AL. ŁAPAREWICZ,

ZASTOSOWANIE FORM KWADRATOWYCH DWÓJKOWYCH DO ROZKŁADU LICZB NA CZYNNIKI PIERWSZE.

Zadanie pracy niniejszej stanowi opis i użycie dwóch sposobów rozkładu liczb na czynniki, podanych przez Gaussa [1]) zamiast zwykłego, niekiedy wielce zmudnego sposobu, który, jak wiadomo, polega na wypróbowaniu podzielności danej do rozkładu liczby przez wszystkie liczby pierwsze, nie większe nad jej pierwiastek kwadratowy. Pierwszy ze sposobów Gaussa ogranicza liczbę tych próbnych dzieleń, drugi zaś prowadzi do wyznaczenia liczby spółdzielnej z daną; o dogodności zaś ich to świadczy, że gdy zwykły sposób już przy liczbie, przekraczającej milion, bywa nieraz wielce uciążliwy, te dwa sposoby nie wymagają większego zachodu, nawet przy rozkładzie liczb dosięgających stu miljonów.

Szczególniej dogodny jest drugi z nich, zwłaszcza gdy w nim za wyznacznik formy, mającej przedstawiać liczbę daną, przyjmiemy jeden z wyznaczników Eulera [2]). Co zaś do pierwszego, to i ten nie mniej jest dogodny, o ile mamy pod ręką tablicę dzielników form kwadratowych [3])

---

[1]) Gauss. Disquisitiones arithmeticae §§ 329—334.

[2]) Euler. De variis modis, numeros praegnandes explorandi, utrum sint primi necne? (Nova Acta Imp. Ac. Sc. Petropol. XIII. 14—44).

[3]) Przykład takiej tablicy mamy w dziele „Teorja srawnienij“ Czebyszewa (str. 265—279); podane są tam wzory liniowe dzielników wszystkich form, których wyznaczniki, tak ujemne jako i dodatnie, liczebnie nie większe nad 101, nie zawierają w swym składzie kwadratów (z wyjątkiem 1). To tylko tablicy tej można zarzucić, że niepotrzebnie spółczynniki tych wzorów liniowych wszędzie wynoszą poczwórny wyznacznik formy, kiedy, jak wiadomo, w razie gdy, wyznacznik $\equiv 1 \pmod 4$, wystarczyłby o połowę mniejszy.

i czynników liczb naturalnych [1]); również i tablica kwadratów liczb naturalnych byłaby przy nim pożądana. Nie mniej i pod względem teoretycznym ważne jest znaczenie tych sposobów, które potrącają o każde niemal twierdzenie z Teoryi liczb, tak, iż dla początkujących zwłaszcza, poznanie tych sposobów jest rzeczą wielkiej wagi. Mając więc to na względzie, zastosowałem swój wykład do wiadomości, zawartych w czterech pierwszych rozdziałach podręcznika Dirichleta [2]), jako najbardziej dziś rozpowszechnionego. Z uwagi zaś na związek drugiego sposobu Gaussa z wyznacznikami Eulera, uwzględniłem w zakończeniu i teoryę tych wyznaczników, przyczem odnośnego twierdzenia Eulera nanowo dowiodłem w sposób acz zbliżony do oryginału, lecz prostszy, bardziej jednolity, i, jak sądzę, ściślej wymotywowany.

Przystępując obecnie do wykładu sposobów Gaussa, zauważę przedewszystkiem, że winniśmy je stosować dopiero po stwierdzeniu niepodzielności danej do rozkładu liczby przez kilka najmniejszych liczb pierwszych (np. < 30), ponieważ one jako czynniki najczęściej się przytrafiają, a gdyby żadna z nich nie okazała się czynnikiem danej liczby, to reszty z tych dzieleń, jak się przekonamy, będą właśnie przydatne przy stosowaniu do tej liczby drugiego sposobu Gaussa. Dla tego też w trakcie wykładu, przez liczbę będziemy rozumieli liczbę niepodzielną przez czynniki małe, a więc w szczególności liczbę nieparzystą. Z tego też względu przez formę będziemy rozumieli tylko formę właściwie pierwotną (albo, jak chce Dirichlet, pierwotną według 1-go sposobu) porządku dodatniego.

§ **1**. Jeżeli forma (a, b, c) o wyznaczniku D za pomocą podstawienia $\begin{pmatrix} m, \mu \\ n, \nu \end{pmatrix}$ jest przekształcalna na formę (L, z, L_1), to spółczynniki ostatniej tworzą się według wzorów:

$$am^2 + 2\,bmn + cn^2 = L\,, \tag{1}$$

$$(am + bn)\,\mu + (bm + cn)\,\nu = z\,, \tag{2}$$

$$a\mu^2 + 2\,b\mu\nu + c\nu^2 = L_1\,, \tag{3}$$

a jej wyznacznik jest:

$$z^2 - LL_1 = D\,(m\nu - \mu n)^2\,. \tag{4}$$

[1]) Mamy tablice: Burckharda (doprowadzoną do 3036000), Dasego (od 3 do 9 mil.), Goldberga (do 251647), Chernac'a (do 102000); dla nas byłaby dostateczną doprowadzona do jakich 10000 lub 15000.

[2]) Lejeune Dirichlet. Vorlesungen über der Zahlentheorie 1879.

Ponieważ cztery te wzory służą do wyznaczenia trzech tylko wielkości, przeto jeden z nich jest zbyteczny.

Z zestawienia wzorów (1), (3) i (4) wnosimy:

I. Jeżeli dwie liczby L i L_1 są przedstawialne przez formę (a, b, c) o wyznaczniku D, to iloczyn ich LL_1 jest przedstawialny przez formę $(1, 0, -D)$.

Formy (a, b, c) i (L, z, L_1) są równoważne, jeżeli

$$m\nu - \mu n = +1\,; \tag{5}$$

warunek ten może być spełniony przy nieskończonej liczbie jednoczesnych wartości na μ i ν, o ile m i n są niespółdzielne; w tym razie wzór (4) prowadzi do kongruencyi

$$z^2 - D \equiv 0 \pmod{L}\,, \tag{6}$$

która, jak to wskazuje wzór (2), jest rozwiązalna, a jak wskazuje wzór (1), zachodzi, jeżeli liczba L jest przedstawialna przez formę (a, b, c) za pomocą przedstawienia (m, n), które na zasadzie powyżej zastrzeżonego warunku jest właściwem. A zatem:

II. Wyznacznik formy jest resztą kwadratową liczby, przedstawialnej przez tę formę za pomocą właściwego przedstawienia.

Twierdzenie to można okazać i w inny sposób. Z równości (1) za pomocą prostego przekształcenia otrzymamy:

$$(am + bn)^2 - (b^2 - ac)\,n^2 = aL\,, \tag{7}$$

czyli:

$$x^2 - Dy^2 \equiv 0 \pmod{L}\,, \tag{8}$$

gdzie przez x i y oznaczyliśmy $am + bn$ i n. Ponieważ m i n możemy zawsze uważać za liczby niespółdzielne (gdyż w razie gdyby miały wspólny największy dzielnik δ, to równość (1) sprowadziłaby się do $a\left(\frac{m}{\delta}\right)^2 + 2\,b\,\frac{m}{\delta}\cdot\frac{n}{\delta} + c\left(\frac{n}{\delta}\right)^2 = \frac{L}{\delta^2}$, poczem liczby m/δ i n/δ byłyby niespółdzielnemi), przeto x i y będą również niespółdzielne zarówno ze sobą jako też i z L, tak iż można dla nich znaleść takie z, aby było $zy \equiv x \pmod{L}$, poczem z kongruencyi (8) otrzymamy (5).

Z równości (7) czytamy nadto, że:

III. Z właściwego przedstawienia (m, n) liczby L

przez formę (a, b, c) o wyznaczniku D wynika właściwe przedstawienie $(am+bn, n)$ liczby aL przez formę $(1, 0, -D)$.

Rozwiązanie kongruencyi (6) przedstawia wzór (2), dający, stosownie do różnych wartości na μ i ν, różne wartości na z, które, jak łatwo okazać, są kongruentne według modułu L, tak iż stanowią jedno tylko rozwiązanie kongruencyi (6), które za pomocą prostego przekształcenia wzoru (2) można otrzymać w zależności od samych tylko m i n, mianowicie:

$$mz \equiv bm + cn \pmod{L}, \tag{9}$$

lub

$$-nz \equiv am + bn \pmod{L}. \tag{9'}$$

Dla tego też powiadamy, że:

IV. Przedstawienie (m, n) liczby L przez formę (a, b, c) należy do rozwiązania kongruencyi (6), określonego za pomocą jednej z kongruencyj (9) lub (9').

§ 2. Z twierdzenia I. § 1 otrzymujemy $x^2 - Dy^2 = LL_1$, skąd przychodzimy do wniosków następujących [1]):

I. Jeżeli D jest liczbą nieparzystą, to stosownie do tego czy $D \equiv 1$, czy też 3 (mod 4), mamy $LL_1 \equiv x^2 - y^2$ lub $x^2 + y^2$ (mod 4); skoro więc LL_1 jest liczbą nieparzystą, tak iż z liczb x i y jedna jest parzysta, druga nieparzysta, wobec czego ich kwadraty $\equiv 0$ lub 1 (mod 4), przeto dla $D \equiv 1$ (mod 4) mamy $LL_1 \equiv \pm 1$ (mod 4), co żadnych nowych wniosków nie nastręcza; w razie zaś gdy $D \equiv 3$ (mod 4), otrzymujemy $LL_1 \equiv 1$ czyli $L \equiv L_1$ (mod 4), skąd $\frac{L-1}{2} \equiv \frac{L_1-1}{2}$ (mod 2); zatem: $(-1)^{\frac{L-1}{2}}$ dla wszystkich liczb, przedstawialnych za pomocą formy o wyznaczniku $D \equiv 3$ (mod 4), ma wartość stałą.

