O PEWNEM TWIERDZENIU Z TEORYI LICZB.

PODAŁ

L. BIRKENMAJER.

Zajmując się pewnemi kwestyami fizyki teoretycznej, natrafiłem na ciekawe twierdzenie z teoryi liczb, którego nie zdołałem znaleść w żadnem dziele zajmującem się teoryą liczb i które z tego powodu uważam za nowe [1]). Dotyczy ono własności liczb t. z. pierwszych (absolute Primzahlen) i to w tym stopniu, że jest ono prawdziwem lub nie, według tego, czy stosujemy je do liczb pierwszych czy też niepierwszych (złożonych).

Twierdzenie. Jeżeli p jest liczbą pierwszą większą niż 3, wówczas licznik ułamka (niewłaściwego) równego sumie

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1}$$

jest podzielnym przez p^2; i odwrotnie: żadna liczba złożona nie posiada tej własności.

Wiadomo, że jeżeli p jest liczbą pierwszą, to suma

$$1^m+2^m+3^m+\ldots+\left(\frac{p-1}{2}\right)$$

dla całkowitego i parzystego $m < p-1$, jest podzielną przez p.

Sposobem analogicznym do dowodu twierdzenia Wilsona można dowieść łatwo prawdziwości kongruencyj:

[1]) Własność, podaną tu przez p. Birkenmajera, udowodnił odmiennie w r. 1890 E. Allardice w „Proceedings" Towarzystwa Edynburskiego, XVII, str. 16—19: On some theorems in the theory of numbers. (Przyp. Redakcyi).

$$1.3.4.5\ldots(p-3)(p-1)\equiv 4^{\frac{p-3}{2}}=(2^2)^{\frac{p-3}{2}}=2^{p-3}\quad(\text{mod. } p),$$

lub

$$\frac{(p-1)!}{2\,(p-2)}\equiv 2^{p-3}\quad(\text{mod. } p);$$

$$1.2.4.5\ldots(p-4)(p-2)(p-1)\equiv 9^{\frac{p-3}{2}}=(3^2)^{\frac{p-3}{2}}=3^{p-3}\quad(\text{mod. } p),$$

lub

$$\frac{(p-1)!}{3\,(p-3)}\equiv 3^{p-3}\quad(\text{mod. } p);$$

$$\frac{(p-1)!}{4\,(p-4)}\equiv 4^{p-3};\quad \frac{(p-1)!}{5\,(p-5)}\equiv 5^{p-3};\ldots;\ \frac{(p-1)!}{\frac{p-1}{2}\cdot\frac{p+1}{2}}\equiv\left(\frac{p-1}{2}\right)^{p-3}(\text{mod. } p).$$

Dodając do siebie wszystkie te kongruencye i dołączając do nich jeszcze tożsamość $\frac{(p-1)!}{1\,(p-1)}=\frac{(p-1)!}{1\,(p-1)}$, otrzymujemy:

$$(p-1)!\left[\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\frac{1}{3(p-3)}+\ldots+\frac{1}{\frac{p-1}{2}\cdot\frac{p+1}{2}}\right]$$

$$\equiv\frac{(p-1)!}{(p-1)}+2^{p-3}+3^{p-3}+\ldots+\left(\frac{p-1}{2}\right)^{p-3}\quad(\text{mod. } p).$$

Oznaczmy lewą stronę krótko głoską P, to będzie

$$(p-1)\,P\equiv[(p-1)!+1]+(p-1)\left[2^{p-3}+3^{p-3}+\ldots+\left(\frac{p-1}{2}\right)^{p-3}\right]$$

$$-\,1^{p-3}\ (\text{mop. } p)\equiv[(p-1)!+1]+p\left[2^{p-3}+\ldots+\left(\frac{p-1}{2}\right)^{p-3}\right]$$

$$-\left[1^{p-3}+2^{p-3}+3^{p-3}+\ldots+\left(\frac{p-1}{2}\right)^{p-3}\right]\quad(\text{mod. } p),$$

a że pierwszy wyraz po prawej stronie jest podzielnym przez p na mocy twierdzenia Wilsona, drugi zaś i trzeci są również podzielne przez p ($(p-3)$ jest liczbą parzystą $<(p-1)$), przeto ostatecznie dla $p>3$:

$$(p-1)\,.\,P\equiv 0\quad(\text{mod. } p),$$

t. j.

$$P\equiv 0\quad(\text{mod. } p),$$

gdyż całkowite p i $(p-1)$ są oczywiście niespółmierne.

