Liczby pierwsze i złożone

Rafał Lisiecki

15 grudnia 2014

Spis treści

1 Wstęp

„Zagadnienie odróżniania liczb pierwszych od złożonych i rozkładanie tych ostatnich na czynniki pierwsze uchodzi za najważniejsze i o dużym praktycznym znaczeniu w arytmetyce. ”

Carl Friedrich Gauss

Iloczyn liczb naturalnych jest zawsze liczbą naturalną, są więc liczby naturalne, będące iloczynami dwóch liczb naturalnych większych od jedności. Są także liczby naturalne większe od jedności, które nie są iloczynami dwóch liczb naturalnych większych od jedności. Takie właśnie liczby nazywamy pierwszymi. Liczby pierwsze to swego rodzaju cegiełki służące do budowania kolejnych liczb naturalnych.
Liczby pierwsze to liczby naturalne, które posiadają dokładnie dwa dzielniki (liczbę 1 i samą siebie).

Przykład 1 *Kilka początkowych liczb pierwszych: 2,3,5,7,11,13,17,19, ...*

Jeśli liczba naturalna większa od 1 nie jest liczbą pierwszą, to jest iloczynem dwóch liczb naturalnych od niej mniejszych. Liczby takie nazywamy liczbami złożonymi.

Liczby złożone to liczby naturalne, które posiadają więcej niż dwa dzielniki.

Przykład 2 *Kilka początkowych liczb złożonych: 4,6,8,9,10,12,14,15, ...*

Liczby 0 i 1 nie należą ani do liczb pierwszych ani do złożonych. Kiedyś uznawano liczbę 1 za pierwszą, jest ona jednak tak różna od właściwych liczb pierwszych, że dziś lokuje się ją w odrębnej klasie, nosi nazwę jedności.

2 Rozpoznawanie liczby pierwszej

2.1 Szukanie dzielników liczby

Aby sprawdzić, czy liczba naturalna jest liczbą pierwszą, należy dzielić ją kolejno przez wszystkie liczby większe od 1 i mniejsze równe pierwiastka kwadratowego z tej liczby. Jeśli przy każdym dzieleniu reszta z dzielenia jest różna od zera, to liczba jest liczbą pierwszą. Natomiast jeżeli choć jedno dzielenie daje resztę równą zero, to sprawdzana liczba naturalna jest liczbą złożoną. Nie jest to więc problem teoretyczny, jednak praktycznie trudny w przypadku bardzo dużych liczb.

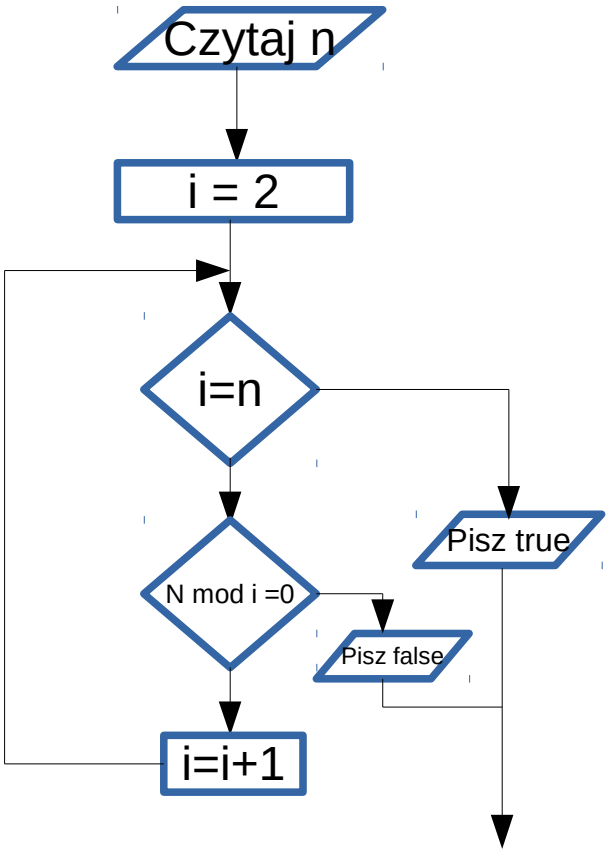

Diagram 1

Jeśli liczba jest stosunkowo niewielka, takie dzielenia możemy przeprowadzić sami, natomiast jeśli liczba nie jest już mała, to można ją sprawdzić z pomocą komputera. Maszynę trzeba zaprogramować, czyli napisać algorytm, który

rozstrzygnie, czy dana liczba jest pierwsza. Algorytm ten musi być przy tym efektywny, taki, który wykona możliwie jak najmniej operacji.

