Nowa metoda rozkładu liczb na czynniki pierwsze.

Wszelkie znane dotąd w matematyce sposoby rozkładu wielkich liczb na czynniki pierwsze nie są właściwie metodami rozkładu, lecz metodami wynajdywania form kwadratowych i linjowych dla dzielników poszukiwanych. Bardzo dowcipne i subtelne sposoby matematyków tej miary, co Lagrange, Legendre, Lucas, a zwłaszcza Czebyszew ustalają przedewszystkim ciąg form kwadratowych, jedynie możliwych dla czynników liczby badanej, — a zarazem ciąg form linjowych, odpowiadających każdej kwadratowej. Kombinując następnie po dwie formy kwadratowe w różnych zestawieniach, wyłączamy z pomiędzy odpowiednich im linjowych te, które nie należą jednocześnie do obu kwadratowych, zestawionych przez nas. W ten sposób otrzymujemy formę linjową coraz ogólniejszą, w której współczynniki liczbowe wciąż wzrastają. Zatrzymujemy się wreszcie na takiej, która da nam możliwie najmniejszą ilość liczb pierwszych jej odpowiadających, i w końcu wykonywamy po kolei dzielenie próbne liczby badanej przez wszystkie znalezione przez nas możliwe jej czynniki.

Postępowanie takie dalekie jest od doskonałości nie tylko dlatego, że nie daje nam czynników gotowych, że je wyczuwa zaledwie. Większą jeszcze jego wadą jest to, że zastosowywane tu działania skomplikowane i długie, a wymagające uwagi skupionej, nie podlegają żadnemu sprawdzaniu się w biegu samej roboty. Możliwe więc są omyłki przypadkowe, unicestwiające wynik ostateczny. Dość zwrócić uwagę na wzór zasadniczy Czebyszewa, na podstawie którego otrzymujemy szereg form kwadratowych na dzielniki liczby badanej. Jest on tak skomplikowany, że wszelkie działania stąd wypływające należy przerobić powtórnie, lub dać do przerobienia osobie innej, by mieć pewność, że punkt wyjścia nie zawiera omyłek.

To, co podaję poniżej, nazwałem metodą rozkładu liczb na czynniki, gdyż mając badaną liczbę N, wykonywam pewne działania algiebraiczne i arytmetyczne, które prowadzą bez żadnego dzielenia próbnego albo do otrzymania gotowych dzielników liczbowych, albo do pewności, że liczba N jest pierwszą. Prócz tego, jeśli N okaże się złożoną, mogę orzec z łatwością i a priori, wiele mianowicie zawiera ona różnych czynników pierwszych. Omyłki przypadkowe wyłączone są absolutnie

w tej metodzie, gdyż mamy tu działania najprostsze i sprawdzenie natychmiastowe roboty głównej, wyznaczającej liczbę dzielników. Wreszcie, jeśli chodzi o szybkość, to np. liczbę 8520191, cytowaną i rozkładaną przez Czebyszewa, zbadałem przy pomocy mojej metody w ciągu $1^1/_2$ godziny, posiłkując się zaś arytmometrem — wciągu 40 minut. Tymczasem, przerobienie tego wszystkiego co wykonywa sam Czebyszew*), zajęło mi przeszło 12 godzin, i prócz tego — robota cała wymaga przerobienia powtórnego.

Wskazuję tu na wyższość mojej metody; słusznym jest zwrócić uwagę i na jej słabą stronę, a mianowicie, że, jak dotąd, może być ona stosowana praktycznie tylko do liczb kształtu $10m \pm 1$. Co zaś do kształtu $10m \pm 3$, to jakkolwiek podaję teoretyczne rozwiązanie kwestji**), lecz wymaga ono przejścia do kwadratu liczby N, co prowadzi do liczb zbyt wielkich i pozbawia metodę jednej z głównych jej zalet, t. j. szybkości. Dla liczb kształtu $10m \pm 3$ należy więc szukać metody innej, krótszej. Zdecydowałem się jednak na publikację wyników już osiągniętych, w nadziei zachęcenia matematyków do opracowania i udoskonalenia dalszego metody tu podanej, jako skierowującej kwestję omawianą na właściwe tory.

Na wynalezienie jej naprowadziły mię badania nad własnościami uogólnionych ciągów Fibonaccie'go, ogłoszone już drukiem***).

Ciekawych niezmiernie badań ciągu Fibonacci'ego dokonał E. Lucas (Bolletino Boncompagni. Tom X. Str. 129. Sur diverses questions d'arithmétique supérieure), gdzie wspomina nawiasowo o uogólnionym ciągu Fibonacci'ego i jego określniku, nie robiąc jednak żadnego stąd wniosku o możliwości zastosowania go do rozkładu liczb na czynniki pierwsze. Lucas rozwinął następnie swą analizę, stosując ją do trzech typów ciągów: Fibonacci'ego, Fermata i Pella (Théorie des fonctions numériques simplement periodiques. American Journal of Mathematics. 1878. Tom I. Str. 184).

Przypomnę tu w streszczeniu wyniki główne badań moich, potrzebne do zrozumienia metody przedstawionej poniżej.

