**WYDZIAŁ MATEMATYKI, MECHANIKI I INFORMATYKI**
**UNIWERSYTET WARSZAWSKI**

# LICZBY PSEUDOPIERWSZE

TOMASZ KRECZMAR

PRACA MAGISTERSKA
NAPISANA POD OPIEKĄ
PROF. DR. HAB. WOJCIECHA GUZICKIEGO

WARSZAWA 1998

# WSTĘP

Niniejsza praca ma na celu pokazanie kilku własności oraz przykładów trzech rodzajów liczb, zwanych dalej liczbami *pseudopierwszymi*, ***s**ilnie pseudopierwszymi* i *bardzo silnie pseudopierwszymi*. Pojęcie pierwszych z nich – czyli pojęcie liczb pseudopierwszych – narodziło się z małego twierdzenia Fermata. Chińczycy wierzyli, że jeśli liczba $n$ spełnia kongruencje $2^n \equiv 2 \pmod{n}$, to jest pierwsza, co oczywiście nie jest prawdą, jeśli znamy liczbę pierwszą 341. To przypuszczenie Chińczyków pozwala nam przypuszczać, że znali oni jakąś wersję małego twierdzenia Fermata.

Z kolei do liczb silnie pseudopierwszych doprowadziły badania Carmichaela, który na początku XX wieku zajmował się liczbami postaci $b^{n-1} \equiv 1 \pmod{n}$ dla $(b, n) = 1$.

Liczby bardzo silnie pseudopierwsze miały być wzmocnieniem liczb silnie pseudopierwszych, a ich definicję podał prof. Jerzy Browkin.

Wszystkie te definicje – liczb psuedopierwszych, silnie pseudopierwszych i bardzo silnie pseudopierwszych – są stosowane do stwierdzania pierwszości danych liczb, a – co za tym idzie – do ich znajdowania.

W rozdziale pierwszym niniejszej pracy zawarto wszystkie informacje ogólne z zakresu algebry i teorii liczb, które potrzebne są w późniejszych rozdziałach. Rozdział drugi i czwarty zawierają definicje i twierdzenia dotyczące – odpowiednio – liczb pseudopierwszych i silnie pseudopierwszych oraz bardzo silnie pseudopierwszych. Natomiast w rozdziałach trzecim i piątym podano przykłady interesujących nas liczb. Przykłady te otrzymano korzystając z trzech programów napisanych przez autora specjalnie dla tego celu. Wszystkie te programy –

pozwalające testować liczby i sprawdzać, czy są one pseudopierwsze, silnie pseudopierwsze lub bardzo silnie pseudopierwsze – wykorzystują nieco zmodyfikowany algorytm zdobyty przy pomocy Sieci komputerowej, dzięki któremu można dokonywać działań na bardzo dużych liczbach.

# ROZDZIAŁ 1
# WIADOMOŚCI PODSTAWOWE

# Twierdzenia i definicje dotyczące teorii grup

## Definicja 1. Grupa

Niech w zbiorze $G$ będzie określone działanie dwuargumentowe $\bullet$ i wyróżniony element $e$. Działanie to nazywamy *mnożeniem*, a element $e$ – *jednością*. Układ $\langle G, \bullet; e\rangle$ nazywamy *grupą*, jeżeli spełnione są warunki.

1) $a\,(bc) = (ab)\,c$ dla $a, b, c \in G$,

2) $ae = ea = a$ dla $a \in G$,

3) Dla każdego $a \in G$ istnieje taki $a' \in G$, że $aa' = a'a = e$.

## Definicja 2. Podgrupa, podgrupa generowana

Niech $H$ będzie takim podzbiorem grupy $G$, że $e \in H$ oraz $ab \in H$ dla dowolnych $a, b \in H$. Mówimy, że $H$ jest *podgrupą* grupy $G$, jeżeli $\langle H, \bullet; e\rangle$ jest grupą. Oczywiście podgrupami dowolnej grupy $G$ są $G$ oraz $\{e\}$.

Jeżeli $H$ jest najmniejszą podgrupą grupy $G$ zawierającą zbiór $X$, to $H$ nazywamy *podgrupą generowaną przez zbiór* $X$, a $X$ *– zbiorem generatorów podgrupy* $H$. Piszemy wtedy $H = (X)$. Jeżeli zbiór $X$ jest jednoelementowy, $X = \{a\}$, to grupę generowaną przez ten zbiór nazywamy *cykliczną* i oznaczamy przez $(a)$.

## Definicja 3. Rząd grupy i elementu

Liczbę elementów grupy $G$ nazywamy jej *rzędem* oraz oznaczamy przez $|G|$. Jeżeli grupa ma skończoną liczbę elementów, to nazywamy ją *grupą skończoną*. *Rzędem elementu* $a$ *grupy* $G$ nazywamy rząd podgrupy $(a)$ generowanej przez ten element; rząd elementu $a$ oznaczamy przez $|a|$.

## Definicja 4. Warstwy lewostronne

Niech *a* będzie elementem grupy *G*. Odwzorowanie $\lambda_a : G \to G$ określone wzorem $\lambda_a(g) = ag$ dla $g \in G$ nazywamy *przesunięciem lewostronnym o element a*. Oczywiście odwzorowania $\lambda_a$ i $\lambda_{a^{-1}}$ są wzajemnie odwrotne, zatem każde przesunięcie lewostronne jest odwzorowaniem wzajemnie jednoznacznym.

Jeżeli *H* jest podgrupą grupy *G*, to obraz zbioru *H* przy przesunięciu lewostronnym $\lambda_a$ nazywamy *warstwą lewostronną grupy G względem podgrupy H wyznaczoną przez element a*. Warstwę tę oznaczamy przez *aH*. Mamy $aH = \lambda_a(H) = \{ah : h \in H\}$.

Analogicznie definiujemy odwzorowanie zwane przesunięciem prawostronnym $(\pi_a)$ i warstwy prawostronne *Ha*.

## Definicja 5. Indeks podgrupy *H* w grupie *G*

Niech $\psi : G \to G$ będzie odwzorowaniem grupy *G* określonym wzorem $\psi(g) = g^{-1}$ dla $g \in G$. Jest to oczywiście odwzorowanie wzajemnie jednoznaczne, przy tym $\psi(aH) = \{\psi(ah) : h \in H\} = \{h^{-1}a^{-1} : h \in H\} = Ha^{-1}$. Zatem odwzorowanie $\psi$ przekształca warstwę lewostronną (patrz *Definicja 4*) wyznaczoną przez element *a* na warstwę prawostronną wyznaczoną przez element $a^{-1}$. Ponieważ odwzorowanie $\psi$ jest wzajemnie jednoznaczne, więc wynika stąd, że liczba (moc zbioru) warstw lewostronnych względem podgrupy *H* jest równa liczbie (mocy zbioru) warstw prawostronnych względem tej podgrupy. Liczbę tę nazywamy *indeksem podgrupy H w grupie G* i oznaczamy przez (*G* : *H*).

