
Spis treści

Przedmowa	9
1. Algorytmy podstawowe	13
1.1. Uwagi wstępne	13
1.2. Dzielenie liczb całkowitych	13
1.3. Algorytm Euklidesa	20
1.4. Najmniejsza wspólna wielokrotność	23
1.5. Rozszerzony algorytm Euklidesa	24
1.6. Elementarne metody faktoryzacji	28
1.7. Istnienie rozkładu na czynniki	30
1.8. Schemat algorytmu kolejnych dzielení	31
1.9. Algorytm faktoryzacji Fermata	33
1.10. Praktyczna realizacja algorytmu Fermata	34
1.11. Jednoznaczność rozkładu	36
1.12. „Wzór wielomianowy” na liczbę pierwszą	36
1.13. „Wzór wykładniczy”. Liczby Mersenne’a	37
1.14. Liczby Fermata	39
1.15. Funkcja $p^\#$	40
1.16. Sito Eratostenesa	41
2. Wykorzystanie arytmetyki reszt	45
2.1. Arytmetyka reszt	45
2.2. Relacja równoważności	45
2.3. Działania na resztach modulo n	48
2.4. Potęgowanie modulo n	51
2.5. Elementy odwracalne i dzielenie modulo n	53
2.6. Rozwiązywanie kongruencji liniowych	56
2.7. Twierdzenie Fermata	59

2.8.	Liczby pseudopierwsze	62
2.9.	Test Millera-Rabina	71
3.	Układy kongruencji	77
3.1.	Układy równań (mod n)	77
3.2.	Chińskie twierdzenie o resztach	78
3.3.	Interpretacja geometryczna	80
3.4.	Chińskie twierdzenie o resztach. Przypadek ogólny	81
3.5.	Przypadek wielu kongruencji	83
3.6.	Wykorzystanie CRT	83
4.	Permutacje, symetrie, grupy	85
4.1.	Permutacje	85
4.2.	Rozkład na cykle	88
4.3.	Definicja grupy	90
4.4.	Przykłady grup	91
4.5.	Grupa \mathbb{Z}_n^* i funkcja Eulera $\varphi(n)$	92
4.6.	Własności funkcji Eulera	93
4.7.	Symetrie trójkąta	96
4.8.	Grupa symetrii kwadratu i pięciokąta foremnego	97
4.9.	Podgrupy	98
4.10.	Grupy cykliczne	100
4.11.	Przykłady podgrup. Wykorzystanie twierdzenia Lagrange'a	102
4.12.	Dowód twierdzenia Lagrange'a	105
4.13.	Twierdzenie o rzędzie elementu	106
4.14.	Test Lucasa-Lehmera	108
4.15.	Wykorzystanie pierwiastków pierwotnych w dowodach pierwszośc...	110
4.16.	Zastosowanie pierwiastków pierwotnych do dowodu twierdzenia Kor-	
	selta	115
4.17.	Badanie rzędów elementów	116
4.18.	Konstrukcja pierwiastków pierwotnych	118
4.19.	Algorytm obliczania rzędów elementów \mathbb{Z}_p^*	119
5.	Kongruencje kwadratowe	123
5.1.	Reszty i niereszytne kwadratowe	123
5.2.	Symbol Legendre'a	125
5.3.	Wykorzystanie prawa wzajemności reszt kwadratowych	129
5.4.	Kongruencje kwadratowe z modułem złożonym	130

6.	Wybrane metody szyfrowania stosowane w przeszłości	135
6.1.	Uwagi wstępne	135
6.2.	Szyfr Cezara	136
6.3.	Szyfr Vigenere'a	138
6.4.	Szyfr Hilla	139
6.5.	Szyfr Vernama	140
7.	Kryptografia z kluczem publicznym	141
7.1.	Logarytmy dyskretne	142
7.2.	Uzgadnianie klucza Diffiego-Hellmana	142
7.3.	Generowanie kluczy w systemie ElGamal	143
7.4.	Szyfrowanie w systemie ElGamal	144
7.5.	Podpis elektroniczny w systemie ElGamal	146
7.6.	System ElGamal w bibliotece Crypto języka Python	147
7.7.	Schemat podpisu DSA	150
7.8.	System DSA w bibliotece Crypto języka Python	152
7.9.	System RSA (Rivest, Shamir, Adleman)	154
7.10.	Podpis RSA	159
7.11.	System RSA w bibliotece Crypto języka Python	160
7.12.	Uzasadnienie poprawności systemu RSA	162
7.13.	Uwagi o bezpieczeństwie systemu RSA	163
7.14.	Praktycznie stosowane systemy kryptograficzne	164
8.	Kryptografia z kluczem symetrycznym	165
8.1.	S-DES	165
8.1.1.	Bloki tekstu i klucz S-DES	166
8.1.2.	Schemat systemu S-DES	166
8.1.3.	Permutacja wstępna w S-DES	167
8.1.4.	Funkcja rozszerzająca EP i inne funkcje pomocnicze S-DES	167
8.1.5.	Generowanie kluczy dla rund S-DES	168
8.1.6.	Operacja xor w S-DES	168
8.1.7.	S-boksy w S-DES	168
8.1.8.	Wykorzystanie S-boksów w S-DES	169
8.1.9.	Realizacja całości algorytmu S-DES	169
8.2.	DES	172
8.2.1.	Bloki tekstu i klucz	172
8.2.2.	Schemat systemu DES	172

