$$\log a + \frac{(x+a)\,(x-a)}{60\,a^3\,x^3}\,[(x-a)^4 + 5\,a\,x\,\{8\,a\,x - (a^2+x^2)\}]\,,$$

szereg zaś (15) stanie się równym

$$-\frac{32}{5}\left[\frac{1}{7}\left(\frac{x-a}{x+a}\right)^7 + \frac{4}{9}\left(\frac{x-a}{x+a}\right)^9 + \frac{10}{11}\left(\frac{x-a}{x+a}\right)^{11} + \frac{20}{13}\left(\frac{x-a}{x+a}\right)^{13} + \ldots\right],$$

t. j. szeregowi (3) Wrońskiego.

Warszawa, w grudniu 1892.

ZASADA NAJWIĘKSZEGO WSPÓLNEGO DZIELNIKA W ZASTOSOWANIU DO TEORYI PODZIELNOŚCI LICZB ALGEBRAICZNYCH.

NAPISAŁ

J. SOCHOCKI.

I. Wstęp.

1. Dla usunięcia wszelkich wątpliwości uważamy za stosowne wyszczególnić przedewszystkiem te pojęcia i określenia, na których opierać się będą dalsze nasze badania.

Rzeczy łatwe pozostawiamy czytelnikowi samemu do sprawdzenia; życzącemu bliżéj oznajmić się z materyałem, wskazujemy znane dzieło: „Vorlesungen über Zahlentheorie“ Lejeune-Dirichleta.

Wszelka ilość, bądź rzeczywista, bądź urojona, czyniąca zadość równaniu

$$x^n + a_1\,x^{n-1} + a_2\,x^{n-2} + \ldots + a_n = 0\,,$$

gdzie $a_1, a_2, \ldots, a_n$ są liczby całkowite zwyczajne, nazywa się liczbą całkowitą algebraiczną, albo poprostu liczbą całkowitą. Liczby całkowite zwyczajne uważają się za szczególny przypadek liczb całkowitych algebraicznych.

Główne własności liczb całkowitych algebraicznych są następujące:

1. Suma lub różnica dwóch liczb całkowitych jest również liczbą całkowitą.

2. Iloczyn dwóch liczb całkowitych jest również liczbą całkowitą.

3. Wszelka ilość, czyniąca zadość równaniu

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0,$$

gdzie $a_1, a_2, \ldots, a_n$ są liczbami całkowitemi, jest również liczbą całkowitą.

Jeżeli stosunek dwóch liczb całkowitych

$$\frac{\alpha}{\beta}$$

jest liczbą całkowitą, to mówimy, że liczba β jest dzielnikiem liczby α, albo że liczba α dzieli się przez liczbę β.

Wszelka liczba całkowita dzieląca liczbę 1 nazywa się j e d n o ś c i ą a l g e b r a i c z n ą, albo poprostu j e d n o ś c i ą. Tak naprzykład, ilości

$$\sqrt{-1}, \quad \frac{-1+\sqrt{-3}}{2}, \quad \frac{1+\sqrt{5}}{2}$$

są jednościami.

2. Dla odkrycia praw podzielności liczb algebraicznych niezbędnem jest ograniczyć się na takich tylko liczbach, które dają się wyrazić przez jednę z nich pod postacią funkcyj całkowitych ze współczynnikami wymiernemi. Taki układ liczb otrzymuje się za pomocą jednéj jakiéjkolwiek liczby danéj α, służącéj za punkt wyjścia, i określonéj równaniem nieprzywiedlnem

$$\alpha^n + a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \ldots + a_n = 0. \qquad (1)$$

Wzór

$$\beta = x_1 + x_2 \alpha + x_3 \alpha^2 + \ldots + x_n \alpha^{n-1}, \qquad (2)$$

przy wszelkich wartościach wymiernych współczynników $x_1, x_2, \ldots, x_n$, przedstawia nieskończone mnóstwo liczb algebraicznych, stanowiących to, co będziemy nazywali o b s z a r e m liczb.

Pomiędzy liczbami danego obszaru znajdować się będzie nieskończone mnóstwo liczb całkowitych, i temi to właśnie liczbami wyłącznie tu zajmować się będziemy; wszystkie inne liczby usuwamy z pod uwagi.

Każda z liczb, należących do danego obszaru, czyni zadość właściwemu sobie równaniu n-go stopnia; ostatni wyraz w tem równaniu wzięty ze znakiem $(-1)^n$ nazywa się n o r m ą liczby: jestto iloczyn n wartości, jakie przyjmuje liczba (2) dla różnych wartości pierwiastka α. Aby liczba całkowita była jednością algebraiczną, jest dostatecznem i niezbędnem, aby jéj norma była równą ± 1, co wyraża się równaniem

$$N(\beta) = \pm 1.$$

3. Równanie (1) ma n pierwiastków

$$\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)};$$

a wszelka liczba β przybiera odpowiednie wartości

$$\beta, \beta', \beta'', \ldots, \beta^{(n-1)},$$

z pomiędzy których, żadna inna, oprócz β, może nie należeć do danego obszaru.

Funkcya symetryczna

$$\Delta = \begin{vmatrix} 1, & \alpha, & \alpha^2, & \ldots & \alpha^{n-1} \\ 1, & \alpha', & \alpha'^2, & \ldots & \alpha'^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \alpha^{(n-1)} & \ldots & & \end{vmatrix}^2$$

przedstawia iloczyn kwadratów różnic pierwiastków $\alpha, \alpha', \ldots$, i nazywa się wyrożnikiem (dyskryminantem) równania (1) albo, inaczéj, wyróżnikiem grupy n liczb

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1};$$

wartość tego wyróżnika jest liczbą całkowitą, zwyczajną, różną od zera, gdyż równanie (1), jako nieprzywiedlne, nie posiada pierwiastków równych.

W ogóle w y r ó ż n i k i e m g r u p y n l i c z b c a ł k o w i t y c h $\beta, \gamma, \ldots, \lambda$ nazywa się funkcya symetryczna

$$\begin{vmatrix} \beta, & \gamma & \ldots & \lambda \\ \beta', & \gamma' & \ldots & \lambda' \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \beta^{(n-1)}, & \gamma^{(n-1)} & \ldots & \lambda^{(n-1)} \end{vmatrix}^2,$$

wartość któréj jest liczbą całkowitą zwyczajną.

Wróćmy teraz do wzoru (2), t. j.

$$\beta = x_1 + x_2\,\alpha + x_3\,\alpha^2 + \ldots + x_n\,\alpha^{n-1},$$

aby pokazać, jaką drogą otrzymać można z niego wszelkie liczby całkowite, należące do danego obszaru. Przy wszelkich całkowitych wartościach zmiennych wymiernych x, otrzymywać będziemy oczywiście liczby całkowite β; pozostaje więc zająć się tylko wartościami ułamkowemi zmiennych x, dla których liczba β będzie również całkowitą.

Uczynimy najprzód uwagę, że jeżeli liczby zwyczajne m i d nie mają wspólnego dzielnika, a ilość

$$\frac{m}{d}\,\beta$$

jest liczbą całkowitą, to napewno i ilość

$$\frac{1}{d}\,\beta$$

jest także liczbą całkowitą; β, rozumie się, jest tu liczbą całkowitą.

Przechodząc do naszego zadania, dajmy, że liczba

$$\beta_1 = \frac{x'_1 + x'_2\,\alpha + \ldots + x'_n\,\alpha^{n-1}}{d} \qquad (3)$$

jest całkowitą, $d > 1$, a $x'_1, x'_2, \ldots$ nie mają żadnego wspólnego dzielnika. Gdyby $x'_1, x'_2, \ldots$ miały jako wspólny dzielnik liczbę pierwszą, która dzieli liczbę d, to powyższe wyrażenie można byłoby skrócić, a jeżeliby też same liczby miały jako wspólny dzielnik liczbę pierwszą, nie dzielącą liczby d, to można byłoby go odrzucić na mocy wyżéj zrobionéj uwagi.

Znajdźmy $n-1$ szeregów liczb całkowitych zwyczajnych po n liczb w każdym, a czyniących zadość równaniu

$$\begin{vmatrix} x'_1, x'_2, \ldots, x'_n \\ y_1, y_2, \ldots, y_n \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ z_1, z_2, \ldots, z_n \end{vmatrix} = 1,$$

co, oczywiście, na mocy zrobionego zastrzeżenia, jest możebnem, i uczyńmy

$$\beta_2 = y_1 + y_2\,\alpha + \ldots + y_n\,\alpha^{n-1},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\beta_n = z_1 + z_2\,\alpha + \ldots + z_n\,\alpha^{n-1}.$$

Do tych równań dołączamy jedno z powyższych, mianowicie

$$d\,\beta_1 = x'_1 + x'_2\,\alpha + \ldots + x'_n\,\alpha^{n-1},$$

i wnosimy stąd, że

$$\begin{vmatrix} d\beta_1, & \beta_2 \ldots \beta_n \\ d\beta'_1, & \beta'_2 \ldots \beta'_n \\ \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots \\ d\beta_1^{(n-1)}, & \ldots\ldots \end{vmatrix}^2 = \begin{vmatrix} x'_1, x'_2, \ldots x'_n \\ y_1, y_2, \ldots y_n \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ z_1, z_2, \ldots z_n \end{vmatrix}^2 \cdot \begin{vmatrix} 1, \alpha & \ldots \alpha^{n-1} \\ 1, \alpha' & \ldots \alpha'^{n-1} \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ 1, \alpha^{(n-1)} & \ldots\ldots \end{vmatrix}^2,$$

czyli, — oznaczywszy wyróżnik grupy $\beta_1, \ldots, \beta_n$ przez D, —

$$d^2\,D = \Delta.$$

Jestto równanie bardzo ważne, bo daje sposób odszukania ze wzoru (2) wszystkich liczb całkowitych, jakie tylko można otrzymać przy wartościach ułamkowych na zmienne x.

Rzeczywiście, z ostatniego równania okazuje się, że d^2 musi być dzielnikiem liczby Δ; jeżeli więc Δ nie posiada żadnego dzielnika kwadratowego, to wtedy tylko całkowite wartości zmiennych x we wzorze (2) dają β całkowite.

W przeciwnym razie niech d^2 przedstawia jeden z dzielników kwadratowych liczby Δ; nadajmy zmiennym x' we wzorze (3) różne wartości całkowite od zera do $d-1$ włącznie i szukajmy, czy nie znajdą się liczby całkowite między otrzymanemi kombinacyami. To, co czynimy z liczbą d, powtórzyć musimy ze wszystkiemi innemi dzielnikami kwadratowemi, i tym sposobem po pewnéj skończonéj liczbie działań odszukamy wszystkie liczby całkowite z wartościami ułamkowemi zmiennych x.

Dajmy, że taką drogą udało się nam znaleść pewną liczbę całkowitą β_1; dołączmy do niéj jeszcze $n-1$ liczb $\beta_2, \ldots, \beta_n$, to otrzymamy grupę

$$\beta_1, \beta_2, \ldots, \beta_n,$$

której wyróżnik równa się

$$D = \frac{\Delta}{d^2};$$

jego wartość liczebna jest więc mniejsza od wartości pierwotnego wyróżnika Δ. Wzór

$$x_1\ \beta_1 + x_2\ \beta_2 + \ldots + x_n\ \beta_n \qquad (4)$$

daje też same liczby co i (2), tylko przy innych wartościach zmiennych x, i każda liczba wyraża się za pomocą (4) jednym tylko sposobem, podobnież jak jednym sposobem wyrażała się przez (2). W przeciwnym bowiem razie między liczbami $\beta_1, \ldots, \beta_n$ zachodziłby związek postaci

$$l_1\ \beta_1 + l_2\ \beta_2 + \ldots + l_n\ \beta_n = 0,$$

gdzie przynajmniéj jeden ze współczynników $l_1, \ldots, l_n$ nie równałby się zeru, i mielibyśmy

$$D = 0.$$

Ze wzorem (4) możemy powtórzyć powyższe działania. Przypuśćmy, że znaleźliśmy liczbę całkowitą γ_1, wyrażającą się przez (4) z wartościami ułamkowemi zmiennych x; znajdziemy wtedy nową grupę liczb całkowitych

$$\gamma_1, \gamma_2, \ldots, \gamma_n$$

z wyróżnikiem $D' < D$ i nie równym zeru; nierówność pojmujemy w znaczeniu arytmetycznem.

Postępując tym sposobem daléj, dojdziemy nakoniec do takiéj grupy

$$\omega_1, \omega_2, \ldots \omega_n,$$

że wzór

$$x_1\ \omega_1 + x_2\ \omega_2 + \ldots + x_n\ \omega_n \qquad (5)$$

nie będzie w stanie dać liczby całkowitéj przy ułamkowych wartościach zmiennych x. Tu kończy się szereg naszych działań, i wzór (5) będzie wzorem ogólnym dla wszystkich liczb całkowitych danego obszaru przy wszelkich wartościach całkowitych zwyczajnych zmiennych x. Grupę liczb $\omega_1, \omega_2, \ldots \omega_n$ możemy nazwać zasadniczą. Główna jéj własność polega na tem, że wyróżnik jéj posiada wartość liczebną najmniejszą; przytem rozumie się samo przez się, że nie mamy na względzie przypadku, kiedy wyróżnik równa się zeru.

4. Jeżeli różnica dwóch liczb całkowitych $\beta - \beta'$ dzieli się przez trzecią jakąkolwiek liczbę γ, to mówimy, że te liczby są kongruentne według modułu γ i piszemy

$$\beta \equiv \beta' \ (\mathrm{mod.}\ \gamma).$$

Dwie liczby kongruentne z trzecią są kongruentne między sobą; ta własność pozwala nam wszystkie liczby kongruentne między sobą uważać jako stanowiące jedną klasę, przedstawicielką której będzie jakakolwiek z liczb do téj klasy należących.

Zachodzi teraz pytanie, czy liczba różnych klas w danym obszarze jest również skończoną jak i dla liczb zwyczajnych?

Tak jest w rzeczy saméj, o czem przekonać się można w następujący sposób:

Niech

$$\omega_1, \omega_2, \ldots, \omega_n$$

przedstawia grupę o wyróżniku najmniejszym, i niech iloczyny $\gamma\,\omega_1, \gamma\,\omega_2 \ldots, \gamma\,\omega_n$ wyrażają się tak:

$$\begin{aligned}
\gamma\,\omega_1 &= a_1\,\omega_1 + a_2\,\omega_2 + \ldots + a_n\,\omega_n,\\
\gamma\,\omega_2 &= b_1\,\omega_1 + b_2\,\omega_2 + \ldots + b_n\,\omega_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\gamma\,\omega_n &= c_1\,\omega_1 + c_2\,\omega_2 + \ldots + c_n\,\omega_n.
\end{aligned}$$

Wyznacznik

$$\delta = \begin{vmatrix} a_1, & a_2, & \ldots & a_n \\ b_1, & b_2, & \ldots & b_n \\ \ldots & \ldots & \ldots & \ldots \\ c_1, & c_2, & \ldots & c_n \end{vmatrix}$$

nie równa się zeru, gdyż między ilościami $\omega_1, \omega_2, \ldots$ nie zachodzi żaden związek liniowy.

Z powyższych równań wnosimy bezpośrednio, że

$$\delta\,\omega_1 \equiv \delta\,\omega_2 \equiv \ldots \equiv \delta\,\omega_n \equiv 0 \pmod{\gamma},$$

a stąd znów wypada, że wszelka liczba całkowita

$$\Omega = x_1\,\omega_1 + x_2\,\omega_2 + \ldots + x_n\,\omega_n$$

jest kongruentną według modułu γ z pewną liczbą

$$\omega = \xi_1\,\omega_1 + \xi_2\,\omega_2 + \ldots + \xi_n\,\omega_n\,,$$

któréj współczynniki $\xi_1, \xi_2, \ldots$ zawierać się będą w granicach między zerem i wartością liczebną δ. Liczba zatem liczb niekongruentnych między sobą według mod. γ jest skończoną; wyznaczymy ją w dalszym ciągu téj pracy.

5. Jeżeli dla danych liczb γ i β można wyznaczyć takie nowe dwie liczby γ_1 i β_1, które będą czyniły zadość warunkowi

$$\beta\,\beta_1 + \gamma\,\gamma_1 = 1\,,$$

wtedy γ i β nazywają się p i e r w s z e m i w z g l ę d e m s i e b i e; w przeciwnym razie mówić będziemy, że γ i β nie są pierwszemi względem siebie.

Mówimy, że liczby γ i β mają wspólny dzielnik, jeśli istnieje taka liczba d, od jedności różna, która dzieli jednocześnie γ i β; w przeciwnym razie γ i β nie mają wspólnego dzielnika.

W teoryi liczb zwyczajnych liczby nie posiadające wspólnego dzielnika są pierwszemi względem siebie i naodwrót; w teoryi liczb algebraicznych nie zawsze tak bywa: z wymienionych dwóch własności może mieć miejsce tylko pierwsza.

