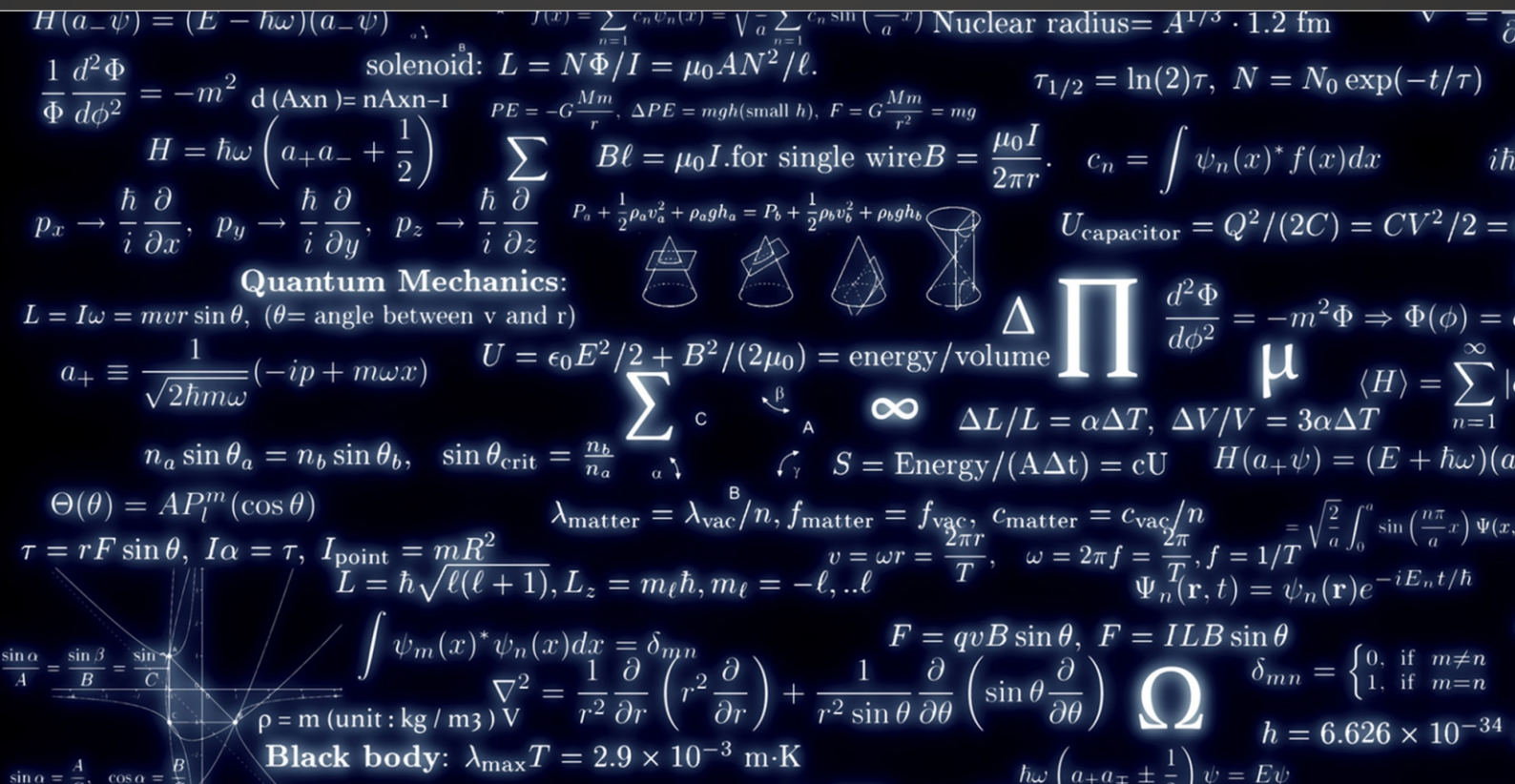
Artykuł IV

KC

PRIME NUMBERS



Article IV: *Szybka faktoryzacja dowolnej liczby złożonej*

I. Na konferencji prasowej w Polskiej Agencji Prasowej w dniu 1 grudnia 2017 r. zaprezentowaliśmy sześć wzorów *generujących wyłącznie, kolejno i wszystkie liczby złożone.* Formuła konferencji nie pozwalała jednak na szczegółowe omówienie ich znaczenia dla nauki i zastosowań praktycznych.

Rangę wszystkich odkryć naukowych określają ich zastosowania: zarówno te ze świata idei, a więc czysto naukowe, jak również i te, które determinują technologię.

W Artykule II na stronie www.prime-numbers.pl wspominaliśmy o kryptografii opartej na liczbach złożonych, będących iloczynami dwóch liczb pierwszych:

***„Liczbom pierwszym zawdzięczamy funkcjonowanie w obecnym kształcie całej naszej cywilizacji:* internet, karty kredytowe, przelewy bankowe, szyfry wojskowe i tajnych służb, podpis cyfrowy to pierwsze z brzegu przykłady. Na tych, które składają się ze stu i więcej cyfr, można już zarabiać duże pieniądze. Przechowywane są w skarbcach i strzeżone równie pilnie jak rezerwy złota – kupców nie brakuje, a liczby pierwsze *determinują funkcjonowanie współczesnych relacji ekonomicznych*."**

Twórcy tych szyfrów wyszli z założenia, że w praktyce, problem szybkiej faktoryzacji liczb złożonych, jest w najbliższych dziesięcioleciach problemem nie do rozwiązania, nawet przy użyciu najbardziej wydajnych komputerów. Chodzi oczywiście o tak zwane szyfry z kluczem publicznym: podaje się do publicznej wiadomości liczbę złożoną, będącą iloczynem dwóch, losowo wybranych liczb pierwszych, które nie są znane ogółowi. Ostatnimi czasy były to liczby dwustucyfrowe. Poniżej pokażemy algorytm szybkiej faktoryzacji dowolnej – w zastosowaniach – liczby. Jego idea jest pewną analogią do sposobu obliczania kolejnych przybliżeń pierwiastka kwadratowego z liczby pierwszej, np. liczby 2, z porównywalną *wydajnością całego procesu*. Każde dwa dzielenia dostarczają informacji o wielkości błędu:

1° Wiemy, że pierwiastek stopnia drugiego z liczby dwa musi być liczbą większą od $\sqrt{1}$, ale mniejszą od $\sqrt{4}$, czyli:

$$\sqrt{1} < \sqrt{2} < \sqrt{4}$$

Tak więc poszukiwana liczba musi być większa od 1, ale mniejsza od 2. Kolejne przybliżenia również otrzymujemy „metodą młotka", czyli na sposób eksperymentalno-intuicyjny:

2° Podnosimy do kwadratu, „na oko" liczbę dającą środek, czyli 1,5 i otrzymujemy wartość nieco większą od 2:

$(1{,}5)^2 = 2{,}25$

3° Podobnie intuicyjnie podnosimy do kwadratu liczbę o jeden mniejszą w ostatnim rzędzie wielkości i otrzymujemy liczbę nieco mniejszą od 2:

$(1{,}4)^2 = 1{,}96$

4° Kolejne wartości przybliżeń otrzymujemy w taki sam sposób, wzmacniając intuicję o pewne rozumowanie: skoro z liczby1,96 brakuje 0,04 do liczby 2, a liczba 2, 25 jest za daleko od liczby 2 o 0,25 (czyli „za daleko" jest ponad 6 razy większe niż „za blisko" to, z uwagi na to, że do dyspozycji mamy jedynie 10 cyfr (od 0 – 9) następną cyfrą musi być albo cyfra 1 albo cyfra 2, gdyż 10:7 ≅ 1,43 :

$(1,41)^2$ = 1, 9881 $(1,42)^2$ = 2,0164

Dokonujemy oszacowania: jest „za blisko" o 0,0119 i „za daleko" o 0,0164 więc intuicja podpowiada kolejną cyfrę 4, i tak dalej ad infinitum.

