Liczby doskonałe *Włodzimierz HOLSZTYŃSKI*

1. Wstęp

Jakie jest najdawniejsze, nierozwiązane zagadnienie naukowe? Chyba problem liczb doskonałych, czyli liczb naturalnych, których suma dzielników, mniejszych od samej liczby, jest jej równa. Na przykład 6 jest doskonałe, także 28: $28 = 1 + 2 + 4 + 7 + 14$. Euklides zauważył ogólniej, że gdy $M(n) := 2^n - 1$ jest liczbą pierwszą, to $E(n) := 2^{n-1} \cdot M(n)$ jest liczbą doskonałą (oczywiście parzystą), a Euler wykazał, że innych liczb parzystych doskonałych już nie ma.

Liczbę $M(n) := 2^n - 1$ nazywamy n-tą liczbą Mersenna, $n \in \mathbb{N}$. By liczba $M(n)$ była pierwsza, konieczna jest pierwszość n – ale nie jest dostateczna, np. $M(11) = 23 \cdot 89$.

Z drugiej strony nie wiemy:
- czy liczb doskonałych jest nieskończenie wiele?
- czy istnieje nieparzysta liczba doskonała?

W niniejszym artykule udowodnię twierdzenie Euklidesa–Eulera oraz twierdzenie Peirce'a: każda ewentualna nieparzysta liczba doskonała dzieli się przez co najmniej cztery różne liczby pierwsze (więcej o nieparzystych liczbach doskonałych – na stronie 4). Równoważnie: każda liczba nieparzysta, o co najwyżej trzech różnych dzielnikach pierwszych, nie jest doskonała.

2. Potęgi mod 8

Pewnie od „zawsze" wiadomo, że:

Twierdzenie 1. *Niech $n \in \mathbb{Z}$ będzie nieparzyste. Wtedy $n^2 \equiv 1 \bmod 8$.*

Wniosek 1. *Dla $e, f \in \mathbb{Z}^+$ oraz nieparzystego $n \in \mathbb{Z}$ zachodzi:*

$$e \equiv f \bmod 2 \quad \Rightarrow \quad n^e \equiv n^f \bmod 8,$$

$$n^f \equiv \begin{cases} 1 \bmod 8 & \text{dla } \ f \equiv 0 \bmod 2 \\ n \bmod 8 & \text{dla } \ f \equiv 1 \bmod 2 \end{cases}$$

Notacja

$\mathbb{Z}^+$ – zbiór nieujemnych liczb całkowitych $0, 1, 2, \ldots$

$\mathbb{N}$ – zbiór liczb naturalnych $1, 2, \ldots$

$\mathbb{P}$ – zbiór liczb pierwszych $2, 3, 5, 7, 11, \ldots$

$\lfloor x \rfloor$ – jedyna liczba całkowita, spełniająca: $x - 1 < \lfloor x \rfloor \leqslant x$;

$\lceil x \rceil$ – jedyna liczba całkowita, spełniająca: $x \leqslant \lceil x \rceil < x+1$;

$ord_p(x) \in \mathbb{Z}$ – wykładnik przy p w rozkładzie dodatniej liczby wymiernej x na iloczyn całkowitych potęg liczb pierwszych:

$$x = \prod_{p \in \mathbb{P}} p^{ord_p(x)};$$

$\gcd(a, b)$ – największy wspólny dzielnik liczb $a, b \in \mathbb{Z}$.

3. Suma dzielników $\sigma(n)$

Funkcja $\sigma : \mathbb{N} \to \mathbb{N}$ jest sumą dzielników: $\sigma(n) := \sum_{d|n} d$. Ponieważ $n|n$, więc liczba n jest doskonała wtedy i tylko wtedy, gdy $\sigma(n) = 2 \cdot n$. Zatem $\sigma(n) \equiv 2 \bmod 4$ dla nieparzystych liczb doskonałych. Charakteryzacja liczb naturalnych spełniających ten warunek będzie podana w twierdzeniu 4. Najpierw odnotujmy kilka własności:

(1) $\gcd(m, n) = 1 \Rightarrow \sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$,
(2) $\sigma(n) = 1 \Leftrightarrow n = 1$,
(3) $\sigma(p^t) = 1 + p + \ldots + p^t = (p^{t+1} - 1)/(p - 1)$,
(4) $s + 1 | t + 1 \Rightarrow \sigma(p^s) | \sigma(p^t)$,
(5) $\sigma(p^t) \equiv 1 \bmod p$,
(6) $q \neq p$ i $q \not| \ p - 1 \Rightarrow q | \sigma(p^{q-2})$,
(7) $p \equiv q \bmod m \Rightarrow \sigma(p^t) \equiv \sigma(q^t) \bmod m$,

dla każdego $m, n \in \mathbb{N}$, $p, q \in \mathbb{P}$, $s, t \in \mathbb{Z}^+$.