Jeżeli wreszcie w otrzymanej kongruencyi

$$(p-1)!\left[\frac{1}{1\,(p-1)}+\frac{1}{2\,(p-2)}+\frac{1}{3\,(p-3)}+\ldots+\frac{1}{\frac{p-1}{2}\cdot\frac{p+1}{2}}\right]\equiv 0 \pmod{p}$$

rozłożymy każdy wyraz wewnątrz klamry według wzoru $\frac{1}{r(p-r)}$ $=\frac{1}{p}\left(\frac{1}{r}+\frac{1}{p-r}\right)$, to znajdziemy

$$\frac{(p-1)!}{p}\left[\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1}\right]\equiv 0 \quad (\mathrm{mod.}\ p),$$

t. j.

$$(p-1)!\left[\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1}\right]\equiv 0 \quad (\mathrm{mod.}\ p^2),$$

a to stanowi właśnie zapowiedziane twierdzenie. Gdy bowiem $(p-1)!$ nie może być podzielnem przez p, a tem mniej przez p^2, gdy p jest liczbą pierwszą, musi p^2 być dzielnikiem licznika L w ułamku $\frac{L}{M}$, jaki otrzymujemy z dodania $(p-1)$ ułamków $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{p-1}$.

Pozostaje jeszcze wykazać, że powyższa własność przestaje istnieć dla liczb złożonych. Jakoż istotnie, przypuszczając p złożonem i oznaczając przez λ największy z jej pierwszych dzielników, doszlibyśmy do wniosku że wyrażenie

$$(p-1)!\left[\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\frac{1}{3(p-3)}+\ldots+\frac{1}{\lambda(p-\lambda)}+\frac{1}{(\lambda+)(p-\lambda-1)}+\ldots+\frac{1}{\frac{p-1}{2}\cdot\frac{p+1}{2}}\right]$$

$$=2.3.4\ldots(p-3)(p-2)+1.3.4.5\ldots(p-3)(p-1)$$
$$+1.2.4.5\ldots(p-4)(p-2)(p-1)+\ldots$$
$$\ldots+[1.2.3\ldots(\lambda-1)(\lambda+1)(\lambda+2)\ldots(p-\lambda-1)(p-\lambda+1)\ldots(p-2)(p-1)]+\ldots$$
$$\ldots+1.2.3\ldots\frac{p-3}{2}\cdot\frac{p+3}{2}\cdot\frac{p+5}{2}\ldots(p-1)$$

musiałoby być podzielnem przez p, a tem bardziej przez λ, co jest niemożebnem, gdyż wszystkie wyrazy po prawej stronie są podzielne przez λ z wyjątkiem jednego (ujętego w klamrę dla wyróżnienia).

O STANIE OBECNYM TEORYI NIEZMIENNIKÓW.

NAPISAŁ

Fr. MEYER.

Przełożył za upoważnieniem autora

S. DICKSTEIN.

Słowo od tłómacza.

Praca, której przekład podajemy, ogłoszona została w tomie I Roczników Stowarzyszenia niemieckiego matematyków (Jahresbericht der Deutschen Mathematiker-Vereinigung, I, 1892, str. I—IV, 81—292). Nadzwyczajny rozwój tej nowej gałęzi nauki algebraicznej, rozliczne związki, jakie łączą ją z innemi gałęziami matematyki, oraz rosnące wciąż zastosowania niezmienników, usprawiedliwiają dostatecznie ważność i użyteczność przeglądu głównych zdobyczy naukowych na tem polu badań. Przegląd taki staje się tem niezbędniejszy dla pracujących w tej dziedzinie algebry, że oryentowanie się w olbrzymiej literaturze, rozproszonej po wszystkich niemal dziennikach matematycznych Europy i Ameryki, jest wcale niełatwem, a dla wielu wprost niemożliwem. Przedstawienie zatem już nie samego tylko historycznego rozwoju badań, genezy pojęć i teoryj, związku i wzajemnego oddziaływania różnych prac, ale i podanie zupełnej niemal bibliografii teoryi niezmienników jest niepospolitą zasługą autora, za którą szczerze są mu wdzięczni wszyscy pracownicy na niwie matematycznej.

Z trudnego zadania swego wywiązał się prof. Meyer z niepospolitą sumiennością. Zapanował on, rzec można, nad całą literaturą przedmiotu,