W tym miejscu chcielibyśmy skomentować sformułowanie: *wydajność tego procesu*. Każde dwa obliczenia, w przykładzie na poszukiwanie $\sqrt{2}$, przesuwają dokładność przybliżenia o rząd wielkości. W przypadku poniższego algorytmu, wydajność faktoryzacji liczby złożonej jest zbliżona: dla pięciocyfrowej liczby to 2 x 4 + 1 = 9 istotnych operacji mnożenia, a dla dwunastocyfrowej 2x29 takich operacji. Ekstrapolując te wielkości dla liczb dwustucyfrowych wymaga on jedynie kilkuset obliczeń (co najwyżej 2 x 10 operacji mnożenia dla każdej cyfry), z czym potrafiłby uporać się bardzo cierpliwy człowiek, o odpowiednim kalkulatorze i komputerach nie wspominając. Co więcej: *proces faktoryzacji nie wymaga znajomości jakichkolwiek liczb pierwszych*. Przejdźmy więc do omówienia algorytmu.

I. Rozmieszczenie liczb złożonych

Wszystkie liczby złożone usytuowane są w następujących podzbiorach liczb naturalnych

1° Liczby złożone podzielne przez dwa są wyrazami ciągu: 2n + 2.

Dla:

n = 1 mamy 2 x 1 + 2 = 4

n = 2 mamy 2 x 2 + 2 = 6

n = 3 mamy 2 x 3 + 2 = 8, etc.

2°Pozostałe liczby złożone podzielne przez trzy, a nie będące wyrazami ciągu 2n + 2, są wyrazami ciągu: 6n + 3.

Dla:

n = 1 mamy 6 x 1 + 3 = 9

n = 2 mamy 6 x 2 + 3 = 15

n = 3 mamy 6 x 3 + 3 = 21, etc.

3°Wszystkie pozostałe liczby złożone są wyrazami dwóch ciągów: 6n – 1 oraz 6n + 1, które zawierają jednak również wszystkie liczby pierwsze oprócz liczb 2 i 3. Poniższe wzory to matematyczna formuła umożliwiająca wyizolowanie liczb złożonych (a więc również pierwszych) z ciągów 6n – 1 oraz 6n + 1. *Tym samym otrzymujemy łącznie 6 wzorów, które generują po kolei, wyłącznie i wszystkie liczby złożone*.

Łatwo zauważyć, że wszystkie liczby złożone w ciągach 6n – 1 oraz 6n + 1 mogą być jedynie następującymi iloczynami:

(1) $6n + 1 = (6k + 1)(6c + 1) = 36kc + 6k + 6c + 1 \quad / -1$

$6n = 36kc + 6k + 6c \quad / :6$

$n = 6kc + k + c$

(2) $6n + 1 = (6k - 1)(6c - 1) = 36kc - 6k - 6c + 1 \quad / -1$

$6n = 36kc - 6k - 6c \quad / :6$

$n = 6kc - k - c$

(3) $6n - 1 = (6k - 1)(6c + 1) = 36kc + 6k - 6c - 1 \quad / +1$

$6n = 36kc + 6k - 6c \quad / :6$

$n = 6kc + k - c$

(4) $6n - 1 = (6k + 1)(6c - 1) = 36kc - 6k + 6c - 1 \quad / +1$

$6n = 36kc - 6k + 6c \quad / :6$

$n = 6kc - k + c$

W tych wzorach n oznacza numer wyrazu ciągu, o którym nie wiadomo czy jest liczbą pierwszą czy też złożoną. Z kolei k i c są również numerami wyrazów tych ciągów, o których co prawda też nie wiadomo, czy wskazują liczby pierwsze czy też liczby złożone, natomiast dostarczają niezwykle istotnej informacji. Wiemy, że wszystkie ich wzajemne i kolejne iloczyny dają wszystkie, kolejno i wyłącznie liczby złożone w tych ciągach. Ponieważ wartość liczbowa każdego takiego iloczynu jest równa pewnemu n, stąd kryterium pierwszości, dla każdej liczby pierwszej, większej od 3:

Kryterium 1: **Każdy numer n w ciągu 6n + 1, którego nie można przedstawić w postaci:**

$n = 6kc + k + c \quad \text{lub} \quad n = 6kc - k - c$

jest takim numerem wyrazu tego ciągu, że ten wyraz jest liczbą pierwszą.

Kryterium 2: **Każdy numer n w ciągu 6n – 1, którego nie można przedstawić w postaci:**

$n = 6kc + k - c \quad \text{lub} \quad n = 6kc - k + c, \; k \geq c$

jest takim numerem wyrazu tego ciągu, że ten wyraz jest liczbą pierwszą.

Przedstawione powyżej kryteria pozwalają zrozumieć mechanizm powstawania liczb pierwszych bliźniaczych (np. 5 i 7), a także trojaczych (np. 41,43 i 47), czworaczych (np.11,13,17 i 19) etc.

6n – 1:		6n + 1:
	dla n = 1 mamy:	
6 x 1 – 1 = 5		6 x 1 + 1 = 7
	dla n = 2 mamy:	
6 x 2 – 1 = 11		6 x 2 + 1 = 13
	dla n = 3 mamy:	
6 x 3 – 1 = 17		6 x 2 + 1 = 19

Satysfakcji czytelników pozostawiamy sprawdzenie, że brak jest takich wartości k i c, które umożliwiałyby przedstawienie n = 1, n = 2 lub n = 3 za pomocą formuł z kryteriów 1 i 2. Dlaczego ? Ponieważ n, k i c są numerami wyrazów ciągów, więc mogą przyjmować jedynie wartości ≥ 1 .

Dla k = 1 i c =1 mamy odpowiednio:

n = 6kc – k + c	n = 6kc – k – c
n = 6 x 1 x 1 – 1 + 1 = 6	n = 6 x 1 x 1 – 1 – 1 = 4
n = 6kc + k – c	n = 6kc + k + c
n = 6 x 1 x 1 + 1 – 1 = 6	n = 6 x 1 x 1 + 1 + 1 = 8
wtedy:	wtedy:
6n – 1 = 6 x 6 – 1 = 35	6n + 1 = 6 x 4 + 1 = 25
	6n + 1 = 6 x 8 + 1 = 49

czyli otrzymaliśmy pierwsze liczby złożone w tych ciągach: dla 6n – 1 pierwszą liczbą złożoną jest 6 wyraz tego ciągu, a dla 6n + 1 to odpowiednio 4 i 8 wyraz tego ciągu.