II. Jeżeli D jest liczbą parzystą, to x może przybierać wartości tylko nieparzyste, y zaś dowolne tak, iż $x^2 \equiv 1$ (mod 4 lub 8), $y^2 \equiv 0, 1$ (mod 4) czyli $y^2 \equiv 0, 1, 4$ (mod 8). Rozważmy z osobna cztery poszczególne przypadki:

a) $D \equiv 0$ (mod 4); w tym razie $LL_1 \equiv x^2 \equiv 1$ (mod 4), skąd jak poprzednio, wynika że $(-1)^{\frac{L-1}{2}}$ ma wartość stałą.

b) $D \equiv 0$ (mod 8). $LL_1 \equiv 1$ czyli $L \equiv L_1$ (mod 8), zatem $L^2 \equiv L_1^2$ (mod 16), skąd $\frac{L^2-1}{8} \equiv \frac{L_1^2-1}{8}$ (mod 2), tak iż w tym razie nie tylko $(-1)^{\frac{L-1}{2}}$, ale nadto jeszcze i $(-1)^{\frac{L^2-1}{8}}$ ma wartość stałą.

[1]) Dirichlet § 121.

c) $D \equiv 2$ (mod 8). $LL_1 \equiv x^2 - 2y^2 \equiv \pm 1$ (mod 8), zatem $L \equiv \pm L_1$ (mod 8), skąd. jak poprzednio wnosimy, że $(-1)^{\frac{L^2-1}{8}}$ ma wartość stałą.

d) $D \equiv -2$ (mod 8). $LL_1 \equiv x^2 + 2y^2$ (mod 8), tak iż $L \equiv L_1$ lub $3L_1$ (mod 8); jeżeli zatem $L \equiv 1, 3, 5, 7$ (mod 8), to odpowiednio $L_1 \equiv 1, 3, 5, 7$ lub $3, 1, 7, 5$ (mod 8), t. j. L i L_1 jednocześnie są liczbami wzoru $8n+1$, $8n+3$ lub $8n+5$, $8n+7$, tak iż w tym razie $(-1)^{\frac{L-1}{2}+\frac{L^2-1}{8}}$ ma wartość stałą.

III. Oznaczając przez δ jakikolwiek czynnik pierwszy nieparzysty wyznacznika D, tak iż $D \equiv 0$ (mod δ), mamy $x^2 \equiv LL_1$ (mod δ), skąd symbol $\left(\frac{LL_1}{\delta}\right) = +1$, czyli $\left(\frac{L}{\delta}\right) = \left(\frac{L_1}{\delta}\right)$. A zatem: dla wszystkich liczb L, przedstawialnych za pomocą formy o wyznaczniku D, podzielnym przez δ, $\left(\frac{L}{\delta}\right)$ ma wartość stałą.

Na zasadzie powyższych wniosków, wartości wyrażeń $(-1)^{\frac{L-1}{2}}$, $(-1)^{\frac{L^2-1}{8}}$ i $\left(\frac{L}{\delta}\right)$ nazywamy cechami poszczególnemi formy; cechę łatwo wyznaczyć na zasadzie jednego ze skrajnych spółczynników, które oczywiście są najprostszemi liczbami przedstawialnemi przez daną formę. Zbiór cech poszczególnych, wyznaczonych dla $(-1)^{\frac{L-1}{2}}$ i $(-1)^{\frac{L^2-1}{8}}$, zgodnie z powyższemi wnioskami, a co do $\left(\frac{L}{\delta}\right)$, to dla wszystkich pierwszych nieparzystych czynników wyznacznika, nazywamy cechą ogólną lub krócej cechą. Wszystkie formy, mające cechę jednakową, zaliczamy do jednego rodzaju [1]), których co najwyżej tyle być może, ile kombinacyj daje się utworzyć z cech poszczególnych. W razie np. $D = -1848 = -8.3.7.11 \equiv 0$ (mod 8), na zasadzie II. *b)* mamy do rozważania dwie cechy poszczególne: $(-1)^{\frac{L-1}{2}}$ i $(-1)^{\frac{L^2-1}{8}}$, na zasadzie zaś III. — trzy: $\left(\frac{L}{3}\right)$, $\left(\frac{L}{7}\right)$ i $\left(\frac{L}{11}\right)$; z 5 zaś wielkości, z których każda może mieć wartość $+1$ lub -1, można ogółem utworzyć 32 kombinacye, — skąd wnosimy, że formy o wyznaczniku -1848 tworzą co najwyżej 32 rodzaje. Wiadomo zaś, że formy te tworzą klas 16; wyznaczając dla każdej z nich cechę, spostrzeżemy, że każda klasa należy do innego rodzaju: klasa zasadnicza $(1, 0, 1848)$ ma za cechę $(-1)^{\frac{L-1}{2}} = +1$, $(-1)^{\frac{L^2-1}{8}} = +1$, $\left(\frac{L}{3}\right) = +1$, $\left(\frac{L}{7}\right) = +1$, $\left(\frac{L}{11}\right) = +1$, co w skróceniu za-

[1]) Dirichlet § 122.

znaczamy w ten sposób: $++++$; klasie (12, 6, 157) odpowiada cecha $+-+-+$; klasie (24, 12, 83) cecha $-----$ i t. d. W ogólności, liczba rodzajów zawsze stanowi tylko połowę liczby kombinacyj z cech poszczególnych, a w każdym rodzaju liczba klas jest jednakowa [1]); lecz twierdzeń tych, jako niezwiązanych z zajmującą nas kwestyą, zbyteczna dowodzić.

§ 3. Kongruencye (8) i (6) § 1, w razie jeżeli moduł L jest liczbą złożoną podzielną przez nieparzystą pierwszą l, prowadzą do następujących: $z^2 - D \equiv 0$, $x^2 - Dy^2 \equiv 0 \pmod{l}$. Druga z nich wskazuje, że przez rzeczony czynnik l jest podzielną forma $x^2 - Dy^2$, i dla tego nazywamy go dzielnikiem tej formy. Że zaś z pierwszej kongruencyi wynika $\left(\frac{D}{l}\right) = 1$, przeto: Aby znaleść nieparzysty czynnik pierwszy danej liczby, winniśmy znaleść dzielnik formy, przez którą jest przedstawialna dana liczba lub jej wielokrotność (§ 1, II i III); ten zaś ostatni jest liczbą, dla której rzeczony wyznacznik jest resztą kwadratową. Na tem się zasadza pierwszy sposób Gaussa.

Zagadnienie o wyznaczeniu liczby l z warunku $\left(\frac{D}{l}\right) = +1$ mamy rozwiązane w teoryi reszt kwadratowych. Mianowicie, jeżeli przez Δ oznaczymy iloczyn czynników nieparzystych wyznacznika D, przez δ zaś $+1$ lub -1, stosownie do tego czy $\pm\Delta \equiv 1$ lub 3 (mod 4) (gdzie Δ zachowuje znak wyznacznika D), przez ε wreszcie $+1$ lub -1, stosownie do tego, czy D jest liczbą nieparzystą lub parzystą, znajdziemy [2]):

$$\left(\frac{D}{l}\right) = \delta^{\frac{l-1}{2}} \varepsilon^{\frac{l^2-1}{8}} \left(\frac{l}{\Delta}\right),$$

tak iż powyższe zagadnienie sprowadza się do wyznaczenia liczby l z równości $\delta^{\frac{l-1}{2}} \varepsilon^{\frac{l^2-1}{8}} \left(\frac{l}{\Delta}\right) = +1$. Wnosimy więc stąd, że w szeregu liczb, mniejszych od $4D$ i względem $4D$ niespółdzielnych (z wyjątkiem $\pm\Delta \equiv 1$ (mod 4), gdy zamiast $4D$ możemy wziąć $2D$), jednę połowę stanowią dzielniki formy $x^2 - Dy^2$, drugą jej niedzielniki. Oczywiście, że wszystkie liczby kongruentne według mod $4D$ (resp. $2D$) z którymkolwiek z ostatnich, nie mogą być czynnikami liczby L, i jako takie, z szeregu liczb pierwszych niewiększych nad $\sqrt{L}$ (które dla krótkości nazwijmy czynnikami domniemanemi), winny być zawczasu usunięte. Stąd wnosimy, że za pomocą jednej formy, mogącej przedstawiać daną liczbę lub jej wielokrotność, liczbę czynników domniemanych zmniejszymy o połowę. Jeżeli więc ogólną ich liczbę oznaczymy przez q, to za pomocą λ form zredukujemy ją do $\frac{q}{2^\lambda}$, skąd łatwo wyznaczyć λ, pod warunkiem, aby ostatnia liczba była nieznaczną, np. niewiększą nad 10. Nie zaszkodzi jednakże, jeżeli tak wyznaczoną liczbę wyznaczników λ powiększymy o 1, ponieważ każda następna forma ruguje mniej niż połowę czynników domniemanych, pozostawionych przez formy poprzednie.

[1]) Dirichlet § 123—126.

[2]) Dirichlet § 52.