Twierdzenie 2. *Niech $2 < p \in \mathbb{P}$ oraz $f \in \mathbb{Z}^+$. Wtedy*

$$\sigma(p^f) \equiv p \cdot \left\lfloor \frac{f}{2} \right\rfloor + \left\lceil \frac{f+1}{2} \right\rceil \bmod 8.$$

Dowód. $\sigma(p^f) = \sum_{k=0}^{f} p^k$. Teraz należy zastosować drugą część Wniosku 1 do każdej potęgi p^k.

Twierdzenie 3. *Niech $n \in \mathbb{N}$. Wtedy:*

$$2 \,|\, \sigma(n) \iff \exists_{p \in \mathbb{P}} \ (p > 2 \ \text{ oraz } \ ord_p(n) \equiv 1 \bmod 2).$$

Dowód. $\sigma(n)$ jest iloczynem liczb postaci $\sigma(p^f)$ dla liczb pierwszych $p|n$. Parzystość $\sigma(n)$ jest równoważna parzystości jednej ze wspomnianych liczb $\sigma(p^f)$ dla $p > 2$ (liczba $\sigma(2^f)$ jest zawsze nieparzysta).

Równie prosty jest dowód następującego twierdzenia:

Twierdzenie 4. *Dla $n \in \mathbb{N}$ mamy: $\sigma(n) \equiv 2 \bmod 4$ wtedy i tylko wtedy, gdy istnieje taka liczba $p \in \mathbb{P}$, że $p \equiv 1 \bmod 4$ oraz $ord_p(n) \equiv 1 \bmod 4$ i dla dowolnej liczby $q \in \mathbb{P}$ różnej od p zachodzi $2|ord_q(n)$.*

4. Suma potęg dzielników

Niech $a \in \mathbb{R}$. Funkcja $\sigma_a : \mathbb{N} \to \mathbb{R}$ jest zdefiniowana następująco:

$$\sigma_a(n) := \sum_{d|n} d^a$$

dla każdego $n \in \mathbb{N}$. Ma ona następujące własności:

(1) $\gcd(k,n) = 1 \Rightarrow \sigma_a(k \cdot n) = \sigma_a(k) \cdot \sigma_a(n)$,

(2) $\sigma_{-a}(n) = \frac{\sigma_a(n)}{n^a}$,

(3) $\sigma_a(n) = 1 \Leftrightarrow n = 1$,

(4) $\sigma_a(p^t) = 1 + p^a + \ldots + p^{a \cdot t} = (p^{a \cdot (t+1)} - 1)/(p^a - 1)$,

dla $k, n \in \mathbb{N}$, $t \in \mathbb{Z}^+$, $p \in \mathbb{P}$.

Twierdzenie 5. *Niech $a \in \mathbb{R}$, $d, k \in \mathbb{N}$, $n := d \cdot k$. Wtedy*

$$\sigma_a(n) \geqslant d^a \cdot \sigma_a(k) + \sigma_a(d) - d^a.$$

Zatem $\sigma_a(n) > d^a \cdot \sigma_a(k)$ dla $d > 1$.

Dowód. Zbiór dzielników liczby n zawiera dwa rozłączne podzbiory:

$$\{t \in \mathbb{N} : d|t \text{ i } t|n\} \qquad \text{oraz} \qquad \{t \in \mathbb{N} : t|d \text{ i } t < d\}$$

Arytmetyczna suma a-tych potęg elementów pierwszego zbioru wynosi $d^a \cdot \sigma_a(k)$, a drugiego $\sigma_a(d) - d^a$.

Dla wartości $a = -1, 0, 1$ otrzymujemy klasyczne funkcje:

- σ_0 – liczba dzielników,
- $\sigma = \sigma_1$ – suma dzielników,
- $brq := \sigma_{-1}$ – współczynnik barokowy, czyli suma odwrotności dzielników.