## Twierdzenie 1. Twierdzenie Lagrange'a (1)

Jeżeli $H$ jest podgrupą grupy skończonej $G$, to $|G| = |H|\ (G : H)$.

**Dowód:** Zbiór elementów $G$ jest sumą parami rozłącznych warstw lewostronnych względem podgrupy $H$ (patrz *Definicja 4*). Warstwy te są równoliczne ze zbiorem $H$. Zatem liczba elementów grupy $G$ jest równa iloczynowi liczby warstw lewostronnych względem podgrupy $H$ i liczby elementów zbioru $H$.

**Wniosek 1**

Rząd podgrupy (patrz *Definicja 3*) jest dzielnikiem rzędu grupy; rząd elementu grupy jest dzielnikiem rzędu grupy.

**Wniosek 2**

Jeżeli rząd grupy $G$ jest liczbą pierwszą $p$, to grupa $G$ jest cykliczna (składa się z potęg jednego elementu).

**Dowód:** Niech $a$ będzie elementem grupy $G$ różnym od $e$. Wtedy $|a| > 1$. Na mocy poprzedniego wniosku wiemy, że liczba $|a|$ jest dzielnikiem liczby $|G|$. Ponieważ $|G|$ jest liczbą pierwszą, więc wynika stąd, że $|a| = |G|$, a zatem $(a) = G$.

# Definicja i własności kongruencji

## Definicja 6

Dla danych trzech liczb całkowitych $a$, $b$ i $m$ mówimy, że *liczba a przystaje do liczby b modulo m* i piszemy $a \equiv b \pmod{m}$, gdy różnica $a - b$ jest podzielna przez $m$. Liczbę $m$ nazywamy *modułem* kongruencji; musi być ona różna od zera, a najczęściej jest od niej większa.

Oczywiście kongruencja jest relacją równoważności, co można łatwo sprawdzić. Kongruencje można również dodawać i mnożyć stronami.

## Własność 1

Jeśli $a$, $b$, $c$ i $m$ są liczbami całkowitymi, takimi że $m > 0$ oraz $a \equiv b \pmod{m}$, to $ac \equiv bc \pmod{m}$. Własność ta wynika bezpośrednio z faktu, iż kongruencje można mnożyć i dodawać stronami. Pozostałe własności również wynikają – nieco mniej bezpośrednio – z tego faktu i innych własności.

## Własność 2

Jeśli $a$, $b$, $c$ i $m$ są liczbami całkowitymi, takimi że $m > 0$, $(c, m) = 1$ oraz $ac \equiv bc \pmod{m}$, to $a \equiv b \pmod{m}$.

## Własność 3

Jeśli $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ oraz liczby $m$ i $n$ są względnie pierwsze, to $a \equiv b \pmod{mn}$.

## Własność 4

Jeśli $(b, n) = 1$, to kongruencja $b^n \equiv b \pmod{n}$ jest równoważna kongruencji $b^{n-1} \equiv 1 \pmod{n}$. Ta własność wynika z *Własności 1* i *Własności 2*.

## Własność 5

Jeśli $a$, $b$, $c$ i $m$ są liczbami całkowitymi, takimi że $m > 0$, $(c, m) = d$ oraz $ac \equiv bc \pmod{m}$, to $a \equiv b \pmod{m/d}$.

### Własność 6

Niech $w(x)$ będzie wielomianem stopnia $n$ o współczynnikach całkowitych, a $m$ danym modułem. Każdą liczbę całkowitą $a$, dla której $f(a) \equiv 0 \pmod{m}$, nazywamy pierwiastkiem kongruencji $f(x) \equiv 0 \pmod{m}$. Jeżeli liczba całkowita $a$ jest pierwiastkiem kongruencji, to także każda liczba całkowita przystająca do $a$ modulo $m$ jest pierwiastkiem tej kongruencji. Całą taką klasę liczb całkowitych, przystających do siebie modulo $m$ i spełniających kongruencję, będziemy uważali za jedno rozwiązanie.

## Pozostałe twierdzenia i definicje

### Algorytm Euklidesa

Algorytm Euklidesa to szybka metoda znajdowania największego wspólnego dzielnika dwóch liczb. Aby znaleźć $(a, b)$, gdzie $a > b$, najpierw dzielimy $a$ przez $b$ i zapisujemy iloraz $q_1$ i resztę $r_1$: $a = q_1 b + r_1$. Następnie wykonujemy drugie dzielenie, w którym $b$ gra rolę $a$ i $r_1$ gra rolę $b$: $b = q_2 r_1 + r_2$. Następnie dzielimy $r_1$ przez $r_2$: $r_1 = q_3 r_2 + r_3$. Kontynuujemy to postępowanie, za każdym razem dzieląc przedostatnią resztę przez ostatnią, otrzymując nowy iloraz i nową resztę. Gdy wreszcie otrzymamy resztę, która dzieli poprzednią, kończymy dzielenie: ostatnia niezerowa reszta jest największym wspólnym dzielnikiem liczb $a$ i $b$. Oczywiście taką resztę otrzymamy, gdyż mamy tu do czynienia ze zstępującym ciągiem reszt.

Algorytm Euklidesa pozwala również rozwiązywać kongruencje oraz równania postaci $d = (a, b) = ax + by$.

## Definicja 7. Funkcja Eulera (Gaussa)

Niech $n$ będzie dodatnią liczbą całkowitą. Funkcja Eulera $\varphi(n)$ jest określona jako liczba tych nieujemnych liczb $b$ mniejszych od $n$, które są względnie pierwsze z $n$:

$$\varphi(n) := |\{0 \le b < n : (b, n) = 1\}|$$

Zauważmy, że $\varphi(1) = 1$ oraz $\varphi(p) = p - 1$ (gdzie $p$ liczba pierwsza). Z kolei dla potęg liczb pierwszych mamy $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$

## Definicja 8

Zredukowany system reszt modulo $m$ to zbiór liczb całkowitych $r_i$ takich, że $(r_i, m) = 1$ oraz dla różnych $i, j$ zachodzi: $r_i$ nie przystaje do $r_j$ modulo $m$, a także dla każdego $x$ względnie pierwszego z $m$, $x$ przystaje modulo $m$ do jakiegoś $r_i$ należącego do zbioru.