Zauważmy przytem, że prócz § 1. II, wyznaczniki tych form winny odpowiadać jeszcze pewnym warunkom. Przedewszystkiem, pożądanem byłoby, aby były liczbami pierwszemi, a przynajmniej liczbami o najprostszym składzie: im mniej bowiem czynników mieści w sobie wyznacznik, tem łatwiejsze jest określenie jego reszt i niereszt, a tem samem dzielników i niedzielników danej formy, a nadto, co ważniejsza, tem więcej wyrugujemy domniemanych czynników: ostatni związek wynika ze związku liczby reszt i niereszt D z liczbą $\varphi(D)$, która równa się $D-1$ gdy D jest liczbą pierwszą, w razie zaś przeciwnym L jest mniejsza od $D-1$, lecz tem bliższą tej granicy, im mniej czynników zawiera L. Nadto, liczby pierwsze są pożądane jako wyznaczniki, i przez to, że nie mogą być zależnemi. Tak nazywamy trzy wyznaczniki, które w iloczynie dają kwadrat; jeden z nich zawsze jest zbyteczny, ponieważ po wyrugowaniu niedzielników form np. $x^2 - aby^2$ i $x^2 - acy^2$, pozostaną już tylko, jak łatwo się przekonać, same dzielniki formy $x^2 - bcy^2$. Z tego względu wśród powyższych λ wyznaczników żadne trzy nie powinny być zależnemi, w razie zaś przeciwnym jeden z nich należy zastąpić nowym. Wreszcie — rzecz prosta — wyznacznik winien być jak najmniejszy; stąd też Czebyszew w swej tablicy uwzględnił wyznaczniki nie większe nad 101.

§ 4. Pozostaje teraz okazać, jak należy dla danej liczby znaleść potrzebną liczbę wyznaczników, odpowiadających powyżej wyłożonym warunkom, a więc przedewszystkiem jak znaleść resztę kwadratową liczby, której składu nie znamy. Rozwiązanie tego zagadnienia wynika z określenia rodzajów form. Jeżeli formy (a_1, b_1, c_1), (a_2, b_2, c_2), $(a_3, b_3, c_3)\ldots$ mające za wyznacznik daną liczbę L, należą do jednego rodzaju, to ich skrajne spółczynniki wszystkie są albo resztami albo nieresztami poszczególnych czynników liczby L (nieparzystych, — parzyste są tak łatwe do odnalezienia, że tylko do nieparzystych liczb wypada stosować sposoby Gaussa); iloczyny więc jednego z tych spółczynników przez każdy z pozostałych będą resztami wszystkich czynników liczby L, a więc i samej liczby L. Stąd wnosimy, że jeżeli jeden z tych spółczynników równa się 1, to wszystkie pozostałe spółczynniki będą resztami liczby L. Oczywiście, że każda kombinacya tych reszt w iloczynie, jako też iloraz którejkolwiek

z nich przez kwadrat, o ile taki znajdzie się w jej składzie, będzie również resztą liczby L, tak iż kombinując je w iloczynach, tak aby te zawierały w swym składzie kwadraty zupełne, osiągniemy dostateczną liczbę reszt liczby L, odpowiadających poprzednio (§ 3) wyłożonym warunkom.

Rzecz więc cała sprowadza się do rozwinięcia należytego szeregu form jednego rodzaju. W tym celu za formę wychodną weźmy formę $(a_0, b_1, -a_1)$, w której $a_0 = 1$, $b_1 = E(\sqrt{L})$, t. j. części całkowitej pierwiastka $\sqrt{L}$, poczem a_1 określimy jako $L - \{E(\sqrt{L})\}^2$, t. j. jako resztę z powyższego pierwiastkowania. Ponieważ z dwóch pierwiastków tej formy $\pm\sqrt{L} - E(\sqrt{L})$, wartość liczebna jednego jest większa od 1, drugiego mniejsza od 1, a same te pierwiastki są oczywiście znaków przeciwnych, przeto forma ta jest sprowadzona (zredukowana) [1]. Za szereg więc form jednego rodzaju najprościej będzie przyjąć szereg form sprowadzonych przyległych [2]: $(a_0, b_1, -a_1)$, $(-a_1, b_2, a_2)$, ..., $((-1)^{n-1} a_{n-1}, b_n, (-1)^n a_n)$, $((-1)^n a_n, b_{n+1}, (-1)^{n+1} a_{n+1})$ ... z których każda poprzedzająca, naprz. $((-1)^{n-1} a_{n-1}, b_n, (-1)^n a_n)$, jest przekształcalna w następującą po niej $((-1)^n a_n, b_{n+1}, (-1)^{n+1} a_{n+1})$ za pomocą podstawienia $\begin{pmatrix} 0, 1 \\ -1, \delta \end{pmatrix}$, gdzie $\delta = -\dfrac{b_n + b_{n+1}}{(-1)^n a_n}$; aby i druga forma była sprowadzoną, wystarczy przyjąć liczbę, co do wielkości równą części całkowitej pierwszego pierwiastka pierwszej formy, a co do znaku z tymże pierwiastkiem zgodną. Z takiego określenia wynika: $\dfrac{b_n + b_{n+1}}{a_n} = E\left(\dfrac{b_n + \sqrt{L}}{a_n}\right)$, skąd, zważając że $b^2_n + a_{n-1} a_n = b^2_{n+1} + a_n a_{n+1} = L$, na zasadzie twierdzenia II i III. § 1 przychodzimy do twierdzenia Czebyszewa [3]:

Jeżeli dla danej liczby L utworzymy szereg liczb $a_0, a_1, a_2 \ldots$ z których $a_0 = 1$, $a_1 = L - \{E(\sqrt{L})\}^2$, a każda następująca z dwiema ją poprzedzającemi jest związana za pomocą wzoru:

$$\frac{\sqrt{L - a_{n-1} a_n} + \sqrt{L - a_n a_{n+1}}}{a_n} = E\left\{\frac{\sqrt{L - a_n a_{n-1}} + \sqrt{L}}{a_n}\right\},$$

to forma $x^2 - Dy^2$, w której $D = (-1)^{\alpha+\beta+\gamma+\cdots} a_\alpha a_\beta a_\gamma \ldots$, może przedstawiać liczbę L lub jej wielokrotność.

---

[1]) Dirichlet § 74.
[2]) Dirichlet § 77.
[3]) Czebyszew, l. c. (str. 184).

Doświadczenie wskazuje, że szereg liczb a winien zawierać trzy razy tyle wyrazów, ile dla danej liczby L winniśmy przyjąć wyznaczników.

§ **5**. Wiadomo, że z dwóch form przyległych (a, b, a_1) i (a_1, b_1, a_2) pierwsza na drugą przekształca się za pomocą przedstawienia właściwego $\begin{pmatrix} 0, 1 \\ -1, \delta \end{pmatrix}$, gdzie $\delta = -\dfrac{b + b_1}{a_1}$, tak iż $b_1 = -b - a_1\delta$ i $a_2 = a + 2b\delta + a_1\delta^2$, z przedstawienia więc (m, n) liczby L przez pierwszą formę wynika przedstawienie $(\delta m - n, m)$ tejże liczby przez drugą formę. Oznaczmy odpowiednie rozwiązania kongruencyi $z^2 \equiv D \pmod{L}$, należące do dwóch powyższych jednoczesnych przedstawień liczby L przez dwie te formy przyległe, przez z i ζ; wówczas, na zasadzie wzorów (9) i (9′) § 1 otrzymamy: dla pierwszej formy:

$$mz \equiv mb + a_1 n; \quad -nz \equiv ma + nb \pmod{L},$$

tak iż:

$$(\delta m - n)\, z \equiv \delta mb + \delta a_1 n + ma + nb \pmod{L}$$

i dla drugiej:

$$(\delta m - n)\, \zeta \equiv (-b - a_1\delta)(\delta m - n) + (a + 2b\delta + a_1\delta^2) \pmod{L}$$

skąd, po należytych uproszczeniach, wypadnie:

$$(\delta m - n)\, \zeta \equiv \delta mb + \delta a_1 n + ma + nb \pmod{L},$$

wnosimy więc o zupełnej tożsamości rozwiązań z i ζ.

Że zaś wszystkie formy równoważne za pomocą odpowiednich szeregów form przyległych prowadzą do jednej i tej samej formy sprowadzonej, przeto odpowiednie przedstawienia danej liczby za pomocą wszystkich form pewnej klasy należą do jednego i tegoż samego rozwiązania kongruencyi zasadniczej. Na tej zasadzie z każdej klasy form możemy wybrać po jednej formie, t. zw. przedstawicielce klasy.

Po tej wstępnej uwadze przechodzimy do drugiego sposobu Gaussa.

§ **6**. Kongruencya stopnia 2-go

$$z^2 \equiv D \pmod{L}, \tag{1}$$

o ile D jest resztą liczby L, ma, jak wiadomo, dwa rozwiązania lub więcej, stosownie do tego, czy L jest liczbą pierwszą czy też złożoną. Skoro więc, według IV. § 1, rozwiązanie takie zależy od właściwego przedstawienia liczby L

za pomocą formy o wyznaczniku D, przeto, jeżeli znajdziemy wszystkie przedstawienia liczby L za pomocą wszystkich poszczególnych przedstawicielek klas o wyznaczniku D, których cecha jest zgodna z cechą liczby L, tem samem znajdziemy i wszystkie rozwiązania kongruencyi (1), a więc i skład liczby L będziemy w stanie określić.