Dla k = 1 i c = 2 oraz k = 2 i c = 1 mamy odpowiednio:

n = 6 x 1 x 2 + 1 – 2 = 11	n = 6 x 1 x 2 – 1 – 2 = 9
n = 6 x 2 x 1 + 2 – 1 = 13	n = 6 x 1 x 2 + 1 + 2 = 15

Jak łatwo zauważyć, dla k = c w ciągu 6n – 1, niepotrzebne są obliczenia z obydwu wzorów, a zastosowanie tych wzorów jest pewną analogią do wzorów na otrzymywanie trójek pitagorejskich.

Zanim przejdziemy do szczegółowego omówienia algorytmu szybkiej faktoryzacji liczb złożonych, chcieliśmy jeszcze zwrócić uwagę na poniższą statystykę – jest pouczająca dla rozumienia procesu rozmieszczania się liczb pierwszych bliźniaczych:

6n – 1	n	6n + 1	6n – 1	n	6n + 1
5	n = 1	7	305	n = 51	307
11	n = 2	13	311	n = 52	313
17	n = 3	19	317	n = 53	319
23	n = 4	25	323	n = 54	325
29	n = 5	31	329	n = 55	331
35	n = 6	37	335	n = 56	337
41	n = 7	43	341	n = 57	343
47	n = 8	49	347	n = 58	349
53	n = 9	55	353	n = 59	355
59	n = 10	61	359	n = 60	361
65	n = 11	67	365	n = 61	367
71	n = 12	73	371	n = 62	373
77	n = 13	79	377	n = 63	379
83	n = 14	85	383	n = 64	385
89	n = 15	91	389	n = 65	391
95	n = 16	97	395	n = 66	397
101	n = 17	103	401	n = 67	403
107	n = 18	109	407	n = 68	409
113	n = 19	115	413	n = 69	415
119	n = 20	121	419	n = 70	421
125	n = 21	127	425	n = 71	426
131	n = 22	133	431	n = 72	433
137	n = 23	139	437	n = 73	439
143	n = 24	145	443	n = 74	445
149	n = 25	151	449	n = 75	451
155	n = 26	157	455	n = 76	457
161	n = 27	163	461	n = 77	463
167	n = 28	169	467	n = 78	469
173	n = 29	175	473	n = 79	475
179	n = 30	181	479	n = 80	481
185	n = 31	187	485	n = 81	487
191	n = 32	193	491	n = 82	493
197	n = 33	199	497	n = 83	499
203	n = 34	205	503	n = 84	505
209	n = 35	211	509	n = 85	511
215	n = 36	217	515	n = 86	517
221	n = 37	223	521	n = 87	523
227	n = 38	229	527	n = 88	529
233	n = 39	235	533	n = 89	535
239	n = 40	241	539	n = 90	541
245	n = 41	247	545	n = 91	547
251	n = 42	253	551	n = 92	553
257	n = 43	259	557	n = 93	559
263	n = 44	265	563	n = 94	565
269	n = 45	271	569	n = 95	571
275	n = 46	277	575	n = 96	577
281	n = 47	283	581	n = 97	583
287	n = 48	289	587	n = 98	589
293	n = 49	295	593	n = 99	595
299	n = 50	301	599	n = 100	601

II. Algorytm faktoryzacji liczb n-cyfrowych.

Faktoryzacja liczb złożonych 4-cyfrowych (i mniejszych) metodą tradycyjną, czyli za pomocą sita Eratostenesa, przy założeniu znajomości liczb pierwszych mniejszych od $\sqrt{10\,000}$ = 100 i użyciu kalkulatora jest oczywiście dogodniejsze niż posłużenie się naszym algorytmem. Powszechnie dostępne listy liczb pierwszych kończą się jednak na pewnych wartościach, a nawet są z oczywistych względów utajniane. Z uwagi na złożoność obliczeniową, począwszy od pewnych wartości, lista kolejnych liczb pierwszych pozostaje tajemnicą, nawet dla tych, którzy utajnić by je mogli. Nasz algorytm efektywnej faktoryzacji nie wymaga znajomości jakichkolwiek liczb pierwszych, a prezentacja faktoryzacji kolejnych liczb: 6-cyfrowych, 7- cyfrowych, 8-cyfrowych, etc. pozwala na ekstrapolację i możliwość przewidywania złożoności procesów obliczeniowych dla liczb n-cyfrowych. Poniżej odpowiednie prezentacje z omówieniem. Chcielibyśmy zwrócić uwagę czytelników na rosnące odległości między parą liczb pierwszych, których iloczyn daje faktoryzowaną liczbę złożoną: o ile bowiem pierwsza para różni się jedynie o kilka jedności, to różnice między kolejnymi parami rosną stopniowo do kilku rzędów wielkości. To bardzo ważna intuicja. Zauważmy, że wraz ze wzrostem tylko o rząd wielkości np. ze 100 do 1000 następuje aż 9-krotny przyrost ilości liczb. Łatwo zauważyć więc, że w przypadku gdy przechodzimy z kodowania liczbami pierwszymi z liczb liczących 199 cyfr na liczby 200-cyfrowe, większość , bo aż 90% liczb przypada na nowopowstały rząd wielkości. To właśnie ten gwałtowny przyrost ilości liczb wraz ze wzrostem o kolejne rzędy wielkości powoduje, że faktoryzacja tak dużych liczb metodami tradycyjnymi wymagałaby pracy superkomputera przez ok.148 lat dla każdej liczby. Proponowana poniżej zmiana podejścia, drastycznie redukuje liczbę operacji, znacząco poniżej granicy tzw. efektywnego czasu wielomianowego, jak ujmują to specjaliści.

Znakomitą ilustracją dla idei prowadzącej do zaproponowanej przez nas faktoryzacji liczb złożonych przy pomocy zaproponowanych 6 wzorów, są... instrukcje strzelania artylerii. Marynarka Wojenna Stanów Zjednoczonych zakłada trafienie pociskiem w cel już przy drugim wystrzale z działa. Dalmierzysta, dzięki namiarom laserowym podaje oficerowi ogniowemu współrzędne położenia celu. Jeżeli pocisk nie trafił w cel, obsługa wspomnianego dalmierza laserowego podaje odległość położenia i kierunku celu od miejsca upadku pocisku w wodę, obsługa działa nanosi niezbędne poprawki w kącie podniesienia i kierunku lufy działa (lewo – prawo), i zgodnie z instrukcją drugi pocisk trafia w cel. Instrukcje strzelania artylerii naziemnej Układu Warszawskiego zakładały trafienie w cel przy... trzeciej próbie, oczywiście w przypadku nietrafienia w cel za pierwszym razem. Jak to wyglądało w praktyce? Zakładano, że dowódca działa, ma do dyspozycji dalmierzystę z tzw. dalmierzem optycznym, który znajduje się pomiędzy działem a celem. Jeżeli ostrzał odbywa się z zakrytego stanowiska ogniowego, co oznacza po prostu tyle, że cel jest na tyle daleko, że jest niewidoczny dla obsługi działa, to dalmierzysta przez radiostację podaje oficerowi ogniowemu współrzędne celu. Po oddaniu strzału,

