Dowód

Przed dowodem obu implikacji wprowadźmy zmienne pomocnicze:

$$\tau = \frac{1+\sqrt{3}}{2}, \quad \overline{\tau} = \frac{1-\sqrt{3}}{2}, \quad \omega = \tau^2 = 2+\sqrt{3}, \quad \overline{\omega} = \overline{\tau}^2 = 2-\sqrt{3}.$$

Zauważmy, że $\tau\overline{\tau} = 1$, $\omega\overline{\omega} = 1$.

Indukcyjnie można pokazać, że ciąg (r_n) jest równy ciągowi $T_n = \omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}}$ (wystarczy sprawdzić, że ciąg (T_n) spełnia dwa warunki definiujące ciąg (r_n)).

$\Rightarrow$: Rozpatrzmy pierścień $R = \left\{a + b\sqrt{3} : a, b \in \{0, 1, 2, \ldots, M_p - 1\}\right\}$ ze standardowym dodawaniem:

$$\left(a + b\sqrt{3}\right) + \left(a_1 + b_1\sqrt{3}\right) = (a + a_1)_{M_p}\sqrt{3} + (b + b_1)_{M_p}\sqrt{3},$$

gdzie $(a+a_1)_{M_p}$, $(b+b_1)_{M_p}$ oznaczają reszty z dzielenia przez M_p. Mnożenie w pierścieniu R określamy tak:

$$(a + b\sqrt{3}) \cdot (a_1 + b_1\sqrt{3}) = (aa_1 + 3bb_1)_{M_p} + (ab_1 + ba_1)_{M_p}\sqrt{3}.$$

Element $2\tau \in R$ podnosimy do potęgi M_p:

$$(1+\sqrt{3})^{M_p} = 1 + \binom{M_p}{1}\sqrt{3} + \ldots + \sqrt{3}^{M_p} \equiv 1 + 3^{\frac{M_p-1}{2}} \pmod{M_p};$$

wykorzystaliśmy podzielność składników $\binom{M_p}{1}\sqrt{3}, \ldots, \binom{M_p}{M_p-1}\sqrt{3}^{M_p-1}$ przez M_p. Ponieważ $M_p \equiv -1 \pmod 8$, więc $2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}$; ponadto $M_p \equiv 1 \pmod 3$ więc

$$3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p}.$$

Stąd

$$\tau^{M_p} \equiv \overline{\tau},\ \tau^{M_p+1} \equiv \tau\overline{\tau} \equiv -1 \pmod{M_p}.$$

Ostatecznie $\tau^2 = \omega$, $\omega^{2^{p-1}} + 1 \equiv 0 \pmod{M_p}$. Mnożąc ostatnią kongruencję przez $\overline{\omega}^{2^{p-2}}$ i korzystając z równości $\omega\overline{\omega} = 1$, otrzymujemy $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$. Ale pokazaliśmy wcześniej, że $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = r_{p-1}$, więc liczba r_{p-1} jest podzielna przez M_p.

$\Leftarrow$: Implikacja ta jest „ważniejsza” w kontekście używania implementacji algorytmu Lucasa-Lehmera.

Zauważmy, że z poprzednich rozważań wynikają dwie kongruencje

$$\omega^{2^{p-1}} \equiv -1 \pmod{M_p}, \ \ \omega^{2^p} \equiv 1 \pmod{M_p}. \tag{1}$$

Załóżmy teraz nie wprost, że M_p jest liczbą złożoną i niech q będzie jej dzielnikiem pierwszym takim, że $q \leqslant \sqrt{M_p}$. Zamiast pierścienia R będziemy teraz rozpatrywać pierścień

$$R_1 = \left\{a + b\sqrt{3} : a, b \in \{0, 1, \ldots, q\}\right\}$$

z podobnie jak w R określonymi działaniami.

Zauważmy, że element $\omega \in R_1$ jest w tym pierścieniu odwracalny ($\omega\overline{\omega} = 1$). Element ω należy do grupy elementów odwracalnych pierścienia R_1 (nazwijmy ją G). Kluczowe dla naszych rozważań równości (1) zachodzą także w R_1, tzn.

$$\omega^{2^{p-1}} \equiv -1 \pmod{q}, \;\; \omega^{2^p} \equiv 1 \pmod{q}.$$

Z powyższych równości wynika, że rząd ω w G jest równy 2^p. Widzimy, że

$$|G| \leqslant (q-1)^2 < M_p,$$

ale z drugiej strony rząd elementu ω przekracza M_p. Otrzymana sprzeczność kończy dowód implikacji $\Leftarrow$. □

Od dawna matematyków interesowało istnienie formuły dającej nieskończony ciąg różnych liczb pierwszych. W średniowieczu rozpowszechnione było przekonanie, że wzór $f(n) = n^2 + n + 41$ jest taką formułą. Rzeczywiście dla $n = 1, 2, \ldots, 39$ wartości $f(n)$ są liczbami pierwszymi, ale $f(40) = 40 \cdot 41 + 41 = 41^2$. Jednak do dziś nie wiadomo, czy ciąg $f(n)$ zawiera nieskończenie wiele liczb pierwszych. Wykażemy teraz, że formuły takiej nie można zbudować za pomocą wielomianu o współczynnikach całkowitych.

Twierdzenie 11.7 (**Goldbach**)
Nie istnieje wielomian $f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_k$, $k \geqslant 1$, $a_i \in \mathbb{Z}$, $a_0 \neq 0$, *taki że* $f(n)$ *jest liczbą pierwszą dla każdego* $n \in \mathbb{N}$.

Dowód
Niech dla $n = n_0$ wartość $f(n_0) = p$ będzie liczbą pierwszą. Dla każdego całkowitego t wyrażenie $f(n_0 + tp)$ można przekształcić następująco:

$$\begin{aligned} f(n_0 + tp) &= a_0(n_0 + tp)^k + \ldots + a_{k-1}(n_0 + tp) + a_k \\ &= a_0n_0^k + a_1n_0^{k-1} + \ldots + a_{k-1}n_0 + a_k + pq(t) \\ &= f(n_0) + pq(t) = p + pq(t) = p(1 + q(t)), \end{aligned}$$

gdzie $q(t)$ jest wielomianem o współczynnikach całkowitych. Stąd $p \,|\, f(n_0 + tp)$, więc albo $f(n_0 + tp)$ jest liczbą złożoną, albo $f(n_0 + tp) = \pm p$ lub 0. Ale t jest dowolne, a wielomian stopnia k o współczynnikach całkowitych może przyjmować tę samą wartość w co najwyżej k argumentach, więc istnieje t_0 takie, że $f(n_0 + t_0p)$ jest liczbą złożoną. □

Twierdzenie 11.7 można uogólnić (por. zad. 70).

W.H. Mills[7] w 1947 roku wykazał, że istnieje liczba rzeczywista r, taka że $f_r(n) = [r^{3^n}] \in \mathbb{P}$ dla każdego $n \geqslant 1$ (por. zad. 75). Jednak występująca w tej formule liczba r nie jest dana explicite. Wiadomo, że istnieje nieskończenie wiele takich liczb r. W 2005 roku Caldwell i Cheng udowodnili, że przy założeniu prawdziwości hipotezy Riemanna $r \geqslant 1{,}3063\ldots$

[7] Mills W.H., A prime-representing function, *Bulletin of the American Mathematical Society* **53**, 604 (1947).