A. ŁAPAREWICZ.

Tabelka do pośpiesznego rozkładu liczb na czynniki pierwsze.

Gaston Tarry. Tablettes des cotes relatives à la base 20580 des facteurs premiers d'un nombre inférieur à N et non divisible par 2, 3, 5 ou 7. I partie, $N = 317^2 = 100489$. Paris. Gauthier-Villars. 1906.

Dotychczasowe tablice czynników w układzie Burckharda w porównaniu z pierwotnemi tablicami, układanemi według t. zw. „sita Eratostenesa“ bez żadnych nastręczających się uproszczeń, stanowiły tak wybitny krok naprzód, że gdy co do tych ostatnich Euler wyrażał powątpiewanie, by ktokolwiek szereg liczb naturalnych doprowadził w nich kiedy choćby tylko do miliona, tablice Burckharda, obejmujące pierwotnie trzy miliony liczb naturalnych, z czasem przez Dasego rozszerzone zostały do dziewięciu miljonów. Stokroć większe uproszczenie w tym względzie wprowadza nowa tabelka Tarrye'go, stanowiąca początek całego prawdopodobnie szeregu tablic analogicznych. Za pomocą tej tabelki, umieszczonej na dwóch pełnych i czterech ponacinanych stronicach, obejmujących 5856 według pewnego sposobu otrzymanych liczb, można bardzo prostym rachunkiem odnaleść czynniki wszystkich liczb mniejszych od 100489, tak iż wystarczy ułożyć jeszcze sześć dalszych tabelek tego rodzaju, aby szereg liczb pierwszych doprowadzić do 3000, t. j. zawrzeć w nich cały materyał, mieszczący się w ogromnym tomie tablic Dasego. Gdy jednak te ostatnie zawierają czynniki jedynie pierwszych 9 milionów liczb naturalnych, przy pomocy wspomnianych siedmiu tabelek Tarry'ego będziemy mogli określić skład i każdej liczby przenoszącej 9 milionów, o ile w tym składzie mieszczą się czynniki nie większe

nad 3000. Słowem, tabelka Tarry'ego w zakresie tablic, podających pierwsze czynniki liczb naturalnych, tem jest niemal, czem tabelki Wrońskiego w zakresie tablic logarytmowych.

Znaczenie to jeszcze się potęguje przez to, że jest zbudowana na nadzwyczaj prostej zasadzie.

Przedewszystkiem zauważyć należy, że przystępując z jej pomocą do rozkładu danej liczby, winniśmy się zawczasu przekonać o niepodzielności tejże przez najmniejsze liczby pierwsze; czynniki takie bowiem najczęściej się przytrafiają, przytem, jak słusznie zauważył Gauss w kwestyi pokrewnej, przykrem i niewłaściwem jest stosowanie całego zasobu najrozmaitszych twierdzeń z teoryi liczb do odnajdywania takich czynników, które niejednokrotnie, dzięki znanym cechom podzielności, same się w oczy rzucają.

Oznaczmy więc takie liczby pierwsze, nie będące czynnikami danej do rozkładu liczby N, przez $p_1, p_2, \ldots p_i$, poczem utworzywszy z nich liczbę $p_1^{\pi_1} p_2^{\pi_2} \ldots p_i^{\pi_i} = A$ (zwaną zasadą tabelki, do której w następstwie przejdziemy), oznaczmy przez m iloraz, i przez ϱ resztę z dzielenia N przez A, tak iż:

$$N = Am + \varrho. \tag{1}$$

Co do ϱ, to można za nią przyjąć tak najmniejszą dodatnią, jako też i bezwzględnie dodatnią resztę liczby N według mod. A; w pierwszym razie $\varrho < A$, w drugim $|\varrho| < \frac{A}{2}$. Ponieważ N i A są, według założenia, niespółdzielne, przeto i $|\varrho|$ jest liczbą niespółdzielną z A, tak iż ϱ może przybierać jednę z $\varphi(A)$ lub $\varphi\left(\frac{A}{2}\right)$ wartości.