Przypuśćmy, że rozwiązania kongruencyi (1) są wiadome, mianowicie:

$$z \equiv \pm z_1, z_2, z_3 \ldots \pmod{L},$$

tak, iż

$$(2) \qquad z_1^2 - D = Lh_1, \quad z_2^2 - D = Lh_2, \quad z_3^2 - D = Lh_3 \ldots,$$

gdzie $h_1, h_2, h_3 \ldots$ są liczbami całkowitemi. Z równości (2) wnosimy, że D jest wyznacznikiem form

$$(3) \qquad (L, \pm z_1, h_1), \quad (L, \pm z_2, h_2), \quad (L, \pm z_3, h_3) \ldots$$

Od tych ostatnich, jak wiemy, za pomocą szeregów form przyległych, przyjdziemy do form sprowadzonych:

$$(4) \qquad F_1, F_{-1}, F_2, F_{-2}, F_3, F_{-3} \ldots,$$

których liczba może być w ogóle różna od liczby rozwiązań kongruencyi (1), gdyż niektóre z form (3) mogą należeć do jednej klasy. Formy zaś (4), jako sprowadzone o wyznaczniku D i mające przedstawiać liczbę L, są wiadome, niezależnie od rozwiązań kongruencyi (1): wystarczy tylko rozwinąć układ zupełny form nierównoważnych o wyznaczniku D i wybrać z niego formy, których cecha jest jednakowa z cechą liczby L. Gdy więc formy (4) w ten sposób mogą być z góry wyznaczone, rozwiązanie kongruencyi (1) sprowadza się do wyszukania wszystkich przedstawień liczby L przez każdą z form (4) z osobna; stąd wnosimy, że jako wyznacznik D dogodniejszą jest liczba ujemna od dodatniej, ponieważ dla wyznaczników ujemnych daleko mniej otrzymujemy form sprowadzonych.

§ 7. Sprowadziliśmy więc zadanie do rozwiązania w liczbach całkowitych równań nieoznaczonych wzoru $ax^2 + 2bxy + cy^2 = L$, gdzie a, b, c są spółczynnikami jednej z form sprowadzonych o wyznaczniku ujemnym $b^2 - ac = -D$. Równanie to, w razie gdy b nie jest zerem, na zasadzie III. § 1, możemy sprowadzić do następującego: $x_1^2 + Dy^2 = aL$, gdzie $x_1 = ax + by$; łatwo przytem okazać, że całkowitym rozwiązaniom nowego odpowiadają takież rozwiązania dawnego równania: skoro bowiem wzór przekształcający: $x = \frac{x_1 - by}{a}$, wskazuje, że x jest liczbą całkowitą, o ile

$x_1 \equiv by_1 \pmod{a}$ czyli $x_1^2 \equiv b^2y^2 \pmod{a}$, a według powyższego równania $x_1^2 + Dy^2 \equiv 0 \pmod{a}$, przeto powyższy warunek prowadzi do kongruencyi: $acy^2 \equiv 0 \pmod{a}$, która oczywiście się sprawdza.

Stąd wnosimy, że winniśmy rozwiązać jedynie równanie postaci:

$$Ax^2 + By^2 = C,$$

w którem: 1) $A = a$, $B = c$, $C = L$, jeżeli w formie (a, b, c) jest $b = 0$,

lub 2) $A = 1$, $B = D$, $C = aL$.

Zauważmy przedewszystkiem, że równanie takie ma skończoną liczbę rozwiązań w tym jedynie razie, jeżeli spółczynniki A i B są znaków jednakowych, co nie jest do osiągnięcia w razie $D > 0$: oto jeszcze powód, dla którego za wyznacznik bierzemy liczbę ujemną. Zważając, że w powyższem równaniu $A < B$, wyrażamy z niego

$$x = \sqrt{\frac{C - By^2}{A}},$$

(znak dwoisty, jako sam przez się widoczny, opuszczamy), poczem na y obieramy takie wartości, aby otrzymać na x wartości: 1) rzeczywiste, 2) całkowite, 3) wymierne.

Każdy z tych trzech warunków rozważmy z osobna.

1) Otrzymamy na x wartość rzeczywistą, jeżeli $y < \sqrt{C/B}$. Zauważmy, że wyrażając y przez x, z warunku rzeczywistej wartości na y przyszlibyśmy do nierówności $x < \sqrt{C/A}$, skąd, ze względu na $A < B$, mielibyśmy na x daleko większy zakres możliwych wartości, niż teraz na y: oto wzgląd, dla którego za nieznaną zależną bierzemy nieznaną o spółczynniku mniejszym.

2) Na x znajdziemy wartość całkowitą, jeżeli $By^2 \equiv C \pmod{A}$, skoro więc B jest niespółdzielne z A (w razie przeciwnym forma byłaby pochodną), przeto z powyższego warunku wynika $(By)^2 \equiv BC \pmod{A}$, co dowodzi, że warunek ten tylko w tym razie może być spełniony, jeżeli BC jest resztą liczby A.

3) Warunek wymierności wreszcie wymaga, aby $AC - ABy^2$ było kwadratem. Zauważmy, że według dowolnego modułu każdy kwadrat jest kongruentny z resztą kwadratową tegoż modułu; jeżeli więc weźmiemy jakąkolwiek liczbę pierwszą E, to rozwiązując szereg kongruencyj $AC - ABy^2 \equiv n_1, n_2, n_3 \ldots n_{\frac{E-1}{2}} \pmod{E}$ gdzie wszystkie n są nieresztami liczby E, możemy być pewni, że dla wartości na y, stąd otrzymanych, wartość na x

nie będzie wymierna, tak iż wszystkie takie wartości na y z szeregu możliwych zawczasu winniśmy wyrugować: z tego względu moduł E nazywamy **rugownikiem** [1]). Oczywiście, że rugownik w obecnym sposobie takież samo ma znaczenie, jakie wyznacznik formy w poprzednim, z tą tylko różnicą, że gdy wyznacznik formy miał być resztą danej liczby, rugownik może być liczbą dowolną; jedynie dla dogodności bierzemy za niego liczbę pierwszą jaknajmniejszą, z wyjątkiem jedynie dzielników A, B i C: w razie bowiem $A \equiv 0$ lub $B \equiv 0 \pmod{E}$, w kongruencyi $AC - ABy^2 \equiv n \pmod{E}$ znika wyraz niewiadomy; w razie zaś $C \equiv 0 \pmod{E}$, co się tylko w tym razie przytrafia, gdy $A = 1$, $B = D$, $C = aL$, tak iż $a \equiv 0 \pmod{E}$, powyższa kongruencya, sprowadzając się do $(by)^2 \equiv n \pmod{E}$, jest nierozwiązalna.

§ 8. Jeżeli podanym sposobem znajdziemy dla kongruencyi $z^2 \equiv D \pmod{L}$ więcej nad jedno rozwiązanie (bez względu na znak jego), tak iż L jest liczbą złożoną, czynniki jej osiągniemy w sposób następujący.

Kongruencya ta w razie $L = l_1 l_2 l_3 \ldots$, daje się rozłożyć na szereg kongruencyj $z^2 \equiv D \pmod{l_i}$, z których każda ma tylko dwa rozwiązania: $z \equiv \pm z_i \pmod{l_i}$; poszukując więc liczb, któreby według mod $l_1, l_2, l_3 \ldots$ odpowiednio były kongruentne liczbom $+z_1$ lub $-z_1$, $+z_2$ lub $-z_2 \ldots$, znajdziemy wszystkie rozwiązania powyższej kongruencyi. Z takiego więc sposobu ich powstawania wynika, że dwa jakiekolwiek, byle różne co do wartości bezwzględnej, są liczbami kongruentnemi według jednego lub kilku, lecz nie wszystkich modułów l. Różnice zatem jednego z tych rozwiązań z każdem z pozostałych zawierają czynniki pierwsze liczby L, najrozmaiciej skombinowane ze sobą w iloczynach. Za pomocą więc dzieleń ciągłych między L a każdą z tych różnic osiągniemy wreszcie i same czynniki.

W szczególnym przypadku, gdy wszystkie rozwiązania kongruencyi $z^2 \equiv D \pmod{L}$ zależą od przedstawień liczby L przez jednę tylko formę (a, b, c), powyższe postępowanie daje się jeszcze uprościć. Jakoż, oznaczając rzeczone przedstawienia przez (m_1, n_1), $(m_2, n_2) \ldots$, będziemy mieli: $m_1 z_1 \equiv (m_1 b + n_1 c)$, $m_2 z_2 \equiv (m_2 b + n_2 c) \ldots \pmod{L}$, skąd $m_1 m_2 (z_1 - z_2) \equiv c (m_2 n_1 - m_1 n_2)$, $m_1 m_3 (z_1 - z_3) \equiv c (m_3 n_1 - m_1 n_3) \ldots \pmod{L}$. Wnosimy przeto, że największe wspólne dzielniki liczby L i $m_1 m_2 (z_1 - z_2)$, $m_1 m_3 (z_1 - z_3) \ldots$ będą zarazem największemi wspólnemi dzielnikami liczby L i $c(m_2 n_1 - m_2 n_1)$, $c(m_3 n_1 - m_1 n_3) \ldots$ tak iż czynniki pierwsze liczby L możemy otrzymać za pomocą dzieleń ciągłych między liczbą L a wyznacznikami 2-go rzędu, złożonemi z wyrazów pierwszego przedstawienia i każdego z pozostałych. Do wniosku tego przyjść

[1]) Gauss, l. c. § 320.

możemy i bezpośrednio z założenia, że liczba L przez formę (a, b, c) jest przedstawialna kilkoma sposobami. Jakoż, jeżeli za pomocą (m_k, n_k) i (m_i, n_i) oznaczymy dwa jakiekolwiek z tych przedstawień, to z otrzymanych stąd równości: $am_k^2 + 2bm_k n_k + cn_k^2 = L$, $am_i^2 + 2m_i n_i + cn_i^2 = L$ przez wyrugowanie liczby c znajdziemy $\{a(m_k n_i + m_i n_k) + 2bn_i n_k\} . (m_i n_k - m_k n_i) = (n_k^2 - n_i^2) L$, skąd wynika, że $(n_k^2 - n_i^2) L$ jest podzielne przez $m_i n_k - m_k n_i$; że zaś $n_k^2 - n_i^2$ nie jest przez nie podzielne, przeto przynajmniej niektóre czynniki $m_i n_k - m_k n_i$ winny być czynnikami i danej liczby L.