## Definicja 9

Niech $m$ będzie dodatnią liczbą naturalną, a $a$ taką liczbą naturalną, że $(a, m) = 1$. Niech $h$ będzie najmniejszą dodatnią liczbą naturalną, taką że $a^h \equiv 1 \pmod{m}$. Mówimy wtedy, że $a$ należy do potęgi $h$ modulo $m$.

## Definicja 10

Jeśli $a$ należy do potęgi $\varphi(m)$ modulo $m$, to wtedy $a$ nazywamy pierwiastkiem pierwotnym modulo $m$.

## Lemat 1

Dla $p$ liczby pierwszej oraz dla $0 < k < p$ zachodzi $p \mid \binom{p}{k}$.

**Dowód:** Oczywiście $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, czyli $p! = \binom{p}{k} k!(p-k)!$, a ponieważ również zachodzi $p! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p$ to $p \mid p!$, stąd także $p \mid \binom{p}{k} k!(p-k)!$.

Jednocześnie $(p, k!(p-k)!) = 1$, więc $p \mid \binom{p}{k}$.

## Twierdzenie 2. Małe twierdzenie Fermata

Niech $p$ będzie liczbą pierwszą. Wtedy każda liczba $n$ niepodzielna przez $p$ spełnia kongruencję $n^{p-1} \equiv 1 \pmod{p}$.

**Dowód:** Kongruencja $n^{p-1} \equiv 1 \pmod{p}$ jest równoważna kongruencji $n^p \equiv n \pmod{p}$, która z kolei jest równoważna (z definicji kongruencji – patrz *Definicja 6*) podzielności $p \mid n^p - n$. Dowodzimy twierdzenia przez indukcję. Dla $n = 1$ oczywiście zachodzi $p \mid 1^p - 1 = 0$. Załóżmy więc, że twierdzenie zachodzi dla $n$ i wykażmy, że spełnione jest również dla $n + 1$, czyli $p \mid (n+1)^p - (n+1)$. Mamy więc

$$(n+1)^p - (n+1) = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \ldots + 1 - n - 1 = n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^{p-k}$$

Oczywiście z założenia indukcyjnego $p \mid n^p - n$, a jednocześnie z *Lematu 1* wiemy, że $p \mid \binom{p}{k}$ dla $k = 1, \ldots, p-1$. Czyli $n^p - n + \sum_{k=1}^{p-1} \binom{p}{k} n^{p-k}$ jest podzielne przez $p$, co kończy dowód.

## Twierdzenie 3. Chińskie twierdzenie o resztach

Przypuśćmy, że chcemy rozwiązać układ kongruencji o różnych modułach:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

... ...

$$x \equiv a_r \pmod{m_r}$$

Przypuśćmy następnie, że każde dwa moduły są względnie pierwsze: $(m_i, m_j) = 1$ dla $i \neq j$. Wtedy istnieje wspólne rozwiązanie $x$ wszystkich tych kongruencji i każde dwa rozwiązania przystają do siebie modulo $M = m_1 m_2 \ldots m_r$.

**Dowód:** Udowodnimy najpierw jednoznaczność modulo $M$. Załóżmy, że $x'$ i $x''$ są dwoma rozwiązaniami. Niech $x = x' - x''$. Wtedy $x$ musi przystawać do 0 względem modułu $m_i$ dla każdego $i$, a więc i modulo $M$ (patrz *Własność 3*). Następnie pokażemy, jak skonstruować rozwiązanie $x$.

Niech $M_i = M/m_i$ będzie iloczynem wszystkich modułów z wyjątkiem $i$-tego. Oczywiście $(m_i, M_i) = 1$, a więc istnieje taka liczba $N_i$ (którą można znaleźć za pomocą algorytmu Euklidesa), że $M_i N_i \equiv 1 \pmod{m_i}$. Przyjmijmy teraz $x = \sum_i a_i M_i N_i$. Wtedy dla każdego $i$ wszystkie składniki sumy poza $i$-tym są podzielne przez $m_i$, gdyż $m_i \mid M_j$ dla $i \neq j$. Zatem dla każdego $i$ mamy: $x \equiv a_i m_i M_i \equiv a_i \pmod{m_i}$, czego należało dowieść.

## Twierdzenie 4. Multyplikatywność funkcji Eulera

Funkcja Eulera $\varphi$ (patrz *Definicja 7*) jest multyplikatywna, tzn. $\varphi(mn) = \varphi(m)\varphi(n)$, jeśli tylko $(m, n) = 1$.

**Dowód:** Musimy policzyć, ile jest liczb całkowitych zawartych między 0 i $mn - 1$ nie mających wspólnych dzielników z liczbą $mn$. Dla każdej liczby $j$ z tego przedziału niech $j_1$ będzie jej resztą z dzielenia przez $M$ (tzn. $0 \le j_1 < m$ oraz $j \equiv j_1 \pmod{m}$) i niech $j_2$ będzie jej resztą z dzielenia przez $n$ (tzn. $0 \le j_2 < n$ oraz $j \equiv j_2 \pmod{n}$). Z chińskiego twierdzenia o resztach (patrz *Twierdzenie 4*) wynika, że dla każdej takiej pary liczb $j_1, j_2$ istnieje dokładnie jedna liczba $j$ między 0 i $mn - 1$, dla której $j \equiv j_1 \pmod{m}$ oraz $j \equiv j_2 \pmod{n}$. Zauważmy, że $j$ nie ma wspólnego dzielnika z $mn$ wtedy i tylko wtedy, gdy nie ma wspólnego dzielnika z $m$ – co jest równoważne temu, że $j_1$ nie ma wspólnego dzielnika z $m$ – oraz nie ma wspólnego dzielnika z $n$ – co jest równoważne temu, że $j_2$ nie ma wspólnego dzielnika z $n$. Zatem te liczby $j$, które musimy zliczyć, dopowiadają wzajemnie jednoznacznie parom $j_1, j_2$, dla których $0 \le j_1 < m$, $(j_1, m) = 1$; $0 \le j_2 < n$, $(j_2, n) = 1$. Liczba takich $j_1$ jest równa $\varphi(m)$ i liczba takich $j_2$ jest równa $\varphi(n)$. Zatem liczba par jest równa $\varphi(m)\varphi(n)$, co kończy dowód.

## Twierdzenie 5. Twierdzenie Eulera

Jeśli $(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Twierdzenie to zwane jest też uogólnieniem małego twierdzenia Fermata.