By sprawdzić podzielność liczby N przez jakąkolwiek liczbę pierwszą p, różną od zaznaczonych wyżej i liczb pierwszych, jako więc taką niespółdzielną z A, zauważmy, że wskutek tej niespółdzielności można zawsze znaleść taką liczbę a, któraby zadość czyniła kongruencyi:

$$aA \equiv 1 \pmod{p}, \tag{2}$$

a tem samem również z p była niespółdzielną.

Mnożąc teraz stronami równość (1) przez a i kładąc:

$$a\varrho \equiv \mathfrak{r} \pmod{p}, \tag{3}$$

gdzie przez r rozumiemy bezwzględnie najmniejszą resztę liczby $a\varrho$ według mod. p, znajdziemy:

$$aN \equiv m + r \pmod{p}, \tag{4}$$

skąd czytamy, że jeżeli:

$$m + r \equiv 0 \pmod{p}, \tag{5}$$

wtedy $aN \equiv 0 \pmod{p}$, czyli wskutek niespółdzielności liczb a i p:

$$N \equiv 0 \pmod{p}. \tag{6}$$

Przypuśćmy, że dla różnych wartości na ϱ i p określiliśmy odpowiednie wartości na r, zestawiając je w tabelce dwuwejściowej. Mając dla danej liczby N, wobec stałej przyjętej zasady A, określoną wartość na ϱ, w powyższej tabelce w kolumnie, mającej tę wartość $|\varrho|$ w nagłówku, i w wierszu odpowiadającym określonej wartości na p, znajdziemy wartość na r, odpowiadającą kongruencyi (5); wtedy, według (4), liczba pierwsza p będzie szukanym czynnnikiem danej N.

Ponieważ liczba kolumn w takiej tabelce powinna wynosić $\varphi(A)$ lub $\varphi\left(\frac{A}{2}\right)$, za zasadę A winniśmy przyjmować liczbę niezbyt dużą, lecz w takim razie liczba m bywa znaczną, co znów utrudnia sprawdzanie kongruencyi (5), które, o ile możności, wykonywać należy w pamięci.

By więc pozostać w zakresie małych wartości na m, a jednocześnie nie powiększać zbytnio liczby kolumn, weźmy jeszcze pomocniczą zasadę B, stanowiącą jeden z czynników dawnej zasady A, i podzielmy znów $|\varrho|$ przez B, otrzymując $|\varrho| = Bq + r$, gdzie $r < B$ lub $|r| < \frac{B}{2}$, poczem kładąc $Bqa \equiv Q$, $ra \equiv R \pmod{p}$, zamiast (4) przyjdziemy do kongruencyi:

$$aN \equiv m \pm (Q + R) \pmod{p}, \tag{4a}$$

czyli:

$$\pm aN \equiv \pm m + (Q + R) \pmod{p}, \tag{4b}$$

zachowując znak górny lub dolny, stosownie do tego, czy reszta ϱ była dodatnią czy ujemną. W ten więc sposob o podzielności lub

niepodzielności liczby N przez p sądzimy teraz ze stosunku m względem dwóch liczb Q i R.

Druga z nich R względem ϱ, przy liczbie zasadniczej B, ma takież samo znaczenie co i dawna reszta r względem N przy zasadzie A wartości więc jej, odpowiadające różnym wartościom na r i p, zawarte będą w $\varphi(B)$ lub $\varphi\left(\frac{B}{2}\right)$ kolumnach tabelki, o której mowa była powyżej. Dla Q zaś możemy utworzyć podobnąż tabelkę z tą tylko różnicą, że zamieszczać w niej będziemy bezwzględnie najmniejsze według mod. p reszty nie wielokrotności ϱ, lecz Bu, o spółczynnikach dowolnych z szeregu liczb naturalnych.