dalmierzysta podaje koordynaty odległości i kierunku uderzenia pocisku w stosunku do celu. Jeżeli dalmierzysta zameldował np. przez radio: ”lewo 50, 200 krótki” to oficer ogniowy dysponował informacją, że pocisk upadł 200 m przed celem, oraz 50 m w lewo od kierunku celu. Oficer ogniowy, zgodnie z instrukcją strzelania artylerii naziemnej musiał teraz tak zmienić nastawy działa, aby drugi pocisk upadł... za celem. Wreszcie dokonując tzw. przepołowienia nastaw, następował trzeci wystrzał i trafienie w cel. Jak łatwo zauważyć przypomina to scenariusz gry komputerowej. Idea faktoryzacji za pomocą poniższego scenariusza sprowadza się do pewnej analogii. Na polu walki zamiast doświadczonego dalmierzysty na posterunku obserwacyjnym znajdzie się niewyszkolony żołnierz bez dalmierza, na miejsce poległego oficera ogniowego staje żołnierz bez przeszkolenia artyleryjskiego i wtedy operacja trafienia w cel nieco się wydłuża. Teoria strzału orzeka uwzględnienie przy kącie i kierunku podniesienia lufy działa uwzględnienie pewnych parametrów: temperatury, siły i kierunku wiatru, masy pocisku oraz masy ładunku prochowego. W takiej sytuacji informacje o kolejnych miejscach upadku pocisku w stosunku do celu mogą być następujące: ”za daleko i bardziej w prawo”, „ za krótko i bardziej w lewo”, „trochę za daleko i dobrze w kierunku” etc. Jakkolwiek proces nieco się wydłuża o dodatkowe strzały pomocnicze, trafienie w cel nastąpi po wyczerpaniu pewnej liczby możliwych parametrów strzału, niekoniecznie wszystkich. A jak ta idea odnosi się do faktoryzacji? Z uwagi na zastosowania prezentacja ogniskuje się oczywiście na faktoryzacji liczb złożonych będących iloczynami jedynie dwóch liczb pierwszych.

III. Faktoryzacje

1. Faktoryzacja liczby 5-cyfrowej 101x109 = 11 009 czyli odpowiednio mnożymy liczby o numerach: c = 17 x k = 18 dające numer liczby 11 009: n = 1835 .

- *metoda klasyczna faktoryzacji liczby złożonej*

1° Obliczamy pierwiastek kwadratowy z liczby 11 009:

$\sqrt{11\,009} \cong$ 104,92

2° Sporządzamy listę liczb pierwszych ≤ 104:

2,3,5,7, ... , 103. Daje to w sumie 27 dzielników pierwszych, a efektywny rozkład otrzymujemy po wykonaniu 26 operacji dzielenia:

11 009 : 2 = 5 504,5

11 009 : 3 = 3 669,9(6)

.

.

11 009 : 101 = 109

- *metoda faktoryzacji Cywińskiego – Książek*

1° Sprawdzamy przynależność liczby 11 009 do odpowiedniego ciągu. Dodając i odejmując liczbę 1, otrzymujemy odpowiednio dwie liczby: 11 010 i 11 008. Sprawdzamy, która z nich

dzieli się przez liczbę 6. Przypomnijmy, że liczba parzysta podzielna przez 3, jest również podzielna przez liczbę 6. Ponieważ to kryterium podzielności spełnia liczba 11 010, stąd wniosek, że liczba 11 009 jest liczbą postaci 6n – 1

2° Ustalamy którym numerem wyrazu tego ciągu jest liczba 11 009, korzystając ze wzorów z Kryterium 2 (dlatego używamy dwóch kolorów: czarny i niebieski). Kolejne 4 kroki algorytmu pozwalają ustalić o ile względem siebie mogą się maksymalnie różnić k i c:

$k \geq c$:			$k \geq c$:
$6n - 1 = (6k + 1)(6c - 1)$			$6n - 1 = (6k - 1)(6c + 1)$
$6n - 1 = 36kc - 6k + 6c - 1$	/ +1	lub	$6n - 1 = 36kc + 6k - 6c - 1$ / +1
$6n = 36kc - 6k + 6c$	/ : 6		$6n = 36kc + 6k - 6c$ / :6
$n = 6kc - k + c$			$n = 6k + k - c$

Podstawiamy wartości liczbowe:

$11\,009 = 36kc - 6k + 6c - 1$	/ +1		$11\,009 = 36kc + 6k - 6c - 1$ /+1
$11\,010 = 36kc - 6k + 6c$	/ : 6	lub	$11\,010 = 36kc + 6k - 6c$ / : 6
$1\,835 = 6kc - k + c$			$1\,835 = 6kc + k - c$
dla k = c:			dla k = c :
$1\,835 = 6k^2$	/ : 6		$1\,835 = 6k^2$ / :6
$305{,}8(3) = k^2$	/ $\sqrt{...}$		$305{,}8(3) = k^2$ / $\sqrt{...}$
$k = k_0 \cong 17{,}49$, więc $k \neq c$			$k = k_0 \cong 17{,}49$, więc $k \neq c$

Pozostając w analogii do poetyki ostrzału artyleryjskiego, oddaliśmy pierwszy strzał, pozwalający ustalić, że numer k jest różny od numeru c. Kolejny krok algorytmu to ustalenie o ile k i c mogą różnić się od siebie maksymalnie.

dla k > c		dla k > c
3° k_{max} jest dla c = 1:		1° k_{max} jest dla c = 1:
$1\,835 = 6xkx1 - k + 1 = 5k + 1$ / -1		$1\,835 = 6xkx1 + k - c = 7k - 1$ / +1
$1\,834 = 5k$	/ :5	$1\,836 = 7k$ / :7
$k = 366{,}8$		$k \cong 262{,}29$
k = 367, c = 1: n = 6x367x1 – 367 + 1 = 1836		k = 263, c = 1: n = 6x263x1 + 263 – 1 = 1 840
„o 1 za daleko”		„o 5 za daleko”
k = 366, c = 1: n = 6x366x1 – 366 + 1 = 1831		k = 262, c = 1: n = 6x262x1 + 262 – 1 = 1 833
„za blisko o 4”		„za blisko o 2”
k = 366, c = 2: n = 6x366x2 – 366 + 2 = 4 028		k = 262, c = 2: n = 6x262x2 + 262 – 2 = 3 404

dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

Wykonaliśmy wstępne „obramowanie celu” , uzyskując informację do jakiego przedziału muszą należeć k i c.