**Dowód:** Dowodzimy najpierw twierdzenie w przypadku, gdy $n$ jest potęgą liczby pierwszej, czyli $n = p^k$. Będziemy stosować indukcję względem $k$. Dla $k = 1$ mamy małe twierdzenie Fermata (patrz *Twierdzenie 2*). Załóżmy, że $l > 1$ i że wzór jest prawdziwy dla $p^{l-1}$. Na podstawie założenia indukcyjnego mamy wtedy $a^{p^{l-1}-p^{l-2}} = 1 + p^{l-1}b$ dla pewnej całkowitej liczby $b$. Jeśli podniesiemy obie strony

równości do potęgi $p$ i skorzystamy z tego, iż wszystkie współczynniki Newtona (z wyjątkiem 1 i współczynnika przy $x^p$ na końcu) w rozwinięciu $(1 + x)^p$ są podzielne przez $p$ (patrz *Lemat 1*) możemy stwierdzić, że liczba $a^{p^l - p^{l-1}}$ jest sumą liczby 1 i pewnej liczby składników podzielnych przez $p^l$. Zatem liczba $a^{\varphi(p^l)} - 1$ jest podzielna przez $p^l$, co kończy dowód twierdzenia dla potęg liczb pierwszych.

Z multyplikatywności funkcji $\varphi$ (patrz *Twierdzenie 4*) wynika, że $a^{\varphi(n)} \equiv 1 \pmod{p^l}$ – wystarczy podnieść obie strony kongruencji $a^{\varphi(p^l)} \equiv 1 \pmod{p^l}$ do potęgi $\varphi(p_1^{l_1} \bullet \ldots \bullet p_m^{l_m})$, gdzie $n = p^l \bullet p_1^{l_1} \bullet \ldots \bullet p_m^{l_m}$. Ponieważ jest to prawdziwe dla każdej potęgi $p^l$ dzielącej $n$ i ponieważ potęgi dwóch różnych liczb pierwszych nie mają wspólnego dzielnika, z *Własności 3* wynika, że $a^{\varphi(n)} \equiv 1 \pmod{n}$.

## Twierdzenie 6

Niech $g = (a, m)$. Wtedy kongruencja $ax \equiv b \pmod{m}$ nie ma rozwiązań, jeśli $g$ nie dzieli $b$. Jeżeli zaś $g$ dzieli $b$, to kongruencja ta ma $g$ rozwiązań $x \equiv (b/g)x_0 + n(m/g) \pmod{m}$, gdzie $n = 0, 1, \ldots, g - 1$, a $x_0$ jest dowolnym rozwiązaniem kongruencji $(a/g)x \equiv 1 \pmod{m/g}$.

**Dowód:** Z definicji (patrz *Definicja 6*) kongruencja $ax \equiv b \pmod{m}$ jest równoważna równaniu $ax - my = b$. Liczba naturalna $x$ będzie rozwiązaniem tej kongruencji wtedy i tylko wtedy, kiedy istnieje liczba $y$, taka że $ax - my = b$. Wpierw rozpatrzmy przypadek $g$ nie dzieli $b$. Z własności podzielności wiemy, że jeśli $g$ dzieli $a$ i $g$ dzieli $m$ to również $g$ dzieli $b$. Stąd, jeśli $g$ nie dzieli $b$, to równanie $ax - my = b$ nie ma rozwiązań, a co za tym idzie kongruencja $ax \equiv b \pmod{m}$.

Załóżmy teraz, że $g$ dzieli $b$. Możemy zapisać, że $g = sa + tm$. Ponieważ $g \mid b$, to istnieje taka liczba naturalna $e$, że $ge = b$. Mnożąc obie strony równości $g = sa + tm$ przez $e$ otrzymujemy: $b = ge = (sa + tm)e = a(se) + m(te)$, tak więc jedno z rozwiązań tego równania to $x = x_0$ i $y = y_0$, gdzie $x_0 = se$, a $y_0 = te$. Niech $x = x_0 + (m/g)n$, a $y = y_0 - (a/g)n$, gdzie $n$ jest liczbą naturalną. Wtedy para $(x, y)$ będzie rozwiązaniem tego równania ponieważ: $ax + my = ax_0 + a(m/g) + my_0 - m(a/g)n = ax_0 + my_0 = b$. Mamy więc nieskończenie wiele rozwiązań postaci $x = x_0 + (m/g)n$, a $y = y_0 - (a/g)n$, gdzie $x = x_0$ i $y = y_0$ są konkretnymi rozwiązaniami równania. Aby stwierdzić, ile jest różnych nieprzystających rozwiązań $x = x_0 + (m/g)n$, trzeba określić warunki opisujące dwa przystające modulo $m$ rozwiązania: $x_1 = x_0 + (m/g)n_1$ i $x_2 = x_0 + (m/g)n_2$. Jeżeli dwa rozwiązania są przystające, to $x_0 + (m/g)n_1 \equiv x_0 + (m/g)n_2 \pmod{m}$. Odejmując od obu stron tego równania $x_0$ otrzymujemy: $(m/g)n_1 \equiv (m/g)n_2 \pmod{m}$. Wiemy dalej, że $(m, m/g) = m/g$, a ponieważ $(m/g) \mid m$, więc z *Własności 5* mamy: $n_1 \equiv n_2 \pmod{m}$, co oznacza, że pełny zbiór nieprzystających rozwiązań otrzymujemy biorąc $x = x_0 + (m/g)n$, gdzie $n = 0, 1, ..., g - 1$.

## Twierdzenie 7

Dla $n \geq 1$ zachodzi $\sum_{d|n} \varphi(d) = n$.

**Dowód:** Jeśli $n = p^e$ i $p$ jest liczbą pierwszą, to wtedy

$$\sum_{d|n} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^e) = 1 + (p-1) + p(p-1) + p^{e-1}(p-1) = p^e = n$$

Tak więc twierdzenie jest prawdziwe dla $n$ będącego potęgą liczby pierwszej $p$. Dowodzimy twierdzenia przez indukcję. Zakładamy, że będzie ono prawdziwe dla liczb naturalnych o $k$ lub mniej różnych pierwszych czynnikach. Niech liczba

naturalna $N$ posiada $k + 1$ różnych pierwszych czynników i niech $p$ będzie jednym z nich, a $p^e$ największą potęgą $p$ dzielącą $N$. Wtedy $N = p^e n$ i $n$ mają $k$ różnych czynników pierwszych, a $(p, n) = 1$. Ponieważ $d$ przebiega dzielniki $n$, więc dzielniki $N$ przebiegają zbiór $d, pd, p^2d, ..., p^ed$. Stąd mamy

$$\sum_{d|N}\varphi(d) = \sum_{d|n}\varphi(d) + \sum_{d|n}\varphi(pd) + \sum_{d|n}\varphi(p^2d) + \ldots + \sum_{d|n}\varphi(p^ed) =$$
$$= \sum_{d|n}\varphi(d)\left(1 + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^e)\right) = \sum_{d|n}\varphi(d)\sum_{\delta|p^e}\varphi(\delta) = np^e = N$$

co kończy dowód.