Wszelka liczba γ, nie mająca żadnych innych dzielników, oprócz saméj siebie i jedności, nazywa się n i e r o z k ł a d a l n ą; w przeciwnym razie liczba jest rozkładalną. Rozumie się samo przez się, że dzielników różniących się między sobą czynnikiem równym jedności, nie należy uważać za różne.

Wszelka liczba γ, posiadająca tę szczególną własność że każda inna liczba β albo dzieli się przez γ, albo jest pierwszą względem γ, nazywa się liczbą p i e r w s z ą; liczba nie posiadająca téj własności nazywa się niepierwszą.

W teoryi liczb zwyczajnych, liczby nierozkładalne są jednocześnie liczbami pierwszemi i naodwrót; w teoryi liczb algebraicznych może się zdarzyć, że liczba nierozkładalna bynajmniej nie jest pierwszą.

6. Każdéj liczbie całkowitéj β odpowiada inna liczba całkowita β_1, należąca do tegoż samego obszaru co i β i określająca się ze wzoru

$$\beta\,\beta_1 = N(\beta);$$

ta liczba β_1 nazywa się s p r z ę ż o n ą z liczbą β. W saméj rzeczy, jeżeli β jest pierwiastkiem równania

$$\beta^n + b_1\,\beta^{n-1} + \ldots + b_{n-1}\,\beta + b_n = 0;$$

to

$$\beta_1 = \pm\frac{b_n}{\beta} = \mp(\beta^{n-1} + b_1\,\beta^{n-2} + \ldots + b_{n-1})\,.$$

Jeżeli normy dwóch liczb β i γ są pierwszemi względem siebie, to takiemi są i same liczby β i γ, gdyż zachodzi równanie

$$\beta\,\beta_1\,x + \gamma\,\gamma_1\,y = 1\,,$$

przy pewnych liczbach całkowitych zwyczajnych na zmienne x i y.

Porównywając jakąkolwiek liczbę β z liczbą zwyczajną k, łatwo jest przekonać się, że wtedy, i tylko wtedy, liczby β i k będą pierwszemi względem siebie, gdy $N(\beta)$ i k będą takiemi.

Zwróciwszy nareszcie uwagę na to, że określenie liczb algebraicznych pierwszych względem siebie jest takie jak i liczb zwyczajnych względnie pierwszych wnosimy stąd, że i charakterystyczne własności liczb względnie pierwszych pozostają teżsame w obydwóch przypadkach, mianowicie:

1. Jeżeli każda z liczb $\beta, \beta_1, \beta_2, \ldots$ jest pierwsza względem każdéj z liczb $\gamma, \gamma_1, \gamma_2, \ldots$, to i iloczyny $\beta\,\beta_1\,\beta_2 \ldots$ i $\gamma\,\gamma_1\,\gamma_2 \ldots$ są pierwszemi względem siebie.

2. Jeżeli δ dzieli się przez β i przez γ, i jeżeli β i γ są względnie pierwszemi, to δ dzieli się przez $\beta\gamma$.

3. Jeżeli iloczyn $\gamma\beta$ dzieli się przez δ, δ i γ zaś są względnie pierwszemi, to β dzieli się przez δ.

Odnośnie do liczb pierwszych należy mieć na uwadze, że:

1. dwie liczby pierwsze, których stosunek równa się jakiejkolwiek jedności, nie uważają się za różne;

2. dwie liczby pierwsze różne są pierwszemi względem siebie;

3. iloczyn $\gamma\beta$ wtedy tylko dzieli się przez liczbę pierwszą $\tilde{\omega}$, kiedy przynajmniéj jeden z czynników γ, β dzieli się przez $\tilde{\omega}$;

4. wszelka liczba pierwsza jest jednorodną, to znaczy, że jéj norma równa się pewnéj potędze liczby pierwszéj zwyczajnéj p; sama zaś liczba pierwsza jest dzielnikiem liczby p.

II. Równoważność liczb i podział ich na klasy według modułu danego.

---

7. Wziąwszy pod uwagę jakąkolwiek liczbę pierwszą zwyczajną p, nazwiemy ją m o d u ł e m.

Stopień najwyższéj potęgi modułu p, dzielącéj normę liczby α, nazywać będziemy r z ę d e m liczby α; oznaczywszy go przez a, mieć będziemy

$$N(\alpha) = p^a h,$$

gdzie h jest liczbą całkowitą zwyczajną, nie dzielącą się przez liczbę p. Rząd iloczynu dwóch liczb równa się sumie ich rzędów.

Liczby rzędu zero są to liczby pierwsze względem modułu p; uważać je będziemy za r ó w n o w a ż n e i zbierzemy je w jednę oddzielną klasę, którą będziemy oznaczali przez K_0; wejdą tu oczywiście między innemi liczbami i wszystkie jedności.

Wszystkie liczby, których normy dzielić się będą przez moduł p, znajdą się na zewnątrz klasy K_0.

Z takiego poglądu wynika, że w przypadku, gdy stosunek

$$\frac{\gamma\,\alpha}{\beta}$$

jest liczbą całkowitą, jeżeli γ jest liczbą pierwszą względem modułu p, to można wtedy powiedzieć, że „α d z i e l i s i ę w e d ł u g m o d u ł u p p r z e z β“, albo też: „β j e s t w e d ł u g m o d u ł u p d z i e l n i k i e m l i c z b y α“. W saméj rzeczy zgodzimy się wyrażać takim sposobem wymienioną własność liczby β względem liczby α.

Łatwo sprawdzić następujące wnioski:

1. J e ż e l i l i c z b a α d z i e l i s i ę p r z e z β, a β d z i e l i s i ę p r z e z γ w e d ł u g m o d u ł u p, t o α, d z i e l i s i ę p r z e z γ w e d ł u g m o d u ł u p.

2. J e ż e l i k a ż d a z l i c z b α, α' d z i e l i s i ę w e d ł u g m o d u ł u p p r z e z β, t o i s u m a $\alpha \pm \alpha'$ d z i e l i s i ę t a k ż e w e d ł u g mod. p p r z e z β.

3. J e ż e l i α d z i e l i s i ę w e d ł u g mod. p p r z e z β, t o i $\alpha\gamma$ d z i e l i s i ę w e d ł u g mod. p p r z e z β.

4. J e ż e l i α d z i e l i s i ę w e d ł u g mod. p p r z e z β, a α', w e d ł u g mod. p, p r z e z β', t o $\alpha\alpha'$ d z i e l i s i ę w e d ł u g mod. p p r z e z $\beta\beta'$.

5. J e ż e l i α d z i e l i s i ę w e d ł u g mod. p p r z e z β, t o r z ę d α j e s t r ó w n y r z ę d o w i l i c z b y β, a l b o g o p r z e w y ż s z a.

6. Wszelka liczba dzieli się według mod. p przez każdą z liczb, należących do klasy K_0.

8. Lecz aby nasze określenie podzielności liczby według mod. p miało należytą wartość, należy pokazać, w jaki sposób przekonać się można, czy dana liczba α dzieli się według mod. p przez β lub nie.

Do tego służy następujące

Twierdzenie. J e ś l i b o z n a c z a r z ę d l i c z b y β, a h j e s t l i c z b a, wzięta z równania

$$N(\beta) = p^b h,$$

t o d o w o l n i e w z i ę t a l i c z b a α b ę d z i e s i ę d z i e l i ł a w e d ł u g mod. p p r z e z β l u b n i e, s t o s o w n i e d o t e g o, c z y s t o s u n e k

$$\frac{h\,\alpha}{\beta}$$

b ę d z i e l i c z b ą c a ł k o w i t ą l u b n i e.

Pierwsza część twierdzenia jest oczywistą, gdyż h jest liczbą pierwszą względem p; pozostaje więc uzasadnić część drugą.

Dajmy, że istnieje pewna liczba γ, pierwsza względem p i taka, że stosunek

$$\frac{\gamma\,\alpha}{\beta} = \delta$$

jest liczbą całkowitą. Pomnóżmy obie strony téj równości przez γ_1, liczbę sprzężoną z γ,

$$\frac{N(\gamma)\,\alpha}{\beta} = \delta\,\gamma_1;$$

wyznaczmy dwie liczby całkowite zwyczajne x i y, czyniące zadość warunkowi

$$x\,N(\gamma) - y\,p^b = 1,$$

i wyrugujmy z poprzedniego równania $N(\gamma)$, to otrzymamy

$$\frac{y\,p^b\,\alpha}{\beta} + \frac{\alpha}{\beta} = x\,\delta\,\gamma_1.$$

Znajdujemy stąd

$$\frac{h\,\alpha}{\beta} = h\,x\,\delta\,\gamma_1 - \frac{y\,N(\beta)}{\beta}\,\alpha;$$

druga strona tego równania jest oczywiście liczbą całkowitą, więc

i $$\frac{h\,\alpha}{\beta}$$

jest liczbą całkowitą, co ostatecznie dowodzi prawdziwości twierdzenia.

Tak więc za pomocą pewnéj ograniczonéj liczby działań zawsze można się przekonać, czy jakakolwiek dana liczba α dzieli się według mod. p przez liczbę β lub nie.

Zwrócimy jeszcze uwagę na szczególny przypadek: liczba α wtedy tylko dzieli się według mod. p przez liczbę p, kiedy α dzieli się bezwzględnie przez liczbę p. Tożsamo zdarza się we wszystkich przypadkach, gdy $h = \pm 1$.

9. Dwie liczby α i β nazywać będziemy równoważnemi, jeżeli jednocześnie, według mod. p, α dzieli się przez β i β dzieli się przez α; oznaczać to będziemy w ten sposób:

$$\beta \equiv \alpha \pmod{p}.$$

Ten algorytm nazwiemy równaniem według mod. p; posiada on następujące własności:

1. Obie strony równania

$$\alpha \equiv \beta \pmod{p}$$

można pomnożyć przez jednę i tęż samą liczbę:

$$\alpha\,\delta \equiv \beta\,\delta \pmod{p}$$

2. Jeżeli obie strony równania mają wspólny czynnik δ, to równanie można skrócić przez δ.

3. Jeżeli

$$\alpha \equiv \beta \pmod{p}$$

i

$$\beta \equiv \gamma \pmod{p},$$

to

$$\alpha \equiv \gamma \pmod{p}.$$

4. Dwa równania według jednego i tegoż samego modułu p, można pomnożyć przez siebie jak równania zwyczajne,

$$\alpha \equiv \beta \pmod{p}$$

$$\alpha' \equiv \beta' \pmod{p},$$

stąd

$$\alpha\,\alpha' \equiv \beta\,\beta' \pmod{p}.$$

5. Liczby, równoważne według mod. p, należą do tego samego rzędu.

6. Jeżeli α dzieli się według mod. p przez β i jeżeli rzęd tych dwóch liczb jest jeden i ten sam, to

$$\alpha \equiv \beta \pmod{p}.$$

7. Jeżeli α dzieli się według mod. p przez β, to istnieje trzecia liczba γ taka, że iloczyn $\beta\gamma$ będzie liczbą równoważną z α:

$$\alpha \equiv \beta\,\gamma \pmod{p}. \tag{1}$$

Odwrotnie, jeżeli ma miejsce równanie (1), to liczba β jest dzielnikiem liczby α, według mod. p.

8. W równaniu

$$\alpha\,\beta \ldots \equiv \gamma\,\delta \ldots \pmod{p},$$

wolno na miejsce każdéj z liczb $\alpha, \beta, \ldots \gamma, \delta, \ldots$ podstawić jakąkolwiek równoważną jéj nową liczbę $\alpha', \beta', \ldots \gamma', \delta' \ldots$. Wszystkie liczby równoważne według mod. p z daną liczbą α są równoważne między sobą, każda z każdą, i tworzą jedną klasę, którą nazwiemy klasą według mod. p. Jedna którakolwiek z liczb, należących do takiéj klasy, reprezentuje całą klasę, bo za jéj pomocą można odszukać wszystkie inne liczby w téj klasie zawarte.

Klasa z przedstawicielką 1 jest tą samą klasą K_0, o któréj była mowa na początku rozdziału.

10. Wszystkie liczby należące do jednéj i téj saméj klasy są jednakowego rzędu, który przyjmiemy za rzęd klasy.

Jeżeli klasy różne będą rzędu jednakowego, to będziemy je nazywali równoległemi.

Dla otrzymania wszystkich klas m-go rzędu i wszystkich liczb zawartych w każdéj z nich, będziemy postępowali w sposób następujący:

Weźmy pod uwagę wzór ogólny wszystkich liczb całkowitych danego obszaru

$$x_1\,\omega_1 + x_2\,\omega_2 + \ldots + x_n\,\omega_n,$$

i nadajmy kolejno każdéj ze zmiennych $x_1, x_2, \ldots$ następujące wartości:

$$0, 1, 2, 3 \ldots, p^{m+1} - 1;$$

otrzymamy szereg liczb

$$\alpha_1, \alpha_2, \ldots, \alpha_k, \qquad (k = p^{n(m+1)}), \tag{1}$$

niekongruentnych względem siebie według mod. p^{m+1}. Jeżeli w (1) nie będzie ani jednéj liczby m-go rzędu, to nie będzie istniała ani jedna klasa m-go rzędu; gdyż w razie przeciwnym istniałaby liczba ω rzędu m go, dla któréj mielibyśmy równanie

$$\omega - p^{m+1}\ \Omega = a_i,$$

skąd bezpośrednio wynikałoby, że a_i jest rzędu m-go, co się sprzeciwia założeniu. Dajmy, że w szeregu (1) znajduje się jedna lub kilka liczb m-go rzędu; niech one będą

$$a_1, a_2, \ldots, a_j; \tag{2}$$

jeżeli w tym szeregu znajdzie się kilka liczb równoważnych między sobą według mod. p, wtedy, pozostawiwszy jednę z nich, pozostałe, jako powtarzające się, odrzucimy; tym sposobem otrzymamy nowy szereg liczb

$$\alpha, \beta, \ldots \gamma, \tag{3}$$

nierównoważnych między sobą i rzędu m-go; będą to właśnie przedstawicielki wszystkich klas m-go rzędu, jakie tylko istnieją.

Aby tego dowieść, dość jest pokazać, że wszelka liczba ω rzędu m-go jest równoważną z jedną z liczb (3).

W saméj rzeczy, liczba ω jest kongruentną z jedną z liczb (2), dajmy z a_1, więc

$$\omega = a_1 + p^{m+1}\ \Omega; \tag{4}$$

lecz równanie

$$N(a_1) = p^m\ Q,$$

wskazuje, że p^m dzieli się według mod. p przez a_1, gdyż Q nie dzieli się przez p; z (4) wnosimy zatem, że liczba ω dzieli się według mod. p przez a_1; a ponieważ ω i a_1 są tegoż samego rzędu, przeto są równoważne według mod. p. Nareszcie liczba a_1 jest równoważną z jedną z liczb (3).

Dla otrzymania wszystkich liczb, należących do danéj klasy, téj, naprzykład, któréj przedstawicielką jest liczba α, zwracamy się do szeregu (2) i wydzielamy z niego wszystkie liczby równoważne z liczbą α; niech one będą

$$a_1, a_2, \ldots, a_l.$$

Liczby szukane otrzymują się bezpośrednio ze wzoru

$$\omega = a_i + p^{m+1}\ \Omega,$$

gdzie Ω oznacza liczbę całkowitą dowolną, a skaźnik i przyjmuje wartości

$$i = 1, 2, 3, \ldots, l;$$

przytem należy zauważyć, że każda liczba otrzymuje się przy jednéj tylko wartości dla i, i tylko raz jeden. Dowiedliśmy więc, że za pomocą pewnéj skończonéj liczby działań można wyznaczać wszystkie istniejące klasy w porządku wzrastania ich rzędu.

Liczba klas różnych jest nieskończenie wielka.

11. Opierając się na wyżéj podanych określeniach łatwo przekonać się, że iloczyn dwóch liczb α i β, z których pierwsza jest wzięta dowolnie z klasy K_1, druga dowolnie z klasy K_2, daje iloczyn γ, zawsze należący do téj saméj klasy K_3, którą będziemy nazywali iloczynem K_1 przez K_2, i pisali

$$K_3 = K_1\ K_2, \tag{1}$$

albo, co na jedno wychodzi,

$$K_3 = K_2\ K_1.$$

Własność zatem charakterystyczna iloczynu (1) polega na tem, że dla liczb

$$\alpha, \beta, \gamma,$$

należących odpowiednio do klas

$$K_1, K_3, K_3.$$

mamy

$$\gamma \equiv \alpha\beta \pmod{p}, \tag{2}$$

i naodwrót.

Klasę K_1, oraz K_2, nazywać będziemy dzielnikami klasy K_3. Szukać dzielników danéj klasy znaczy to samo, co szukać dzielników, według mod. p, jakiéjkolwiek liczby, wziętéj za przedstawicielkę danéj klasy.