4°Ponieważ k „musi być znacząco bliżej c” i jednocześni dla k = c = k_0 mamy:

k_0 = 17,49 ≅ 17, więc ponieważ k > c, kontynuujemy „ostrzał celu” zmieniając stopniowo odpowiednie wartości:

k = 18, c = 17: n = 6x18x17 – 18 + 17 = 1836 – 1 = 1835 wartość poszukiwana

c. b. d. o.

Ponieważ numery k i c były najbliżej siebie, jak to tylko było możliwe, więc rozkład otrzymaliśmy niemal natychmiast. Zanim jednak przejdziemy do rozkładu liczb, dla których k i c różnią się znacząco, chcielibyśmy pokazać dwa warunki, wspierające intuicję , podobnie jak w przypadku znajdowania wartości dla $\sqrt{2}$. Wynikają one wprost z analizy wzorów do generowania liczb złożonych:

1° k + c > $2k_0$ ale $k + c < 2k_0$ - relacja między połową obwodu prostokąta i połową obwodu kwadratu

2° k x c > k_0^2 ale $k \times c < k_0^2$ - pole prostokąta i pole kwadratu

w zadanych wzorami warunkach. Obszerniej nawiążemy do tych rozumowań przy okazji kolejnych prezentacji.

2. Faktoryzacja liczby 5-cyfrowej 101x127 = 12 827 czyli odpowiednio mnożymy liczby o numerach: c = 17 x k = 21 dające numer liczby 12 827: n = 2 138 .

- *metoda klasyczna faktoryzacji liczby złożonej*

1° Obliczamy pierwiastek kwadratowy z liczby 12 827:

$\sqrt{12\,827} \cong$ 113.26

2° Sporządzamy listę liczb pierwszych ≤ 113:

2,3,5,7, ... , 113. Daje to w sumie 30 dzielników pierwszych, a efektywny rozkład otrzymujemy po wykonaniu 26 operacji dzielenia:

12 827 : 2 = 6 413,5

12 827 : 3 = 4 275,(6)

.

.

12 827 : 101 = 127

- *metoda faktoryzacji Cywińskiego – Książek*

1° Sprawdzamy przynależność liczby 12 827 do odpowiedniego ciągu. Dodając i odejmując liczbę 1, otrzymujemy odpowiednio dwie liczby: 12 828 i 12 826. Sprawdzamy, która z nich dzieli się przez liczbę 6. Przypomnijmy, że liczba parzysta podzielna przez 3, jest również podzielna przez liczbę 6. Ponieważ to kryterium podzielności spełnia liczba 12 828, stąd wniosek, że liczba 12 827 jest liczbą postaci 6n – 1

2° Ustalamy którym numerem wyrazu tego ciągu jest liczba 12 827, korzystając ze wzorów z Kryterium 2 (dlatego używamy dwóch kolorów: czarny i niebieski). Kolejne 4 kroki algorytmu pozwalają ustalić o ile względem siebie mogą się maksymalnie różnić k i c:

$k \geq c$:			$k \geq c$:
$6n - 1 = (6k + 1)(6c - 1)$			$6n - 1 = (6k - 1)(6c + 1)$
$6n - 1 = 36kc - 6k + 6c - 1$	/ +1	lub	$6n - 1 = 36kc + 6k - 6c - 1$ / +1
$6n = 36kc - 6k + 6c$	/ : 6		$6n = 36kc + 6k - 6c$ / :6
$n = 6kc - k + c$			$n = 6k + k - c$

Podstawiamy wartości liczbowe:

$12\,827 = 36kc - 6k + 6c - 1$	/ +1		$12\,827 = 36kc + 6k - 6c - 1$ / +1
$12\,828 = 36kc - 6k + 6c$	/ : 6	lub	$12\,828 = 36kc + 6k - 6c$ / : 6
$2\,138 = 6kc - k + c$			$2\,138 = 6kc + k - c$
dla k = c:			dla k = c :
$2\,138 = 6k^2$	/ : 6		$2\,138 = 6k^2$ / :6
$356{,}(3) = k^2$	/ $\sqrt{...}$		$356{,}(3) = k^2$ / $\sqrt{...}$
$k = k_0 \cong 18{,}88$, więc $k \neq c$			$k = k_0 \cong 18{,}88$, więc $k \neq c$

gdyż nie otrzymaliśmy liczby naturalnej

Pozostając w analogii do poetyki ostrzału artyleryjskiego, oddaliśmy pierwszy strzał, pozwalający ustalić, że numer k jest różny od numeru c. Kolejny krok algorytmu to ustalenie o ile k i c mogą różnić się od siebie maksymalnie.

dla k > c

3° k_{max} jest dla c = 1:
2 138 = 6xkx1 – k +1 = 5k +1 / -1
2 137 = 5k / :5
k = 427,4
k = 428, c = 1: n = 6x428x1 – 428 + 1 = 2 141 „o 3 za daleko”
k = 427, c = 1: n = 6x427x1 – 427 + 1 = 2 136 „za blisko o 2”
k = 426, c = 2: n = 6x426x2 – 426 + 2 = 4 262 dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

dla k > c

1° k_{max} jest dla c = 1:
2 138 = 6xkx1 + k – c = 6k – 1 / +1
2 139 = 7k / :7
k ≅ 305,57
k = 306, c = 1: n = 6x306x1 + 306 – 1 = 2 141 „o 3 za daleko”
k = 305, c = 1: n = 6x305x1 + 305 – 1 = 2 134 „za blisko o 4”
k = 262, c = 2: n = 6x262x2 + 262 – 2 = 3 142 dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

Wykonaliśmy wstępne „obramowanie celu” , uzyskując informację do jakiego przedziału muszą należeć k i c.

4°Ponieważ k „musi być znacząco bliżej c” i jednocześni dla k = c = k_0 mamy:
k_0 ≅ 18,88 więc ponieważ k > c, kontynuujemy „ostrzał celu” zmieniając stopniowo odpowiednie wartości:
k = 20, c = 18: n = 6x20x18 – 20 + 18 = 2 160 – 2 = 2 158 „za daleko o 20”
k = 20, c = 18: n = 6x20x18 + 20 – 18 = 2 160 + 2 = 2 160 „za daleko o 22”
k = 21, c = 17: n = 6x21x17 – 21 + 17 = 2 142 – 4 = 2 138 wartość poszukiwana

c. b. d. o.

3.Faktoryzacja liczby pięciocyfrowej 199 x 101 = 20 099, czyli odpowiednio mnożymy liczby o numerach: c = 17 x k = 33, dające numer liczby 20 099: n = 3 350

- metoda klasyczna faktoryzacji liczby złożonej

1° Obliczamy pierwiastek kwadratowy z liczby 20 099:
$\sqrt{20\,099} \cong 141{,}77$
2° Sporządzamy listę liczb pierwszych ≤ 141:

2,3,5,7, … , 139. Daje to w sumie 32 dzielniki pierwsze, a efektywny rozkład otrzymujemy po wykonaniu 26 operacji dzielenia:

20 099 : 2 = 10 049,5

20 099 : 3 = 6 699,(6)

.

.