By uniknąć, przy sprawdzaniu kongruencyi (4b), potrzeby zmiany znaków odczytanych w powyższej tabelce wartości na R i Q, umówmy się, że tylko w wyrażeniu na N uważać będziemy ϱ za resztę bezwzględnie najmniejszą, w wyrażeniu zaś na ϱ przyjmiemy r za resztę najmniejszą dodatnią. Jeżeli nadto się umówimy, że obie tabelki, tak dla R jako i dla Q, mają zawierać po równej liczbie kolumn, czyli po $\varphi(B)$, skutkiem czego za największą wartość q przyjmiemy $\varphi(B)$, to największą wartość na $|\varrho|$ określimy jako $B\varphi(B)+r<B(\varphi(B)+1)$, że zaś, według poprzedniej umowy, $|\varrho|<\frac{A}{2}$, najwłaściwiej i najprościej więc przyjąć: $A=2B(\varphi(B)+1)$.

Przypuśćmy teraz, że kolumny, z których każda dla pewnej wartości na q podaje szereg wartości na Q, odpowiadających kolejnym p, są ruchome, tak iż każdą z nich można umieścić obok odpowiedniej kolumny, podającej przy pewnem r wartości R dla kolejnych p; wtedy jednoczesne wartości na P i Q, które kłaść należy w kongruencyę (4b), znajdą się tuż obok siebie, dzięki czemu sprawdzenie tej kongruencyi będzie wielce ułatwione.

Z szeregu liczb pierwszych najmniejszych, o których wspomniano tu na samym początku, Tarry przyjął 2, 3, 5 i 7, tworząc z nich $B=210$, poczem zważając, że $\varphi(B)=48$, otrzymał $A=2.210.49=20580$. Łatwo zauważyć, że, o ile poprzestajemy na tych 4 co najwyżej liczbach pierwszych, na A otrzymamy liczbę, nie zawierającą innych czynników. Obie tabelki na R i Q zawierają po 48 kolumn, mieszczących dla poszczególnych r i q wartości R i Q, odpowiadające kolejnym liczbom pierwszym, których szereg, poczynając od $p=11$,

w obecnej tabelce Tarry doprowadził do $p=313$. Kolumny na R (nieruchome) mają w nagłówku jednę z 48 liczb, mniejszych od 210 i z 210 niespółdzielnych, na Q zaś (ruchome) jednę z liczb od 1 do 48: idą zaś po sobie w ten sposób, że nagłówkowe ich liczby w pierwszej tabelce dopełniają się do 210, w drugiej do 49, tak iż obok kolumn z nagłówkami r i q mamy w nich odpowiednio kolumny $210-r$ i $49-q$; przy takim bowiem porządku kolumn, z dwóch sąsiednich wartości na R i Q, jako tworzących sumy kongruentne według mod.p z liczbami stałemi 210 w pierwszym i 210.49 w drugim razie, wystarczy jednę z nich znaleźć bezpośrednim rachunkiem, poczem drugą otrzymamy przez proste odejmowanie; w ten więc sposób rachunek przy układaniu tabelki zmniejsza się o połowę. Wreszcie co do tabelki ruchomej (na Q), to ona pomiędzy dwiema takiemi dopełniającemi się kolumnami zawiera kolumnę kolejnych liczb pierwszych (NP), dwie zaś sąsiednie takie trójki kolumn przedzielone są kolumną wyciętą którą umieścić należy na miejscu odpowiedniej kolumny tabelki nieruchomej.