Chcąc, by ciąg uogólniony nie był skracalny, obieramy dwie wielkości dodatnie: a i b względnie pierwsze, i otrzymujemy postać algiebraiczną takich szeregów

$$a,\ b,\ a+b,\ a+2b,\ 2a+3b,\ 3a+5b,\ 5a+8b,\ \ldots \qquad (1)$$

gdzie, oczywiście, spółczynniki przy a i b w każdym wyrazie poszczególnym są kolejnemi wyrazami ciągu Fibonacci'ego

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ \ldots \qquad (2)$$

Ciąg liczbowy, czy też rozważany w kształcie algiebraicznym, należy rozumieć zawsze, jako doprowadzony do właściwego swego początku, co jest uwarunkowane przez nierówność

---

*) *Czebyszew.* Sobranje Soczinienij. Tom I. Str. 73.

**) *R. Niewiadomski.* Nowyj metod razłożenja czisieł na pierwonaczalnyje mnożiteli. Moskwa 1912.

***) Wiadomości Matematyczne. Tom XV. 1911. Str. 235.

$$b-a>a \qquad \text{czyli} \qquad b>2a \tag{3}$$

Przy zachowaniu tego warunku ciąg rozpoczynać się będzie od liczby możliwie najmniejszej.

Dla każdego ciągu uogólnionego istnieje pewna liczba stała, nieparzysta D, czyli określnik szeregu, która równa się

$$D=\pm(U^2_N-U_{N-1}\cdot U_{N+1}) \tag{4}$$

Przy N parzystym otrzymujemy przed nawiasem znak $+$, przy N zaś nieparzystym znak $-$.

Kształt algiebraiczny określnika ciągu typowego (1) będzie

$$D=b^2-a(a+b)=b^2-ab-a^2 \tag{5}$$

czyli odpowiada mu pewna specjalna forma kwadratowa.

Określnik D jest liczbą pierwszą względem wszystkich wyrazów szeregu, lub szeregów mu odpowiadających (o ile a jest pierwsze względem b).

Jeśli mamy jakikolwiek ciąg (1) o określniku D, to istnieje co najmniej drugi jeszcze ciąg o tymże określniku, a mianowicie

$$b-2a,\ 2b-3a,\ 3b-5a,\ 5b-8a,\ 8b-13a,\ 13b-21a,\ \ldots \tag{6}$$

Oba te ciągi (1) i (6) mają jednakowy przedwyraz: $U_0=b-a$; będziemy je nazywali sprzężonemi. Z dwuch sprzężonych ciągów nazywać będziemy zasadniczym ten, którego wyrazy początkowe są względnie mniejsze.

Dwa jedynie ciągi nie posiadają sprzężonych: 1) ciąg Fibonacci'ego (2), gdzie $U^F_0=1$ i $D^F=1$; 2) ciąg 1, 3, 4, 7, 11, 18, ... w którym $U^R_0=2$ i $D^R=5$.

Określniki D mogą być tylko kształtu $10m\pm1$, o ile nie zawierają czynnika 5, który zresztą występować może w określniku jedynie w potędze pierwszej.

Badając kształt ogólny ciągu sprzężonego (6), widzimy, iż spółczynniki przy a i b są kolejnemi wyrazami ciągu (2), poczynając od wyrazu trzeciego. Rozważywszy zasadę formowania ciągu (6) z ciągu (1), znalazłem, iż zupełnie identycznie powstaje ciąg o określniku złożonym $D=d_1d_2$ z dwuch innych ciągów, których określniki równają się d_1 i d_2. Mianowicie, jeśli pierwsze wyrazy ciągu mnożonego są a i b, to postać ogólna wyrazów ciągu złożonego będzie

$$pb-qa \tag{7}$$

gdzie spółczynniki zmienne p i q są wyrazami kolejnemi ciągu mnożącego. Naturalnie, role ciągów mnożonego i mnożącego mogą się nawzajem zamieniać. W przypadku szczególnym, ciągi (6) i (1) mają ten sam określnik, ponieważ określnik ciągu mnożącego (Fibonacci'ego) równa się 1.

Przypuśćmy, że dane ciągi o określnikach d_1 i d_2 mają postać

(α) $\quad a,\ b,\ a+b,\ a+2b,\ 2a+3b,\ \ldots \quad$ gdzie $d_1=b^2-ab-a^2$

(β) $\quad p,\ q,\ p+q,\ p+2q,\ 2p+3q,\ \ldots \quad$ gdzie $d_2=q^2-pq-p^2$.

Kształt ciągu o określniku złożonym $D=d_1 d_2$ powinien być

$$(\gamma) \qquad pb-qa,\ qb-(p+q)a,\ (p+q)b-(p+2q)a,\ (p+2q)b-(2p+3q)a,\ \ldots$$

Ciąg (γ) jest, oczywiście, jednym z uogólnionych ciągów Fibonacci'ego, ponieważ spółczynniki przy b i a w każdym jego wyrazie również tworzą taki ciąg, w którym suma dwuch wyrazów kolejnych równa się trzeciemu.