## Twierdzenie 8. Twierdzenie Lagrange'a (2)

Niech $\mathbf{Z}[x]$ ∋ $f(x) = a_0 + a_1x + a_1x^2 + \ldots + a_nx^n$ i $(a_n, p) = 1$, a $p$ jest liczbą pierwszą. Wtedy kongruencja wielomianowa $f(x) \equiv 0 \pmod p$ ma co najwyżej $n$ różnych mod $p$ rozwiązań.

**Dowód:** Przez indukcję względem $n$. Dla $n = 1$ oczywiście $a_0 + a_1x \equiv 0 \pmod p$. Załóżmy, że twierdzenie zachodzi dla $n - 1$ i niech $x_0, x_1, \ldots, x_n$ będą rozwiązaniami kongruencji $f(x) \equiv 0 \pmod p$. Wtedy

$$f(x) - f(x_0) = a_n (x^n - x_0^n) + a_2 (x^{n-1} - x_0^{n-1}) + \ldots + a_1 (x - x_0) =$$
$$= a_n (x - x_0) (x^{n-1} + x^{n-2}x_0 + \ldots + x x_0^{n-2} + x_0^{n-1}) +$$
$$+ a_{n-1} (x - x_0) (x^{n-2} + x^{n-3}x_0 + \ldots + x x_0^{n-3} + x_0^{n-2}) +$$
$$+ \ldots + a_1 (x - x_0) =$$
$$= (x - x_0)\, g\,(x),$$

gdzie $g(x)$ jest wielomianem stopnia $n - 1$. Pokażemy teraz, że $x_0, x_1, \ldots, x_n$ są rozwiązaniami kongruencji $g(x) \equiv 0 \pmod p$. Niech $k$ będzie liczbą naturalną, taką że $1 \le k \le n$. Ponieważ $f(x_k) \equiv f(x_0) \equiv 0 \pmod p$, mamy $f(x_k) - f(x_0) = (x_k - x_0)\, g(x_k) \equiv 0$

(mod $p$). Stąd $g(x_k) \equiv 0 \pmod{p}$, gdyż $(x_k - x_0)$ nie przystaje do 0 modulo $p$. Wynika z tego, że kongruencja wielomianowa $g(x) \equiv 0 \pmod{p}$ o współczynniku przy najwyższej potędze niepodzielnym przez $p$ posiada $n$ różnych rozwiązań modulo $p$, co przeczy zasadzie indukcji. A więc kongruencja wielomianowa $f(x) \equiv 0 \pmod{p}$ nie może mieć więcej niż $n$ różnych rozwiązań modulo $p$, co kończy dowód.

## Twierdzenie 9

Jeżeli $a$ należy do potęgi $h$ modulo $m$, to $h \mid \varphi(m)$. Ponadto $a^j \equiv a^k \pmod{m}$ wtedy i tylko wtedy, gdy $h \mid (j - k)$.

**Dowód:** Bez straty ogólności możemy założyć, że $j > k$, a ponieważ $(a, m) = 1$, więc kongruencja $a^j \equiv a^k \pmod{m}$ jest równoważna kongruencji $a^{j-k} \equiv 1 \pmod{m}$. Jednocześnie fakt, iż $a$ należy do potęgi $h$ modulo $m$ oznacza, że $a^h \equiv 1 \pmod{m}$ i $h$ jest najmniejszą taką liczbą, więc $h \mid (j - k)$. Jednocześnie z definicji należenie do potęgi (patrz *Definicja 9*) musi zachodzić $(a, m) = 1$. Z twierdzenia Eulera (patrz *Twierdzenie 5*) wiemy jednocześnie $a^{\varphi(m)} \equiv 1 \pmod{m}$ dla $(a, m) = 1$. Z tego wynika więc również fakt, iż $h \mid \varphi(m)$.

## Twierdzenie 10

Jeżeli $a$ należy do potęgi $h$ modulo $m$, to $a^k$ należy do potęgi $h/(h, k)$ modulo $m$.

**Dowód:** Z *Twierdzenia 9* wiemy, że $(a^k)^j \equiv 1 \pmod{m}$ wtedy i tylko wtedy, gdy $[h/(h, k)] \mid j$. Tak więc ostatnią dodatnią liczbą naturalną $j$ taką, że $(a^k)^j \equiv 1 \pmod{m}$ jest $j = h/(h, k)$, co kończy dowód.

## Twierdzenie 11

Jeśli $p$ jest pierwsza, to istnieje $\varphi(p-1)$ pierwiastków pierwotnych (patrz *Definicja 10*) modulo $p$. Jedyne liczby naturalne posiadające pierwiastek pierwotny to: $p^e$, $2p^e$, 2 i 4, gdzie $p$ jest liczbą pierwszą.

**Dowód:** Każda liczba naturalna $a$ z przedziału $\langle 1, p-1\rangle$ należy do pewnej potęgi $h$ modulo $p$ (patrz *Definicja 9*), gdzie $h \mid (p-1)$. Jeżeli $a$ należy do potęgi $h$, to $(a^k)^h \equiv 1 \pmod{p}$ dla wszystkich $k$, a jednocześnie $1, a, a^2, \ldots, a^{h-1}$ są różne modulo $p$. Dalej, z *Twierdzenia 8*, liczby $h$ są rozwiązaniami wszystkich kongruencji $x^h \equiv 1 \pmod{p}$. Z *Twierdzenia 10* wiemy, że tylko $\varphi(h)$ tych liczb należy do potęgi $h$ modulo $p$, a pozostałe należą do mniejszych potęg. Tak więc każda liczba naturalna $a$ należąca do potęgi $h$ modulo $p$ jest rozwiązaniem kongruencji $x^h \equiv 1 \pmod{p}$. Dalej, dla każdej liczby $h$, która dzieli $(p-1)$ zachodzić będzie albo $\varphi(h)$, albo nie będzie żadnych liczb naturalnych $a$ z przedziału $\langle 1, p-1\rangle$, takich że $a$ należy do potęgi $h$ modulo $p$. Niech $\psi(h)$ oznacza liczbę tych $a$, które należą do potęgi $h$ modulo $p$. Wtedy $\psi(h) \le \varphi(h)$ dla $h$ dzielącego $(p-1)$ oraz $\sum_{h \mid p-1} \psi(h) = p-1$. Jednak z *Twierdzenia 7* wiemy, że $\sum_{h \mid p-1} \varphi(h) = p-1$, mamy więc $\sum_{h \mid p-1} (\psi(h) - \varphi(h)) = 0$ i $\psi(h) - \varphi(h) \le 0$, co implikuje fakt, że $\psi(h) = \varphi(h)$ dla $h$ dzielących $p-1$, a w szczególności $\psi(p-1) = \varphi(p-1) > 0$, co dowodzi pierwszej części twierdzenia.