Każda klasa, podobnie jak i każda liczba posiadają dwa dzielniki oczywiste, których nie będziemy tu brali pod uwagę, są to: klasa rzędu zero, K_0 czyli jedność, i sama klasa dana albo liczba, która ją przedstawia. Inne dzielniki muszą być rzędu niższego niż klasa dana, gdyż rzęd iloczynu równa się sumie rzędów czynników.

Zadanie znalezienia wszystkich dzielników klasy danéj rozwiązuje się za pomocą pewnéj ograniczonéj liczby działań, drogą prób bezpośrednich: bierzemy pod uwagę po kolei każdą z klas rzędu niższego i próbujemy, czy jest ona dzielnikiem danéj klasy, czy nie.

Dwie klasy równoległe nie mogą dzielić żadna żadnéj, bo jeżeliby jedna z nich dzieliła drugą, to byłyby równemi sobie.

Przechodząc od klasy do liczby, przedstawicielki klasy, otrzymamy twierdzenie:

Dla wszelkiéj liczby danéj, liczba dzielników nierównoważnych między sobą według mod. p jest skończoną, i wszystkie te dzielniki można znaleść za pomocą skończonéj liczby działań.

Z pomiędzy dzielników liczby danéj wyróżnia się ten, którego rzęd jest najmniejszy; taki dzielnik już nie posiada dla siebie żadnego dzielnika według mod. p, jest on więc liczbą nierozkładalną według mod. p.

Przyszliśmy zatem do wniosku, że wszystkie liczby całkowite stanowią dwa działy: do jednego należą liczby rozkładalne, do drugiego — nierozkładalne.

Wszelka liczba rozkładalna rozkłada się według mod. p na iloczyn z kilku czynników nierozkładalnych.

Ten sam podział odnosi się i do klas: wszelka klasa rozkładalna jest iloczynem kilku klas nierozkładalnych.

III. Twierdzenie zasadnicze.

12. Mieliśmy już nieraz sposobność zauważyć, że czasem udaje się wyznaczyć rzęd liczby na zasadzie jéj formy zewnętrznéj; obecnie w tym względzie chcemy zrobić jeszcze krok naprzód: pokażemy jak, w pewnych razach, korzystając z równania, któremu czyni zadość liczba α, można odrazu znaleść rzęd liczby

$$\alpha^b - p^a h,$$

gdzie h oznacza liczbę nie dzielącą się przez p. Aby otrzymać rezultat w formie jak można najogólniejszéj, przypuścimy, że α jest liczbą ułamkową, równą stosunkowi dwóch jakichkolwiek liczb całkowitych; w takim razie rzęd α może być liczbą ujemną.

Twierdzenie pomocnicze. Niech liczba α, nierówna zeru, czyni zadość równaniu

$$q_0 \alpha^n + q_i p^{m_i} \alpha^{n-i} + q_j p^{m_j} \alpha^{n-j} + \ldots + q_n p^{m_n} = 0, \qquad (1)$$

gdzie $q_0, \ldots, q_n$ są liczby całkowite zwyczajne, nie dzielące się przez p i różne od zera; $m_i, m_j, \ldots, m_n$ — liczby całkowite zwyczajne dodatnie, ujemne lub równe zeru; niech będzie liczba

$$\omega = \alpha^b - p^a h, \qquad (2)$$

gdzie b oznacza liczbę całkowitą zwyczajną, a—liczbę całkowitą zwyczajną dodatnią lub zero, h — liczbę całkowitą zwyczajną jakąkolwiek, nie dzielącą się przez p.

Jeżeli wszystkie liczby zawarte w szeregu

$$na, \quad (n-i)\,a + m_i\,b, \quad (n-j)\,a + m_j\,b, \ldots\ldots, m_n\,b \qquad (3)$$

są różne, to w takim razie rzęd liczby (2) równa się najmniejszéj z liczb (3).

Aby tego dowieść, weźmy pod uwagę funkcyą

$$f(x) = q_0 p^{m_0} x^n + q_i p^{m_i + m_0} x^{n-i} + \ldots + q_n p^{m_n + m_0},$$

gdzie p uważać będziemy za parametr dowolny; $q_0, \ldots, q_n$, $m_i, \ldots, m_n$ oznaczają téż same liczby, co w (1), wreszcie m_0 jest dowolną liczbą całkowitą, zwyczajną tak wielką, że żadna z liczb

$$m_0, \quad m_i + m_0, \quad m_j + m_0, \ldots, m_n + m_0$$

nie jest ujemną.

Weźmy jeszcze równanie

$$x^b - p^a h = 0, \qquad (4)$$

gdzie a i b oznaczają toż samo, co w (2), a p jest tym samym parametrem dowolnym, co w wyrażeniu $f(x)$.

Rugownik funkcyi $f(x)$ względem (4) jest funkcyą całkowitą ilości p ze współczynnikami, które są liczbami całkowitemi zwyczajnemi; oznaczywszy go przez R, uczyńmy

$$R = A p^r + A_1 p^{r+1} + \ldots,$$

gdzie r jest liczbą dodatnią albo zerem, A — nierówne zeru. Nie wdając się w obliczanie współczynników $A_1, A_2, \ldots$, poszukamy wartości liczb A i r. W tym celu oznaczmy przez $x_1, x_2, \ldots x_b$ pierwiastki równania (4), a przez $\tilde{\omega}_1, \tilde{\omega}_2, \ldots, \tilde{\omega}_b$ pierwiastki równania

$$x^b - 1 = 0.$$

Jest

$$R = f(x_1)\, f(x_2) \ldots f(x_b),$$

$$x_1 = \tilde{\omega}_1 h^{\frac{1}{b}} p^{\frac{a}{b}}, \ldots, x_b = \tilde{\omega}_b h^{\frac{1}{b}} p^{\frac{a}{b}},$$

a więc

$$f(x_1) = \tilde{\omega}_1^n q_0 h^{\frac{n}{b}} p^{n\frac{a}{b}+m_0} + \tilde{\omega}_1^{n-i} q_i h^{\frac{n-i}{b}} p^{(n-i)\frac{a}{b}+m_i+m_0} + \ldots$$

$$\ldots + q_n p^{m_n+m_0}.$$

W skutek założenia, że wszystkie liczby w (3) są różne, przychodzimy do wniosku, że wszystkie wykładniki nad p w ostatniem równaniu są różne, i jeżeli najmniejszą z liczb (3) nazwiemy przez μ, to najmniejszy wykładnik nad p w tem równaniu będzie

$$\frac{\mu}{b} + m_0.$$

Dajmy, że temu wykładnikowi odpowiada skaźnik l; więc w rozwinięciu ilości $f(x_1)$ według potęg rosnących liczby p pierwszy wyraz jest

$$\tilde{\omega}_1^{n-l} q_l h^{\frac{n-l}{b}} p^{\frac{\mu}{b}+m_0}.$$

W podobnych rozwinięciach ilości $f(x_2), f(x_3), \ldots$ pierwsze wyrazy będą odpowiednio:

$$\tilde{\omega}_2^{n-l} q_l h^{\frac{n-l}{b}} p^{\frac{\mu}{b}+m_0},$$

$$\ldots\ldots\ldots$$

$$\tilde{\omega}_b^{n-l} q_l h^{\frac{n-l}{b}} p^{\frac{\mu}{b}+m_0}.$$

Stąd wnosimy, że pierwszy wyraz w rozwinięciu rugownika R podług potęg rosnących głoski p będzie

$$(-1)^{(n-l)(b-1)} q_l^b h^{n-l} p^{\mu+m_0 b}.$$

Jestto właśnie wyraz szukany $A p^r$,

$$R = \varepsilon q_l^b h^{n-l} p^{\mu+m_0 b} + A_1 p^{\mu+m_0 b+1} + \ldots,$$

gdzie dla skrócenia uczyniliśmy

$$(-1)^{(n-1)(b-1)} = \varepsilon.$$

Nadajmy teraz parametrowi p wartość liczby pierwszéj p, wchodzącéj w (1) i (2), i weźmy pod uwagę normę liczby $\alpha^b - p^a h$; mamy

$$q_0^b p^{m_0 b} N(\alpha^b - p^a h) = (-1)^{nb} R,$$

stąd otrzymujemy

$$N(\alpha^b - p^a h) = (-1)^{nb} p^{\mu} \frac{\varepsilon q_l^b h^{n-l} + A_1 p + \ldots}{q_0^b};$$

co przekonywa nas, że rzęd liczby ω (2) równa się μ. Co było do okazania.

13. ***Twierdzenie.*** Niech będą dwie liczby całkowite α i β, różne od zera, i przypuśćmy, że β nie dzieli się według mod. p przez α; w takim razie można zawsze znaleść taką liczbę całkowitą ω, że rzęd różnicy $\frac{\alpha}{\beta} - \omega$ będzie mniejszy od rzędu stosunku $\frac{\alpha}{\beta}$.

Stosunek

$$\frac{\alpha}{\beta} = \xi \tag{1}$$

jest pierwiastkiem równania

$$q_n \xi^n + q_{n-i} p^{m_{n-i}} \xi^{n-i} + q_{n-j} p^{m_{n-j}} \xi^{n-j} + \ldots + q_0 p^{m_0} = 0, \tag{2}$$

gdzie $q_n, q_{n-i}, \ldots$ przedstawiają liczby całkowite, zwyczajne, nie dzielące się przez p i nie równe zeru; $m_{n-i}, m_{n-j}, \ldots m_0$ są to także liczby całkowite zwyczajne, z których każda może być dodatnią, ujemną, lub zerem.

Uczyniwszy

$$\frac{q_0}{\xi} = \frac{q_0 \beta}{\alpha} = \eta,$$

otrzymujemy z (2)

$$\eta^n + q_l q_0^{l-1} p^{m_l - m_0} \eta^{n-l} + \ldots + q_n q_0^{n-1} p^{-m_0} = 0, \tag{3}$$

a ponieważ liczba η, według założenia, nie jest liczbą całkowitą, przeto w szeregu wykładników

$$m_l - m_0, \ldots, m_j - m_0, m_i - m_0, -m_0$$

znajduje się przynajmniéj jeden ujemny; niech r oznacza odpowiedni mu skaźnik, więc

$$m_0 - m_r > 0. \tag{4}$$

Jeżeliby istniało kilka wykładników ujemnych, to r miałoby kilka różnych wartości; z pomiędzy nich wybór nasz padnie na tę, dla której odpowiednia wartość stosunku

$$\frac{m_0 - m_r}{r}$$

jest największą.

Mając to na uwadze, zwróćmy się teraz do równania, któremu czyni zadość taka liczba:

$$\zeta = p^\lambda \eta = p^\lambda q_0 \frac{\beta}{a}.$$

Jest ono następujące:

$$\zeta^n + q_l q_0^{l-1} p^{m_l - m_0 + l\lambda} \zeta^{n-l} + \ldots + q_n q_0^{n-1} p^{-m_0 + n\lambda} = 0, \tag{5}$$

widać stąd, że, jeżeli uczynimy

$$\lambda = \frac{m_0 - m_r}{r},$$

to wszystkie wykładniki nad głoską p w (5) będą liczbami wymiernemi dodatniemi lub zerem, lecz żaden z nich nie będzie ujemnym, tak że każdy współczynnik w (5) będzie liczbą całkowitą, a przeto i

$$\zeta = p^{\frac{m_0 - m_r}{r}} q_0 \frac{\beta}{a} \tag{6}$$

będzie liczbą całkowitą.

Lecz może się okazać, że liczba (6) wcale nie należy do naszego obszaru; aby tego uniknąć, weźmy zamiast ζ liczbę ω

$$\omega = \zeta^{ra} = p^{(m_0 - m_r)a} q_0^{ra} \left(\frac{\beta}{a}\right)^{ra}, \tag{7}$$

która oczywiście przy wszelkiéj wartości całkowitéj i dodatniéj a przedstawia liczbę należącą do naszego obszaru.

Co się tyczy liczby a, to zrobimy tu zastrzeżenie, że chociaż ta liczba jest dowolną, powinna jednak być tak wzięta, iżby żadna z dwóch liczb w szeregu

$$n\frac{(m_0 - m_r)a}{ra+1}, \quad (n-i)\frac{(m_0 - m_r)a}{ra+1} + m_{n-i}, \tag{8}$$

$$(n-j)\frac{(m_0 - m_r)a}{ra+1} + m_{n-j}, \ldots, r\frac{(m_0 - m_r)a}{ra+1} + m_r,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots m_0$$

nie były równe sobie; jestto warunek łatwy do zadość uczynienia, bo jakiekolwiek dwie liczby w (8) mogą być sobie równe tylko przy jednéj jedynéj wartości na a.

Liczba ω (7), tym sposobem określona jest właśnie taką, o jakiéj jest mowa w twierdzeniu; pozostaje nam tylko to sprawdzić.

Dla ułatwienia wykładu zgodzimy się tu chwilowo rzęd jakiejkolwiek liczby α według mod. p oznaczać za pomocą znaku

$$N_p(\alpha);$$

szukając rzędu liczby $(\xi - \omega)\xi^{ra}$, znajdziemy

$$N_p[(\xi - \omega)\xi^{ra}] = N_p(\xi^{ra+1} - p^{(m_0 - m_r)a} q_0^{ra}).$$

Lecz rzęd ostatniéj liczby znajdziemy na zasadzie wyżéj dowiedzionego twierdzenia pomocniczego; jeżeli oznaczymy najmniejszą z liczb (8) przez μ, to

$$N_p(\xi^{ra+1} - p^{(m_0 - m_r)a} q_0^{ra}) = \mu(ra+1).$$

W szeregu (8) znajduje się liczba

$$r\frac{(m_0 - m_r)a}{ra+1} + m_r,$$

która nigdy nie jest końcową, i może być napisaną tak:

$$(m_0 - m_r)\frac{ra}{ra+1} + m_r;$$

wartość jéj jest mniejszą od m_0, gdyż

$$m_0 - m_r > 0, \quad \frac{ra}{ra+1} < 1;$$

tem bardziéj więc

$$\mu < m_0,$$

i z powyższego równania wynika

$$N_p(\xi^{ra+1} - p^{(m_0 - m_r)a} q_0^{ra}) < m_0(ra+1),$$

czyli

$$N_p[(\xi - \omega)\xi^{ra}] < m_0(ra+1),$$

albo

$$N_p(\xi - \omega) + N_p(\xi^{ra}) < m_0(ra+1).$$

Na zasadzie (2) mamy

$$N_p(\xi^{r\alpha}) = m_0\, r\, a;$$

więc

$$N_p(\xi - \omega) < m_0,$$

albo

$$N_p(\xi - \omega) < N(\xi),$$

co było do okazania.

Wniosek. Jeżeli liczba β nie dzieli się według mod. p przez liczbę α, to można znaleść taką liczbę ω, iż rzęd różnicy $\alpha - \beta\omega$ będzie mniejszy od rzędu liczby α.

Oczywiście wniosek ten jest wyrażeniem w innéj formie samego twierdzenia.

Można się zgodzić nazywać ω ilorazem, a różnicę $\alpha - \beta\omega$ resztą dzielenia według mod. p liczby α przez liczbę β.

Łatwo zauważyć, że w przypadku, kiedy β dzieli się według mod. p przez α, twierdzenie miejsca mieć nie może, gdyż przy liczbie całkowitéj dowolnéj ω, rzęd różnicy $\alpha - \beta\omega$ nigdy nie będzie mniejszy od rzędu liczby α.

IV. O największym wspólnym dzielniku według mod. p.

14. Zastosujmy dowiedzione wyżéj twierdzenie do dwóch jakichbądź liczb danych α i β, w tem założeniu, że, według mod. p, ani α nie dzieli się przez β, ani β przez α; otrzymamy wtedy pewną liczbę całkowitą ϱ_2,

$$\varrho_2 = \alpha - \beta\,\omega,$$

rzędu niższego od rzędu liczby α.

Przypuśćmy następnie, że, według mod. p, β nie dzieli się przez ϱ_2, ani ϱ_2 przez α; otrzymamy nową liczbę

$$\varrho_3 = \beta - \varrho_2\,\omega',$$

rzędu niższego od rzędu liczby β.

Przypuściwszy następnie że, według mod. p, ϱ_2 nie dzieli się przez ϱ_3, ani ϱ_3 przez ϱ_2, otrzymamy

$$\varrho_4 = \varrho_2 - \varrho_3\,\omega''.$$

Postępując tym sposobem daléj, dojdziemy do dwóch liczb ϱ_{m-1} i ϱ_m, z których jedna będzie się dzieliła przez drugą, według mod. p; wtedy nasze działania się skończą i szereg liczb ϱ zamykamy na liczbie ϱ_m.

Do tego wszystkiego dodamy uwagę, że każdą z liczb ϱ można zastąpić jakąkolwiek inną liczbą jéj równoważną według mod. p, jeżeli taka zamiana okaże się dogodną.