Określnik ciągu (γ) jest

$$D_\gamma = \{qb-(p+q)a\}^2-(pb-qa)\{(p+q)b-(p+2q)a\} \qquad (8)$$

Wystarcza sprawdzić, że zachodzi tu tożsamość z iloczynem

$$(b^2-ab-a^2)(q^2-pq-p^2) \qquad (8a)$$

Zachodzi to w rzeczy samej, jak łatwo się przekonać po wykonaniu mnożeń odpowiednich.

A więc, iloczyn form kwadratowych kształtu (5) b^2-ab-a^2 ma taką samą formę kwadratową (5), zupełnie analogicznie do znanej własności form a^2+b^2.

Na rozwiązaniu odwrotnego zagadnienia drogą algiebraiczną opiera się moja metoda rozkładu liczb określnikowych na czynniki pierwsze.

Ponieważ przekonaliśmy się, że istnieje równość (8)=(8a), możemy więc wnioskować w związku z tym, co dowiedzione zostało powyżej, iż określnikami ciągów rozważanych mogą być jedynie: 1) liczba 5; 2) wszystkie liczby pierwsze kształtu $10m\pm1$; 3) wszystkie kombinacje czynników grupy poprzedniej, z powtórzeniami lub bez takowych, i w kombinacji z liczbą 5 w potędze pierwszej.

Tablicę określników, doprowadzoną prawie do 1000, podałem w innym miejscu *). Tamże znajdzie czytelnik dowód tego, co następuje:

Szereg mnożący o określniku 5 nie powiększa liczby ciągów złożonego, jak również nie ma wpływu na ten rezultat potęga czynników, zawartych w danym złożonym. Wogóle, dwom różnym określnikom

$$D=5.\ s^\alpha.\ t^\beta.\ u^\gamma.\ v^\delta\ldots \qquad \text{i} \qquad D_1=s.\ t.\ u.\ v\ldots$$

odpowiada ta sama liczba ciągów, sprzężonych parami **).

Dowodzę też sposobem popularnym ***), że jeśli dany określnik złożony zawiera m różnych czynników pierwszych, nie rachując czynnika 5, to wszystkich ciągów o tym samym określniku mamy 2^m, czyli 2^{m-1} par ciągów sprzężonych. Ponieważ jednak wyrażenie (5) jest prócz tego formą kwadratową, zatym rezultat znaleziony przezemnie wypływa bezpośrednio z teorji tych form, gdzie dowiedziono, iż, mając $N=\alpha.\ \beta.\ \gamma\ldots$ zawierające m czynników pierwszych, możemy N przedstawić w postaci 2^m różnych form kwadrato-

*) Wiadomości Matematyczne. Tom XV. 1911. Str. 239.
**) Tamże. Str. 243—246.
***) *R. Niewiadomski.* Nowyj Metod rozłożenja czisieł na pierwonaczalnyje mnożiteli. Moskwa 1912.

wych, czyli otrzymamy 2^m różnych pierwiastków na a i b, t. j. 2^m różnych ciągów typu Fibonacci'ego.

Gdy D jest liczbą złożoną, niezbędnym jest mieć przynajmniej dwie pary ciągów mu odpowiadających, by zastosować moją metodę rozkładu.

Przypomnę tu, co pokazałem w innym miejscu na przykładzie liczbowym *), w jaki mianowicie sposób z dwuch par ciągów o określnikach d_1 i d_2 otrzymuje się dwie pary nowych ciągów, których określnik równa się $d_1 d_2$. Weźmy $d_1 = 11$ i $d_2 = 19$.

$$d_1 = 11 \begin{cases} \text{zasadniczy: } 1, 4, 5, 9, 14, 23, 37, .. & (\alpha) \\ \text{sprzężony: } 2, 5, 7, 12, 19, 31, 50, ... & (\beta) \end{cases}$$

$$d_2 = 19 \begin{cases} \text{zasadniczy: } 1, 5, 6, 11, 17, 28, 45, ... & (\gamma) \\ \text{sprzężony: } 3, 7, 10, 17, 27, 44, 71, ... & (\delta) \end{cases}$$

$$D = 209; \quad \begin{cases} U_0 = 13, \begin{cases} \text{zasadniczy: } 5, 18, 23, 41, 64, 105, 169, ... & (\varepsilon) \\ \text{sprzężony: } 8, 21, 29, 50, 79, 129, 208, ... & (\zeta) \end{cases} \\ U_0 = 14 \begin{cases} \text{zasadniczy: } 1, 15, 16, 31, 47, 78, 125, ... & (\varkappa) \\ \text{sprzężony: } 13, 27, 40, 67, 107, 174, 281, ... & (\lambda) \end{cases} \end{cases}$$

By uniknąć, o ile to możliwe, otrzymywania wyrazów ujemnych w ciągu złożonym, co mogłoby prowadzić do mimowolnych omyłek w obliczeniach, znalazłem następującą regułę empiryczną na tworzenie się jego wyrazów. Mianowicie: zgodnie z postacią ogólną (7) i zamieszczonym tamże ciągiem (γ) — ciąg złożony (ε) powstaje z ciągu (α) przez spółczynniki ciągu (δ), poczynając od pierwszego; (ζ) powstaje z ciągu (β) przez spółczynniki ciągu (γ), poczynając od trzeciego; ciąg ($\varkappa$) powstaje z (γ) przez spółczynniki ciągu (α), poczynając od pierwszego, i wreszcie (λ) powstaje z ciągu (δ) przez spółczynniki ciągu (β), poczynając od trzeciego. Czyli: przy tworzeniu zasadniczych ciągów złożonych spółczynniki mnożącego ciągu zaczynają się od pierwszego; przy tworzeniu zaś sprzężonych złożonych, spółczynniki zaczynają się od trzeciego.