Niech $m = 2^f \prod_{i=1}^{k} p_i^{e_i}$ gdzie $p_i$ to różne liczby pierwsze, $f \ge 0$, $e_i > 0$, a $k \ge 1$. Jeśli $(a, m) = 1$, to zachodzi $a^{\varphi(p_i^{e_i})} \equiv 1 \pmod{p_1^{e_1}}$ oraz $a^{\varphi(m/p_i^{e_1})} \equiv 1 \pmod{m / p_1^{e_1}}$. Załóżmy, że

$k \geq 2$ lub $f \geq 2$. Wtedy $\varphi(p_1^{e_1})$ i $\varphi(m / p_1^{e_1})$ są równe, a co za tym idzie $a^{\frac{1}{2}\varphi(p_i^{e_i})\varphi(m/p_i^{e_i})}$ przystaje do 1 modulo $p_i^{e_i}$ oraz modulo $m / p_i^{e_i}$, skąd również modulo *m*. Stąd widać, że jedyna liczba *m*, która może mieć pierwiastki pierwotne, to $p^e$, $2p^e$, 2 i 4, gdzie *p* to liczba pierwsza, a to kończy dowód drugiej części twierdzenia.

## Twierdzenie 12

Załóżmy, że *m* posiada pierwiastek pierwotny *g*. Wtedy $g^j \equiv g^k \pmod{m}$ wtedy i tylko wtedy, gdy $j \equiv k \pmod{\varphi(m)}$. W szczególności $g^j \equiv 1 \pmod{m}$ wtedy i tylko wtedy, gdy $\varphi(m) \mid j$. Zbiór $g, g^2, \ldots, g^{\varphi(m)}$ tworzy zredukowany system reszt modulo *m* (patrz *Definicja 8*), więc jeśli *a* jest liczbą naturalną, taką że $(a, m) = 1$, to istnieje tylko jedna liczba $g^j$ w zbiorze spełniająca kongruencję $g^j \equiv a \pmod{m}$.

**Dowód:** Pierwsza część tego twierdzenia to specjalny przypadek *Twierdzenia 9*. Zakłada ona, że $g, g^2, \ldots, g^{\varphi(m)}$ są parami nieprzystające modulo *m*, a co za tym idzie zbiór ten tworzy zredukowany system reszt modulo *m*.

## Twierdzenie 13

Jeśli *p* jest liczbą pierwszą i $(a, p) = 1$, to kongruencja $x^n \equiv a \pmod{p}$ ma $(n, p - 1)$ rozwiązań lub zero rozwiązań, w zależności od tego, czy $a^{(p-1)/(n,\ p-1)}$ przystaje do 1 mod *p* czy też nie przystaje.

**Dowód:** Niech $b = (n, p - 1)$. Jeśli kongruencja $x^n \equiv a \pmod{p}$ ma rozwiązanie *u*, to wtedy $a^{(p-1)/b} \equiv u^{n(p-1)/b} \equiv u^{(p-1)(n/b)} \equiv 1 \pmod{p}$. I analogicznie $x^n \equiv a \pmod{p}$ nie ma rozwiązań, jeśli $a^{(p-1)/b}$ nie przystaje do 1 $\pmod{p}$.

Załóżmy, że $a^{(p-1)/b} \equiv 1 \pmod{p}$. Z *Twierdzenia 11* i *Twierdzenia 12* wiemy, że istnieje pierwiastek pierwotny $g$ modulo $p$ oraz wykładnik $j$, takie że $g^j \equiv a \pmod{p}$. Mamy więc $g^{j(p-1)/b} \equiv a^{(p-1)/b} \equiv 1 \pmod{p}$, co implikuje (na mocy *Twierdzenia 12*), że $j(p-1)/b \equiv 0 \pmod{p-1}$, więc $b \mid j$. Każde rozwiązanie $x^n \equiv a \pmod{p}$, jeśli tylko istnieje, można również zapisać jako potęgę $g$ (na przykład $g^y$) modulo $p$. Stąd rozwiązania $x$ (jeśli istnieją) kongruencji $x^n \equiv a \pmod{p}$ odpowiadają rozwiązaniom $y$ kongruencji $g^{yn} \equiv g^j \pmod{p}$. Ta kongruencja, na mocy *Twierdzenia 9* wtedy i tylko wtedy, gdy $yn \equiv j \pmod{p-1}$ ma rozwiązania, które posiada na mocy *Twierdzenia 6*, ponieważ $b \mid j$. Ponadto z *Twierdzenia 6* wynika również, że mamy $(n, p-1)$ rozwiązań tej kongruencji, a więc i kongruencji $x^n \equiv a \pmod{p}$.

# ROZDZIAŁ 2

# WIADOMOŚCI TEORETYCZNE O LICZBACH PSEUDOPIERWSZYCH I SILNIE PSEUDOPIERWSZYCH

# Definicje

## Definicja liczb pseudopierwszych

Niech $b$ będzie liczbą całkowitą dodatnią. Jeśli $n$ jest liczbą całkowitą złożoną i $b^n \equiv b \pmod{n}$, to $n$ nazywamy liczbą *pseudopierwszą przy podstawie b* ($n$ jest pp($b$)).

Jeśli $(b, n) = 1$, to kongruencja $b^n \equiv b \pmod{n}$ jest równoważna kongruencji $b^{n-1} \equiv 1 \pmod{n}$. Wykorzystując *Własność 2* możemy podzielić kongruencję $b^n \equiv b \pmod{n}$ przez $b$ (jest to uprawnione, gdyż $(b, n) = 1$ – patrz *Własność 4*) i otrzymamy w ten sposób kongruencję $b^{n-1} \equiv 1 \pmod{n}$. Z kolei wykorzystując *Własność 1* możemy pomnożyć przez $b$ obie strony kongruencji $b^{n-1} \equiv 1 \pmod{n}$, by otrzymać kongruencję $b^n \equiv b \pmod{n}$.

**Przykład:** Liczba 341 (nie jest złożona, ponieważ $341 = 11 \cdot 31$) jest pseudopierwsza, ponieważ $2^{340} \equiv 1 \pmod{341}$, gdyż $2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$ i jednocześnie $2^{340} = (2^5)^{68} \equiv 1 \pmod{34}$.