Przykład. Zastosujmy powyższe sposoby do liczby

$$L = 2941759 .$$

Ponieważ $\sqrt{L} = 1715, \ldots$, przeto liczba domniemanych czynników wynosi 268 (łącznie z 2); z warunku więc $\frac{q}{2^\lambda} < 10$ wnosimy, że λ winno być przynajmniej $= 5$, tak iż liczb Czebyszewa należy znaleść z 15. Przedewszystkiem, jako resztę z pierwiastkowania $\sqrt{L}$, znajdziemy $a_1 = 534$. Że zaś $a_0 = 1$, przeto $\sqrt{L - a_0 a_1} = 1715$, tak iż $E\left(\frac{\sqrt{L - a_0 a_1} + \sqrt{L}}{a_1}\right) = 6$, poczem $1715 + \sqrt{L - a_1 a_2} = 534.6$, skąd $\sqrt{L - a_1 a_2} = 1489$, $L - a_1 a_2 = 2217121$, skąd $a_2 = 1357$. Następnie $\sqrt{L - a_1 a_2} + \sqrt{L} = 3204$, $E\left(\frac{3204}{1357}\right) = 2$, $1489 + \sqrt{L - a_2 a_3} = 2714$, $a_3 = 1062$. W podobnyż sposób znajdziemy stopniowo: $a_4 = 2009$, $a_5 = 851$, $a_6 = 1010$, $a_7 = 419$, $a_8 = 2697$, $a_9 = 414$, $a_{10} = 1325$, $a_{11} = 1302$, $a_{12} = 529$, $a_{13} = 270$, $a_{14} = 1801$, $a_{15} = 1603$. Rozkładając każdą z tych liczb na czynniki i odrzucając ze składu ich kwadraty, oraz mnożąc przez siebie te z nich, które w swym składzie zawierają czynniki jednakowe, i znów ze składu tych iloczynów odrzucając kwadraty, dla form, mogących przedstawiać daną liczbę lub jej wielokrotności, otrzymamy następujące wyznaczniki: z a_{13} -30, a_4 $+41$, a_9 -46, a_{10} $+53$, z iloczynu $a_5 a_9$ $+74$, $a_6 a_{13}$ -303, z których ostatni zastosujemy przy rozkładzie danej liczby według drugiego sposobu, pozostałe zaś—według pierwszego.

I. Wyznaczamy przedewszystkiem dzielniki każdej z wymienionych form, a więc najpierw formy $x^2 + 30y^2$.

Ponieważ $-30 = 2 . -15$, a $-15 \equiv 1 \pmod{4}$, przeto $\delta = +1$, $\varepsilon = -1$, tak iż dzielniki te odpowiadają równości $(-1)^{\frac{l^2-1}{8}} \left(\frac{l}{15}\right) = (-1)^{\frac{l^2-1}{8}} \left(\frac{l}{3}\right)\left(\frac{l}{5}\right) = +1$ czyli według modułów 8, 3 i 5 jednocześnie winny być kongruentne z następującemi układami liczb: *a)* 1 lub 7; 1; 1, 4, *b)* 1, 7; 2; 2, 3, *c)* 3, 5; 2; 1, 4, *d)* 3, 5; 1; 2, 3, skąd wynika ich wzór ogólny:

$$120k + 1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 67, 79, 101, 113 .$$

Ponieważ $41 \equiv 1 \pmod 4$, przeto $\delta = +1$, a że przytem i $\varepsilon = +1$, przeto dzielniki formy $x^2 - 41y^2$ otrzymamy z warunku $\left(\frac{l}{41}\right) = +1$, skąd wnosimy, że nieparzyste z pośród nich winny być postaci:

$$82k + 1, 5, 9, 21, 23, 25, 31, 33, 37, 39, 43, 45, 49, 51, 57, 59, 61, 73, 77, 81.$$

W podobnyż sposób dla dzielników $x^2 - 53y^2$ znajdziemy:

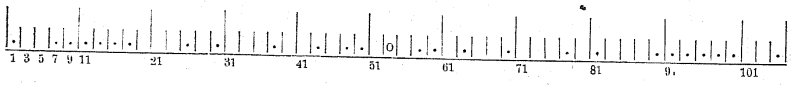
$$106k + 1, 7, 9, 11, 13, 15, 17, 25, 29, 37, 43, 47, 49, 57, 59, 63, 69, 77, 81, 89, 91, 93, 95, 97, 99, 105.$$

Dla $x^2 + 46y^2$ z warunku $(-1)^{\frac{p-1}{8}} \left(\frac{l}{23}\right) = +$ znajdziemy:

$$184k + 1, 5, 9, 11, 19, 21, 25, 31, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 61, 67, 71, 73, 81, 83, 87, 91, 95, 99, 105, 107, 109, 119, 121, 125, 127, 149, 151, 155, 157, 167, 169, 171, 177, 181.$$

Dla formy $x^2 - 74y^2$ postaci dzielników już nie poszukujemy, ponieważ poprzednie formy tyle już wyrugują domniemanych czynników, że daleko łatwiej będzie wybrać z pośród pozostałych dzielniki ostatniej formy. Przystępujemy więc do rzeczonego rugowania.

W tym celu wypiszmy, w równych od siebie odstępach, wszystkie liczby nieparzyste od 1 aż do 1715 i przekreślmy wśród nich liczby złożone; w takich samych odstępach, na pasku papieru wypiszmy niedzielniki jednej z tych form, mniejsze od poczwórnego (resp. podwójnego) jej wyznacznika; przytaczam dla przykładu, odstępy dla niedzielników formy $x^2 - 53y^2$



gdzie, na zasadzie powyższego wzoru, zaznaczamy za pomocą punktów dzielniki, kółko odpowiada liczbie niepierwszej względem wyznacznika, poczem pozostaną niezajęte miejsca niedzielników. Przykładając raz po razie taki pasek do powyższego szeregu liczb nieparzystych, przekreślamy w tym szeregu liczby, odpowiadające pustym miejscom na pasku; dla umożliwienia zaś w następstwie sprawdzenia na miejscu liczby przekreślonej, stawiamy wyznacznik odnośnej formy. Wynik takiego mechanicznego rugowania przedstawi tabliczka następująca:

	1	3	5	7	9	11	21	31	41	51	61	71	81	91	101	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1	9	7	5	3	1
0	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
1	41	30	—	30	30	—	30	—	41	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
2	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
3	—	—	—	—	—	—	30	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
4	30	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
5	—	41	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6	41	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
7	53	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
8	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
9	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
10	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
1	—	46	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
2	41	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
3	41	30	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
4	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
5	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6	30	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
7	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

skąd widzimy, że za pomocą czterech form liczba domniemanych czynników sprowadzi się do dwudziestu:

$$1, 37, 43, 271, 409, 523, 647, 733, 857, 863, 907, 941, 1097, 1109, 1123, 1229, 1499, 1553, 1597, 1697.$$

Z nich 37 jest liczbą niepierwszą względem wyznacznika formy x^2-74y^2; następnie $\left(\frac{43}{37}\right)=\left(\frac{6}{37}\right)=-\left(\frac{3}{37}\right)=-\left(\frac{37}{3}\right)=-1$, a że $43\equiv 3 \pmod 8$, więc 43 jest dzielnikiem tej formy; podobnież $\left(\frac{271}{37}\right)=\left(\frac{12}{37}\right)=\left(\frac{3}{37}\right)=+1$, $271\equiv -1 \pmod 8$, więc 271—dzielnik; $\left(\frac{409}{37}\right)=\left(\frac{2}{37}\right)=-1$, $409\equiv 1 \pmod 8$, przeto niedzielnik i t. d. W ten sposób znajdziemy, że wśród powyższych dwudziestu domniemanych czynników znajdzie się tylko 10 dzielników wszystkich danych form:

$$1, 37, 43, 271, 523, 863, 907, 1123, 1229, 1553, 1597;$$

z których tylko 37 i 43 są istotnie czynnikami danej liczby, tak iż:

$$2941759 = 37.43^3.$$

II. Znaleźliśmy poprzednio dla danej liczby resztę ujemną -303, tę więc przyjmiemy za wyznacznik przedstawiającej ją formy. Ze względu na czynniki 3 i 101 tego wyznacznika, cechami poszczególnemi odpowiednich form będą $\left(\frac{L}{3}\right)$ i $\left(\frac{L}{101}\right)$. Ponieważ zaś dla $L=2941759$ obie te cechy są $+1$, przeto cechą rodzaju, przedstawiającego daną liczbę będzie $++$; z 14 zaś klas właściwych danemu wyznacznikowi cechę taką posiada 7 klas, których przedstawicielkami są formy:

$$(1, 0, 303), \quad (16, \pm 1, 19), \quad (13, \pm 3, 24) \text{ i } (16, \pm 5, 21).$$