Szereg otrzymany

$$\alpha,\ \beta,\ \varrho_2,\ \varrho_3,\ \ldots,\ \varrho_{m-1},\ \varrho_m \qquad (1)$$

posiada następujące dwie własności:

1. Wszelki dzielnik według mod. p, wspólny dwóm sąsiednim liczbom ϱ_{i-1}, ϱ_i, będzie dzielnikiem według mod. p wszystkich pozostałych liczb (1).

2. Każda z liczb $\varrho_2, \varrho_3 \ldots, \varrho_m$ wyraża się przez α i β za pomocą wzoru postaci

$$h_i\,\varrho_i = A_i\,\alpha + B_i\,\beta,$$

gdzie A_i i B_i oznaczają pewne liczby całkowite, h_i jest liczbą pierwszą względem p.

Obie te własności bezpośrednio wynikają z układu równań

$$k_i\,\varrho_i = \omega_i\,\varrho_{i+1} + k'_i\,\varrho_{i+2}, \qquad (i=2,\ldots,m-2) \qquad (2)$$

gdzie k_i i k'_i oznaczają liczby pierwsze względem p.

W saméj rzeczy, równanie (2) wskazuje, że jeżeli dwie sąsiednie liczby ϱ_{i+1} i ϱ_{i+2} dzielą się według mod. p przez liczbę δ, to i ϱ_i dzieli się według mod. p przez δ; wskutek tego i ϱ_{i-1} dzieli się przez δ, i tak daléj.

Co się tyczy drugiéj własności, to ona sprawdza się bezpośrednio dla $i=1$ i $i=2$; mamy bowiem

$$\varrho_1 = 0\,.\,\alpha + \beta,$$
$$k'_0\,\varrho_2 = k_0\,\alpha - \omega_0\,\beta;$$

pozostaje tylko dowieść, że jeżeli zachodzą dwa równania

$$h_{i-1}\,\varrho_{i-1} = A_{i-1}\,\alpha + B_{i-1}\,\beta,$$
$$h_i\,\varrho_i = A_i\,\alpha + B_i\,\beta,$$

to niezbędnie zachodzić będzie i równanie

$$h_{i+1}\,\varrho_{i+1} = A_{i+1}\,\alpha + B_{i+1}\,\beta\,. \tag{3}$$

Weźmy w tym celu równanie (2)

$$k'_{i-1}\,\varrho_{i+1} = k_{i-1}\,\varrho_{i-1} - \omega_{i-1}\,\varrho_i\,,$$

pomnóżmy obie jego strony przez $h_{i-1}\,h_i$ i podstawmy po stronie prawéj zamiast $h_{i-1}\,\varrho_{i-1}$, $h_i\,\varrho_i$ odpowiednie wartości z powyższych równań; otrzymamy wtedy równanie postaci (3). Nazwijmy teraz przez d tę z dwóch ostatnich liczb (1), która dzieli pozostałą, według mod. p; liczba ta jest wspólnym dzielnikiem według mod. p liczb ϱ_{m-1} i ϱ_m, posiada zatem następujące własności:

1. jest wspólnym dzielnikiem według mod. p liczb α i β,

$$\alpha \equiv d\,\alpha'\,, \quad \beta \equiv d\,\beta' \pmod{p}\,, \tag{4}$$

2. wyraża się przez α i β za pomocą wzoru

$$h\,d = A\,\alpha + B\,\beta\,, \tag{5}$$

gdzie h jest liczbą pierwszą względem p.

Wnosimy stąd, że wszystkie dzielniki według mod. p wspólne liczbom α i β są dzielnikami liczby d według mod. p, i naodwrót; tak że kwestya odszukania wszystkich dzielników według mod. p, wspólnych liczbom α i β, sprowadza się do odszukania wszystkich dzielników, według mod. p, liczby d. Z pomiędzy wszystkich dzielników liczby d jeden jest rzędu najwyższego: jestto sama liczba d; liczba więc d, określona tym sposobem, jest największym wspólnym dzielnikiem liczb α i β.

Umiejąc znaleść największy wspólny dzielnik dwóch liczb, potrafimy znaleść największy wspólny dzielnik, według mod. p, trzech, czterech i t. d. liczb.

Największy wspólny dzielnik trzech liczb α, β, γ wyraża się równaniem

$$h\,d = A\,\alpha + B\,\beta + C\,\gamma\,,$$

w którem h jest liczbą pierwszą względem p, i t. d.

15. Jeżeli liczby α i β nie mają żadnego wspólnego dzielnika według mod. p, oprócz jedności, to $d = 1$, równanie zaś (5) przyjmuje postać

$$A\,\alpha + B\,\beta = h\,, \tag{6}$$

gdzie h jest liczbą pierwszą względem p.

Naodwrót, jeśli zachodzi (6), to oczywiście α i β nie mogą mieć żadnego wspólnego dzielnika oprócz jedności; takie liczby nazywać będziemy względnie pierwszemi według mod. p.

Mamy więc dwa określenia równoważne liczb względnie pierwszych: nie mają żadnego wspólnego dzielnika według mod. p, albo czynią zadość równaniu postaci (6), gdzie h jest liczba równoważna jedności.

Łatwo zauważyć, że warunek (6) można zastąpić następującym

$$A\,\alpha + B\,\beta + C\,p = 1\,, \tag{7}$$

gdzie C, A, B są liczby całkowite, inne wogóle od tych, które wchodzą w (6); równanie (6) można przekształcić na (7), i naodwrót.

Powyższe określenia pozostają bez zmiany i dla trzech, czterech liczb, i t. d.

16. Liczby względnie pierwsze według mod. p posiadają także inne własności analogiczne z własnościami liczb zwyczajnych:

1. Jeżeli każda z liczb $\alpha, \alpha', \ldots, \alpha''$ jest, według mod. p, pierwszą względem każdéj z liczb $\beta, \beta', \ldots, \beta''$, to i iloczyn $\alpha\,\alpha' \ldots \alpha''$ jest, według mod. p, liczbą pierwszą względem $\beta\,\beta' \ldots \beta''$.

2. Jeżeli, według mod. p, γ dzieli się przez α i przez β, i jeżeli α i β są względnie pierwsze według mod. p, to γ dzieli się według mod. p przez $\alpha\,\beta$.

3. Jeżeli $\alpha\beta$ dzieli się według mod. p przez γ, i jeżeli α i γ są względnie pierwsze według mod. p, to β dzieli się według mod. p przez γ.

Pojęcie o najmniejszéj wielokrotności dwóch lub kilku liczb ustanawia się zupełnie w taki sam sposób, jak i dla liczb zwyczajnych; charakterystyczne własności pozostają te same.

17. Wszelka liczba π nierozkładalna według mod. p, czyli nie mająca żadnego dzielnika według mod. p, oprócz jedności i saméj siebie, — posiadać będzie następujące własności.

1. Jakakolwiek liczba α albo się dzieli według mod. p, przez π, albo jest pierwszą według mod. p, względem π.

Największy bowiem wspólny dzielnik, według mod. p, dla α i π jest równoważny albo α albo 1.

2. Jeżeli iloczyn $\alpha\beta$ dzieli się według mod. p przez π, to przynajmniéj jeden z czynników α lub β dzieli się według mod. p przez π.

Ta ostatnia własność jest bezpośredniem następstwem poprzedniéj, bo jeżeliby ani α, ani β nie dzieliły się według mod. p przez π, to obie liczby α i β, a zatem i ich iloczyn $\alpha\beta$ byłyby liczbami pierwszemi względem π, według mod. p.

Własność pierwsza jest charakterystyczną dla liczb nierozkładalnych; dzięki jéj liczby nierozkładalne nazywać możemy pierwszemi według mod. p.

Jako wniosek z drugiéj własności wynika następujące

Twierdzenie. Wszelka liczba rozkłada się według mod. p na iloczyn czynników pierwszych według mod. p, i tylko jednym sposobem.

Prawo podzielności jednéj liczby przez drugą, według mod. p, pozostaje takie same, jak i prawo zwyczajnéj podzielności liczb zwyczajnych.

Znane wyrażenia największego wspólnego dzielnika lub najmniejszéj wielokrotności pozostają według naszéj teoryi takiemiż, jak i dla liczb zwyczajnych.

Wszystko, co się tu mówiło o liczbach, stosuje się bezpośrednio i do klas. Dwie klasy są wzajemnie pierwsze, jeżeli ich przedstawicielki są wzajemnie pierwsze według mod. p. Jeżeli przedstawicielka klasy idealnéj jest liczbą pierwszą według mod. p, to i sama klasa będzie pierwsza i t. d.

Klasa jedność nie uważa się za pierwszą.

18. Łatwo przekonać się, że liczba liczb pierwszych według mod. p jest skończona. W saméj rzeczy rozłóżmy mod. p na iloczyn czynników pierwszych według mod. p,

$$p \equiv \pi_1^{m_1} \pi_2^{m_2} \ldots \pi_i^{m_i} \pmod{p},$$

i niech π przedstawia jakąkolwiek liczbę pierwszą według mod. p, różną od $\pi_1, \pi_2, \ldots, \pi_i$; ponieważ p i π nie są liczbami względnie pierwszemi, więc nie mogą być względnie pierwszemi i według mod. p, zatem p dzieli się przez π według mod. p; lecz do tego trzeba koniecznie, aby jedna z liczb $\pi_1, \pi_2, \ldots, \pi_i$ dzieliła się według mod. p przez π; niech π_1 dzieli się przez π; ponieważ π_1 jest liczbą pierwszą, przeto

$$\pi \equiv \pi_1 \pmod{p}.$$

Więcéj przeto liczb pierwszych według mod. p, oprócz $\pi_1, \ldots, \pi_i$, nie istnieje.

V. Własności głównych przedstawicielek klas idealnych.

---

19. Dotąd nie czyniliśmy żadnéj różnicy między przedstawicielkami jednéj klasy; teraz zaś chcemy uczynić pewien wybór pomiędzy niemi bardzo użyteczny: między liczbami klasy K poszukamy takiéj, któréj norma, co do liczebnéj wartości, byłaby równą potędze modułu p,

$$\pm N(\alpha) = p^a,$$

gdzie a oznacza rzęd klasy K. Nie będziemy zastanawiali się nad tem, jak znaleść taką liczbę, jeżeli istnieje, albo jak dowiedzieć się, że takiéj liczby wcale nie ma; przeciwnie, przypuścimy z góry, że takie liczby istnieją dla każdego modułu i dla każdéj klasy, i postaramy się tylko poznać ich własności.

Jeżeliby w jednéj klasie istniały dwie liczby takie, jak powyżéj określone, to każda z nich musiałaby się dzielić,—w zwyczajnem znaczeniu tego wyrazu,—przez pozostałą; więc stosunek takich liczb równym być musi jedności: nie będziemy uważali ich za różne i powiemy, że każda klasa posiada tylko jednę główną przedstawicielkę.

Oto są następujące charakterystyczne własności głównych przedstawicielek klas:

1. Powiedzieć, że jakakolwiek liczba ω dzieli się lub nie dzieli się według mod. p przez główną przedstawicielkę α, oznacza to samo, co powiedzieć, że ω dzieli się lub nie dzieli się przez α, w zwyczajnem znaczeniu tego wyrazu.

2. Wszystkie liczby należące do danéj klasy K z główną przedstawicielką α, otrzymują się ze wzoru

$$\alpha\ \omega,$$

gdzie ω oznacza liczbę dowolną, pierwszą względem p.

Jeżeli więc K_0 oznacza klasę rzędu zero, to klasę K można przedstawić symbolicznie tak:

$$K = \alpha\ K_0.$$

3. Główna przedstawicielka klasy pierwszéj jest liczbą pierwszą w zwyczajnem znaczeniu tego wyrazu.

Dla stwierdzenia tego trzeba naprzód dowieść, że liczba pierwsza względem głównéj przedstawicielki α, według mod. p, jest liczbą pierwszą względem α w zwyczajnem znaczeniu tego wyrazu.

W saméj rzeczy, wszelka liczba pierwsza względem α jest także pierwszą względem α według mod. p, jestto rzecz oczywista; przypuśćmy teraz naodwrót, że uważana liczba ω jest pierwszą względem α według mod. p; będzie więc

$$\omega\ \omega' + \alpha\ \alpha' = Q,$$

gdzie Q oznacza liczbę zwyczajną nie dzielącą się przez p; przy pewnych zatem wartościach całkowitych zwyczajnych liczb x i y będzie

$$x\ Q + y\ p^m = 1,$$

gdzie m oznacza rzęd liczby α.

Z dwóch powyższych równań otrzymujemy

$$\omega\,(x\,\omega') + \alpha\,(x\,\alpha') + p^m\,y = 1\,;$$

lecz

$$p^m = \pm N\,(\alpha) = \alpha\,\alpha_1\,,$$

przeto

$$\omega\,(x\,\omega') + \alpha\,(x\,\alpha' + y\,\alpha_1) = 1\,;$$

skąd widać, że ω jest liczbą pierwszą względem α w zwyczajnem znaczeniu wyrazu.

Na zasadzie tego, cośmy tu dowiedli, oraz tego, co było wypowiedziane nieco wyżéj (**1.**), wnosimy, że wszelka liczba ω albo się dzieli przez α, przedstawicielkę główną klasy pierwszéj, albo jest względem niej liczbą pierwszą, biorąc obie własności w zwyczajnem ich znaczeniu. To dowodzi, że α jest liczbą bezwzględnie pierwszą (**5.**).

Oczywista, że, odwrotnie, wszelka liczba pierwsza w zwyczajnem znaczeniu wyrazu jest główną przedstawicielką pewnéj klasy pierwszéj.

4. Oznaczywszy przez $\pi_1, \pi_2, \ldots, \pi_i$ główne przedstawicielki wszystkich liczb pierwszych, będziemy mieli

$$p = \pi_1^{m_1}\,\pi_2^{m_2}\,\ldots\,\pi_i^{m_i}\,\varepsilon\,,$$

gdzie ε oznacza pewną jedność, a każdy z wykładników $m_1, m_2, \ldots m_i$ jest dodatnim.

Wogóle wszelka główna przedstawicielka, czyli liczba jednorodna, może być przedstawioną w podobny sposób jako iloczyn z czynników pierwszych, tylko wykładniki mogą tu być równe zeru.

5. Wszelka liczba niejednorodna może być rozłożona na iloczyn kilku liczb jednorodnych.

W saméj rzeczy, niech

$$\pm N\,(\omega) = p^a\,q^b\,r^c\,,$$

i niech ω należy do klasy K, według mod. p; główną przedstawicielkę klasy K oznaczmy przez P, będzie (2)

$$\omega = P\,\omega'\,,$$

gdzie ω' przedstawia liczbę pierwszą względem p; stąd otrzymujemy

$$\pm N\,(P)\,N\,(\omega') = q^b\,r^c\,p^a\,,$$

po skróceniu

$$\pm N\,(\omega') = q^b\,r^c\,.$$

Rozumując podobnym sposobem daléj, przychodzimy do równości

$$\omega = P\,Q\,R\,,$$

gdzie P, Q, R są liczby jednorodne, należące odpowiednio do modułów p, q, r.

Rozłożywszy każdy z mnożników P, Q, R na czynniki pierwsze, w ostatecznym rezultacie mieć będziemy rozkład liczby ω na iloczyn czynników pierwszych.

Kończąc ten rozdział, znowu przypominamy, że wszystko, cośmy tu dowiedli, odnosi się do przypadku, kiedy każda klasa posiada główną przedstawicielkę. Lecz aby uniknąć wyjątków, zgódźmy się, aby mówić, że każda klasa posiada przedstawicielkę idealną główną, rozumiejąc pod wyrazem „idealna“ dodatkowe określenie: „mogąca istnieć lub nie istnieć“. Pod takim warunkiem będziemy mogli mówić, że wszelka liczba niejednorodna rozkłada się na iloczyn kilku liczb jednorodnych idealnych; zresztą, dla zachowania zupełnéj ścisłości, poświęcimy teoryi liczb idealnych jeden z następnych rozdziałów.

VI. Zasadnicze prawa bezwzględnéj podzielności liczb.

20. Ustanowiwszy w poprzednich rozdziałach prawa podzielności według mod. p, przechodzimy teraz do zbadania praw podzielności bezwzględnéj.

Dwa twierdzenia, które podamy tu na wstępie, rzucą dostateczne światło na nasze zadanie: oba są elementarne i prawie oczywiste.

Twierdzenie 1. Warunkiem koniecznym i dostatecznym, by dana liczba α dzieliła się przez liczbę β, jest, aby liczba α dzieliła się przez β według każdego z modułów, wchodzących w skład $N\,(\beta)$.

Niech

$$\pm N\,(\beta) = p^a\,q^b\,r^c;$$

oznaczmy dla skrócenia

$$P = q^b\,r^c, \quad Q = p^a\,r^c, \quad R = p^a\,q^b.$$

Że warunek przytoczony w twierdzeniu jest niezbędnym, jestto rzecz oczywista; pozostaje nam tylko dowieść, że jest dostatecznym.

