varepsilon\,\varphi_t\,(\varepsilon)\,\varphi\left(\frac{n}{\varepsilon}\right),$$

skąd widzimy, że można φ_t wyrazić za pomocą sum zależnych tylko od φ_1, jeżeli t jest liczbą całkowitą dowolną.

14. Aby wskazać drugie zastosowanie naszéj teoryi, uczyńmy

$$Q\left(\frac{n}{d}\right)=1, \qquad \text{(}d\text{ dowolny dzielnik liczby }n\text{, która jest dzielnikiem liczby }D\text{)}$$

wtedy

$$P(n)=N(n),$$

gdzie N jest liczbą dzielników liczby n; będzie zatem

$$\sum_1^D Q\left(\frac{D}{d}\right) d^t=\sum_1^D N(\delta)\,\varphi_t(d), \qquad (d\,\delta=D)$$

lub

$$\sum_1^D d^t=\sum_1^D N(\delta)\,\varphi_t(d)$$

Strona pierwsza jest sumą potęg t-ych dzielników liczby D; suma ta wyraża się przy pomocy liczb N i φ. Dla $t=1$ będzie

$$\sum_1^D d=\sum_1^D N(\delta)\,\varphi(d).$$

Niechaj w szczególności $D=a^\alpha$, gdzie a jest liczbą pierwszą, α liczbą całkowitą; wtedy $d=a^{\alpha'}$, gdzie α' przyjmuje wartości $0, 1, 2, \ldots \alpha$; a więc

$$\sum_1^D a^{\alpha'}=1+a+\ldots+a^\alpha=\frac{a^{\alpha+1}-1}{a-1}$$

$$\varphi(a^{\alpha'})=a^{\alpha'}\left(1-\frac{1}{a}\right)$$

$$N(\delta)=N(a^{\alpha-\alpha'})=\alpha-\alpha'+1,$$

prócz $\alpha'=0$, a zatem

$$\frac{a^{\alpha+1}-1}{a-1}=\alpha+1+\sum_{\alpha'=1}^{\alpha'=\alpha}(\alpha+1-\alpha')\,a^{\alpha'}\left(1-\frac{1}{a}\right).$$

Równość ta ma miejsce dla jakiéjkolwiek liczby pierwszéj a i całkowitéj α, a więc i dla dowolnych liczb a i α: jest to tożsamość algebraiczna.

15. Można w ten sposób z powyższych wzorów ogólnych wyprowadzić mnóstwo tożsamości; dodam jeszcze, że wzory wyprowadzone z uważania dzielników liczby D utrzymują się, gdy liczbę D zastąpimy wielomianem całkowitym ze zmienną x, ale należy wtedy uczynić równym jedności współczynnik przy wyrazie najwyższego stopnia, nietylko w tym wielomianie, ale i w jego dzielnikach. Wynikają wtedy z powyższych wzorów rozmaite przekształcenia algebraiczne, w których funkcye φ nie mają już tego znaczenia co w arytmetyce, ale forma ich utrzymuje się bez zmiany.

Paryż, 1892.