Na zasadzie zaś § 1. III, przedstawienie takie sprowadza się do rozwiązania trzech równań nieoznaczonych:

$$x^2+303y^2 = \quad a)\ L, \quad b)\ 13\,L, \quad c)\ 16\,L.$$

Przedewszystkiem więc mamy: $y < a)\ 99,\ b)\ 355,\ c)\ 394$; ponieważ warunek rozwiązań całkowitych sam przez się sprawdza, przeto pozostaje tylko warunek wymierności i dla jego zaspokojenia uciekamy się do rugowników. Ponieważ $303\equiv 0 \pmod 3$, $16\,M\equiv 0 \pmod 4$, przeto 3 wcale, a 4 w razie $c)$ nie nadaje się jako rugownik; skoro zaś $13\,L\equiv L \pmod 4$, przeto w przy-

padkach $a)$ i $b)$ rugownik 4 przyczyni się do usunięcia tych wartości na y, które odpowiadają jednej z kongruencyj: $L-303y^2\equiv 3+y^2\equiv 2, 3 \pmod 4$, z których pierwsza nie daje się rozwiązać, druga zaś prowadzi do $y^2\equiv 0 \pmod 4$, skąd $y\equiv 0 \pmod 2$. Następnie, ponieważ $L\equiv -1$, $303\equiv -2$, $13\equiv -2$, $16\equiv 1 \pmod 5$, przeto $E=5$ (którego resztami są 1 i 4) wyruguje y, odpowiadające kongruencyom: w razach $a)$ i $c)$ $-1+2y^2\equiv 2, 3 \pmod 5$, skąd $y\equiv \pm 2 \pmod 5$, w razie zaś $b)$ $2+2y^2\equiv 2, 3$, skąd $y\equiv 0 \pmod 5$. W ten sposób zakres możliwych wartości na y sprowadza się w razie $a)$ do 30 liczb, kończących się na 1, 5 lub 9, $b)$ do 142 liczb na 1, 3, 7 i 9, $c)$ do 236, na 0, 1, 4, 5, 6 i 9. Dalej, wyrugowaniu ulegną wszelkie $y\equiv \pm$ $a)$ 3, $b)$ 0, 1, $c)$ 2 (mod 7); $\pm$ $a)$ 0, 3, 4 $b)$ 1, 4, 5 $c)$ 2, 3, 5 (mod 11), $\pm$ $a)$ 0, 1, 3, 5 $c)$ 0, 4, 6 (mod 13). Teraz już w razie $a)$ otrzymamy na y tylko pięć możliwych wartości: 9, 35, 61, 71 i 89, z których tylko ostatnia jest istotną, gdyż $\sqrt{2941759-303.89^2}=736$. Kładąc następnie $E=17$, wyrugujemy $y\equiv \pm$ $b)$ 0, 1, 5, 8 $c)$ 0, 4, 6, 8 (mod 17) i w razie $E=19$, $-y\equiv \pm$ $b)$ 1, 2, 3, 5, 9 $c)$ 0, 1, 2, 6, 8 (mod 19). Jakkolwiek zakres możliwych wartości na y sprowadziliśmy już tylko do następujących: $b)$ 11, 19, 31, 53, 121, 129, 163, 201, 317, 319, 327; $c)$ 10, 15, 29, 66, 99, 155, 216, 224, 231, 235, 301, 326, 330, 356, 370 i 389, zastosujmy jednak dwa jeszcze rugowniki sposobem skróconym. Zważając mianowicie, że $L\equiv 13$, $303\equiv 4$, $13\,.\,13\equiv 8$, $13\,.\,16\equiv 1 \pmod{23}$, w razie $b)$ wyznaczmy reszty wyrażenia $8-4y^2$, w razie zaś $c)$ $1-4y^2$ według mod 23, jeżeli za y będziemy kładli powyższe po kolei wartości [1]). I tak, dla $y=11$ mamy $8-4y^2\equiv 7$, a że $\left(\frac{7}{23}\right)=-\left(\frac{23}{7}\right)=-\left(\frac{2}{7}\right)=-1$, przeto 11 nie odpowiada zagadnieniu. W ten sposób znajdziemy, że wyrugowaniu jeszcze ulegną $b)$ 11, 31, 53 i 163; $c)$ 10, 15, 66, 216, 231, 330. Po zastosowaniu w ten sposób jeszcze $E=29$, jako najprawdopodobniejsze wartości na y znajdziemy: $b)$ 129, 201, 317, 319, 327; $c)$ 29, 224, 301, 356, z których tylko $b)$ 129, $c)$ 301 i 356 istotnie odpowiadają zagadnieniu, ponieważ:

$$b)\ \sqrt{13\,L-303.\,129^2}=5762$$

$$c)\ \sqrt{16\,L-303.\,301^2}=4429,\ \sqrt{16\,L-303.\,356}=2944.$$

Ostatnie z tych przedstawień (2944, 356), jako niewłaściwe o czynniku $\delta=4$, prowadzi do przedstawienia (736, 89) liczby $\frac{16\,L}{4^2}=L$ przez formę (1, 0, 303), które otrzymaliśmy poprzednio. Dwa inne zaś (5762, 129) i (4429, 301), jako również niewłaściwe o czynniku $\delta=43$, prowadzą do

[1]) A jeszcze lepiej, ich bezwzględnie najmniejsze reszty według mod 23.

przedstawień właściwych (124, 3) i (103, 7) przez tęż samą formę liczb $^{13}L/_{43^2} = 13.1591$ i $^{16}L/_{43^2} = 16.1591$; stąd w dalszym ciągu przychodzimy do przedstawienia liczby 1591 przez formę $(13, -3, 24)$ za pomocą $(11, 3)$ i przez formę $(16, +1, 19)$ za pomocą $(6, 7)$. Formy zaś $(13, +3, 24)$, $(16, -1, 19)$ i $(16, \pm 5, 21)$ żadnych przedstawień nie dają.

Aby więc ostatecznie L rozłożyć na czynniki pierwsze, pozostaje wyznaczyć, czy 1591 jest liczbą pierwszą czy złożoną. W tym celu winniśmy znaleść rozwiązania kongruencyi $z^2 \equiv -303 \pmod{1591}$, zależne od przedstawień $(11, 3)$ i $(6, 7)$. Pierwsze z tych przedstawień należy do rozwiązania, określonego przez kongruencyę $11z \equiv -3.11 + 24.3 = 39$, skąd $y \equiv -575$, drugie zaś do rozwiązania $6z \equiv 139$, skąd $y \equiv -242 \pmod{1591}$. Wnosimy więc, że 1591 jest liczbą złożoną, a czynnik jej jest zarazem czynnikiem $575 - 242 = 333 = 9.37$. Zatem ostatecznie $L = 37.43^3$.

§ **9**. Im mniej klas mieści w sobie rodzaj form, odpowiadających co do cechy danej liczbie L, tem prędzej daje się uskutecznić jej rozkład za pomocą drugiego sposobu Gaussa. Na szczególne więc uwzględnienie zasługują te wyznaczniki, przy których każdy rodzaj zawiera tylko jednę klasę; wyznaczniki takie, zgodnie z Eulerem, nazwijmy dogodnemi. Wiadomo, że jeżeli dana liczba przez pewną formę przedstawialna jest dwoma sposobami, to liczba ta, jako spółdzielna z wyznacznikiem, złożonym z elementów tych dwóch przedstawień (§ 8), jest liczbą złożoną; lecz w razie jedynego tylko przedstawienia niepodobna jeszcze wnosić, że liczba ta jest pierwszą, ponieważ w rodzaju cechowanym przez daną liczbę mogą być i formy innej klasy, które liczbę tę przedstawią za pomocą przedstawienia, należącego do innego rozwiązania kongruencyi zasadniczej. Stąd wnosimy, że wyznaczniki dogodne można określić jako takie, którym odpowiadające formy jedynym sposobem przedstawiają liczbę pierwszą. Co zaś do form, które jedynym sposobem mogą przedstawiać liczby złożone, okażmy, że jeżeli pewna forma jedynym sposobem przedstawia jednę liczbę złożoną, to można znaleść i cały szereg liczb złożonych, przez tęż formę również jedynym sposobem przedstawialnych.

Zanim to jednak okażemy, zauważmy tymczasem, że jeżeli forma (a, b, c) o wyznaczniku $-D$ przedstawia dwie liczby M i N, każdą sposobem jedynym, to (§ 1. III) forma $(1, 0, D)$ również każdą z liczb aM i aN przedstawia sposobem jedynym; z przedstawień zaś $m^2 + Dn^2 = aM$, $m_1^2 + Dn_1^2 = aN$ wynika $(mm_1 \pm Dnn_1)^2 + D(mn_1 \mp m_1 n)^2 = a^2 MN$, tak iż forma $(1, 0, D)$ liczbę $a^2 MN$ przedstawia dwoma sposobami. W razie szczególnym $M = N$, tak iż $m_1 = m$, $n_1 = n$, mamy stąd:

$$(m^2 \pm Dn^2)^2 + D(mn \mp mn)^2 = (aM)^2,$$

skąd wnosimy, że kwadrat zawsze jest przedstawialny przez formę za pomocą dwóch przedstawień, lecz w jednem z nich drugi wyraz zawsze jest

zerem. Wyłączając więc wartość zerową, powiemy, że kwadrat jest przedstawialny przez jakąkolwiek formę tylko jednym sposobem, a stąd mówiąc o liczbach złożonych przedstawialnych przez formę jedynym sposobem, możemy dojść do niejakich wniosków tylko w założeniu, że liczby te składają się z czynników nierównych.