Aby układ i sposób użycia tabelki Tarry'ego dokładniej wyjaśnić, przytaczam tu ją w formie zmniejszonej, biorąc za zasadę liczbę złożoną nie z 4, lecz tylko z 3 liczb pierwszych: 2, 3 i 5, mianowicie: $B=30$, $\varphi(B)=8$ i $A=540$:

NP	1	29	7	23	11	19	13	17
7	1	1	0	2	4	$\overline{2}$	$\overline{1}$	3
11	1	$\overline{4}$	$\overline{4}$	1	0	$\overline{3}$	2	$\overline{5}$
13	2	6	1	$\overline{6}$	$\overline{4}$	$\overline{1}$	0	$\overline{5}$
17	4	$\overline{3}$	$\overline{6}$	7	$\overline{7}$	8	1	0
19	$\overline{7}$	6	8	$\overline{9}$	$\overline{1}$	0	4	$\overline{5}$
23	$\overline{2}$	11	9	0	1	8	$\overline{3}$	$\overline{11}$

Tabelka wartości R.

1	NP	8		2	NP	7		3	NP	6		4	NP	5
2	7	2		$\overline{3}$	7	0		$\overline{1}$	7	$\overline{2}$		1	7	3
$\overline{3}$	11	$\overline{2}$		5	11	1		2	11	4		$\overline{1}$	11	$\overline{4}$
$\overline{5}$	13	$\overline{1}$		3	13	4		$\overline{2}$	13	$\overline{4}$		6	13	1
1	17	8		2	18	7		3	17	6		4	17	5
$\overline{1}$	19	$\overline{8}$		$\overline{2}$	19	$\overline{7}$		$\overline{3}$	19	$\overline{6}$		$\overline{4}$	19	$\overline{5}$
9	23	3		$\overline{5}$	23	$\overline{6}$		4	23	8		$\overline{10}$	23	$\overline{1}$

Tabelka wartości Q.

Przykład 1. $N=731$, $m=1^+$ (w ten sposób zaznaczać będziemy. że $\varrho > 0$); $q=6$, $r=11$. Dla $p=17$ mamy $Q=6$, $R=-7$, tak iż $m+(Q+R)=0$ (mod. 18), co dowodzi, że dana liczba podzielna jest przez 17; jakoż $731=17.43$.

Przykład 2. $N=10013$, $m=19^-(\varrho<0)$; $q=8$, $r=7$. Dla $p=17$ mamy $Q=8$, $R=-6$, tak iż $-m+(Q+R)\equiv 0$ (mod. 17); dla $p=19$, $Q=-8$, $R=8$, również $-m+(Q+R)\equiv 0$ (mod. 19), $10013=17.19.31$.

W ogóle, aby przy pomocy tabelki Tarry'ego określić skład danej liczby, winniśmy naprzód podzielić ją przez 20580, otrzymany zaś iloraz m oznaczyć znakiem + lub —, stosownie do tego, czy na liczebnie najmniejszą resztę otrzymamy liczbę dodatnią czy ujemną; powyższą resztę podzielić znów przez 210, otrzymując q i r; kolumnę q tabelki ruchomej przesunąć do kolumny r tabelki nieruchomej, kolejne ich liczby Q i R kładąc w wyrażeniu $\pm m+(Q+R)$, dopóki nie sprawdzi się kongruencya (4b), wyznaczając czynnik szukany p, lub też nie wyczerpiemy całego szeregu zawartych w tabelce liczb pierwszych.

Zaznaczyć wreszcie należy, że gdy $m>p$, można m zastąpić przez najmniejszą jej dodatnią resztę według mod. p; w obecnej tabelce, którą autor przeznacza dla liczb <100489, przypadek ten nie zachodzi. W dalszych jednak tabelkach autor zamierza wprowadzić jeszcze dodatkowe kolumny do podobnej zamiany liczby m.

Przypisek. W czasopiśmie „L'Enseignement mathématique“ t. IX str. 185—191 E. Lebon opisuje ułożoną przez siebie jeszcze w r. 1905, tabelkę wartości R dla $A=30030=2.3.5.7.11.13$, która jak z powyższego wynika, może jedynie mieć znaczenie jako pierwowzór obecnej tabelki Tarry'ego.