Gdy będziemy rozważali postać algiebraiczną ciągów, przytoczony przykład przedstawi się jak poniżej

$$(9) \qquad d_1 \begin{cases} k, \quad l, \quad k+l, \quad k+2l, \quad 2k+3l, \ ... & (\alpha) \\ l-2k, \ 2l-3k, \ 3l-5k, \ 5l-8k, \ 8l-13k, \ ... & (\beta) \end{cases}$$

$$d_2 \begin{cases} v, \quad t, \quad v+t, \quad v+2t, \quad 2v+3t, \ ... & (\gamma) \\ t-2v, \ 2t-3v, \ 3t-5v, \ 5t-8v, \ 8t-13v, \ ... & (\delta) \end{cases}$$

*) Wiadomości Matematyczne. Tom XV. 1911. Str. 246—247.

$$D=d_1d_2\begin{cases}(t-2v)l-(2t-3v)k,\ (2t-3v)l-(3t-5v)k,\ (3t-5v)l-(5t-8v)k,\ \ldots & (\varepsilon)\\ (v+t)(2l-3k)-(v+2t)(l-2k),\ (v+2t)(2l-3k)-(2v+3t)(l-2k),\\ \qquad (2v+3t)(2l-3k)-(3v+5t)(l-2k)\ \ldots & (\zeta)\end{cases}$$

$$\begin{cases}kt-lv,\ lt-(k+l)v,\ (k+l)t-(k+2l)v,\ \ldots & (\varkappa)\\ (3l-5k)(2t-3v)-(5l-8k)(t-2v),\ (5l-8k)(2t-3v)-\\ \qquad -(8l-13k)(t-2v),\ (8l-13k)(2t-3v)-(13l-21k)(t-2v),\ \ldots & (\lambda)\end{cases}$$

Tym sposobem, w ciągach algiebraicznych (ε), (ζ), (ϰ), (λ) mamy właśnie tę konstrukcję wyrazów ciągów o określniku złożonym $D=d_1d_2$, która pozwoli nam wynaleźć elementy ciągów o określnikach d_1 i d_2.

Przypuśćmy teraz, że liczbę D kształtu $10m\pm1$ mamy rozłożyć na czynniki pierwsze. Wymaga to przedewszystkim rozwiązania równania kwadratowego nieoznaczonego (5) — i wynalezienia początkowych wyrazów a i b ciągów, odpowiadających danemu określnikowi D

$$b^2-ab-a^2=D \tag{5}$$

Podstawimy w ostatnim równaniu wyrażenie na przedwyraz $U_0=b-a$ i rozwiążemy przekształcone równanie (5a)

$$U_0b-a^2=D \qquad \text{lub inaczej} \qquad U_0(U_0+a)-a^2=D \tag{5a}$$

Wyrażenia na a i b przedstawimy w postaci funkcji zmiennych U_0 i D; mianowicie

$$a=\frac{U_0\pm\sqrt{5U_0^2-4D}}{2} \qquad b=\frac{3U_0\pm\sqrt{5U_0^2-4D}}{2} \tag{10}$$

Znaki (—) przed pierwiastkiem stosują się do ciągu zasadniczego (liczby mniejsze), znaki zaś + do sprzężonego z nim.

Chcąc z (10) otrzymać a i b wymierne, należy dobrać przez próbowanie takie całkowite U_0, abyśmy otrzymali pod pierwiastkiem kwadrat zupełny.

Dobór ten dokonywa się za pomocą tablicy kwadratów. Sądzę, że uprościłem go i udoskonaliłem do możliwych granic, a jednak czynność ta pochłania 80% — 90% czasu, potrzebnego do rozkładu liczby na czynniki pierwsze na podstawie mojej metody.

Poszukiwanie wszystkich całkowitych pierwiastków na U_0 upraszcza się przez warunek

$$U_0<\sqrt{D} \tag{11}$$

dowiedziony już uprzednio *).

---

*) Wiadomości Matematyczne. Tom XV. Str. 241.

