ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE VII (1963)

wmptm 1897

W. SIERPIŃSKI (Warszawa)

Ministerstwo Nauki i Szkolnictwa Wyższego

O pewnym twierdzeniu równoważnym twierdzeniu o postępie arytmetycznym

Celem niniejszego artykułu jest dowód, że następujące dwa twierdzenia T_1 i T_2 są równoważne (w tym sensie, że łatwo jest z każdego z nich wyprowadzić drugie).

T_1 (TWIERDZENIE LEJEUNE-DIRICHLETA O POSTĘPIE ARYTMETYCZNYM): *Jeżeli a i b są liczbami naturalnymi względnie pierwszymi, to dla nieskończenie wielu liczb naturalnych k liczba $ak+b$ jest pierwsza.*

T_2: *Na to, żeby kongruencja $f(x) \equiv 0 \pmod m$, gdzie $f(x)$ jest wielomianem stopnia $\geqslant 1$ o współczynnikach całkowitych, zaś m dowolną liczbą naturalną, miała nieskończenie wiele rozwiązań w liczbach pierwszych x, potrzeba i wystarcza, żeby kongruencja ta miała co najmniej jedno rozwiązanie w liczbach całkowitych x oraz żeby było $\big(f(0), m\big) = 1$.*

Dowód wynikania $T_1 \Rightarrow T_2$. Przypuśćmy, że twierdzenie T_1 jest prawdziwe i że wielomian $f(x)$ spełnia warunki twierdzenia T_2. Istnieje więc liczba całkowita x_0, taka iż $f(x_0) \equiv 0 \pmod m$, przy czym możemy oczywiście założyć, że x_0 jest liczbą naturalną. Pokażemy, że $(x_0, m) = 1$. W samej rzeczy, gdyby było $(x_0, m) = d > 1$, mielibyśmy $x_0 \equiv 0 \pmod d$ skąd $f(x_0) \equiv f(0) \pmod d$, a ponieważ $f(x_0) \equiv 0 \pmod d$ (gdyż $d \mid m$), więc $f(0) \equiv 0 \pmod d$, czyli $d \mid f(0)$, a ponieważ $1 < d \mid m$, więc nie mogłoby być $\big(f(0), m\big) = 1$, wbrew założeniu. Jest więc $(x_0, m) = 1$ i, w myśl twierdzenia T_1, istnieje nieskończenie wiele liczb naturalnych k, takich że liczba $p = mk + x_0$ jest pierwsza. Lecz $f(p) = f(mk+x_0) \equiv f(x_0) \equiv 0 \pmod m$. Wynikanie $T_1 \Rightarrow T_2$ zostało więc udowodnione.

Dowód wynikania $T_2 \Rightarrow T_1$. Przypuśćmy, że twierdzenie T_2 jest prawdziwe i niech a i b będą liczbami naturalnymi, takimi iż $(a, b) = 1$. Możemy tu założyć, że $a > 1$, gdyż dla $a = 1$ twierdzenie T_1 jest oczywiście prawdziwe (gdyż istnieje nieskończenie wiele liczb pierwszych). Kongruencja $x - b \equiv 0 \pmod a$ spełnia warunki twierdzenia T_2. Z twierdzenia tego wynika więc, że istnieje nieskończenie wiele liczb pierwszych p, takich iż $p - b \equiv 0 \pmod a$, zatem liczb pierwszych, należących do postępu arytmetycznego $ak+b$. Wynikanie $T_2 \Rightarrow T_1$ zostało więc udowodnione.