Ze wszystkich form o wyznaczniku $-D$, bez szkody dla ogólności wniosków, można poprzestać na formie zasadniczej $(1, 0, D)$: jakoż, jeżeli forma (a, b, c) o wyznaczniku $-D$ przedstawia jedynym sposobem liczbę złożoną MN, w której $M < N$, to $(1, 0, D)$ również jedynym sposobem przedstawi $M.aN$, w której tembardziej $M < aN$. Przypuśćmy więc, że forma zasadnicza $(1, 0, D)$ jedynym sposobem przedstawia liczbę MN, złożoną z czynników nierównych, np. $M < N$; okażmy, że taż sama forma w takim razie przedstawi również sposobem jedynym liczbę złożoną MP, podzielną przez mniejszy z czynników poprzedniej liczby. W tym celu, kładąc $MN = m^2 + Dn^2$, $MP = p^2 + Dq^2$, i rugując D znajdziemy: $m^2q^2 - n^2p^2 = M(Nq^2 - Pn^2)$, t. j. jeden z czynników $mq \pm np$ jest podzielny przez M (w razie $M = 2$ mogą być i oba). Przypuśćmy np. $mq - np = M\delta$, poczem $P = \frac{1}{n^2}\left\{Nq^2 - (mq + np)\delta\right\}$, tak iż wystarczy tylko przyjąć $q = 1$, aby być przekonanym, że nowa liczba MP przez formę $(1, 0, D)$ istotnie jedynym sposobem jest przedstawialna, ponieważ o ile MP nie jest kwadratem, przypadek $q = 0$ jest niedopuszczalny. Oczywiście, że jeżeli $q = 1$, wtedy $P < N$, t. j. sposobem podanym znajdziemy nową liczbę złożoną, mniejszą od danej.

Łatwo zauważyć, że założenie $q = 1$ zawsze się daje urzeczywistnić. Skoro bowiem, według założenia $mq \equiv np \pmod{M}$, przeto $q \equiv nr$, $p \equiv mr \pmod{M}$ czyli $q = nr - Mt$, $p = mr - Ms$; że zaś n i M są niespółdzielne ze sobą, przeto równanie nieoznaczone $nr - Mt = 1$, w którem nieznanemi są r i t, jest rozwiązalne.

Ponieważ forma $x^2 + Dy^2$ dla $y = 0$ przedstawia kwadrat zupełny, który z zakresu liczb przedstawialnych wyłączyliśmy, a dla $y = 2$ liczbę nie mniejszą od $4D$, przeto jedna z liczb złożonych, jedynym sposobem przedstawialnych przez formę $x^2 + Dy^2$, winna być mniejsza od $4D$; stąd wnosimy, że jeżeli sposobem podanym będziemy wynajdywali coraz to mniejsze liczby złożone, przyjdziemy wreszcie do liczby mniejszej od $4D$.

Przykład. Forma $x^2 + 14y^2$ przedstawia $7729 = 59.131$ za pomocą jedynego przedstawienia $(85, 6)$, tak iż $m = 85$, $n = 6$, $M = 59$, $N = 131$. Przedstawienie (pq) liczby $59P$ za pomocą tejże formy otrzymamy więc z kongruencyi $85q \equiv 6p \pmod{59}$ czyli $-33q \equiv 6p$ czyli wreszcie $-11q \equiv 2p \pmod{59}$, tak iż $q \equiv 2r$, $p \equiv -11r \pmod{59}$. Kładąc $q = 1$, mamy $2r - 59t = 1$, skąd $r = \frac{59t+1}{2} = 29t + \frac{t+1}{2}$, tak iż najmniej-

szą wartością na t, dla której r jest liczbą całkowitą, będzie $t=1$, poczem $r=30$, tak iż $p=-330-59u$, skąd dla $u=-6$ otrzymamy wartość najmniejszą $p=24$. Zatem $MP=24^2+14.1^2=59.10>4D$. Kładąc teraz $m=24$, $n=1$, $M=10$, $N=59$, w podobnyż sposób przyjdziemy do jedynego przez x^2+14y^2 przedstawienia (4, 1) liczby $3.10<4D$.

§ **10**. Z powyższego twierdzenia wnosimy, że jeżeli forma x^2+Dy^2 przedstawia liczbę złożoną $RS<4D$, to można znaleść cały szereg innych liczb złożonych przedstawialnych przez tęż formę sposobem jedynym, tak iż $-D$, jako wyznacznik nie jest liczbą dogodną. Jakoż, jeżeli $a^2+D=RS$, i $x^2+Dy^2=RT$, to $(x+ay)(x-ay)=R(T-Sy^2)$; o ile więc $R>2$, jedna tylko z liczb $x\pm ay$ jest podzielna przez R. Kładąc więc $x-ay=R\delta$, mamy $T=Sy^2+2ay\delta+R\delta^2$ czyli $RT=(R\delta+ay)^2+Dy^2$, skąd stosownie do różnych y i δ, wartości T będą coraz inne, dla każdej więc liczby otrzymamy przedstawienie jedyne, — o ile czynniki pierwszej liczby $<4D$ były większe nad 2 i różne od siebie.

W razie $R=2$ dowoli można przyjąć $x_1-ay_1=R\delta_1$ lub $x_2+ay_2=R\delta_2$, poczem $RT=(R\delta_1+ay_1)^2+Dy_1^2$ lub $RT=(R\delta_2-ay_2)^2+Dy_2^2$. Podobnież jeżeli $R=S$, tak iż $T=Ry^2+2ay\delta+R\delta^2$, wskutek symetryi y i δ możemy położyć jednę zamiast drugiej, tak iż obok przedstawienia $(R\delta+ay, y)$ znajdziemy w tym razie i przedstawienie $(Ry+a\delta, \delta)$. W tych więc dwóch przypadkach każda z liczb złożonych daje się przez formę x^2+Dy^2 przedstawić dwoma sposobami.

Na zasadzie powyższych rozważań, zważywszy, że forma x^2+Dy przedstawia liczbę $<4D$, o ile $y=1$, $x<\sqrt{3D}$, przychodzimy do twierdzenia Eulera [1]):

Jeżeli forma x^2+D dla wszystkich wartości na x, pierwszych względem D i mniejszych od $\sqrt{3D}$, przedstawia same tylko liczby pierwsze lub dwukrotności lub wreszcie kwadraty, to liczba $-D$, jako wyznacznik jest liczbą dogodną.

Przykłady. 1) $D=7$. $x=1, 2, 3, 4$. $x^2+D=8, 11, 16, 23$ — liczba dogodna.

2) $D=52$. Kładąc za x liczby <12, pierwsze względem 52, znajdziemy: $x^2+52=53, 61, 77, 101, 133, 173$, z których $77=7.11$, $133=7.19$ — liczba niedogodna.

3) $D=63$. W szeregu wartości 64, 67, 79, 88, 127, 163, 184, 232 liczby nieparzyste są pierwsze, ale parzyste — podzielne przez 8 — liczba niedogodna.

[1]) Nova Acta Petropolitana. XIII. 14—44.

4) $D=1848$. W tym razie w szeregu wartości x^2+D mamy $1849=43^2$, $2209=47^2$, $2809=53^2$, $5329=73^2$, $6889=83^2$, pozostałe zaś pierwsze; jest to największa z liczb dogodnych.

5) Ponieważ w razie $D=3063$ dla $x=8, 32, 52, 88$ forma x^2+D przedstawia odpowiednio 53×59, 61×67, 73×79, 101×107, a dla każdej nieparzystej — liczbę podzielną przez 8, przeto liczba ta jest niedogodna.

§ **11**. Jeżeli D jest liczbą nieparzystą, to forma x^2+D dla każdej nieparzystej wartości na x przedstawia liczbę parzystą, która, jak wiemy, nie wpływa na niedogodność liczby D; stąd winniśmy rozważać jedynie wartości tej formy dla parzystych wartości x. Należy jednak zauważyć, że jeżeli $D\equiv-1 \pmod 4$, to forma x^2+D dla każdej nieparzystej wartości x przedstawia liczbę podwójnie parzystą; zważając więc, że najmniejszemi wielokrotnościami liczby 4 złożonemi z dwóch nierównych czynników i większych od 2, są 12 i 20, a krańcowemi wartościami liczb x^2+D są $1+D$ i $4D$, wnosimy, że liczby $D=4n+3$, nie mniejsze nad 19, są niedogodne, nie większe zaś nad 3— dogodne; co zaś do liczb 7, 11, 15, to na zasadzie poprzedniego § przekonywamy się, że 7 i 15 są dogodne, 11 — niedogodna. Oczywiście, że dla tych z pomiędzy $D=4n+3$, które są przytem postaci $8n+7$, odnośne wartości liczby x^2+D są podzielne przez 8.

Podobnież z szeregu liczb naturalnych należy jako niedogodne wyrugować D odpowiadające równości $\left(\frac{-D}{p}\right)=+1$, gdzie p jest liczbą pierwszą nieparzystą, ponieważ warunek ten wskazuje możliwość takiej wartości na x, dla której $x^2\equiv-D \pmod p$. Że zaś zakres możliwych wartości na x^2+D rozciąga się od $1+D$ do $4D$, a liczba podzielna przez p, po usunięciu liczb podzielnych przez $<p$, wynosi przynajmniej p^2, przeto o ile $D<\frac{p^2}{4}$, D jest w tym razie liczbą dogodną, o ile zaś $D>p^2$, jest niedogodną; co zaś do liczb, odpowiadających równości $\left(\frac{-D}{p}\right)=+1$ a zawartych w granicach od $p^2/4$ do p^2, to o ich dogodności lub niedogodności możemy zawyrokować dopiero na zasadzie § 10. Tak np. wszystkie $D\equiv2 \pmod 3$ większe od 9 t. j. 11, 14, 17.. są niedogodne, mniejsze od $9/4$ (taką jest tylko 2) — dogodne; dogodność zaś liczb 5 i 8 uznamy dopiero na zasadzie § 10. Począwszy od 25, wszystkie $D\equiv1, 4 \pmod 5$ są niedogodne, mniejsze od $25/4$, t. j. 1, 4 i 6 — dogodne; liczby zaś pośrednie 9, 16, 21 i 24 ulegają zbadaniu, z którego wypływa ich dogodność i t. d.