Znalazłszy to $max.U_0$ na podstawie (11), obliczamy największą możliwą wartość wyrażenia podpierwiastkowego

$$5(max.U_0)^2-4D=Q \tag{12}$$

Podstawiając następnie liczby kolejne: $max.\ U_0-1$, $max.\ U_0-2$, i t. d., nie mnożymy już za każdym razem przez 5 kwadratu liczby kolejnej w tablicach, by odjąć potym $4D$, lecz dobór próbny sprowadzamy do odejmowania. Mianowicie, ponieważ różnica kwadratów dwuch liczb kolejnych równa się sumie tychże liczb, wystarcza odjąć najprzód od znalezionego Q wielkość $5\{max.U_0+(max.U_0-1)\}$,

$$Q-5\{max.U_0+(max.U_0-1)\}=Q_1 \tag{13}$$

Każdy nowy odjemnik będzie mniejszy od poprzedniego o 10, gdyż suma dwuch liczb kolejnych różni się o 2 od sumy liczb sąsiednich.

Odejmując tym sposobem liczby coraz mniejsze, prowadzimy tę czynność tak długo, aż odejmnik okaże się większym od ostatniej reszty Q_n. Wtedy należy sprawdzić działania arytmetyczne, posiłkując się bezpośrednio zależnością

$$5(minU_0)^2-4D=Q_n \tag{14}$$

Gdy odejmowań jest bardzo wiele, należy to sprawdzenie stosować częściej, np. w każdej zakończonej kolumnie pionowej. Wogóle ilość odejmowań będzie w przybliżeniu $=\frac{max.U_0}{10}+5\%$; czyli np. dla liczby D bliskiej miljonowi, należy wykonać około 105 odejmowań.

Przekonawszy się ze sprawdzenia Q_n według (14), że nie zaszły żadne pomyłki, porównywamy wszystkie reszty: Q, Q_1, Q_2, ... Q_n z tablicą kwadratów, odznaczając te z nich, które się okażą kwadratami zupełnemi. Liczba tych ostatnich powinna być równą 2^k.

Ponieważ otrzymujemy stąd 2^k różnych U_0, które czynią kwadratami zupełnemi wyrażenie podpierwiastkowe (10), zatym wszystkich ciągów typu Fibonacci'ego o tym samym określniku D będzie 2^{k+1}, ze względu że każdemu U_0 odpowiadają dwa ciągi sprzężone. Liczbę więc D można przedstawić w postaci $k+1$ różnych form kwadratowych kształtu (5), czyli zawiera ona $k+1$ różnych czynników pierwszych.

Oczywistym jest, iż metoda niniejsza dostarcza zupełnego sprawdzenia działań arytmetycznych, wykazując jednocześnie liczbę różnych dzielników pierwszych w rozkładanej przez nas liczbie D.

Gdy $k=1$, różnych U_0 będzie 2, i stąd dwa tylko dzielniki. Przy $k=0$, liczba D będzie pierwszą, gdyż $2^0=1$, czyli otrzymujemy jedyne U_0, zamieniające wyrażenie podpierwiastkowe (10) w kwadrat zupełny.

Jeśli się okaże, że żadna z reszt Q nie jest kwadratem zupełnym, oznacza to oczywiście, iż dana liczba D, jakkolwiek kształtu $10m\pm1$, nie może być jednak określnikiem żadnego ciągu typu Fibonaccie'go. Zatym musi ona zawierać czynniki postaci $10m\pm3$. Taka liczba n i e o k r e ś l n i k o w a (lub mieszana) będzie bezwątpienia złożoną, gdyż czynniki kształtu $10m\pm3$ muszą znaleźć się co najmniej w liczbie dwuch, by iloczyn ich otrzymał postać $10m\pm1$.

Znaleźliśmy zatym 2^k różnych U_0. Stosownie do ich wartości liczbowej, na zasadzie wzorów (10) układamy 2^{k+1} różnych ciągów typu Fib. Wystarczy przytym obliczyć jedynie ich pierwsze wyrazy a, by rozwiązać zajmujące nas zagadnienie. Obieramy następnie dowolne dwie pary ciągów sprzężonych, bacząc by wyrazy a były liczbami możliwie małemi. Oznaczmy wielkości na a w jednej parze ciągów przez f i g, w drugiej przez h i i i przyrównajmy do nich wyrażenia (9) na pierwsze wyrazy ciągów (ε), (ζ), (κ), (λ). Otrzymamy wtedy cztery równania algiebraiczne

$$\begin{gathered}(t-2v)l-(2t-3v)k=f\\(v+t)(2l-3k)-(v+2t)(l-2k)=g\\kt-lv=h\\(3l-5k)(2t-3v)-(5l-8k)(t-2v)=i\end{gathered}\tag{15}$$

Rozwiązując je, znajdziemy

$$\begin{aligned}lv&=\frac{f+4g-4h-i}{5} & vk&=\frac{2f+3g-3h-2i}{5}\\kt&=\frac{f+4g+h-i}{5} & tl&=\frac{3f+7g+3h+2i}{5}\end{aligned}\tag{16}$$

Wszystkie liczniki w (16) dzielić się powinny przez 5. Łatwo sprawdzić, że wszystkie one są porównalne względem modułu 5; zatym, gdy jeden okaże się wielokrotnością 5-iu, zachodzi to samo i dla reszty liczników. Wystarczy więc najprostszy z nich (np. w wyrażeniu na kt) poddać podstawianiu próbnemu, które w danym wypadku konieczne jest z tego względu, że oznaczenie literami f, g i h, i pierwszych wyrazów a w obranych przez nas ciągach — było w gruncie rzeczy tymczasowo dowolnym. Niewiadomo bowiem a priori z wyrażeń (9), które mianowicie z ciągów (α), (β), (γ), (δ) okażą się mnożącemi, a które mnożonemi, które zasadniczemi a które sprzężonemi.

