Spis treści

Rozdział 1

Wprowadzenie do teorii liczb; trochę historii

Pierwsi rachmistrzowie

1.1 Jak człowiek zaczął liczyć

—klik

1.2 Egipt i Grecja; systemy kodowania liczb

—klik

1.3 Ułamki egipskie

—klik

1.4 Starożytna Babylonia – trójki pitagorejskie

—klik

1.5 Pitagoras

—klik

1.6 Liczby trójkątne . . .

—klik

1.7 . . . i ich własności

—klik

Rozdział 2

Podzielność liczb. Liczby pierwsze i liczby złożone

2.1 **Podzielność, $NWD = (a, b)$, algorytm Euklidesa**

—klik

2.2 **Parzystość, nieparzystość, systemy liczbowe**

—klik

2.3 **liczby pierwsze, rozkład liczby złożonej na czynniki**

—klik

2.4 **Suma i iloczyn dzielników; liczby doskonałe i liczby zaprzyjaźnione**

—klik

2.5 **Funkcje arytmetyczne – 1; funkcja ϕ Eulera**

—klik

2.6 **Liczby pierwsze Mersenne'a i Fermata**

—klik

2.7 **Rozmieszczenie liczb pierwszych, hipoteza Goldbacha, tw.L̃ejeune-Dirichleta**

—klik

Rozdział 3

Równania diofantyczne i ułamki łańcuchowe

Rozdział 4

Kongruencje

Rachunek kongruencji

4.1 Pierwsze kroki

—klik

4.2 Skromne pożytki praktyczne

—klik

4.3 Rachunek kongruencji

—klik

4.4 Kongruencje kwadratowe; symbol Legendre'a i Jacobiego

—klik

4.5 Twierdzenie Wilsona

—klik

4.6 Twierdzenie Eulera

—klik

4.7 Funkcje arytmetyczne – 2; Funkcja Carmichaela i funkcja Möbiusa

—klik

4.8 Pierwiastki pierwotne i logarytmy dyskretne

—klik

4.9 Odwrotne twierdzenie Fermata

—klik

4.10 Hipoteza (twierdzenie) Waringa

—klik

Rozdział 5

Współczesne zastosowania teorii liczb

5.1 Zastosowania różne

—klik

obliczenia modułowe

kongruentne generatory liczb losowych

weryfikacja poprawności numerów (np. ISBN)

Bardzo krótki wstęp do kryptografii

5.2 Kilka epizodów z historii kryptografii

—klik

5.3 Kryptografia z kluczem tajnym

—klik

5.4 Kryptografia z kluczem publicznym

—klik

potwierdzenie tożsamości

wymiana klucza – Diffie, Hellman

System RSA

Rozdział 6

Noty biograficzne

6.1 Leonard Euler

—klik

6.2 Pierre Fermat

—klik

6.3 Karl Gauss

—klik

6.4 Derrick Lehmer

—klik

6.5 Marin Mersenne

—klik

Rozdział 7

Wykorzystane źródła . . .

. . . czyli skąd autor czerpał mądrości

Spis książek na następnej stronie

Bibliografia

[Yan 06] Song Y. Yan, *Teoria liczb w informatyce*, PWN, Warszawa, 2006.

[Knuth 66] R. L. Graham, D. E. Knuth, O. Patashnik, *Matematyka konkretna*,
PWN, Warszawa, 1996.

[O_Ore 88] Oystein Ore, *Number Theory and Its History*,
Dover, Publ. Inc., New York, 1988 (reprint wydania 1948).

[Burton 97] D. M. Burton, *The History of Mathematics, an Introduction*,
McGraw-Hill Co., 1997.

[Conway 04] J. H. Conway, R. K. Guy, *Księga liczb*, WNT, Warszawa, 2004.

[Ma-Zar 06] W. Marzantowicz, P. Zarzycki, *Elementarna teoria liczb*,
PWN, Warszawa, 2006.

[Riben 97] P. Ribenboim, *Mała księga wielkich liczb pierwszych*,
WNT, Warszawa, 1997.

[Sierp 70] W. Sierpiński, *250 Problems in Elementary Number Theory*,
Elsevier(New York)–PWN(Warszawa),1970.

[Sierp 87] W. Sierpiński, *Elementary Theory of Numbers*,
North-Holland(Amst.)-PWN(W-wa),1987.

[Kourl 01] L. Kourliandtchik, *Impresje liczbowe*, OW „Tutor", Toruń, 2001.

[Koblz 94] N. Koblitz, Wykład z teorii liczb i kryptografii,
WNT, Warszawa, 1994.

[Ifrah 90] G. Ifrah, *Dzieje liczby czyli historia wielkiego wynalazku*,
ZNiO, Wrocław 1990.

[Singh 00] S. Singh, *The Code Book*, Anchor Books, NY, 2000.