W saméj rzeczy, jeżeli przypuścimy, że a dzieli się przez β według każdego z modułów p, q, r, zachodzić będą takie równania:

$$\frac{P\,a}{\beta} = a_1\,, \quad \frac{Q\,a}{\beta} = a_2\,, \quad \frac{R\,a}{\beta} = a_3\,,$$

gdzie a_1, a_2, a_3, są liczby całkowite.

Oznaczywszy przez x, y, z liczby całkowite zwyczajne, czyniące zadość równaniu

$$P\,x + Q\,y + R\,z = 1\,,$$

z powyższych równań otrzymujemy

$$\frac{a}{\beta} = x\,a_1 + y\,a_2 + z\,a_3\,;$$

liczba więc a dzieli się przez liczbę β w zwyczajnem znaczeniu wyrazu.

Na zasadzie dowiedzionego twierdzenia wszelkie pytanie o podzielności dwóch liczb jednéj przez drugą, bezpośrednio sprowadza się do warunków podzielności według różnych modułów, wchodzących w skład normy dzielnika.

21. ***Twierdzenie 2.*** Warunkiem koniecznym i dostatecznym, by dwie liczby α i β były względnie pierwszemi jest, aby α i β były względnie pierwszemi według każdego z modułów, wchodzących jednocześnie w skład $N(\alpha)$ i $N(\beta)$.

Że wskazany warunek jest niezbędnym, uważać to można za oczywiste; pozostaje dowieść, że warunek ten jest wystarczającym.

Niech

$$d = p^a\,q^b\,r^c$$

przedstawia największy wspólny dzielnik norm

$$N(\alpha)\,, \quad N(\beta)\,.$$

Przypuściwszy, że α i β są względnie pierwsze według każdego z modułów p, q, r, mamy (**15.**)

$$\begin{aligned} \alpha\,\omega + \beta\,\omega' &= P\,,\\ \alpha\,\omega_1 + \beta\,\omega'_1 &= Q\,,\\ \alpha\,\omega_2 + \beta\,\omega'_2 &= R\,, \end{aligned}$$

gdzie P, Q, R przedstawiają pewne liczby całkowite zwyczajne, nie dzielące się odpowiednio przez p, q, r; wskutek tego można znaleść liczby całkowite zwyczajne x, y, z takie, że suma

$$P\,x + Q\,y + R\,z = S$$

będzie liczbą pierwszą względem d.

Kładąc dla skrócenia

$$\begin{aligned} x\,\omega + y\,\omega_1 + z\,\omega_2 &= \Omega\,,\\ x\,\omega' + y\,\omega'_1 + z\,\omega'_2 &= \Omega'\,, \end{aligned}$$

z powyższych równań otrzymujemy

$$\alpha\,\Omega + \beta\,\Omega' = S\,.$$

Ponieważ liczby S i d są względnie pierwsze, więc liczby S, $N(\alpha)$, $N(\beta)$ są także względnie pierwsze; możemy przeto znaleść liczby całkowite zwyczajne x', y', z', czyniące zadość równaniu

$$S\,x' + N(\alpha)\,y' + N(\beta)\,z' = 1\,.$$

Rugując z dwóch ostatnich równań ilość S i czyniąc

$$N(\alpha) = \alpha\,\alpha_1\,, \quad N(\beta) = \beta\,\beta_1\,,$$

znajdujemy

$$(x'\,\Omega + y'\,a_1)\,\alpha + (x'\,\Omega' + z'\,\beta_1)\,\beta = 1\,,$$

skąd widać, że α i β są względnie pierwszemi. Twierdzenie oczywiście ma miejsce nietylko dla dwóch, lecz dla jakiéjkolwiek liczby liczb $\alpha, \beta, \gamma, \ldots$

22. Postawmy sobie teraz jedno z najważniejszych i przytem najprostszych zadań: odszukać wszystkie dzielniki danéj liczby α.

Rozumie się samo przez się, że dzielniki, różniące się czynnikiem jedność, nie uważają się za różne.

Rozłożywszy normę liczby α na iloczyn czynników pierwszych

$$\pm N(\alpha) = p^a\,q^b\,r^c\,,$$

zauważymy, że wszelki dzielnik δ liczby α powinien być dzielnikiem liczby α według każdego z modułów p, q, r. Lecz wiemy już, jak za pomocą skończonéj liczby działań odszukać można wszystkie dzielniki liczby α według danego jakiegobądź modułu; niech $\delta_1, \delta_2, \delta_3$ przedstawiają pewne dzielniki liczby α według odpowiednich modułów p, q, r. Będziemy tedy mieli następującą grupę równań (równoważności):

$$\delta \equiv \delta_1 \pmod{p}, \quad \delta \equiv \delta_2 \pmod{q}, \quad \delta \equiv \delta_3 \pmod{r}\,;$$

są to warunki, służące do określenia liczby δ, do których jeszcze należy dołączyć jeden, mianowicie: norma dzielnika δ nie powinna się dzielić przez żadną z liczb pierwszych, nie wchodzących w skład $N(\alpha)$, to jest, różnych od p, q, r.

Odwrotnie, wszelka liczba δ, czyniąca zadość równaniom

$$\left.\begin{aligned} \delta &\equiv \delta_1 \pmod{p}, \\ \delta &\equiv \delta_2 \pmod{q}, \\ \delta &\equiv \delta_3 \pmod{r}, \\ \pm N(\delta) &= p^a q^b r^c, \end{aligned}\right\} \tag{1}$$

gdzie a, b, c wyrażają rzęd odpowiedni każdéj z liczb

$$\delta_1, \delta_2, \delta_3$$

względem modułu

$$p, q, r,$$

— jest dzielnikiem liczby α.

Zadanie odszukania wszystkich dzielników liczby α sprowadza się tedy do znalezienia liczby δ, czyniącéj zadość równaniom (1). Rozumie się, że takich układów będzie tyle, ile można utworzyć kombinacyj z różnych wartości liczb $\delta_1, \delta_2, \delta_3$.

Nie możemy tu zatrzymywać się nad tém nowem zadaniem, które może być rozwiązanem za pomocą pewnéj skończonéj liczby działań, — bo to, oddaliłoby nas od naszego głównego celu; wystarczy mieć tymczasem na widoku dwa punkty:

1. Zadanie nie może mieć dwóch rozwiązań, jeżeli liczb różniących się czynnikiem równym jedności, nie będziemy uważali za różne.

2. Zadanie może nie mieć wcale żadnego rozwiązania.

Jeżeli przypuścimy, że warunkom (1) czynią zadość dwie liczby δ i δ', to bezpośrednio na mocy twierdzenia 1-go wniesiemy, że δ dzieli się przez δ', δ' zaś przez δ; zatem stosunek $\delta : \delta'$ równa się jedności.

Wogóle mówiąc, związek między grupą

$$\delta_1, \delta_2, \delta_3$$

i odpowiednim dzielnikiem δ jest takiéj natury, że jedna grupa wyznacza rzeczywiście pewien dzielnik, inna zaś nic nie daje; jestto niedogodność, która zdaje się utrudniać bezpośrednie przejście od praw podzielności według danego modułu do praw podzielności bezwzględnéj.

Aby utrzymać formę tych praw i dla podzielności bezwzględnéj, należy wprowadzić koniecznie dzielniki fikcyjne, odpowiadające tym przypadkom, w których równania (1) są niemożebne.

W saméj rzeczy, zgodzimy się na to, aby mówić, że równania (1) mają zawsze jedno rozwiązanie δ, domyślając się przytem, że δ może być czasem liczbą nieistniejącą, i dlatego nazywać będziemy tę liczbę — liczbą idealną.

23. Przejdźmy do innego zadania:

Znaleść największy wspólny dzielnik dwóch lub kilku liczb danych.

Niech będą dane dwie liczby α i β, i niech

$$p^a q^b r^c$$

przedstawia największy wspólny dzielnik norm $N(\alpha)$ i $N(\beta)$; znajdźmy za pomocą znanego sposobu największe wspólne dzielniki liczb α i β według odpowiednich modułów p, q, r, i nazwijmy je przez d_1, d_2, d_3; oznaczmy nareszcie przez D liczbę idealną, określoną warunkami

$$\left.\begin{aligned} D &\equiv d_1 \pmod{p}, \\ D &\equiv d_2 \pmod{q}, \\ D &\equiv d_3 \pmod{r}, \\ \pm N(D) &= p^{a'} q^{b'} r^{c'}. \end{aligned}\right\} \tag{2}$$

Widoczną jest rzeczą, że, jeżeli D istnieje, to wszelki dzielnik wspólny dla α i β będzie dzielnikiem liczby D, i naodwrót: ta liczba D właśnie nazywa się największym wspólnym dzielnikiem liczb α i β.

Zadanie nasze, które ostatecznie sprowadziło się do (2), może nie mieć rozwiązania, ale na mocy wprowadzonych przez nas liczb idealnych będziemy mówili, że ma ono zawsze jedno rozwiązanie, i nazywać je będziemy największym wspólnym dzielnikiem liczb α i β.

To, cośmy tu mówili o dwóch liczbach, stosuje się widocznie do jakiéjkolwiek liczby liczb: ich największy wspólny dzielnik przedstawia się zawsze, jako rozwiązanie równań takich jak (2).

Największy wspólny dzielnik będzie równoważny jedności wtedy, i tylko wtedy, kiedy dane liczby będą względnie pierwsze: jest to bezpośredni wynik z twierdzenia 2-go.

VI. Teorya liczb idealnych.

24. Przechodząc do bliższego rozpatrzenia zasadniczych własności liczb idealnych, weźmiemy pod uwagę równania, określające pewną liczbę idealną x:

$$\left.\begin{aligned} x &\equiv \alpha \pmod{p},\\ x &\equiv \beta \pmod{q},\\ x &\equiv \gamma \pmod{r},\\ \pm N(x) &= p^a q^b r^c, \end{aligned}\right\} \qquad (1)$$

a oznacza rzęd liczby α, b — rzęd liczby β, i t: d.

Liczbę idealną, czyniącą zadość powyższym warunkom, zgodzimy się przedstawiać w sposób taki:

$$x = \begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix}. \qquad (2)$$

Elementy drugiéj kolumny są to moduły, a pierwszéj — składowe liczby x według odpowiednich modułów. Liczba wierszy w (2) może się zmieniać od jedności do jakiéjkolwiek liczby.

Będziemy mieli zawsze na pamięci, że wyrażenie (2) odgrywa rolę podwójną: raz przedstawia liczbę, innym znów razem jest znakiem symbolicznym przedstawiającym warunki (1). Odpowiednio do tego każda własność, każde twierdzenie odnoszące się do wyrażenia (2) musi być sprawdzane dwa razy.

Jeżeli symbol (2) składa się z jednego tylko wiersza, wtedy $N(x)$ jest potęgą liczby pierwszéj, i liczba x nazywa się jednorodną, przez analogią do liczb istniejących.

Cała teorya liczb idealnych polega na następujących zasadniczych ich własnościach.

1. Wszelka liczba może być uważaną jako liczba idealna.

Rzeczywiście niech α oznacza jakąkolwiek liczbę daną i niech $\pm N(\alpha) = p^a q^b r^c$; mamy

$$\alpha = \begin{vmatrix} \alpha & p \\ \alpha & q \\ \alpha & r \end{vmatrix}.$$

2. W wyrażeniu liczby idealnéj pozwala się dowolnie przestawiać wiersze:

$$\begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix} = \begin{vmatrix} \beta & q \\ \gamma & r \\ \alpha & p \end{vmatrix}$$

Oczywista, że w przypadku, gdy liczba idealna jest istniejącą, przestawienie wierszy w wyrażeniu jéj symbolicznem nie zmienia wartości liczby; w przypadku zaś, gdy liczba nie istnieje, to przestawienie wierszy w niczem nie zmienia warunków określających liczbę, i dlatego zgodzimy się uważać symbole różniące się porządkiem wierszy za tożsame.

3. W wyrażeniu liczby idealnéj pozwala się przypisać ilekolwiek nowych wierszy z modułami dowolnemi, byleby odpowiednie im pierwsze elementy były równe jedności:

$$\begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix} = \begin{vmatrix} \alpha & p \\ \beta & q \\ 1 & r \end{vmatrix}.$$

W saméj rzeczy, łatwo spostrzedz, że warunki odpowiednie dwóm powyższym symbolom są tożsame; gdy więc liczba idealna istnieje, oba symbole będą oczywiście przedstawiały jednę i tęż samą liczbę; w przypadku zaś, gdy liczba nie istnieje, winniśmy zgodzić się na to, aby takie symbole za tożsame uważać.

Wniosek. Wyrażenia dwóch lub kilku liczb idealnych można sprowadzić do wspólnéj kolumny modułów.

Naprzykład, niech będą dwie liczby

$$x = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix}, \qquad y = \begin{vmatrix} \gamma & q \\ \delta & r \end{vmatrix};$$

możemy napisać:

$$x = \begin{vmatrix} \alpha & p \\ \beta & q \\ 1 & r \end{vmatrix}, \qquad y = \begin{vmatrix} 1 & p \\ \gamma & q \\ \delta & r \end{vmatrix}.$$

4. W wyrażeniu liczby idealnéj wolno jest na miejsce każdego elementu w pierwszéj kolumnie podstawić nową liczbę, równoważną mu według odpowiedniego modułu.

Mamy

$$\begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix} = \begin{vmatrix} \alpha' & p \\ \beta' & q \\ \gamma' & r \end{vmatrix},$$

z warunkiem, że

$$\alpha \equiv \alpha' \pmod{p},$$
$$\beta \equiv \beta' \pmod{q},$$
$$\gamma \equiv \gamma' \pmod{r}.$$

Równość powyższa jest oczywistą w przypadku, kiedy liczba idealna istnieje; w przeciwnym zaś razie, ponieważ warunki wyrażone przez obydwa symbole są tożsame, przeto nic nam nie przeszkadza zgodzić się raz na zawsze na to, aby podobne symbole uważać jako tożsame.

5. Aby dwie liczby idealne były równe, niezbędnem jest i dostatecznem, by elementy w pierwszych kolumnach, odpowiednie modułom równym były równoważne według tychże modułów.

Dostateczność warunków jest widoczną na zasadzie wyżéj przytoczonych własności; niezbędność ich jest także oczywistą, gdy obydwie liczby są istniejące, w innych zaś razach zależy od naszéj umowy uważać liczby jako równe tylko przy wyżéj podanych warunkach.

6. Iloczyn dwóch liczb idealnych równa się liczbie idealnéj, określonéj wzorem

$$\begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix} . \begin{vmatrix} \alpha' & p \\ \beta' & q \\ \gamma' & r \end{vmatrix} = \begin{vmatrix} \alpha\,\alpha' & p \\ \beta\,\beta' & q \\ \gamma\,\gamma' & r \end{vmatrix}.$$

Jeżeli oba czynniki po stronie lewéj są liczbami istniejącemi, wtedy prawdziwość równania sprawdza się bezpośrednio; w przeciwnym zaś razie, kiedy jeden albo oba czynniki są liczbami nieistniejącemi, lewa strona równości nie posiada żadnego określonego znaczenia, wolno nam wszakże pod takim iloczynem rozumieć, co zechcemy, umawiamy się więc na zawsze, aby rozumieć to, co przedstawia nam strona prawa powyższéj równości.

7. Iloczyn ilukolwiek liczb idealnych nie zmienia się w skutek przestawienia czynników.

Twierdzenie to jest bezpośrednim wynikiem poprzedzającego.

8. Wszelka liczba idealna niejednorodna rozkłada się na iloczyn liczb jednorodnych i tylko jednym sposobem.

W saméj rzeczy mamy

$$\begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix} = \begin{vmatrix} \alpha & p \\ 1 & q \\ 1 & r \end{vmatrix} . \begin{vmatrix} 1 & p \\ \beta & q \\ 1 & r \end{vmatrix} . \begin{vmatrix} 1 & p \\ 1 & q \\ \gamma & r \end{vmatrix} = (\alpha, p)\ (\beta, q)\ (\gamma, r).$$

9. Jeżeli $A, B, \ldots$ oznaczają pewne liczby idealne, to równanie $AB = AC$ można skrócić i napisać $B = C$, albo naodwrót.

Twierdzenie to wynika ze znanéj własności równoważności według danego modułu (9).

10. Norma liczby idealnéj równa się iloczynowi jéj modułów, podniesionych do potęgi równéj rzędowi odpowiedniego elementu w pierwszéj kolumnie.

Kładąc naprzykład,

$$x = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix},$$

i nazywając przez a rzęd liczby α według mod. p, a przez b rzęd liczby β według mod. q, będziemy mieli

$$\pm N(x) = p^a q^b.$$

W przypadku, gdy x jest liczbą istniejącą, jestto własność znana z określenia; w przeciwnym zaś razie umawiamy się, aby za normę liczby x uważać iloczyn takimże samym sposobem utworzony.