Jeśli licznik wyrażenia na kt nie dzieli się przez 5, to należy zastosować litery f i g do drugiej pary ciągów obranych, litery zaś h i i do pierwszej. Gdy i to nie pomoże, należy w jednej lub obu parach ciągów przestawić te oznaczenia literowe z szeregu zasadniczego do sprzężonego i odwrotnie. W rezultacie jedna z tych kombinacji okaże się niewątpliwie trafną. Co do tego łatwo się przekonać, wziąwszy zamiast licznika $(f+4g+h-i)$ porównalne z nim względem modułu 5 wyrażenie $(f-g+h-i)$ i podstawiając z (9) znaczenia na f, g, h, i. Otrzymamy wtedy ostatecznie $5v(k-l)$, czyli wielokrotność 5-iu.

Dobór ten próbny wykonywa się bardzo szybko, gdyż nie obliczamy za każdym razem całkowitej wartości na kt, lecz orjentujemy się według ostatnich cyfr liczb f, g, h, i, aby przekonać się, przy jakiej kombinacji oznaczeń ostatnia cyfra licznika kt będzie 5 lub 0.

Znajdujemy tym sposobem na podstawie (16) wartości liczbowe na lv, kt, vk i tl. Będą one bardzo małemi liczbami w porównaniu z D, i bez trudności najmniejszej dobierzemy z nich natychmiast liczby całkowite na

k, l, v, t, będące czynnikami poprzednich. Że zaś są one jednocześnie wyrazami początkowemi ciągów (α) i (β) w (9), obliczywszy więc określniki d_1 i d_2 tych ciągów, otrzymamy dwa gotowe czynniki liczby D.

Gdy liczba D zawiera kilka dzielników pierwszych, wówczas jedna z liczb d_1 i d_2, lub też obie mogą okazać się złożonemi. Z taką nową liczbą złożoną postępujemy zupełnie analogicznie, jak dotąd z liczbą D. Lecz otrzymane d_1 i d_2 są bez porównania mniejszemi od D, i na rozkład ich dalszy wystarczy kilka minut czasu.

Rezultat ten można osiągnąć inną drogą. Zamiast prowadzić rozkład liczb d_1 i d_2 za pomocą metody, zastosowanej do liczby D, zauważmy, iż mamy do rozporządzenia $k+1$ ciągów, z których dotąd wyzyskaliśmy tylko cztery. Biorąc dwie inne pary ciągów, otrzymamy rozkład liczby D na dwa inne czynniki d_3 i d_4, przyczym naturalnie

$$d_1 d_2 = d_3 d_4 .$$

Znajdując największe wielokrotne czynników po obie strony tej równości, będziemy już w posiadaniu 3-ch lub 4-ch dzielników różnych liczby D, i t. d.

Zdarzyć się może, że gdy wymnożymy wszystkie otrzymane czynniki proste rozkładu i podzielimy D przez ich iloczyn, to iloraz okaże się większym od 1. Jest to zrozumiałe, gdyż potęga czynników, zawartych w D nie wpływa na liczbę odpowiadających mu ciągów. Zatym, iloraz ewentualny będzie się dzielił jedynie przez czynniki już znalezione.

Cały przebieg czynności powyższej objaśnimy teraz na przykładzie liczbowym. Rozłóżmy np. liczbę $D=638219$ na czynniki pierwsze.

Na podstawie nierówności (11), znajdujemy $max.\ U_0=798$. Za pomocą wyrażenia (12) obliczamy resztę Q

$$5 \times \overline{798}^2 - 4 \times 638219 = 631144 = Q .$$

Zgodnie z (13), należy odjąć od otrzymanego Q

$$5(798+797)=7975 .$$

Reszta będzie $Q_1=623169$. Odejmujemy od niej 7965; od nowej reszty odejmujemy 7955 i t. d., jak to widać poniżej:

631144	465769	304804	148249
7975	7765	7555	7345
623169	458004	297249	140904
7965	7755	7545	7335
615204	450249	289704	133569
7955	7745	7535	7325
607249	442504	282169	126244
7945	7735	7525	7315
599304	434769	274644	118929

599304	434769	274644	118929
7935	7725	7515	7305
591369	427044	267129	111624
7925	7715	7505	7295
583444	419329	259624	104329 *
7915	7705	7495	7285
575529	411624	252129	97044
7905	7695	7485	7275
567624	403929	244644	89769
7895	7685	7475	7265
559729	396244	237169 *	82504
7885	7675	7465	7255
551844	388569	229704	75249
7875	7665	7455	7245
543969	380904	222249	68004
7865	7655	7445	7235
536104	373249	214804	60769
7855	7645	7435	7225
528249	365604	207369	53544
7845	7635	7425	7215
520404	357969	199944	46329
7835	7625	7415	7205
512569	350344	192529	39124
7825	7615	7405	7195
504744	342729	185124	31929
7815	7605	7395	7185
496929	335124	177729	24744
7805	7595	7385	7175
489124	327529	170344	17569
7795	7585	7375	7165
481329	319944	162969	10404 *
7785	7575	7365	7155
473544	312369	155604	3249 *
7775	7565	7355	
465769	304804	148249	