20 099 : 101 = 199

- metoda faktoryzacji Cywińskiego – Książek

1° Sprawdzamy przynależność liczby 20 099 do odpowiedniego ciągu. Dodając i odejmując liczbę jeden otrzymujemy odpowiednio dwie liczby: 20 100 i 20 098. Sprawdzamy, która z nich dzieli się przez liczbę 6. Przypomnijmy, że liczba parzysta podzielna przez 3, jest również podzielna przez liczbę 6. Ponieważ to kryterium podzielności spełnia liczba 20 100, stąd wniosek, że liczba 20 099 jest liczbą postaci 6n – 1

2° Korzystając ze wzorów z Kryterium 2 mamy:

$k \geq c$:			$k \geq c$:
$6n - 1 = (6k + 1)(6c - 1)$			$6n - 1 = (6k - 1)(6c + 1)$
$6n - 1 = 36kc - 6k + 6c - 1$	/ +1	lub	$6n - 1 = 36kc + 6k - 6c - 1$ / +1
$6n = 36kc - 6k + 6c$	/ : 6		$6n = 36kc + 6k - 6c$ / :6
$n = 6kc - k + c$			$n = 6k + k - c$

Podstawiamy wartości liczbowe:

$20\,099 = 36kc - 6k + 6c - 1$	/ +1		$20\,099 = 36kc + 6k - 6c - 1$ /+1
$20100 = 36kc - 6k + 6c$	/ : 6	lub	$20\,100 = 36kc + 6k - 6c$ / : 6
$3\,350 = 6kc - k + c$			$3\,350 = 6kc + k - c$
dla k = c:			dla k = c :
$3\,350 = 6k^2$	/ : 6		$3\,350 = 6k^2$ /:6
$558{,}33 = k^2$	/ $\sqrt{\ldots}$		$558{,}33 = k^2$ / $\sqrt{\ldots}$
$k = k_0 = 23{,}63$, więc $k \neq c$			$k = k_0 = 23{,}63$, więc $k \neq c$

dla k > c			dla k > c
3° k_{max} jest dla c = 1:			1° k_{max} jest dla c = 1:
$3\,350 = 6xkx1 - k + 1 = 5k + 1$	/ -1		$3\,350 = 6xkx1 + k - c = 6k - 1$ / +1
$3\,349 = 5k$	/ :5		$3\,351 = 7k$ / :7
$k = 669{,}8 \cong 670$			$k \cong 479$

k = 670, c = 1: n = 6x670x1 – 670 + 1 = 3351 k = 479, c = 1: n = 6x479x1 + 479 – 1 = 3352 „o 1 za daleko”

k = 669, c = 1: n = 6x669x1 – 669 + 1 = 3346 k = 478, c = 1: n = 6x478x1 + 478 – 1 = 3345 „za blisko” „za blisko”

k = 669, c = 2: n = 6x669x2 – 669 + 2 = 7361 k = 478, c = 2: n = 6x478x2 + 478 – 2 = 6212 dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c” dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

4°Ponieważ k „musi być znacząco bliżej c” i jednocześni dla k = c = k_0 mamy:

k_0 = 23,63 ≅ 24 więc dla odpowiednich wartości otrzymujemy:

k = 24, c =23: n = 6x24x23 – 24 + 23 = 3312 – 1 = 3311, 3350 – 3311 = 39 „za blisko”

k = 24, c =23: n = 6x24x23 + 24 – 23 = 3312 + 1 = 3313, 3350 – 3313 = 37 „ za blisko”

Otrzymana różnica „za blisko 39” („za blisko 37”) informuje nas, że iloczyn 6xkxc oraz jego pomniejszenie o (– k + c) lub powiększenie o (k – c) musi być „trochę większe”; zmieniamy wartości parametrów k i c o 1:

k = 25, c = 22 : n = 6x25x22 – 25 + 22 = 3297

k = 25, c = 22 : n = 6x25x22 + 25 – 22 = 3303

Otrzymaliśmy „bardziej za blisko”, stąd wniosek, że wartość iloczynu trzeba „trochę” podnieść. W tym miejscu możemy jednak intuicję wesprzeć pewnym rozumowaniem, podobnie jak w przypadku pierwiastkowania. Dla k = c = k_0 mamy:

n = 6xkxc – k + c = 6 x k_0 x k_0 – k_0 + k_0 = 6k_0^2 i n = 6xkxc + k – c = 6 x k_0 x k_0 + k_0 – k_0 = 6k_0^2

Zależność n = 6k_0^2 możemy rozumieć, na przykład, jako sześciokrotność pola kwadratu o boku k_0. W takim razie zależność, w której k ≠ c , możemy rozumieć jako sześciokrotność pola prostokąta o bokach k i c, pomniejszoną (powiększoną) o wartość liczbową różnicy długości tych boków: n = 6xkxc – k + c (n = 6xkxc + k – c). Tak więc mamy stosunkowo łatwy problem do rozwiązania: pole prostokąta musi być odpowiednio większe (mniejsze) od pola kwadratu o ile sześciokrotność tego pola zostanie pomniejszona (powiększona) o różnicę jego boków:

k + c > 2k_0 i k x c > k_0^2 oraz k + c < 2k_0 i k x c < k_0^2

Dla k = 27 i c = 21 oraz k_0 = 24 mamy 48 = 48 ale 27 x 21 > 553,8 i rzeczywiście:

k = 27, c = 21: n = 6x27x21 – 27 + 21 = 3 396 „ trochę za daleko”

k = 27, c = 21: n = 6x27x21 + 27 – 21 = 3 408 „ trochę za daleko”

Stąd wniosek, że k + c > 48, k powinno wzrosnąć, a c powinno zostać pomniejszone:

k = 31, c = 18: n = 6x31x18 – 31 + 18 = 3335 „trochę za blisko”

k = 30, c = 17: n = 6x30x17 + 30 – 17 = 3073 „dużo za blisko”

Ponieważ k + c = 49 daje wartość „trochę za blisko” więc sprawdzamy opcje dla k + c = 50:
Ponieważ otrzymaliśmy „dużo za blisko” więc sprawdzamy kolejne sumy k + c < 48

k = 32, c = 18: n = 6x32x18 – 32 + 18 = 3442 „mniej za blisko”
k = 32, c = 15: n = 6x32x15 + 32 – 15 = 2897 „jeszcze bardziej za blisko”
k = 33, c = 17: n = 6x33x17 – 33 + 17 = 3350 „ wartość poszukiwana”:
6n – 1 = 6 x 3350 – 1 = 20 099

c. b. d. o.