Tak więc:

(1) $brq(n) = \sigma(n)/n$; stąd $ord_p(brq(n)) \leqslant ord_p(\sigma(n))$,

(2) $\big(\gcd(k,m) = 1 \text{ oraz } brq(n) = \frac{k}{m}\big) \Rightarrow (m|n \text{ oraz } k|\sigma(n))$,

(3) $p \not| \ n \iff ord_p(brq(n)) = ord_p(\sigma(n))$,

(4) $\frac{p+1}{p} \leqslant brq(p^f) = \frac{p^{f+1}-1}{(p-1)\cdot p^f} < \frac{p}{p-1}$,

(5) $p < q \Rightarrow brq(p^f) > brq(q^g)$

dla każdego $f, g, n \in \mathbb{N}$, $p, q \in \mathbb{P}$.

Poniżej definiujemy między innymi – na nowo, ale równoważnie – liczby doskonałe:

Definicja 1. *Liczba $n \in \mathbb{N}$ nazywa się:*

- *szczupła* $\iff brq(n) < 2$,
- *doskonała* $\iff brq(n) = 2$,
- *otyła* $\iff brq(n) > 2$.

Powiemy także, że liczba n jest:

- barokowa $\iff brq(n) \in \mathbb{N}$;
- gotycka $\iff \exists_{k \in \mathbb{N}}\ brq(n) = \frac{k+1}{k}$.

Twierdzenie. *Liczba $n \in \mathbb{N}$ jest gotycka wtedy i tylko wtedy, gdy n jest pierwsza lub doskonała.*

Twierdzenie 6. *Każda potęga liczby pierwszej oraz każda nieparzysta liczba n, która ma tylko dwa różne dzielniki pierwsze, jest szczupła.*

Dowód. Udowodnię drugą część: niech $n = p^f \cdot q^g$, gdzie $2 < p < q$, oraz $p, q \in \mathbb{P}$. Wtedy mamy $p \geqslant 3$ oraz $q \geqslant 5$, więc:

$$brq(n) = brq(p^f) \cdot brq(q^g) < \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8} < 2.$$

5. Trzy dzielniki pierwsze

Twierdzenie 7. *Nieparzysta liczba doskonała nie dzieli się przez* $3 \cdot 5 \cdot 7$.

Dowód. Nieparzysta liczba doskonała spełnia $\sigma(n) \equiv 2 \bmod 4$. Zatem (patrz twierdzenie 4) wykładniki liczb 3 i 7 w rozkładzie n na czynniki pierwsze są parzyste, skąd podzielność $3 \cdot 5 \cdot 7 \,|\, n$ prowadziłaby do otyłości:

$$brq(n) \geqslant brq(3^2 \cdot 5 \cdot 7^2) = \frac{13}{9} \cdot \frac{6}{5} \cdot \frac{57}{49} = 2 \cdot \frac{247}{245} > 2.$$

Lemat 1. *Niech* $p < q < r$ *będą jedynymi dzielnikami pierwszymi nieparzystej liczby doskonałej* n. *Wtedy* $p = 3,\ q = 5$ *oraz* $r = 11$ *lub* 13.

Dowód. Gdyby $q \neq 5$, to $q \geqslant 7$ oraz $r \geqslant 11$, skąd:

$$brq(n) \leqslant brq(3^f \cdot 7^g \cdot 11^h) < \frac{3}{2} \cdot \frac{7}{6} \cdot \frac{11}{10} = \frac{77}{40} < 2.$$

Liczba n byłaby szczupła. Zatem $p = 3,\ q = 5$ oraz

$$2 = brq(n) < \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{r}{r-1} = \frac{15}{8} \cdot \frac{r}{r-1},$$

więc liczba pierwsza r jest mniejsza od 16. Ale $r \neq 7$ (patrz twierdzenie 7).

Twierdzenie 8. (Peirce) *Nieparzysta liczba doskonała* n *ma co najmniej* 4 *różne dzielniki pierwsze.*

Dowód. Wiemy, że nie może mieć mniej niż trzech. Gdyby tylko $p < q < r$ były dzielnikami pierwszymi n, to mielibyśmy $p = 3,\ q = 5$ oraz $r = 11$ lub 13. Zatem

$$2 = brq(n) = brq(3^f) \cdot brq(5^g) \cdot brq(r^h)$$

dla pewnych $f, g, h \in \mathbb{N}$, gdzie f jest parzyste. Ponieważ $ord_5(brq(5^g)) < 0$, to $ord_5(brq(3^f)) > 0$ lub $ord_5(brq(r^h)) > 0$. Ale $ord_5(brq(3^f)) = ord_5(3^{f+1} - 1)$, oraz $5 \not| \ 3^{f+1} - 1$ dla nieparzystego $f + 1$. Zatem $ord_5(brq(r^h)) > 0$, czyli $5 | \sigma(r^h)$.