Wszystkich odejmowań wykonaliśmy tu 83. Zatym

$$min.\ U_0 = 798 - 83 = 715\ .$$

Otrzymane $min.\ U_0$ służy do sprawdzenia ostatniej reszty, t. j. powinna zachodzić równość

$$5 \times \overline{715}^2 - 4 \times 638219 = 3249\ .$$

Przedtym jeszcze, w trakcie wykonywania odejmowań, sprawdzamy tą samą drogą reszty na końcu każdej kolumny. Że zaś mamy w kolumnie 21 odejmowań, należy w wyrażenie podpierwiastkowe (10) wstawiać za U_0 liczby: 777, 756 i 735.

Zwrócimy tu uwagę, że odejmowania powyższe możemy zastąpić przez dodawania, wychodząc z *min.* $U_0=715$, które łatwo wyszukamy przy pomocy tablicy kwadratów, i orjentując się według wskazanej powyżej ogólnej przybliżonej liczby wszystkich odejmowań oczekiwanych. Pierwsza dodajna będzie się równała $5(715+716)=7155$; każda następna będzie większa o 10 od poprzedniej. Szereg kolejnych dodawań powinien nas doprowadzić do sumy $Q=631144$.

Po sprawdzeniu odejmowań (czy też dodawań), przekonywamy się, że śród naszych reszt istnieją cztery kwadraty zupełne. Oznaczone są one gwiazdkami i równają się: 487^2, 323^2, 102^2 i 57^2. Odpowiadające im przedwyrazy U_0 będą: 747, 729, 716 i 715 — co łatwo się wynajduje przez obliczanie ogólnej liczby odejmowań, wykonanych od samego początku.

W danym przypadku $4=2^2$, t. j. $k=2$, a więc liczba D zawiera trzy czynniki pierwsze. Wszystkich ciągów o określniku $D=638219$ będzie 8; otrzymamy je łatwo na podstawie wzorów (10). Mianowicie

$$\begin{array}{llll} U_0=747 \begin{cases} 130, & 877, \ldots \\ 617, & 1364, \ldots \end{cases} & & U_0=729 \begin{cases} 203, & 932, \ldots \\ 526, & 1255, \ldots \end{cases} \\ U_0=716 \begin{cases} 307, & 1023, \ldots \\ 409, & 1125, \ldots \end{cases} & & U_0=715 \begin{cases} 329, & 1044, \ldots \\ 386, & 1101, \ldots \end{cases} \end{array} \qquad (17)$$

Z pomiędzy (17) obierzmy dwie pary górne ciągów, i zgodnie z układem równań (15)— oznaczmy: $f=130$, $g=617$, $h=203$, $i=526$. Przy pomocy wzorów (16) znajdujemy

$$lv=252; \quad kt=455; \quad vk=90; \quad tl=1274.$$

Stąd oczywiście

$$k=5, \quad v=18, \quad t=91, \quad l=14$$

czyli poszukiwane ciągi czynnikowe (α) i (γ) w (9) będą

$$\begin{array}{lll} 5, & 14, & 19, \quad 23, \ldots \qquad d_1=101 \\ 18, & 91, & 109, \quad 200, \ldots \qquad d_2=6319. \end{array}$$

A więc 101 jest jednym z czynników pierwszych liczby 638219; iloczyn dwuch innych równa się 6319.

Obierzmy z pomiędzy (17) dwie pary ciągów lewych, i oznaczmy: $f=307$, $g=409$, $h=617$, $i=130$. Wzory (16) dadzą

$$lv=-131; \quad kt=486; \quad vk=-54; \quad tl=1179.$$

Skąd

$$v=-1; \quad k=54; \quad t=9; \quad l=131$$

a same ciągi czynnikowe będą

$$\begin{array}{llll} 54, & 131, & 185, & 316, \ldots \qquad d_3=7171 \\ -1, & 9, & 8, & 17, \ldots \qquad d_4=89 \end{array}$$

Otrzymaliśmy więc drugi czynnik poszukiwany 89. Trzeci znajdzie się już łatwo jako 71. Dość jest podzielić d_2 przez d_4 lub też d_3 przez d_1.

Gdybyśmy zaś rozkładali liczbę $d_2=6319$ za pomocą metody ogólnej, to rezultat byłby równie szybki.