4.Faktoryzacja liczby 6-cyfrowej 1423 x 701 = 997 523, czyli odpowiednio mnożymy liczby o numerach: c = 117 x k = 235, dające numer liczby 997 523: n = 166 254

- ***metoda klasyczna faktoryzacji liczby złożonej***

1° Obliczamy pierwiastek kwadratowy z liczby 997 523:
$\sqrt{997\,523} \cong$ **999**
2° Sporządzamy listę liczb pierwszych ≤ 999:
2,3,5,7, … , 997. Daje to w sumie 168 dzielników pierwszych, a efektywny rozkład otrzymujemy po wykonaniu 127 operacji dzielenia:
997 523 : 2 = 498 761,5
997 523 : 3 = 332 507,(6)
.
.
997 523 : 701 = 1 423

- ***metoda faktoryzacji Cywińskiego – Książek***

1° Sprawdzamy przynależność liczby 998 981 do odpowiedniego ciągu. Dodając i odejmując liczbę jeden otrzymujemy odpowiednio dwie liczby: 997 524 i 997 522. Sprawdzamy, która z nich dzieli się przez liczbę 6. Przypomnijmy, że liczba parzysta podzielna przez 3, jest również podzielna przez liczbę 6. Ponieważ to kryterium podzielności spełnia liczba 997 524, stąd wniosek, że liczba 997 523 jest liczbą postaci 6n – 1

2° Korzystając ze wzorów z Kryterium 2 mamy:

$k \geq c$:		$k \geq c$:
$6n - 1 = (6k + 1)(6c - 1)$		$6n - 1 = (6k - 1)(6c + 1)$
$6n - 1 = 36kc - 6k + 6c - 1$ / +1	lub	$6n - 1 = 36kc + 6k - 6c - 1$ / +1
$6n = 36kc - 6k + 6c$ / : 6		$6n = 36kc + 6k - 6c$ / :6
$n = 6kc - k + c$		$n = 6k + k - c$

Podstawiamy wartości liczbowe:

$997\,523 = 36kc - 6k + 6c - 1$ / +1		$997\,523 = 36kc + 6k - 6c - 1$ / +1
$997\,524 = 36kc - 6k + 6c$ / : 6	lub	$997\,524 = 36kc + 6k - 6c$ / : 6
$166\,254 = 6kc - k + c$		$166\,254 = 6kc + k - c$
dla $k = c$:		dla $k = c$:
$166\,254 = 6k^2$ / : 6		$166\,254 = 6k^2$ / : 6
$27\,709 = k^2$ / $\sqrt{...}$		$27\,709 = k^2$ / $\sqrt{...}$
$k = k_0 = 166{,}46$, więc $k \neq c$		$k = k_0 = 166{,}46$, więc $k \neq c$
dla $k > c$		dla $k > c$
3° k_{max} jest dla $c = 1$:		1° k_{max} jest dla $c = 1$:
$166\,254 = 6xkx1 - k + 1 = 5k + 1$ / -1		$166\,254 = 6xkx1 + k - c = 7k - 1$ / +1
$166\,253 = 5k$ / :5		$166\,255 = 7k$ /:7
$k = 33\,250{,}6 \cong 33\,251$, $c = 1$:		$k = 23\,750{,}71... \cong 23\,751$, $c = 1$:
$n = 6x33\,251x1 - 33\,251 + 1 = 166\,256$		$n = 6x23\,751x1 + 23\,751 - 1 = 166\,256$
„o 2 za daleko”		„o 2 za daleko”
$k = 33\,250$, $c = 1$:		$k = 23\,750$, $c = 1$:
$n = 6x33\,250x1 - 33\,250 + 1 = 166\,251$		$n = 6x23\,750x1 + 23\,750 - 1 = 166\,249$
„o 3 za blisko”		„o 5 za blisko”
$k = 33\,250$, $c = 2$:		$k = 23\,750$, $c = 2$:
$n = 6x33\,250x2 - 33\,250 + 2 = 365\,752$		$n = 6x23\,750x2 + 23\,750 - 2 = 308748$
dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”		dużo „za daleko”, stąd wniosek, że k „jest znacząco bliżej c”

4°Ponieważ k „musi być znacząco bliżej c”, n = 166 254 i jednocześni dla $k = c = k_0$ mamy:
$k_0 = 166{,}46 \cong 166{,}5$ więc dla odpowiednich wartości otrzymujemy:
k = 167, c = 166: n = 6x167x166 – 167 + 166 = 166 331, 166 331 – 166 254 = 77 „za daleko”
k = 167, c = 166: n = 6x167x166 + 167 – 166 = 166 333, 166 333 – 166 254 = 79 „ za daleko”

Otrzymana różnica „za daleko 77” („za daleko 79”) informuje nas, że iloczyn 6xkxc oraz jego pomniejszenie o (– k + c) lub powiększenie o (k – c) musi być „trochę większe”; zmieniamy wartości parametrów k i c, ale tak by $k + c > 2k_0$, a więc $k + c > 333$:

k = 169, c = 165: n = 6x169x165 – 169 +165 = 167 306 „bardziej za daleko”

k = 169, c = 165: n = 6x169x165 + 169 – 165 = 167 314 „bardziej za daleko”

Różnica 167 306 – 166 254 = 1052. Otrzymaliśmy „bardziej za daleko”, stąd wniosek, że wartość iloczynu trzeba „trochę” obniżyć. W tym miejscu możemy jednak intuicję wesprzeć pewnym rozumowaniem, podobnie jak w przypadku pierwiastkowania. Dla $k = c = k_0$ mamy:

$n = 6xkxc – k + c = 6 \times k_0 \times k_0 – k_0 + k_0 = 6k_0^2$ i $n = 6xkxc + k – c = 6 \times k_0 \times k_0 + k_0 – k_0 = 6k_0^2$

Zależność $n = 6k_0^2$ możemy rozumieć, na przykład, jako sześciokrotność pola kwadratu o boku k_0. W takim razie zależność, w której $k \neq c$, możemy rozumieć jako sześciokrotność pola prostokąta o bokach k i c, pomniejszoną (powiększoną) o wartość liczbową różnicy długości tych boków: n = 6xkxc – k + c (n = 6xkxc + k – c). Tak więc mamy stosunkowo łatwy problem do rozwiązania: pole prostokąta musi być odpowiednio większe (mniejsze) od pola kwadratu o ile sześciokrotność tego pola zostanie pomniejszona (powiększona) o różnicę (sumę) jego boków:
$2k_0 = 2x166{,}5 = 333$, $n = 166\,254$, $k_0^2 = 27\,709$

$k + c > 2k_0$ i $k \times c > k_0^2$ oraz $k + c < 2k_0$ i $k \times c < k_0^2$

Dla k = 175 i c = 159 oraz $2k_0 = 2x166$ mamy $334 > 333$ i $175 \times 159 > k_0^2$ i rzeczywiście:

k = 175, c = 159: n = 6x175x159 – 175 + 159 = 166 934 „mniej za daleko”

k = 175, c = 157: n = 6x175x157 + 175 – 157 = 164 868 „ za daleko”

Różnica wynosi 166 934 – 166 254 = 680 „mniej za daleko”. Stąd wniosek, że $k + c > 333$, ale z uwagi na odległość trafienia, k powinno wzrosnąć np. o ok. 50, a c powinno zostać o ok. 50 pomniejszone, jednak tak aby otrzymać $k \times c \cong k_0^2$

k = 230, c = 120: n = 6x230x120 – 230 + 120 = 165 490 „za blisko”

k = 220, c = 112: n = 6x220x112 + 220 – 112 = 147 948 „dużo za blisko”