11. Norma iloczynu dwóch lub więcéj liczb równa się iloczynowi ich norm.

$$N(AB) = N(A)\,N(B).$$

12. Niech będą dwie liczby idealne

$$A = \begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix}, \qquad B = \begin{vmatrix} \alpha' & p \\ \beta' & q \\ \gamma' & r \end{vmatrix},$$

Aby liczba A dzieliła się przez liczbę B, niezbędnem jest i dostatecznem, by liczba α dzieliła się według mod. p przez liczbę α', liczba β dzieliła się według mod. q przez liczbę β', it. d.

Aby tego dowieść, trzeba naprzód wyjaśnić, co należy rozumieć pod wyrażeniem: „liczba idealna A dzieli się przez liczbę B“.

Umawiamy się, aby wogóle, podobnie jak to bywa z liczbami istniejącemi, przez wyrażenia: „liczba A dzieli się przez B“, rozumieć to, że można znaleść taką idealną liczbę C, która będąc pomnożoną przez liczbę B, daje wynik równy liczbie A. Liczbę C nazywać będziemy stosunkiem $A:B$; oczywiście, dwóch wartości różnych liczba C mieć nie może, jeśli nie zwracamy uwagi na czynnik równy jedności. Niech szukana liczba C wyraża się tak:

$$C=\begin{vmatrix}\lambda & p\\ \mu & q\\ \nu & r\end{vmatrix},$$

z równania $A = BC$ otrzymujemy

$$\alpha \equiv \alpha'\lambda \pmod{p},$$
$$\beta \equiv \beta'\mu \pmod{q},$$
$$\gamma \equiv \gamma'\nu \pmod{r},$$

a to dowodzi prawdziwości twierdzenia.

13. Jeżeli dwie liczby idealne dzielą wzajemnie, jedna drugą, to są równemi sobie.

14. Jeżeli liczba idealna A dzieli się przez liczbę B, to i AC dzieli się przez B.

15. Jeżeli każda z liczb istniejących α, β, γ dzieli się przez liczbę idealną A, to i suma $\alpha+\beta+\gamma$ dzieli się przez A.

16. Jeżeli liczba idealna A dzieli się przez liczbę B, a B dzieli się przez C, to A dzieli się przez C.

17. Jeżeli liczby A i B dzielą się odpowiednio przez liczby A' i B' to AB dzieli się przez $A'B'$.

18. Norma liczby idealnéj dzieli się przez samą liczbę.

19. Liczba dzielników liczby idealnéj jest skończoną i można znaleść wszystkie dzielniki za pomocą skończonéj liczby działań.

Niech liczba idealna będzie

$$A=\begin{vmatrix}\alpha & p\\ \beta & q\end{vmatrix};$$

wszystkie jéj dzielniki otrzymują się ze wzoru

$$\delta=\begin{vmatrix}\delta_1 & p\\ \delta_2 & q\end{vmatrix},$$

gdzie δ_1 oznacza jeden z dzielników liczby α według mod. p, δ_2 — jeden z dzielników liczby β, według mod. q.

20. Dwie liczby idealne

$$A=\begin{vmatrix}\alpha & p\\ \beta & q\\ \gamma & r\end{vmatrix}, \qquad B=\begin{vmatrix}\alpha' & p\\ \beta' & q\\ \gamma' & r\end{vmatrix}$$

tylko wtedy są pierwszemi względem siebie, jeżeli liczby α i α' są pierwszemi względem siebie według mod. p, liczby β i β' są pierwszemi względem siebie według mod. q, it. d.

W przypadku, gdy liczby A i B są istniejące, twierdzenie jest oczywiste na mocy twierdzenia 2-go w poprzednim rozdziale; jeżeli zaś przynajmniéj jedna z liczb A i B jest nieistniejącą, w takim razie umawiamy się, aby liczby A i B nazywać pierwszemi względem siebie tylko wtedy, kiedy wszystkie warunki podane w twierdzeniu będą spełnione.

Uwaga. Twierdzenie rozciąga się na jakąkolwiek liczbę liczb idealnych.

21. Jeżeli dwie liczby idealne A i B są pierwszemi względem siebie, to zawsze można znaleść dwie liczby istniejące λ i μ, z których pierwsza dzielić się będzie przez A, a druga — przez B, i których suma równać się będzie 1,

$$\lambda+\mu=1.$$

W saméj rzeczy, niech

$$A=\begin{vmatrix}\alpha & p\\ \beta & q\end{vmatrix}, \qquad B=\begin{vmatrix}\alpha' & p\\ \beta' & q\end{vmatrix}.$$

Na mocy założenia mamy

$$\alpha\,\omega + \alpha'\,\omega' + p\,\omega'' = 1\,,$$
$$\beta\,\omega_1 + \beta'\,\omega'_1 + q\,\omega''_1 = 1\,.$$

Równania te łatwo przywieść do postaci

$$x\,\alpha + y\,\alpha' + z\,p^l = 1\,,$$
$$x'\,\beta + y'\,\beta' + z'\,q^m = 1\,,$$

gdzie $x, x', \ldots, z'$ są liczby całkowite, a l i m dowolne liczby całkowite, zwyczajne, obie dodatnie; przypuśćmy, że liczba l jest tak dobraną, że p^l dzieli się według mod. p i przez α, i przez α', liczba m zaś tak, że q^m dzieli się według mod. q przez β i przez β'.

Pomnóżmy następnie obie strony pierwszego równania przez $u\,q^m$, a drugiego przez vp^l i dobierzmy u i v tak, aby zachodziło równanie

$$uq^m + vp^l = 1\,.$$

Dodając odpowiednio obie strony, znajdujemy

$$x\,u\,q^m\,\alpha + x'\,v\,p^l\,\beta + \ldots + (z\,u + z'\,v)\,p^l\,q^m = 1\,.$$

Łatwo przekonać się, że każdy wyraz strony lewéj dzieli się przynajmniej przez jednę z liczb A lub B; oznaczywszy więc przez λ sumę wyrazów dzielących się przez A, a przez μ sumę wyrazów, dzielących się przez B, mamy

$$\lambda + \mu = 1\,,$$

co było do okazania.

Uwaga. Przytoczony dowód stosuje się oczywiście i do jakiéjkolwiek liczby liczb idealnych, pierwszych względem siebie.

Liczba wierszy w danych liczbach także nie ma żadnego wpływu na dowód.

22. Jeżeli istnieją dwie liczby całkowite λ i μ, z których pierwsza dzieli się przez liczbę idealną A, a druga przez B, a których suma $\lambda + \mu$ równa się 1, to liczby A i B są pierwszemi względem siebie.

Jeżeli obydwie liczby A i B są istniejące, twierdzenie jest widocznem.

Niechaj

$$A = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix}, \qquad B = \begin{vmatrix} \alpha' & p \\ \beta' & q \end{vmatrix}.$$

Oznaczywszy przez h_1, h_2 pewne liczby zwyczajne, nie dzielące się przez p, a przez k_1, k_2 pewne liczby zwyczajne, nie dzielące się przez q, według założenia mamy

$$\frac{h_1\,\lambda}{\alpha} = \alpha_1\,, \qquad \frac{k_1\,\lambda}{\beta} = \beta_1\,,$$
$$\frac{h_2\,\mu}{\alpha'} = \alpha'_1\,, \qquad \frac{k_2\,\mu}{\beta'} = \beta'_1\,,$$

do tych równań dołączamy

$$\lambda + \mu = 1\,,$$

i wyprowadzamy stąd

$$h_2\,\alpha_1\,\alpha + h_1\,\alpha'_1\,\alpha' = h_1\,h_2\,,$$
$$k_2\,\beta_1\,\beta + k_1\,\beta'_1\,\beta' = k_1\,k_2\,.$$

Równania te wskazują, że A i B są liczbami pierwszemi względem siebie.

Uwaga. Twierdzenie pozostaje w mocy i dla jakiejkolwiek liczby liczb $A, B, \ldots$; dowód bez zmiany.

23. Jeżeli każda z liczb idealnych $A, A', \ldots$ jest pierwszą względem każdéj z liczb $B, B', \ldots$, to i iloczyn $AA'\ldots$ jest pierwszy względem iloczynu $BB'\ldots$

24. Jeżeli dwie liczby idealne B i C są pierwszemi względem siebie i jeżeli liczba A dzieli się przez każdą z nich, to dzieli się też i przez iloczyn BC.

25. Jeżeli A i C są pierwszemi względem siebie, i iloczyn AB dzieli się przez liczbę C, to liczba B dzieli się przez liczbę C.

26. Dla każdych dwóch liczb idealnych istnieje największy wspólny dzielnik, który zawsze może być znalezionym za pomocą skończonéj liczby działań.

W saméj rzeczy, niech będą dwie liczby

$$A = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix} \qquad B = \begin{vmatrix} \alpha' & p \\ \beta' & q \end{vmatrix};$$

oznaczywszy przez d_1 największy wspólny dzielnik według mod. p liczb α i α', a przez d_2 największy wspólny dzielnik według mod. q liczb β i β', widzimy, że wszelki wspólny dzielnik liczb A i B jest dzielnikiem liczby

$$D = \begin{vmatrix} d_1 & p \\ d_2 & q \end{vmatrix},$$

i odwrotnie; ta liczba nazywa się dla tego największym wspólnym dzielnikiem liczb A i B (23).

Podobnym sposobem znajduje się największy wspólny dzielnik dla kilku liczb.

27. Jeżeli dwie liczby idealne są pierwszemi względem siebie, to ich największy wspólny dzielnik równa się 1, i odwrotnie.

Toż samo ma miejsce i dla kilku liczb pierwszych względem siebie.

28. Niech będą dane liczby idealne $A, B, \ldots$ i niech D przedstawia ich największy wspólny dzielnik.

Wszelka liczba γ istniejąca, która się dzieli przez D, może być przedstawioną pod postacią sumy kilku liczb, z których pierwsza dzieli się przez A, druga przez B i t. d.

W saméj rzeczy, czyniąc

$$A = D\,A', \quad B = D\,B', \ldots$$

łatwo zauważyć, że liczby idealne $A', B' \ldots$ są pierwszemi względem siebie, gdyż oznaczywszy przez D' ich największy wspólny dzielnik, będziemy mieli

$$A = D\,D'\,A'', \quad B = D\,D'\,B'', \ldots,$$

skąd wnosimy, że $D\,D'$ jest wspólnym dzielnikiem liczb $A, B, \ldots$; D więc dzieli się przez DD'; 1 zatem dzieli się przez D', skąd wynika, że $D' = 1$.

Skoro więc liczby idealne $A', B', \ldots$ są pierwszemi względem siebie, można znaleść takie liczby $\alpha', \beta', \ldots$, które się będą dzieliły odpowiednio przez $A', B', \ldots$, i których suma będzie się równała 1,

$$\alpha' + \beta' + \ldots = 1.$$

Pomnożywszy obie strony przez γ, otrzymujemy

$$\gamma = \alpha'\,\gamma + \beta'\,\gamma + \ldots$$

Pierwszy wyraz po stronie prawéj dzieli się przez A, gdyż α' dzieli się przez A', a γ dzieli się przez D; podobnież drugi wyraz dzieli się przez B, i t. d.; twierdzenie więc jest dowiedzionem.

29. Liczba jednorodna (α, p), w któréj pierwszy element α jest liczbą pierwszą według mod. p, jest liczbą idealną pierwszą; liczby nie czyniące zadość temu warunkowi nie są pierwszemi.

Twierdzenie to jest oczywistem w przypadku, jeśli (α, p) jest liczbą istniejącą; wtedy (α, p) jest właśnie główną przedstawicielką klasy pierwszéj, do któréj należy liczba α; innych liczb pierwszych istniejących, jak to wiadomo z poprzedniego rozdziału, nie ma.

Teraz zgodzimy się wogóle nazywać liczbami idealnemi pierwszemi te tylko liczby, które czynią zadość warunkom podanym w twierdzeniu.

30. Jeżeli liczba (α, p) jest pierwszą, to wszelka inna liczba idealna A albo dzieli się przez (α, p), albo téż jest pierwszą względem (α, p).

W saméj rzeczy, niech

$$A = \begin{vmatrix} \lambda & p \\ \mu & q \\ \nu & r \end{vmatrix};$$

mamy

$$(\alpha, p) = \begin{vmatrix} \alpha & p \\ 1 & q \\ 1 & r \end{vmatrix}.$$

Widzimy stąd, że jeżeli λ dzieli się przez α według mod. p, to A dzieli się przez (α, p); jeśli zaś λ nie dzieli się przez α według mod. p, to λ i α są liczbami pierwszemi względem siebie i oczywiście A i (α, p) są także pierwszemi względem siebie.

31. Jeżeli liczba idealna A nie jest pierwszą, to można znaleść taką liczbę istniejącą ω, która nie będzie się dzieliła przez A i nie będzie pierwszą względem liczby A.

Przypuśćmy naprzód, że liczba A jest jednorodną:

$$A = (\alpha, p);$$

α więc nie jest liczbą pierwszą według mod. p i posiada dzielnik δ, według mod. p. Liczba δ nie dzieli się przez A i nie jest pierwszą względem A.

Przejdźmy do przypadku, kiedy A nie jest liczbą jednorodną, naprzykład,

$$A = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix};$$

tu należy domyślać się, że $N(\alpha)$ dzieli się przez p, a $N(\beta)$ dzieli się przez q. Liczba q, oczywiście, nie dzieli się przez A i nie jest liczbą pierwszą względem A.

32. Liczba idealna pierwsza nie ma żadnych dzielników, oprócz saméj siebie i jedności, i odwrotnie, jeżeli liczba idealna nie posiada żadnego dzielnika, to jest liczbą pierwszą.

33. Dwie liczby idealne pierwsze i różne są pierwszemi względem siebie.

34. Aby iloczyn kilku liczb idealnych dzielił się przez liczbę pierwszą idealną P, potrzeba i wystarcza, by przynajmniéj jeden z czynników dzielił się przez liczbę P.

35. Wszelka liczba idealna rozkłada się, i tylko jednym sposobem, na iloczyn z czynników idealnych pierwszych.

Cała trudność podobnego rozkładu sprowadza się do rozkładu liczby jednorodnéj na iloczyn czynników pierwszych. Aby rozłożyć podobną liczbę, naprzykład (α, p), należy rozłożyć liczbę α, według modułu p, na iloczyn z czynników pierwszych według mod. p,

$$\alpha \equiv \pi_1^{m_1} \pi_2^{m_2} \ldots \pi_i^{m_i}, \quad (\text{mod. } p);$$

dokonawszy tego, mamy

$$(\alpha, p) = (\pi_1, p)^{m_1} \ldots (\pi_i, p)^{m_i}.$$

36. Mając liczbę idealną rozłożoną na czynniki idealne pierwsze, można wypisać wszystkie jéj dzielniki.

Każdy dzielnik będzie iloczynem kilku czynników pierwszych liczby danéj, każdy zaś z czynników będzie miał wykładnik nie wyższy od tego, z jakim wchodzi w skład liczby danéj.

37. Mając kilka liczb idealnych rozłożonych na czynniki pierwsze, otrzymujemy bezpośrednio ich największy wspólny dzielnik i najmniejszą wspólną wielokrotność pod postacią iloczynu z czynników pierwszych, postępując podług prawa, znanego w swem zastosowaniu do liczb zwyczajnych.

Określenie najmniejszéj wielokrotności jest takież, jak i dla liczb zwyczajnych.

VIII. O ideałach.

25. Dedekind, autor teoryi ideałów, daje następujące określenie:

Ideałem jest pewien dany zbiór, złożony z nieskończonego mnóstwa liczb całkowitych, mający dwie własności:

1. Suma lub różnica dwóch liczb w zbiorze należy do tegoż zbioru.
2. Pomnożywszy jakąkolwiek liczbę w zbiorze przez dowolną liczbę całkowitą, należącą do zbioru lub nie należącą, — otrzymujemy zawsze w iloczynie liczbę, należącą do zbioru danego.

W rozdziale tym zajmiemy się teoryą ideałów z nowego punktu widzenia: postaramy się wykazać, że teorya ta sprowadza się bezpośrednio do teoryi liczb idealnych, wyłożonéj w rozdziale poprzedzającym.

Przedewszystkiem należy poznać, jakiéj postaci będzie wzór, z którego można otrzymywać wszystkie liczby, należące do danego ideału.

Jeżeli dany ideał zawiera jedność, zwyczajną lub algebraiczną, wtedy zlewa się z danym obszarem liczb, to jest, zawiera w sobie wszystkie liczby całkowite danego obszaru. Taki ideał, między innemi, jest pod wieloma względami tem samem, czem 1 między innemi liczbami; dla tego Dedekind nazywa go ideałem „jedność“. Wszystkie liczby w nim zawarte otrzymujemy ze znanego wzoru

$$x_1 \omega_1 + x_2 \omega_2 + \ldots + x_n \omega_n, \tag{1}$$

nadając współczynnikom $x_1, x_2, \ldots$ wartości całkowite zwyczajne.