2.2 Sito Eratostenesa

Problemem liczb pierwszych zajmowali się matematycy od bardzo dawna. Jednym z nich był matematyk grecki Eratostenes z Cyreny, żyjący w III w. p.n.e. Wymyślona przez niego metoda wyznaczania wszystkich liczb pierwszych nie większych od zadanej liczby nosi do dziś nazwę sita Eratostenesa.

Aby sprawdzić, czy liczba naturalna n jest liczbą pierwszą, należy dzielić ją przez każdą taką liczbę $k > 1$, gdzie $k^2 \leqslant n$. Sposób ten nie jest najbardziej efektywną metodą, ponieważ trzeba wykonać dużą liczbę czasochłonnych dzieleń, tym większą, im większą wartość ma badana liczba.

Skoro łatwiej jest mnożyć niż dzielić, Eratostenes zamiast sprawdzać podzielność kolejnych liczb naturalnych, zaproponował usuwanie ze zbioru liczb naturalnych wielokrotności kolejnych liczb, które nie zostały wcześniej usunięte.

Sprawdźmy na przykładzie. Niech n=100. Należy postępować następująco: wypisać wszystkie liczby do 100, wykreślić wszystkie wielokrotności liczby pierwszej 2, w każdym następnym kroku należy wykreślić wszystkie wielokrotności najmniejszej kolejnej nie wykreślonej liczby p, które są większe od p. Wystarczy to zrobić dla takich p, że $p^2 \leqslant 100$, w naszym przypadku dla liczb pierwszych 2,3,5,7. Wszystkie wielokrotności liczb 2,3,5,7 należy odsiać, liczby, które nie zostały wykreślone są liczbami pierwszymi.[3]

Krok 1

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Krok 2

	2	**3**	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Krok 3

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Krok 4

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Krok 5

	2	3	4	5	6	7	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

$$\begin{bmatrix} 2 & 3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 \\ 31 & 37 & 41 & 43 & 47 & 53 & 59 & 61 & 67 & 71 \\ 73 & 79 & 83 & 89 & 97 & 101 & 103 & 107 & 109 & 113 \\ 127 & 131 & 137 & 139 & 149 & 151 & 157 & 163 & 167 & 173 \\ 179 & 181 & 191 & 193 & 197 & 199 & 211 & 223 & 227 & 229 \end{bmatrix}$$

W powyższej macierzy prezentuję liczby pierwsze takie że $1 \leqslant p < 230$

2.3 Twierdzenie Legrange'a

Twierdzenie 1 *Jeżeli p jest liczbą pierwszą, wielomian* $f(x) = a_0 * x^n + a_1 * x^{n-1} + \ldots + a_{n-1} * x + a_n$ *jest wielomianem stopnia n o współczynnikach całkowitych, gdzie współczynnik a0 jest niepodzielny przez p, to wśród liczb* $x = 0, 1, 2, \ldots, p-1$ *istnieje nie więcej niż n takich, dla których liczba f(x) jest podzielna przez p.[2]*

Wniosek z twierdzenia Lagrange'a: Jeżeli p jest liczbą pierwszą, a f(x) jest wielomianem stopnia n o współczynnikach całkowitych, oraz jeżeli istnieje więcej niż n liczb naturalnych x¡p, dla których f(x) jest podzielne przez p, to wszystkie współczynniki wielomianu f(x) muszą być podzielne przez p.

2.4 Funkcja L. Eulera

L. Euler, poszukując różnowartościowej funkcji przporządkowującej liczbom naturalnym liczby pierwsze, zwrócił uwagę na funkcję f: $N \to N$ taką, że:

$$f(n) = n^2 + n + 41 \text{ [1]}$$

X	$f(x) = x^2 + x + 41$
0	41
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151

W powyżej tabeli prezentuje wartości funkcji$f(n)$ dla x takich że: $0 < x \leqslant 10$

Literatura

[1] Jerzy Topp, *Wstęp do MATEMATYKI*. Gdańsk: Wydawnictwo Politechniki Gdańskiej 2012

[2] Wikipedia, *http://pl.wikipedia.org/wiki/Liczba_pierwsza*.

[3] Math.edu.pl, *http://www.math.edu.pl/liczby-pierwsze*