Różnica n =166 254 – 165 490 = 764 „za blisko”. Ponieważ k + c = 350 daje wartość „za blisko” więc sprawdzamy dla k + c = 352:

k = 232, c = 120: n = 6x232x120 – 232 + 120 = 166 928 „mniej za daleko”

Różnica wynosi 166 928 – 166 254 = 674, więc zmniejszamy c o 1:

k = 232, c = 119: n = 6x232x119 – 232 + 119 = 165 535 „za blisko”

Różnica 166 254 – 165 535 = 719 dostarcza nam informacji o symetrii między „za daleko” i „za blisko”. Wystarczy teraz pomniejszać pojedynczo parametry:

k = 233, c = 119: n = 6x233x119 – 234 + 119 = 166 248 „trochę za blisko”

k = 235, c = 118: n = 6x235x118 – 235 + 118 = 166 263 „trochę za daleko”
k = 236, c = 118: n = 6x236x118 – 236 + 118 = 166 970 „bardziej za daleko”
k = 236, c = 117: n = 6x236x117 – 236 + 117 = 165 553 „bardziej za blisko”
k = 237, c = 117: n = 6x237x117 – 237 + 117 = 165 254 „wartość poszukiwana
k = 235, c = 117: n = 6x235x117 – 235 + 117 = 166 254 „ wartość poszukiwana”:
6n – 1 = 6 x 166 254 – 1 = 997 523 c. b. d. o.

5.Faktoryzacja liczby 12-cyfrowej:1 000 151 x 901 009 = 901 145 052 359, czyli odpowiednio mnożymy liczby o numerach c = 150 168 x k = 166 692, dające numer liczby 997 523:
n = 166 254

- ***metoda klasyczna faktoryzacji liczby złożonej***

1° Obliczamy pierwiastek kwadratowy z liczby 901 145 052 359:
$\sqrt{901145052359} \cong$ **949 287, co daje 74 854 liczb pierwszych, a efektywny rozkład otrzymujemy po wykonaniu**
2° Sporządzamy listę liczb pierwszych ≤ 949 287:
2,3,5,7, … , 103. Daje to w sumie 74 854 dzielników pierwszych !!!

6n – 1 = (6k – 1)(6c+1)
901 145 052 359 = 36kc + 6k – 6c – 1 / +1
901 145 052 360 = 36kc + 6k – 6c / :6
150 190 842 060 = 6kc + k – c
dla k = c:
150 190 842 060 = $6k^2$ /:6
25 031 807 010 = k^2 / $\sqrt{\ldots}$
k = 158 214,43 więc k ≠ c
dla k > c
1° k_{max} dla c = 1:
25 031 807 010 = 6xkx1 + k – 1 / +1
25 031 807 011 = 7k / :7
k = 3 575 972 430,14 ≅ 3 575 972 430, c = 1:
n = 6 x 3 575 972 430 x 1 + 3 575 972 430 – 1 = 25 031 807 009 krótki
k = 3 575 972 430, c = 2:
n = 6 x 3 575 972 430 x 2 + 3 575 972 430 – 2 = 46 487 641 588 b. długi
n = 6 x 3 575 972 429 x 2 + 3 575 972 429 – 2 = 46 487 641 575 b. długi
2° 150 190 842 060 = 6kc – k + c
25 031 807 010 = k^2 / $\sqrt{\ldots}$

k = 158 214,43
k = 158 215, c =158 214:
n = 6 x 158 215 x 158214 +1 = 150 190 968 061
150 190 968 061 - 150 190 842 060 = 126 001

k = 170 000, c = 150 000: n = 6 x 170 000 x 150 000 + 20 000 = 153 000 020 000
k = 165 000, c = 150 000: n = 6 x 165 000 x 150 000 + 15 000 = 148 500 015 000
k = 167 000, c = 150 000: n = 6 x 167 000 x 150 000 +17 000 = 150 300 017 000
k = 166 000, c = 150 000: n = 6 x 166 000 x 150 000 + 16 000 = 149 400 016 000
k = 166 900, c = 150 000: n = 6 x 166 900 x 150 000 + 16 900 = 150 210 016 900
k = 166 200, c = 150 000: n = 6 x 166 200 x 150 000 + 16 200 = 149 580 016 200
k = 166 700, c = 150 000: n = 6 x 166 700 x 150 000 + 16 700 = 150 030 016 700
k = 166 700, c = 150 100: n = 6 x 166 700 x 150 100 + 16 600 = 150 130 036 600
k = 166 700, c = 150 200: n = 6 x 166 700 x 150 200 + 16 500 = 150 230 056 500
k = 166 690, c = 150 200: n = 6 x 166 690 x 150 200 + 16 490 = 150 221 044 490
k = 166 680, c = 150 200: n = 6 x 166 680 x 150 200 + 16 480 = 150 210 032 480
k = 166 680, c = 150 150: n = 6 x 166 680 x 150 150 + 16 530 = 150 162 028 530
k = 166 685, c = 150 150: n = 6 x 166 685 x 150 150 + 16 535 = 150 166 533 035
k = 166 690, c = 150 150: n = 6 x 166 690 x 150 150 + 16 540 = 150 171 037 540
k = 166 690, c = 150 160: n = 6 x 166 690 x 150 160 + 16 530 = 150 181 038 930
k = 166 695, c = 150 160: n = 6 x 166 695 x 150 160 + 16 535 = 150 185 543 735
k = 166 695, c = 150 165: n = 6 x 166 695 x 150 165 + 16 530 = 150 190 544 580
k = 166 695, c = 150 170: n = 6 x 166 695 x 150 170 + 16 525 = 150 195 545 425
k = 166 694, c = 150 170: n = 6 x 166 694 x 150 170 + 16 524 = 150 194 644 404
k = 166 693, c = 150 170: n = 6 x 166 693 x 150 170 + 16 523 = 150 193 743 383
k = 166 692, c = 150 170: n = 6 x 166 692 x 150 170 + 16 522 = 150 192 842 362
k = 166 691, c = 150 170: n = 6 x 166 691 x 150 170 + 16 521 = 150 191 941 341
k = 166 690, c = 150 170: n = 6 x 166 690 x 150 170 + 16 520 = 150 191 040 320
k = 166 689, c = 150 170: n = 6 x 166 689 x 150 170 + 16 519 = 150 190 139 299
k = 166 689, c = 150 171: n = 6 x 166 689 x 150 171 + 16 518 = 150 191 122 914
k = 166 690, c = 150 169: n = 6 x 166 690 x 150 169 + 16 521 = 150 190 040 181
k = 166 691, c = 150 169: n = 6 x 166 691 x 150 169 + 16 522 = 150 190 941 196
k = 166 691, c = 150 168: n = 6 x 166 691 x 150 168 + 16 523 = 150 189 941 051
k = 166 692, c = 150 168: n = 6 x 166 692 x 150 168 + 16 524 = 150 190 842 060

6n – 1 = 6 x 150 190 842 060 – 1 = 901 145 052 359

c.b.d.o.

Oczywiście dla ciągów postaci 6n+1 proces zachodzi analogicznie.
C.D.N ☺