Przejdźmy do innych ideałów. Niech $a > 0$ oznacza jednę z liczb zwyczajnych całkowitych zawartych w danym ideale J,—na mocy określenia łatwo spostrzedz, że taka liczba zawsze się znajdzie, — i niech $\alpha_1, \alpha_2, \ldots \alpha_m$ oznaczają liczby, otrzymane ze wzoru (1) przy wartościach na $x_1, x_2, \ldots$, sprawdzających nierówność

$$0 \leqq x_i < a,$$

a należące do ideału J.

Wszelka liczba, należąca do ideału J, może być oczywiście otrzymana ze wzoru

$$a\,\Omega + \alpha_1 \Omega_1 + \alpha_2 \Omega_2 + \ldots + \alpha_m \Omega_m, \tag{2}$$

gdzie $\Omega, \Omega_1, \ldots$ oznaczają liczby całkowite dowolne; tylko liczby ideału J mogą stąd być otrzymane.

Na mocy wzoru (2) przychodzimy do nowego określenia, mianowicie:

Ideałem jest zbiór wszystkich liczb, otrzymanych ze wzoru:

$$\alpha_0\,\Omega_0 + \alpha_1\,\Omega_1 + \ldots + \alpha_{m-1}\,\Omega_{m-1}, \tag{3}$$

w którym $\alpha_0, \alpha_1, \ldots$ są dane liczby całkowite, a $\Omega_0, \Omega_1, \ldots$ oznaczają dowolne liczby całkowite.

Niedogodność wzoru (3) polega na tem, że powtarza on jednę i tęż samę liczbę nieskończenie wiele razy; a lubo można znaleść zawsze wzór postaci (1), który przy wszelkich wartościach całkowitych zwyczajnych $x_1, x_2, \ldots$ dawać będzie wszystkie liczby ideału (3), każdą raz jeden, wystarczy jednak dla naszego celu zadowolnić się wzorem (3).

Jeżeli dwa ideały J_1 i J_2 są takie, że każda liczba, zawarta w jednym z nich zawiera się i w drugim, to uważamy je za równe, i piszemy

$$J_1 = J_2.$$

26. Niech będzie daną liczba idealna δ; zbiór wszystkich liczb całkowitych istniejących, dzielących się przez δ, tworzy ideał, gdyż oczywiście posiada obydwie własności do tego potrzebne. Takim sposobem otrzymany ideał uważać będziemy, jako swojego rodzaju funkcyą liczby δ i przedstawiać za pomocą znaku $J(\delta)$.

Twierdzenie. Dla każdego ideału J można znaleść jednę i tylko jednę odpowiednią liczbę idealną δ, taką, że $J = J(\delta)$.

Dajmy, że ideał J określa się wzorem

$$\alpha_1\,\Omega_1 + \alpha_2\,\Omega_2 + \ldots + \alpha_m\,\Omega_m; \tag{4}$$

uważając liczby $\alpha_1, \alpha_2, \ldots, \alpha_m$ jako idealne, znajdźmy ich największy wspólny dzielnik δ. Wszelka liczba, którą daje wzór (4), dzieli się oczywiście przez δ; odwrotnie, wszelka liczba, dzieląca się przez δ, może być na zasadzie twierdzenia 28-go poprzedniego rozdziału przedstawioną pod postacią (4), jest więc $J = J(\delta)$.

Pozostaje dowieść, że nie może istnieć liczba δ', różna od δ, dla któréj miałoby miejsce równanie $J(\delta') = J(\delta)$.

W saméj rzeczy, niech

$$\delta' = \begin{vmatrix} \alpha' & p \\ \beta' & q \end{vmatrix}, \qquad \delta = \begin{vmatrix} \alpha & p \\ \beta & q \end{vmatrix};$$

Ponieważ wszystkie liczby $\alpha_1, \ldots, \alpha_m$ w (4) dzielą się przez δ', więc i ich największy wspólny dzielnik δ dzieli się przez δ'. Gdyby liczba δ' dzieliła się przez δ, mielibyśmy wtedy $\delta = \delta'$; dajmy, że δ' nie dzieli się przez δ,

i niech, naprzykład, α' nie dzieli się według mod. p przez α. Oznaczywszy przez b' rzęd liczby β' według mod q, mamy liczbę

$$\alpha'\,q^{b'},$$

która widocznie dzieli się przez δ' i nie dzieli się przez δ; ta liczba zawiera się w $J(\delta')$, lecz nie zawiera się w $J(\delta)$; więc równanie $J(\delta') = J(\delta)$ jest niemożebnem, c. b. d. o.

27. Dedekind nazywa iloczynem dwóch ideałów J_1 i J_2 taki ideał trzeci J_3, którego każda liczba daje się wyrazić pod postacią sumy iloczynów z liczby pierwszego ideału przez liczbę drugiego ideału. Wtedy piszemy

$$J_3 = J_1\,J_2 = J_2\,J_1.$$

Jeżeli ideały J_1 i J_2 określają się wzorami

$$J_1 = \alpha_1\,\Omega_1 + \alpha_2\,\Omega_2 + \ldots + \alpha_{m_1}\,\Omega_{m_1}, \tag{5}$$

$$J_2 = \beta_1\,\Omega_1 + \beta_2\,\Omega + \ldots + \beta_{m_2}\,\Omega_{m_2}, \tag{6}$$

to iloczyn ich przedstawia

$$J_1\,J_2 = \alpha_1\,\beta_1\,\Omega_1 + \alpha_1\,\beta_2\,\Omega_2 + \ldots + \alpha_{m_1}\,\beta_{m_2}\,\Omega_{m_1 m_2}. \tag{7}$$

Można w miejsce (5) i (6) wziąć inne wzory, wyrażające téż same ideały, wtedy i wzór (7) przyjmie inną postać, lecz wyrażać będzie zawsze jeden i ten sam ideał J_3.

Mnożenie można widocznie rozciągnąć na jakąkolwiek liczbę ideałów; porządek mnożników wolno zmieniać dowolnie.

Twierdzenie. Niech α i β oznaczają dwie jakiekolwiek liczby idealne. Iloczyn dwóch ideałów $J(\alpha)$ i $J(\beta)$ równa się ideałowi odpowiedniego iloczynu, to jest,

$$J(\alpha)\,J(\beta) = J(\alpha\,\beta).$$

W saméj rzeczy, dajmy, że ideały $J(\alpha)$ i $J(\beta)$ są określone wzorami

$$\left.\begin{aligned} J(\alpha) &= \alpha_1\,\Omega_1 + \ldots + \alpha_{m_1}\,\Omega_{m_1}, \\ J(\beta) &= \beta_1\,\Omega_1 + \ldots + \beta_{m_2}\,\Omega_{m_2}; \end{aligned}\right\}$$

mamy

$$J(\alpha)\,J(\beta) = \alpha_1\,\beta_1\,\Omega_1 + \ldots + \alpha_{m_1}\,\beta_{m_2}\,\Omega_{m_1 m_2}. \tag{8}$$

Największym wspólnym dzielnikiem liczb

$$\alpha_1, \alpha_2, \ldots, \alpha_{m_1}$$

jest α, a największym wspólnym dzielnikiem liczb

$$\beta_1, \beta_2, \ldots, \beta_{m_2}$$

jest β; stąd bezpośrednio wypada, że największy wspólny dzielnik liczb

$$\alpha_1\beta_1, \quad \alpha_1\beta_2, \ldots\ldots, \alpha_{m_1}\beta_{m_2}$$

równa się iloczynowi $\alpha\beta$; więc ideał (8) równa się $J(\alpha\beta)$, to jest, mamy

$$J(\alpha)\,J(\beta) = J(\alpha\beta). \qquad \text{C. b. d. o.}$$

28. Twierdzenie to daje nam możność sprowadzenia teoryi ideałów do teoryi liczb idealnych, wyłożonéj w rozdziale poprzedzającym; w dalsze więc szczegóły wdawać się tu nie będziemy; aby jednak bardziej zbliżyć się do teoryi Dedekinda postaramy się tu dać dowód jednego twierdzenia, które w jego teoryi przedstawia największą trudność i które samo przez się jest wielkiéj wagi.

Przedewszystkiem zauważymy, że jeśli liczba idealna α jest istniejącą, w takim razie ideał $J(\alpha)$ nazywa się g ł ó w n y m.

Wszystkie liczby takiego ideału otrzymują się ze wzoru

$$J(\alpha) = \alpha\,(x_1\,\omega_1 + x_2\,\omega_2 + \ldots + x_n\,\omega_n),$$

gdzie $\omega_1, \omega_2, \ldots, \omega_n$ przedstawia grupę zasadniczą danego obszaru, a $x_1, x_2, \ldots, x_n$ są dowolne liczby całkowite zwyczajne.

Twierdzenie. D l a k a ż d e g o i d e a ł u $J(\beta)$ m o ż n a z n a l e ś ć i n n y i d e a ł $J(\gamma)$ t a k i, ż e i l o c z y n $J(\beta)\,J(\gamma)$ b ę d z i e i d e a ł e m g ł ó w n y m.

Aby dowieść tego, dość jest pokazać, że dla jakiéjkolwiek liczby idealnéj β można znaleść taki mnożnik γ, iż iloczyn $\beta\gamma = \alpha$ będzie liczbą istniejącą. Jestto widoczna, bo wszelka liczba zawarta w ideale $J(\beta)$ może być wziętą za liczbę α.

Jeżeli dwie liczby idealne α i β są takie, że wszelka liczba istniejąca, która się dzieli przez α, dzieli się także i przez β, to α dzieli się z pewnością przez β.

W saméj rzeczy, niech

$$J(\alpha) = \alpha_1\,\Omega_1 + \ldots + \alpha_m\,\Omega_m.$$

Z założenia wypada, że wszystkie liczby $\alpha_1, \ldots, \alpha_m$ dzielą się przez β, więc i największy wspólny dzielnik liczb $\alpha_1, \ldots, \alpha_m$, to jest α dzieli się przez β.

Na mocy powyższéj uwagi łatwo przekonać się o prawdziwości następującego twierdzenia Dedekinda:

J e ż e l i w s z e l k a l i c z b a, n a l e ż ą c a d o i d e a ł u J, z a w i e r a s i ę w i d e a l e J_2, t o w t e d y m o ż n a z n a l e ś ć t a k i t r z e c i i d e a ł J_3, ż e m i e ć b ę d z i e m y

$$J_1 = J_2\,J_3.$$

IX. O kongruencyach, w których moduł jest liczbą idealną.

29. Jeżeli różnica dwóch liczb $\alpha - \beta$ dzieli się przez liczbę idealną A, to mówić będziemy, że liczby α i β są kongruentne według modułu A i będziemy pisali

$$\alpha \equiv \beta \pmod{A}.$$

Dwie liczby, z których każda jest kongruentna z trzecią według mod. A, widocznie są kongruentne względem siebie według tegoż modułu A. Ta własność pozwala nam rozdzielić wszystkie liczby w danym obszarze na klasy nowe, zupełnie różne od tych, o których była mowa w rozdziale drugim. Teraz do jednéj klasy zaliczać będziemy wszystkie liczby kongruentne według mod. A. Jedna jakakolwiek z liczb, należących do danéj klasy, naprzykład liczba ω, określa wszystkie inne liczby z téj saméj klasy za pomocą wzoru

$$\omega + J(A),$$

i dla tego ω może być wziętą za przedstawicielkę całéj klasy.

Liczby niekongruentne ze sobą według mod. A są przedstawicielkami klas różnych; ile jest klas, tyle jest liczb niekongruentnych według mod. A.

Liczby, należące do jednéj klasy, posiadają tę szczególną własność, że mają z modułem A jeden i ten sam największy wspólny dzielnik.

Wszystkie własności kongruencyi zwyczajnéj, znane z teoryi liczb zwyczajnych, mają miejsce i w obecnym przypadku, kiedy modułem jest liczba idealna. Nie będziemy się przeto nad przedmiotem tym zastanawiali, zwłaszcza, że i sposoby dowodzenia pozostają te same, a przejdziemy do rozwiązania zadania o liczbie różnych klas, tych, o których tylko co była mowa.

30. Naprzód zajmiemy się tym przypadkiem, kiedy moduł A jest liczbą istniejącą.

Weźmy pod uwagę grupę zasadniczą

$$\omega_1, \ \omega_2, \ \ldots, \ \omega_n \tag{1}$$

i wyraźmy przez nią n iloczynów $A\omega_1, A\omega_2, \ldots, A\omega_n$; otrzymamy n równań

$$\left.\begin{aligned} A\omega_1 &= a_{1,1}\,\omega_1 + \ldots + a_{1,n}\,\omega_n, \\ A\omega_2 &= a_{2,1}\,\omega_1 + \ldots + a_{2,n}\,\omega_n, \\ &\ldots\ldots\ldots\ldots \\ A\omega_n &= a_{n,1}\,\omega_1 + \ldots + a_{n,n}\,\omega_n, \end{aligned}\right\} \tag{2}$$

Z uwagi, że wybór liczb (1) jest do pewnego stopnia dowolnym, i grupę (1) można zastąpić inną, byleby wyznacznik układu równań liniowych, wyrażających nowe liczby, był równy ± 1; dobieramy grupę (1) w ten sposób, iż wszystkie współczynniki

$$\begin{array}{l} a_{2,1} \\ a_{3,1}\ \ a_{3,2} \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ a_{n,1}\ \ a_{n,2}\ \ldots\ldots\ a_{n,n-1}, \end{array}$$

leżące pod przekątną, będą równe zeru.

Będziemy tedy zamiast (2) mieli

$$\left.\begin{aligned} A\omega_1 &= a_1\,\omega_1 + a_2\,\omega_2 + \ldots + a_n\,\omega_n, \\ A\omega_2 &= \quad\ b_2\,\omega_2 + \ldots + b_n\,\omega_n, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots\ldots \\ A\omega_n &= \quad\ k_n\,\omega_n. \end{aligned}\right\} \tag{3}$$

Rugując z tych równań ilości $\omega_1, \omega_2, \ldots, \omega_n$, otrzymujemy równanie n-go stopnia, któremu czyni zadość liczba A, skąd znajdujemy

$$N(A) = a_1 b_2 \ldots k_n\,\omega'_1.$$

Weźmy teraz jakąkolwiek liczbę całkowitą ω,

$$\omega = x_1\,\omega_1 + x_2\,\omega_2 + \ldots + x_n\,\omega_n,$$

i odejmijmy od niéj dowolną wielokrotność liczby $A\omega'_1$,

$$\omega - l_1 A\omega'_1 = (x_1 - l_1 a_1)\,\omega_1 + (x_2 - l_1 a_2)\,\omega_2 + \ldots + (x_n - l_1 a_n)\,\omega_n.$$

Dajmy liczbie l_1 taką wartość, aby różnica $x_1 - l_1 a_1$ zawartą była między -1 i wartością liczebną a_1, oznaczmy dla skrócenia współczynniki z prawéj strony przez $y_1, x'_2, \ldots, x'_n$; to

$$\omega - l_1 A\omega'_1 = y_1\,\omega_1 + x'_2\,\omega_2 + \ldots + x'_n\,\omega_n. \tag{4}$$

Odejmijmy od obu stron (4) dowolną wielokrotność liczby $A\omega'_2$,

$$\omega - l_1 A\omega'_1 - l_2 A\omega'_2 = y_1\,\omega_1 + (x'_2 - l_2 b_2)\,\omega_2 + \ldots$$
$$\ldots + (x'_n - l_2 b_n)\,\omega_n,$$

i dobierzmy dla l_2 taką wartość, aby różnica $x'_2 - l_2 b_2$ zawierała się między -1 i wartością liczebną b_2, nadto oznaczmy dla skrócenia współczynniki $(x'_2 - l_2 b_2), \ldots, (x'_n - l_2 b_n)$ przez $y_2, x''_3, \ldots, x''_n$; to

$$\omega - l_1 A\omega'_1 - l_2 A\omega'_2 = y_1\,\omega_1 + y_2\,\omega_2 + x''_3\,\omega_3 + \ldots + x''_n\,\omega_n.$$

Odejmując następnie od obu stron pewną wielokrotność liczby $A\omega_3$ i rozumując podobnież jak przedtem, dojdziemy ostatecznie do równania

$$\omega - A(l_1\,\omega'_1 + \ldots + l_n\,\omega'_n) = y_1\,\omega_1 + \ldots + y_n\,\omega_n, \tag{5}$$

w którem współczynniki $y_1, y_2, \ldots, y_n$ będą się zawierały między granicami

$$0 \leqq y_1 < (a_1), \quad 0 \leqq y_2 < (b_2), \ \ldots\ldots, \ 0 \leqq y_n < (k_n);$$

$(a_1), (b_2), \ldots$ przedstawiają wartości liczebne ilości $a_1, b_2, \ldots$

Równanie (5) można przedstawić tak:

$$\omega \equiv y_1\,\omega_1 + \ldots + y_n\,\omega_n \pmod{A},$$

skąd wnosimy, że liczba wszystkich liczb niekongruentnych według mod. A jest równą liczbie liczb postaci

$$y_1\,\omega_1 + \ldots + y_n\,\omega_n\,, \tag{6}$$

niekongruentnych według mod. A.