## Definicja liczb silnie pseudopierwszych

Niech $n$ będzie nieparzystą liczbą złożoną i niech $n - 1 = 2^s t$, gdzie liczba $t$ jest nieparzysta. Niech $b \in (\mathbf{Z}/n\mathbf{Z})^*$. Jeśli liczby $n$ i $b$ spełniają warunek (I):

$b^t \equiv 1 \pmod{n}$ lub

istnieje liczba całkowita $h$ z przedziału $[0, s)$, taka że $b^{2^h t} \equiv -1 \pmod{n}$

to liczbę $n$ nazywamy liczbą *silnie pseudopierwszą przy podstawie b* ($n$ jest spp($b$)).

# Własności i twierdzenia dotyczące liczb pseudopierwszych i silnie pseudopierwszych

## Test Millera-Rabina

Test Millera-Rabina jest testem pierwszości, opierający się na własności liczb silnie pseudopierwszych (czasem liczby silnie pseudopierwsze definiuje się jako takie, które „pozytywnie przechodzą" test Millera-Rabina).

Weźmy liczbę naturalną nieparzystą $n$. Chcemy sprawdzić, czy jest ona pierwsza, czy złożona. Wpierw szukamy specyficznego rozkładu liczby $n - 1$: $n - 1 = 2^s t$, gdzie $t$ jest liczbą nieparzystą. Następnie wybieramy losowo liczbę $b$ należącą do przedziału $(0, n)$, a potem obliczamy $b^t \bmod n$. Jeśli otrzymamy $\pm 1$, to stwierdzamy, że liczba $n$ przeszła pomyślnie test sprawdzający warunek (I) dla naszej podstawy $b$ i wybieramy następną losową podstawę $b$. Jeżeli zaś nie otrzymamy $\pm 1$, to podnosimy do kwadratu $b^t$ modulo $n$, a potem otrzymany wynik podnosimy do kwadratu modulo $n$, aż otrzymamy $-1$. Jeśli otrzymamy $-1$, to liczba pomyślnie przeszła test. Jeżeli jednak nigdy nie otrzymamy $-1$, tzn. jeśli osiągniemy $b^{2^{r+1}} \equiv 1 \pmod{n}$, a jednocześnie $b^{2^r} \neq -1 \pmod{n}$ to wiemy, że liczba $n$ nie przeszła testu, więc jest złożona.

**Przykład:** Liczba 2047 (nie jest złożona: $2047 = 23 \cdot 89$) przechodzi test Millera-Rabina dla $b = 2$, ponieważ $2^{2046/2} = 2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1 \pmod{2047}$.

## Twierdzenie 14

W przypadku, gdy liczba $n$ spełni warunek (I) dla każdej z $k$ losowo wybranych podstaw $b$, to wiemy, że ma ona jedną na $4^k$ szansę być złożona, ponieważ co najwyżej 1/4 podstaw $b$ z przedziału $(0, n)$ spełnia (I) dla $n$ złożonych.

## Lemat 2

Jeśli $n$ jest liczbą złożoną, to $N = 2^n - 1$ również jest złożona.

**Dowód:** Jeżeli $n$ jest złożona, to istnieją $k$ i $l$ takie że $n = kl$. Rozważmy równość $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \ldots + 1)$, w której za $x$ podstawimy $2^l$. Otrzymujemy wówczas, że $2^n - 1 = (2^l - 1)(2^{l(k-1)} + 2^{l(k-2)} + \ldots + 2^l + 1)$, a więc $N = 2^n - 1$ jest również złożona.

## Twierdzenie 15

Istnieje nieskończenie wiele liczb pseudopierwszych przy podstawie 2.

**Dowód:** Pokażemy, że jeśli $n$ jest nieparzystą liczbą pseudopierwszą przy podstawie 2, to $m = 2^n - 1$ jest również pseudopierwsza przy podstawie 2. Ponieważ istnieje przynajmniej jedna liczba pseudopierwsza przy podstawie 2 (na przykład, $n_0 = 341$, ponieważ $2^{340} \equiv 1 \pmod{341}$), możemy skonstruować nieskończenie wiele złożonych liczb pseudopierwszych o podstawie 2, biorąc $n_0 = 341$, a $n_{k+1} = 2^{n_k} - 1$ dla $k = 0, 1, 2,\ldots$ Wszystkie te liczby będą różne, gdyż $n_0 < n_1 < n_2 < \ldots < n_k < n_{k+1} < \ldots$

Niech $n$ będzie nieparzystą liczbą pseudopierwszą i $2^{n-1} \equiv 1 \pmod{n}$. Ponieważ $n$ jest złożona, wiemy że istnieją $d$ i $t$, takie że $n = dt$ i $1 < d < n$ oraz $1 < t < n$. Wykażemy, że $m = 2^n - 1$ jest również pseudopierwsza. Z *Lematu 2* wiemy, że $m$ jest złożona, wystarczy więc pokazać, że $2^{m-1} \equiv 1 \pmod{m}$.

Z założenia mamy, że $2^n \equiv 2 \pmod{n}$, a stąd możemy wywnioskować istnienie $k$, takiego że $2^n - 2 = kn$ i dalej $2^{m-1} = 2^{2^n-2} = 2^{kn}$. W analogiczny sposób co wyżej możemy

wywnioskować, że $m = (2^n - 1) \mid (2^{kn} - 1) = 2^{m-1} - 1$. Stąd $2^{m-1} - 1 \equiv 0 \pmod{m}$ i dalej $2^{m-1} \equiv 1 \pmod{m}$, a stąd wynika, że $m$ jest również pseudopierwsza przy podstawie 2.

## Twierdzenie 16

Istnieje nieskończenie wiele liczb silnie pseudopierwszych przy podstawie 2.

**Dowód:** Pokażemy, że jeśli $n$ jest pseudopierwsza przy podstawie 2, to $N = 2^n - 1$ jest silnie pseudopierwsza przy podstawie 2.

Niech $n$ będzie nieparzystą liczbą złożoną, która jest pseudopierwsza przy podstawie 2, a więc $2^{n-1} \equiv 1 \pmod{n}$. Z tej kongruencji możemy wywnioskować, że $2^{n-1} - 1 = nk$, dla pewnego $k$ całkowitego i nieparzystego. Mamy więc

$$N - 1 = 2^n - 2 = 2\,(2^{n-1} - 1) = 2^1\, nk,$$

czyli jest to faktoryzacja $N - 1$ na iloczyn nieparzystej liczby całkowitej i potęgi dwójki. Zauważmy jeszcze, że

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

ponieważ $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \pmod{N}$. Dzięki temu wiemy, że $N$ przechodzi test Millera-Rabina, a więc jest silnie pseudopierwsza.