W ten to sposób, wypisując szereg liczb naturalnych do 10000 i przyjmując za rugowniki najpierw 4, potem szereg liczb pierwszych nieparzystych, Euler znalazł 65 liczb dogodnych: 1. 2. 3. 4. 5. 6. 7. 8. 9. 10.— 12. 13. 15. 16. 18. 21. 22. 24. 25. 28. — 30. 33. 37. 40. 42. 45. 48. 57. 58. 60.—

70. 72. 78. 85. 88. 93. 102. 105. 112. 120. — 130. 133. 165. 168. 177. 190. 210. 232. 240. 253. — 273. 280. 312. 330. 345. 357. 385. 408. 462. 520. — 760. 840. 1320. 1365. 1848.

Ponieważ od 2000 Euler nie znalazł już żadnej liczby dogodnej, można przypuszczać, że i ponad 10000 wcale ich nie ma, — tembardziej, że w miarę wzrostu liczby D, mamy do rozważania coraz więcej wartości x^2+D, tak iż coraz mniej staje się prawdopodobnem, by wśród nich nie znalazła się ani jedna liczba złożona. Zaznaczyć przytem należy, że wobec podanej granicy liczb naturalnych, szereg rugowników wypadałoby doprowadzić do 200, — tymczasem już 43 usuwa resztki liczb niedogodnych.

Aby dać przykład jak dalece wyznaczniki Eulera, zwłaszcza większe, ułatwiają zajmujące nas zadanie, rozłóżmy na czynniki $L=88341067$. Nie uciekając się tym razem do wyznaczenia reszty tej liczby, obierzmy wśród wyznaczników Eulera taki, aby $\left(\frac{-D}{L}\right)=+1$. Ponieważ $\left(\frac{-1848}{L}\right)=\left(\frac{-2}{L}\right)\left(\frac{231}{L}\right)=\left(\frac{L}{231}\right)=\left(\frac{199}{231}\right)=\left(\frac{32}{199}\right)=\left(\frac{2}{199}\right)=+1$, a przytem $(-1)^{\frac{L-1}{2}}=-1$, $(-1)^{\frac{L^2-1}{8}}=-1$, $(L/_3)=+1$, $(L/_7)=-1$, $(L/_{11})=+1$, przeto możemy się spodziewać przedstawialności danej liczby przez formę $(3, 0, 616)$.

Rozwiązując więc równanie $3x^2+616y^2=88341067$, uważamy najpierw, że dla rzeczywistej wartości na x potrzeba, by y było <378, dla całkowitej zaś: $L-616y^2\equiv 0 \pmod 3$, a że $L\equiv 1$, $616\equiv 1 \pmod 3$, przeto $y\equiv\pm 1 \pmod 3$, poczem zwracamy się do rugowników.

Przyjmując $E=5$, mamy do wyrugowania pierwiastki kongruencyi $3(L-616y^2)\equiv 2, 3 \pmod 5$, które ze względu na to, że $L\equiv 2$, tak iż $3L\equiv 1$, a $616\equiv 1$, tak iż $3.616\equiv -2 \pmod 5$, prowadzą do $1+2y^2\equiv 2, 3 \pmod 5$, skąd $y\equiv\pm 1 \pmod 5$.

W podobny sposób jako wielkości do wyrugowania znajdziemy: $y\equiv\pm 2, 4, 6 \pmod{13}$; $1, 3, 5, 6 \pmod{17}$; $0, 3, 5, 7, 8 \pmod{19}$; $0, 2, 3, 4, 7, 8 \pmod{23}$; $0, 1, 4, 7, 8, 9, 10 \pmod{29}$; $4, 5, 7, 9, 11, 13, 14 \pmod{31}$.

Wynik tych rugowań przedstawia tabelka następująca:

	0	2	3	5	7	8		0	2	3	5	7	8		0	2	3	5	7	8		0	2	3	5	7	8
0	—	13	3	17	13	19	13	17	3	17	3	13	3	26	17	13	19	29	3	23							
1	29	3	31	3	13	3	4	19	17	—	13	3	17	7	3	23	3	13	13	17							
2	13	13	17	23	3	13	5	3	13	3	19	19	13	8	13	3	17	3	—	3							
3	3	13	3	13	13	19	6	13	3	13	3	13	3	9	13	13	13	13	3	29							
4	17	3	13	3	—	3	7	29	31	13	13	3	13	30	3	23	3	13	17	13							
5	13	17	23	31	3	13	8	3	17	3	19	19	13	1	13	3	—	3	17	3							
6	3	17	3	17	13	19	9	17	3	13	3	13	3	2	17	17	13	23	3	17							
7	—	3	17	3	23	3	20	23	13	17	17	3	31	3	3	13	3	17	17	23							
8	13	13	19	13	3	17	1	3	13	3	13	13	17	4	13	3	17	3	13	3							
9	3	19	3	13	13	13	2	17	3	13	3	13	3	5	19	17	13	13	3	13							
10	13	3	17	3	17	3	3	13	13	17	17	3	13	6	3	13	3	23	29	13							
1	13	29	13	13	3	17	4	3	19	3	13	19	—	7	13	3	13	3	17	3							
2	3	17	3	17	—	13	5	17	3	13	3	23	3	—	—	—	—	—	—	—							

$E=13$

0	2	3	5	7	8
—	—			—	
			—	—	
—	—				
—	—		—		
				—	
					—
—					
		—			
				—	—
	—				
—			—		
					—

Wypisujemy w 6 kolumnach, stosownie do ostatniej cyfry, wszystkie liczby nie większe nad 378, z wyjątkiem $\equiv \pm 1 \pmod 5$ czyli 1, 4, 6, 9 (mod 10) i odrzucamy z nich podzielne przez 3, poczem przystępujemy do wyrugowania liczb $\equiv \pm 2, 4, 6 \pmod{13}$. W tym celu wypisujemy wszystkie liczby tych wzorów < 130 i, zachowując tylko $\equiv 0, 2, 3, 5, 7, 8 \pmod{10}$, wypisujemy je również w 6 kolumnach, stosownie do cyfry jednostek każdej z nich i zachowując odpowiednie odległości między dziesiątkami; wystarczy teraz tylko przyłożyć taką tabelkę (którą podaliśmy tu pod $E = 13$) do każdej z części poprzedniej tabelki, aby w tej ostatniej odrzucić nieprzydatne wartości na y. Postępując w ten sam sposób z $E = 17$, szereg możliwych wartości na y sprowadzimy do 42. Znajdując według mod 19 bezwzględnie najmniejsze reszty każdej z nich, odrzucimy z nich jeszcze 14 liczb $\equiv \pm 0, 3, 5, 7, 8 \pmod{19}$; postępując w podobnyż sposób z $E = 23$, 29 i 31, otrzymamy wreszcie siedm najprawdopodobniejszych wartości [1]: 47, 70, 127, 143, 248, 287 i 313, z których 70 i 248 odpowiadają zagadnieniu, tak iż forma (3, 0, 616) przedstawia daną liczbę dwoma sposobami: (5333, 70) i (4101, 248). Stąd wnosimy, że czynnik L jest zarazem czynnikiem wyznacznika

$$\begin{vmatrix} 5333, & 35 \\ 4101, & 124 \end{vmatrix} = 517757 ,$$

skąd łatwo już przyjdziemy do żądanego rozkładu:

$$88341067 = 9769 \,.\, 9043 .$$

§ **12.** W razie, jeżeli żadna z liczb dogodnych nie nadaje się na wyznacznik formy, mającej przedstawiać daną do rozkładu liczbę, winniśmy się uciec do innych wyznaczników, dla których klasyfikacya jest bardziej złożona. Przedewszystkiem więc Gauss [2]) zaleca następujące wyznaczniki: 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148 i 193, którym właściwy jest jeden rodzaj dwuklasowy; z kolei winniśmy się zwrócić do wyznaczników z rodzajem trzyklasowym: 11, 19, 23, 27, 31, 43, 67 i 163, pięcioklasowym: 47, 79, 103 i 127, siedmioklasowym: 71, 151, 223, 303, 463 i 487; pozostałe wyznaczniki jeszcze mniej są dogodne.

Ponieważ sposobem Czebyszewa (§ 4) można nie dość szybko dojść do takiej reszty ujemnej, która by należała do wyznaczników Eulera

[1]) W powyższej tabelce na miejscu każdej z odrzuconych wartości wymieniony jest odpowiedni rugownik.

[2]) Gauss. Disq. Ar. § 303. Wszystkie wymienione tu wyznaczniki, jak w ogóle w rozważanym sposobie, są ujemne.

lub Gaussa, przeto w ogóle dogodniej wśród tych ostatnich wybrać dla danej liczby L taki wyznacznik D, aby było $\left(\frac{-D}{L}\right) = +1$ (jakeśmy to uczynili w ostatnim przykładzie). Lecz nie zapominajmy, że warunek ten niekoniecznie oznacza, że $-D$ jest resztą liczby L, tem więc samem forma odnośna może nie przedstawiać danej liczby; choć więc zyskujemy w ten sposób dowód na to, że jest ona liczbą złożoną, lecz przez podobne uproszczenie tracimy niekiedy możność odnalezienia jej czynników.