Dla $r = 11 \equiv 1 \bmod 5$ oznaczałoby to $5 \,|\, h + 1$, czyli $\sigma(11^4) \,|\, \sigma(11^h)$. Ponieważ $\sigma(11^4) = 16105 = 5 \cdot 3221$, gdzie 3221 jest pierwsze, więc $3221 | n$, sprzeczność.

Pozostał przypadek $r = 13$. Tym razem $5 \,|\, \sigma(13^h)$, więc $4 \,|\, h + 1$, skąd $\sigma(13^3) \,|\, \sigma(13^h)$. Ale $\sigma(13^3) = 2380 = 2^2 \cdot 5 \cdot 7 \cdot 17$, więc na przykład $7 | n$ – sprzeczność.

6. Parzyste liczby doskonałe

Twierdzenie 9. (Euklides–Euler) *Parzysta liczba naturalna* n *jest doskonała wtedy i tylko wtedy, gdy istnieje liczba naturalna* p, *taka że*

$$M(p) \in \mathbb{P} \text{ oraz } n = 2^{p-1} \cdot M(p).$$

Dowód. Pokażę tylko implikację Eulera, czyli wykażę, że innych parzystych liczb doskonałych nie ma. Przedstawmy parzystą liczbę doskonałą w postaci $n = 2^k \cdot m$, gdzie $k, m \in \mathbb{N}$, m – nieparzyste. Równość $\sigma(n) = 2 \cdot n$ oznacza, że $\sigma(2^k) \cdot \sigma(m) = 2^{k+1} \cdot m$, czyli $M(k+1) \cdot \sigma(m) = 2^{k+1} \cdot m$. Zatem $M(k+1) | m$, oraz dla $b := m/M(k+1) = \sigma(m)/2^{k+1} \in \mathbb{N}$ mamy

$$\sigma(m) = b \cdot 2^{k+1}, \tag{1}$$

$$m = b \cdot M(k+1). \tag{2}$$

Zastosujmy σ do (2) oraz skorzystajmy z twierdzenia 5:

$$\begin{aligned} \sigma(m) &= \sigma(b \cdot M(k+1)) \geqslant \\ &\geqslant b \cdot \sigma(M(k+1)) + \sigma(b) - b \geqslant \\ &\geqslant b \cdot 2^{k+1} + \sigma(b) - b. \end{aligned} \tag{3}$$

Z (1) i (3) wynika $\sigma(b) - b \leqslant 0$, skąd $b = 1$. Więc (1) i (2) daje $\sigma(m) = m + 1$, czyli m jest pierwsze, przy czym $m = M(k+1)$. Zatem $n = 2^{p-1} \cdot M(p)$ dla $p := k + 1$ i $M(p) \in \mathbb{P}$. (Część Euklidesa zostawiam Czytelnikom.)

Rozwiązanie zadania F 705.
Siła nacisku na tłok pompki jest w przybliżeniu równa wadze człowieka, powiedzmy $F_0 \approx 500\,\mathrm{N}$. Przekrój tłoka w przykładowej pompce jest równy $S \approx 0{,}003\,\mathrm{m}^2$, zatem wytworzone jest ciśnienie $\Delta p \approx F_0/S \approx 2000\,\mathrm{hPa}$. Na cząsteczkę żwirku działa zatem siła $F \sim \Delta p \pi r^2 \approx 1\,\mathrm{N}$, gdzie $r \approx 1{,}5\,\mathrm{mm}$. Zatem przyspieszenie cząsteczki jest równe

$$a \approx F/m = \frac{3F}{4\rho\pi r^3} \approx 3 \cdot 10^3\,\mathrm{m/s^2},$$

gdzie $\rho \approx 3 \cdot 10^3\,\mathrm{kg/m^3}$. Przyjmując, że długość wychodzącego z pompki przewodu jest równa $l \approx 0{,}5\,\mathrm{m}$, otrzymujemy $v_{\mathrm{maks}} \approx \sqrt{al} \approx 5\,\mathrm{m/s}$.