Odpowiednie jej *max.* $U_0=79$ i reszta Q

$$5\times 79^2-4\times 6319=5929=Q\ .$$

Wykonamy następnie odejmowania, poczynając od $5(79+78)=785$

5929 *	2849
785	745
5144	2104
775	735
4369	1369 *
765	725
3604	644
755	
2849	

Dwie z reszt powyższych są kwadratami zupełnemi: $5929=77^2$ i $1369=37^2$. Odpowiednie U_0 równają się: 79 i 73 i na podstawie (10) ciągi odnośne

$$U_0=79\ \begin{cases} 1,\ 80,\ 81,\ \ldots \\ 78,\ 157,\ 235,\ \ldots \end{cases} \qquad U_0=73\ \begin{cases} 18,\ 91,\ 109,\ \ldots \\ 55,\ 128,\ 183,\ \ldots \end{cases}$$

Oznaczając: $f=1$, $g=78$, $h=55$, $i=18$, znajdujemy według (16)

$$lv=15;\quad kt=70;\quad vk=7:\quad tl=150$$

czyli

$$k=7,\quad v=1,\quad t=10,\quad l=15$$

i napiszemy ciągi czynnikowe, obliczając ich określniki

$$7,\ 15,\ 22,\ 37,\ \ldots \qquad d_3=71$$
$$1,\ 10,\ 11,\ 21,\ \ldots \qquad d_4=89.$$

Wybór tego lub innego sposobu zależy od wielkości liczby rozkładanej, od ilości ogólnej zawartych w niej czynników pierwszych, większej lub też mniejszej złożoności pierwszej pary d_1 i d_2 znalezionych dzielników. Wogóle łatwo zorjentować się, który z nich należy zastosować.

Z przytoczonego przykładu liczbowego widoczne są korzyści zastosowania metody tu wyłożonej. Wszystkie czynniki pierwsze otrzymujemy jako liczby g o t o w e, nie zaś za pomocą dzielenia próbnego liczby danej przez liczby, znalezione drogą uboczną, jako możliwe jej czynniki. I l o ś ć zawartych w liczbie badanej czynników pierwszych wskazujemy a priori. Wreszcie co do s z y b k o ś c i rozwiązania, to przeciętnie robi się cztery odejmowania na minutę. Posiłkując się zaś arytmometrem, można to przyspieszyć 2 do 3-ch razy, przyczym jedna osoba działa arytmometrem, a druga porównywa otrzymane reszty z tablicą kwadratów. Gdy liczba okaże się złożoną, to na

wszelkie czynności pozostałe, jakoto: ułożenie odpowiadających jej ciągów, układu równań (16), znalezienie ciągów czynnikowych, dość jest 10 — 15 minut, zależnie od wielkości liczby rozkładanej i liczby jej czynników pierwszych. Np. w celu zbadania liczby Czebyszowa $D=8520191$ należy wykonać 307 odejmowań, co wymaga około 80 minut, (z arytmometrem najwyżej 30 min.). Okaże się przytym, że jedna tylko reszta 58081 jest kwadratem zupełnym, więc liczba badana jest pierwszą, i żadnych więcej już z nią czynności niema potrzeby wykonywać. Również np. dla liczby 1 111 111 znajduję w ciągu 30 min. bez arytmometru czynniki jej 239×4649.

Największą zbadaną przezemnie liczbą był wyraz 37-y szeregu 1, 3, 4, 7, 11, ... który proponuję nazywać szeregiem R, by go wyodrębnić ze względu na pewne specjalne własności.

$$U_{37}^{R} = U_{37}^{F} + U_{39}^{F} = 54018521 .$$

Liczba ta jest pierwszą. Wszystkich odejmowań było 772, co wykonałem w ciągu 70 minut przy pomocy arytmometru. Tablica kwadratów I. Claudela pozwala na rozkładanie liczb określnikowych do wielkości około 100 miljonów, i cała metoda moja zależną jest od dokładnej a obszernej tablicy kwadratów.

Pozwolę tu powołać się na taką powagę w teorji liczb, jak E. Lucas (Théorie des Nombres. 1891. Str. 36), który powiada: „Tablica kwadratów pozwala na ogromne uproszczenie rachunków arytmetyki; nie wątpię, że tablica ta była w rękach Fermata cudownym narzędziem obserwacyjnym w jego poszukiwaniach arytmetycznych i punktem wyjścia jakiejś szybkiej, dziś prawie nieznanej metody rozkładania liczb na czynniki pierwsze“.

Otóż zdaje mi się, iż rezultaty metody mojej wskrzeszają w tym względzie powagę tablicy kwadratów i uchylają rąbek owej tajemniczej zasłony.

Do dalszej pracy nad tą kwestją wzywam matematyków kompetentniejszych odemnie, sam badań tych nie zarzucając. Jest do zrobienia jeszcze bardzo wiele; mianowicie należy: 1) wynaleźć formę ogólną dla liczb nieokreślnikowych, poczym łatwo będzie stworzyć metodę ich rozkładu; 2) znaleźć krótszy od mego sposób oddzielania czynników określnikowych od nieokreślnikowych w liczbie badanej; 3) może uda się komu odkryć jeszcze szybszy sposób na wynajdywanie całkowitych U_0 w wiadomym nam wyrażeniu podpierwiastkowym, by uniknąć ogromnej ilości odejmowań, koniecznych, jak dotąd, przy rozkładzie liczb bardzo wielkich.

R. Niewiadomski.