8.2.3.	Permutacja wstępna	173
8.2.4.	Funkcja rozszerzająca E	173
8.2.5.	Generowanie kluczy dla rund	173
8.2.6.	Operacja xor	175
8.2.7.	S-boksy	175
8.2.8.	Permutacja P	176
8.2.9.	Czynności końcowe	176
8.2.10.	Realizacja całości algorytmu DES w Sage	177
8.3.	System DES w bibliotece Crypto języka Python	180
8.4.	Mini-AES	181
8.4.1.	Schemat systemu Mini-AES	182
8.4.2.	S-boksy w Mini-AES	183
8.4.3.	Generowanie kluczy dla rund	184
8.4.4.	Wykorzystanie S-boksów w szyfrowaniu Mini-AES	185
8.4.5.	Operacje <code>shift_row</code> i <code>mix_column</code>	185
8.4.6.	Realizacja całości algorytmu Mini-AES	186
8.5.	AES	188
8.5.1.	Funkcja <code>sub_byte</code>	191
8.5.2.	Rozszerzanie klucza	191
8.5.3.	Schemat algorytmu AES	194
8.5.4.	Funkcja <code>AddRoundKey(P,K)</code>	194
8.5.5.	Funkcja <code>SubBytes</code>	194
8.5.6.	Funkcja <code>ShiftRows</code>	195
8.5.7.	Funkcja <code>MixColumns</code>	195
8.5.8.	Funkcja <code>KeyExpansion</code>	196
8.5.9.	Wykonanie całości procedury	196
8.6.	System AES w bibliotece Crypto języka Python	197
9.	Funkcje skrótu	199
9.1.	SHA-1	200
9.2.	Wykonanie całości procedury	204
9.3.	Funkcje skrótu w bibliotece Crypto języka Python	208
10.	Ułamki łańcuchowe	209
10.1.	Skończone ułamki łańcuchowe	209
10.2.	Redukty ułamków łańcuchowych	213
10.3.	Nieskończone ułamki łańcuchowe	217

10.4.	Rozwijanie liczb niewymiernych w ułamki łańcuchowe	219
10.5.	Nierówności pomocnicze	222
11.	Pierścienie, ciała, wielomiany	223
11.1.	Pierścienie i ciała	223
11.2.	Ciała skończone	224
11.3.	Wielomiany nierozkładalne	226
11.4.	Konstrukcja ciał skończonych	229
12.	Faktoryzacja	233
12.1.	Metoda $p - 1$ Pollarda	233
12.2.	Metoda ρ Pollarda	236
12.3.	Wykorzystanie kongruencji $x^2 \equiv y^2 \pmod{n}$	242
12.4.	Bazy rozkładu	244
12.5.	Wykorzystanie ułamków łańcuchowych w faktoryzacji	248
12.6.	Metoda sita kwadratowego w ujęciu Koblitz'a	250
12.7.	Uproszczona wersja sita kwadratowego w ujęciu Pomerance'a	258
13.	Logarytmy dyskretne	261
13.1.	Metoda przeliczania	263
13.2.	Algorytm małych i wielkich kroków	263
13.3.	Algorytm ρ Pollarda wyznaczania logarytmu	265
13.4.	Algorytm Pohlinga-Hellmana znajdowania logarytmu	268
13.5.	Wykorzystanie baz rozkładu	274
13.6.	Logarytmy bazy rozkładu	275
14.	Krzywe eliptyczne	279
14.1.	Definicja krzywej eliptycznej	279
14.2.	Płaszczyzna rzutowa. Podejście algebraiczne	282
14.3.	Płaszczyzna rzutowa. Podejście geometryczne	282
14.4.	Związek podejścia algebraicznego i geometrycznego	283
14.5.	Krzywe eliptyczne na płaszczyźnie rzutowej	283
14.6.	Krzywa eliptyczna jako grupa	284
14.7.	Geometryczne dodawanie punktów	284
14.8.	Dodawanie punktów. Podejście analityczne	285
14.9.	Dodawanie punktów krzywej eliptycznej w Sage	286
14.10.	Metoda Lenstry faktoryzacji	289
14.11.	System ElGamal na krzywej eliptycznej	293

14.12. ECDSA	295
A. Szyfrowanie z GnuPG	299
A.1. Przygotowanie do szyfrowania	300
A.2. Szyfrowanie i odszyfrowywanie.....	305
A.2.1. Szyfrowanie	305
A.2.2. Odszyfrowywanie	308
A.3. Szyfrowanie w gpg z linii poleceń	308
A.3.1. Generowanie pary kluczy	308
A.3.2. Export klucza publicznego	310
A.3.3. Generowanie certyfikatu odwołania klucza	310
A.3.4. Import klucza innego użytkownika gpg	311
A.3.5. Wyświetlanie kluczy	311
A.3.6. Podpisanie zaimportowanego klucza	311
A.3.7. Szyfrowanie	312
A.3.8. Odszyfrowanie i weryfikacja podpisu.....	313
A.3.9. Usuwanie klucza ze zbioru kluczy	314
A.3.10. Szyfrowanie symetryczne	314
Skorowidz.....	315
Bibliografia	327