Lecz łatwo dowieść, że wszystkie liczby (6) są niekongruentne według mod. A.

W saméj rzeczy, różnica dwóch takich liczb ma postać

$$z_1\,\omega_1 + \ldots + z_n\,\omega_n\,, \tag{7}$$

$$(z_1) < (a_1)\,,\quad (z_2) < (b_2)\,,\ \ldots\ldots\,,\ (z_n) < (k_n)\,.$$

Na mocy (3), wszelka liczba, dzieląca się przez A, otrzymuje się ze wzoru

$$x_1\,(a_1\,\omega_1 + \ldots + a_n\,\omega_n) + x_2\,(b_2\,\omega_2 + \ldots + b_n\,\omega_n) + \ldots + x_n\,k_n\,\omega_n\,; \tag{8}$$

gdzie $x_1, \ldots, x_n$ oznaczają liczby całkowite zwyczajne.

Widoczną jest rzeczą, że liczba (7), przy dołączonych warunkach co do $z_1, \ldots, z_n$, nie może być wyrażoną pod postacią (8).

Wszystkie więc liczby (6) są niekongruentne między sobą; a ponieważ ich liczba jest

$$\pm\, a_1\,b_2 \ldots k_n = \pm\, N\,(A)\,,$$

przeto liczba wszystkich liczb niekongruentnych według mod. A równa się liczebnéj wartości $N\,(A)$.

31. Przejdźmy teraz do drugiego przypadku, kiedy A jest liczbą nieistniejącą, i ograniczmy się na przypuszczeniu, że A jest liczbą jednorodną,

$$A = (\alpha,\ p)\,.$$

Postarajmy się przedewszystkiem znaleść wzór dla ideału $J\,(A)$.

Niech ω przedstawia jakąkolwiek liczbę, dzielącą się przez A; to znaczy, że ω dzieli się według mod. p przez α, czyli, że stosunek

$$\frac{h\,\omega}{\alpha} = \omega'\,, \qquad (N\,(\alpha) = p^a\,h)\,,$$

jest liczbą całkowitą.

Oznaczywszy przez x i y dwie liczby całkowite zwyczajne, czyniące zadość równaniu

$$h\,x - p^a\,y = 1\,,$$

z dwóch ostatnich równań znajdujemy

$$\omega = \alpha\,\Omega + p^a\,\Omega'\,, \tag{1}$$

gdzie Ω i Ω' oznaczają pewne liczby całkowite.

Odwrotnie, jeżeli liczbom Ω i Ω' nadawać będziemy dowolne wartości całkowite, to wzór (1) da nam liczbę, dzielącą się przez A, gdyż obie liczby α i p^a dzielą się według mod. p przez α.

Wzór więc (1) określa nam ideał $J\,(A)$, i możemy napisać

$$J\,(A) = \alpha\,\Omega + p^a\,\Omega'\,. \tag{2}$$

Wróćmy teraz do głównego zadania naszego.

Oznaczając, jak w numerze poprzednim, przez $\omega_1, \omega_2, \ldots, \omega_n$ i $\omega'_1, \omega'_2 \ldots, \omega'_n$ dwie grupy zasadnicze, z których ostatnia jest dobraną pewnym szczególnym sposobem, możemy założyć

$$\left.\begin{aligned} \alpha\,\omega'_1 &= a_1\,\omega_1 + a_2\,\omega_2 + \ldots + a_n\,\omega_n\,,\\ \alpha\,\omega'_2 &= \qquad\quad b_2\,\omega_2 + \ldots + b_n\,\omega_n\,,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ \alpha\,\omega'_n &= \qquad\qquad\qquad\quad k_n\,\omega_n\,. \end{aligned}\right\} \tag{3}$$

Znajdziemy stąd

$$N\,(\alpha) = p^a\,h = a_1\,b_2 \ldots k_n\,.$$

Uczyńmy następnie

$$a_1 = p^{m_1}\,h_1\,,\quad b_2 = p^{m_2}\,h_2\,,\ \ldots\,,\ k_n = p^{m_n}\,h_n\,,$$

gdzie $h_1, \ldots, h_n$ oznaczają liczby zwyczajne, nie dzielące się przez p; mamy

$$m_1 + m_2 + \ldots + m_n = a\,.$$

Znajdźmy teraz szereg liczb zwyczajnych $x, y, x', y', \ldots$, czyniących zadość warunkom

$$\begin{aligned} x\,a_1 + y\,p^a &= p^{m_1}\,,\\ x'\,b_2 + y'\,p^a &= p^{m_2}\,,\\ &\ldots\ldots\ldots\\ x^{(n-1)}\,k_n + y^{(n-1)}\,p^a &= p^{m_n}\,, \end{aligned}$$

i oznaczmy dla skrócenia

$$\left.\begin{aligned} x\,(\alpha\,\omega'_1) + y\,p^{\alpha}\,\omega_1 &= \alpha_1\,,\\ x'\,(\alpha\,\omega'_2) + y'\,p^{\alpha}\,\omega_2 &= \alpha_2\,,\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\\ x^{(n-1)}\,(\alpha\,\omega'_n) + y^{(n-1)}\,p^{\alpha}\,\omega_n &= \alpha_n\,; \end{aligned}\right\} \qquad (4)$$

to

$$\left.\begin{aligned} \alpha_1 &= p^{m_1}\,\omega_1 + \alpha'_2\,\omega_2 + \ldots + \alpha'_n\,\omega_n\,,\\ \alpha_2 &= \qquad p^{m_2}\,\omega_2 + \ldots + b'_n\,\omega_n\,,\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ &\\ \alpha_n &= \qquad\qquad\qquad p^{m_n}\,\omega_n\,. \end{aligned}\right\} \qquad (5)$$

Wszystkie te liczby dzielą się przez A, co widać z (4), i łatwo przekonać się, że wszystkie liczby ideału $J\,(A)$ (2) otrzymujemy z wzoru

$$x_1\,\alpha_1 + \ldots + x_n\,\alpha_n\,,$$

nadając współczynnikom $x_1, \ldots, x_n$ wartości całkowite zwyczajne.

Na mocy równań (3), rozumując tak samo, jak w poprzednim numerze, wnosimy, że liczba wszystkich liczb niekongruentnych według mod. A równa się iloczynowi

$$p^{m_1}\,p^{m_2}\ldots p^{m_n} = p^{\alpha} = \pm N\,(A)\,.$$

Otrzymaliśmy więc znowu ten sam rezultat, co i w numerze poprzednim.

32. Przejdźmy teraz do przypadku najogólniejszego; niech modułem kongruencyi będzie jakakolwiek liczba idealna

$$A = \begin{vmatrix} \alpha & p \\ \beta & q \\ \gamma & r \end{vmatrix}.$$

Weźmy pod uwagę liczby jednorodne

$$A_1 = (\alpha, p)\,,\quad A_2 = (\beta, q)\,,\quad A_3 = (\gamma, r)\,,$$

i przyjmując po kolei każdą z nich za moduł, wypiszmy odpowiednie grupy ze wszystkich liczb niekongruentnych:

$$\begin{aligned} &r_1, r_2, \ldots, r_\lambda, && \text{dla} && \text{mod. } A_1\\ &s_1, s_2, \ldots, s_\mu, && \text{„} && \text{mod. } A_2\\ &t_1, t_2, \ldots, t_\nu, && \text{„} && \text{mod. } A_3 \end{aligned}$$

Jakakolwiek liczba ω będzie miała odpowiednią sobie grupę

$$r_i,\ s_k,\ t_l, \qquad (1)$$

która się określa z warunków

$$\left.\begin{aligned} \omega &\equiv r_i \pmod{A_1}\,,\\ \omega &\equiv s_k \pmod{A_2}\,,\\ \omega &\equiv t_l \pmod{A_3}\,. \end{aligned}\right\} \qquad (2)$$

Dwom różnym liczbom ω i ω' wtedy, i tylko wtedy, odpowiadać będzie jedna i taż sama grupa (1), gdy one są kongruentne według mod. A, to jest,

$$\omega \equiv \omega' \pmod{A}\,.$$

Dowiedziemy teraz, że dla wszelkiéj kombinacyi (1) zawsze znajdzie się taka liczba ω, która będzie czyniła zadość wszystkim warunkom (2).

Weźmy w tym celu następujące liczby:

$$A_1\,A_2 = B_3\,,\quad A_2\,A_3 = B_1\,,\quad A_1\,A_3 = B_2\,,$$

które widocznie są względnie pierwsze; można więc znaleść takie liczby $\delta_1, \delta_2, \delta_3$, dzielące się odpowiednio przez B_1, B_2, B_3, które będą czyniły zadość równaniu

$$\delta_1 + \delta_2 + \delta_3 = 1\,.$$

Mamy zatem

$$\begin{aligned} &\delta_1 \equiv 1 \pmod{A_1}, && \delta_2 \equiv 0 \pmod{A_1}, && \delta_3 \equiv 0 \pmod{A_1},\\ &\delta_1 \equiv 0 \pmod{A_2}, && \delta_2 \equiv 1 \pmod{A_2}, && \delta_3 \equiv 0 \pmod{A_2},\\ &\delta_1 \equiv 0 \pmod{A_3}, && \delta_2 \equiv 0 \pmod{A_3}, && \delta_3 \equiv 1 \pmod{A_3}; \end{aligned}$$

liczba więc $\omega = r_i\,\delta_1 + s_k\,\delta_2 + t_l\,\delta_3$ czyni oczywiście zadość warunkom (2).

Z tego wszystkiego, cośmy tu dowiedli wynika, że liczba liczb niekongruentnych według mod. A, równa się liczbie grup (1), to jest iloczynowi $\lambda\,\mu\,\nu$. Lecz na mocy tego, co okazano w poprzednim numerze, mamy

$$\lambda = \pm N(A_1), \quad \mu = \pm N(A_2), \quad \nu = \pm N(A_3),$$

zatem

$$\lambda\,\mu\,\nu = \pm N(A_1)\,N(A_2)\,N(A_3),$$

albo

$$\lambda\,\mu\,\nu = \pm N(A).$$

Tym sposobem dowiedliśmy następującego twierdzenia ogólnego:

Twierdzenie. Liczba wszystkich liczb niekongruentnych według mod. A równą jest liczebnéj wartości $N(A)$.

33. Dla uniknięcia podwójnych znaków zgodzimy się tu pod $N(\omega)$ rozumieć liczebną wartość normy ω.

Oznaczmy przez d jeden którykolwiek z dzielników liczby idealnéj A i, wziąwszy pod uwagę układ pełny liczb niekongruentnych według mod. A

$$0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{i-1}, \qquad (i = N(d)), \tag{1}$$

wybierzmy z pomiędzy (1) liczby, niekongruentne względem siebie według mod. d,

$$0,\ \beta_1,\ \beta_2,\ \ldots,\ \beta_{j-1}, \qquad (j = N(d)); \tag{2}$$

otrzymamy układ pełny liczb niekongruentnych według mod. d.

Z pomiędzy (1) wybierzmy jeszcze wszystkie liczby dzielące się przez d,

$$0,\ \gamma_1,\ \gamma_2,\ \ldots,\ \gamma_{x-1};$$

x oznacza liczbę takich liczb.

Łatwo zauważyć, że każda z liczb (1) przedstawić się może jednym, i tylko jednym sposobem pod postacią

$$\alpha_m \equiv \beta_r + \gamma_s \pmod{A};$$

stąd wynika, że $N(A) = x\,N(d)$, więc

$$x = N\left(\frac{A}{d}\right).$$

Wzór ten dowodzi prawdziwości następującego twierdzenia:

Liczba liczb niekongruentnych według mod. A, i dzielących się przez liczbę d, t. j. przez dany dzielnik liczby A, równą jest $N\left(\frac{A}{d}\right)$.

Dajmy teraz, że stosunek $A:d$ jest przedstawiony pod postacią iloczynu z czynników pierwszych, tak że

$$A = d\,\pi_1^{m_1}\,\pi_2^{m_2}\,\ldots\,\pi_i^{m_i};$$

i rozważmy wszystkie liczby dzielące się przez d i niekongruentne według mod. A,

$$0,\ \gamma_1,\ \gamma_2,\ \ldots,\ \gamma_{x-1}. \tag{3}$$

Z pomiędzy (3) wybierzmy liczby nie dzielące się przez $d\,\pi_1$,

$$\gamma'_1,\ \gamma'_2,\ \ldots,\ \gamma'_{x_1}; \tag{4}$$

a z pomiędzy (4) liczby nie dzielące się przez $d\,\pi_2$,

$$\gamma''_1,\ \gamma''_2,\ \ldots,\ \gamma''_{x_2}, \tag{5}$$

i tak daléj, dopóki nie dojdziemy do grupy, która składać się będzie z takich liczb (3), które się nie dzielą przez żaden z iloczynów $d\pi_1, d\pi_2, \ldots, d\pi_i$,

$$\gamma_1^{(i)},\ \gamma_2^{(i)},\ \ldots,\ \gamma_{x_i}^{(i)}.$$

Oznaczmy przez y_1 liczbę takich liczb w (3), które się dzielą przez $d\pi_1$; przez y_2 liczbę takich liczb w (4). które się dzielą przez $d\pi_2$, i tak daléj aż nakoniec dojdziemy do liczby liczb w szeregu

$$\gamma_1^{(i-1)},\ \gamma_2^{(i-1)},\ \ldots,\ \gamma_{x_{i-1}}^{(i-1)},$$

dzielących się przez $d\pi_i$, którą to liczbę oznaczemy przez y_i.

Mamy oczywiście szereg równań

$$x = N\left(\frac{A}{d}\right); \tag{7}$$

$$\left.\begin{aligned} x &= x_1 + y_1,\\ x_1 &= x_2 + y_2,\\ &\ldots\ldots\ldots\\ x_{i-1} &= x_i + y_i. \end{aligned}\right\} \tag{8}$$

Lecz y_1, jako liczba liczb niekongruentnych według mod. A i dzielących się przez $d\pi_1$, wyraża się według (7) — należy tylko w miejsce d podstawić $d\pi_1$, .

$$y_1 = N\left(\frac{A}{d\pi_1}\right).$$

Wstawiając tę wartość w pierwsze z równań (8), znajdujemy

$$x_1 = N\left(\frac{A}{d}\right)\left(1 - \frac{1}{N(\pi_1)}\right). \qquad (9)$$

Liczba y_2, jako liczba liczb, niekongruentnych według mod. A i dzielących się przez $d\pi_2$, a nie dzielących się przez $d\pi_1$, albo, co wychodzi na to samo, nie dzielących się przez $d\pi_2\,\pi_1$, — wyrazi się według wzoru (9), w którym w miejsce d należy podstawić $d\pi_2$; mamy więc

$$y_2 = N\left(\frac{A}{d\pi_2}\right)\left(1 - \frac{1}{N(\pi_1)}\right),$$

zatem

$$x_2 = x_1 - y_2 = N\left(\frac{A}{d}\right)\left(1 - \frac{1}{N(\pi_1)}\right)\left(1 - \frac{1}{N(\pi_2)}\right).$$

Rozumując tak samo daléj, znajdziemy analogiczne wzory dla $x_3, \ldots$ i nakoniec dla x_i

$$x_i = N\left(\frac{A}{d}\right)\left(1 - \frac{1}{N(\pi_1)}\right)\ldots\left(1 - \frac{1}{N(\pi_i)}\right).$$

Stąd bezpośrednio otrzymujemy

Twierdzenie. Jeżeli $\pi_1, \pi_2, \ldots, \pi_i$ oznaczają wszystkie liczby idealne pierwsze, wchodzące w skład danéj liczby idealnéj A, to przedstawiając za pomocą znaku $\varphi(A)$ liczbę liczb niekongruentnych według mod. A i pierwszych z A, mieć będziemy

$$\varphi(A) = N(A)\left(1 - \frac{1}{N(\pi_1)}\right)\ldots\ldots\left(\frac{1}{N(\pi_i)}\right),$$

a liczba liczb, niekongruentnych według mod. A i mających największy wspólny dzielnik z A równy d, wyraża się wzorem

$$\varphi\left(\frac{A}{d}\right).$$

Na tem kończymy naszą pracę, w któréj uwzględniliśmy tylko zasady teoryi podzielności liczb algebraicznych, ustalając je na podstawie teoryi największego wspólnego dzielnika; sądzimy, że, cel jaki sobie założyliśmy, osiągnięty został.

Petersburg, styczeń 1893.