Z *Lematu 2* wiemy, że $N = 2^n - 1$ jest złożona, a więc wiemy, że $N$ przechodzi test Millera-Rabina i jest złożona, a więc jest liczbą silnie pseudopierwszą przy podstawie 2.

Jeśli liczba $n$ jest pseudopierwsza przy podstawie 2, to liczba $2^n - 1$ jest silnie pseudopierwsza przy podstawie 2. W *Twierdzeniu 15* (patrz wcześniej) wykazaliśmy, że istnieje nieskończenie wiele liczb pseudopierwszych przy podstawie 2. Z powyższych przesłanek wnioskujemy, że istnieje nieskończenie wiele liczb silnie pseudopierwszych przy podstawie 2.

# ROZDZIAŁ 3

# DANE O LICZBACH PSEUDOPIERWSZYCH I SILNIE PSEUDOPIERWSZYCH

## Informacje wstępne

Większość poniższych danych została opracowana przez autora pracy w oparciu o wyniki otrzymane dzięki dwóm specjalnie do tego celu napisanym programom, z których pierwszy sprawdzał pseudopierwszość danych liczb, a drugi – silną pseudopierwszość. W przypadku bardzo dużych liczb (szczególnie w przypadku danych zamieszczonych w części *Informacje dodatkowe*) informacje zaczerpnięto z książek, podanych w bibliografii.

W rozpatrywanym przez nas przedziale liczb naturalnych od 1 do 100001 włącznie występuje 9591 liczb pierwszych.

## Liczby pseudopierwsze przy podstawie 2

Istnieje 78 liczb mniejszych od 100001, które są pseudopierwsze przy tej podstawie. Podajemy pierwsze dziesięć z nich i największą.

$n = 341$; $n = 561$; $n = 645$; $n = 1105$; $n = 1387$; $n = 1729$; $n = 1905$; $n = 2047$; $n = 2465$; $n = 2701$; $n = 93961$

## Liczby pseudopierwsze przy podstawie 3

Istnieje 76 liczb mniejszych od 100001, które są pseudopierwsze przy tej podstawie. Podajemy pierwsze dziesięć z nich i największą.

$n = 91$; $n = 121$; $n = 671$; $n = 703$; $n = 949$; $n = 1105$; $n = 1541$; $n = 1729$; $n = 1891$; $n = 2465$; $n = 97567$

## Liczby pseudopierwsze przy podstawie 5

Istnieje 66 liczb mniejszych od 100001, które są pseudopierwsze przy tej podstawie. Podajemy pierwsze dziesięć z nich i największą.

$n = 217$; $n = 561$; $n = 781$; $n = 1541$; $n = 1729$; $n = 1891$; $n = 2821$; $n = 4123$; $n = 5461$; $n = 5611$; $n = 98173$

## Liczby pseudopierwsze przy podstawie 7

Istnieje 69 liczb mniejszych od 100001, które są pseudopierwsze przy tej podstawie. Podajemy pierwsze dziesięć z nich i największą.

$n = 25$; $n = 325$; $n = 561$; $n = 703$; $n = 817$; $n = 1105$; $n = 1825$; $n = 2101$; $n = 2353$; $n = 2465$; $n = 97921$

## Liczby pseudopierwsze dla podstaw 2 i 3

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 17.

$n = 1105$; $n = 1729$; $n = 2465$; $n = 2701$; $n = 2821$; $n = 6601$; $n = 8911$; $n = 10585$; $n = 15841$; $n = 18721$; $n = 29341$; $n = 31621$; $n = 41041$; $n = 46657$; $n = 49141$; $n = 52633$; $n = 63973$

## Liczby pseudopierwsze dla podstaw 2 i 5

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 16.

$n = 561$; $n = 1729$; $n = 2821$; $n = 5461$; $n = 6601$; $n = 8911$; $n = 12801$; $n = 13981$; $n = 15841$; $n = 29341$; $n = 41041$; $n = 46657$; $n = 52633$; $n = 63973$; $n = 68101$; $n = 75361$

## Liczby pseudopierwsze dla podstaw 2 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 11.

$n = 561$; $n = 1105$; $n = 2465$; $n = 3277$; $n = 8321$; $n = 10585$; $n = 18721$; $n = 29341$; $n = 46657$; $n = 62745$; $n = 75361$

## Liczby pseudopierwsze dla podstaw 3 i 5

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 14.

$n = 1541$; $n = 1729$; $n = 1891$; $n = 2821$; $n = 6601$; $n = 8911$; $n = 15841$; $n = 29341$; $n = 41041$; $n = 46657$; $n = 52633$; $n = 63973$; $n = 75361$; $n = 88831$

## Liczby pseudopierwsze dla podstaw 3 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 13.

$n = 703$; $n = 1105$; $n = 2465$; $n = 10585$; $n = 18721$; $n = 19345$; $n = 29341$; $n = 38503$; $n = 46657$; $n = 50881$; $n = 75361$; $n = 76627$; $n = 88831$

## Liczby pseudopierwsze dla podstaw 5 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 9.

$n = 561$; $n = 11041$; $n = 29341$; $n = 38081$; $n = 46657$; $n = 50737$; $n = 75361$; $n = 79381$; $n = 88831$

## Liczby pseudopierwsze dla podstaw 2, 3 i 5

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 11.

$n = 1729$; $n = 2821$; $n = 6601$; $n = 8911$; $n = 15841$; $n = 29341$; $n = 41041$; $n = 46657$; $n = 52633$; $n = 63973$; $n = 75361$

## Liczby pseudopierwsze dla podstaw 2, 3 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Jest ich 7.

$n = 1105$; $n = 2465$; $n = 10585$; $n = 18721$; $n = 29341$; $n = 46657$; $n = 75361$

## Liczby pseudopierwsze dla podstaw 2, 5 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Są tylko 4 takie.

$n = 561$; $n = 29341$; $n = 46657$; $n = 75361$

## Liczby pseudopierwsze dla podstaw 3, 5 i 7

Oto wszystkie liczby mniejsze od 100001, które są pseudopierwsze przy tych podstawach. Są tylko 4 takie.

$n = 29341$; $n = 46657$; $n = 75361$; $n = 88831$

## Informacje dodatkowe

Istnieje stosunkowo niewiele liczb pseudopierwszych dla podstawy $b$ i tylko nieliczne liczby złożone przechodzą test $b^n \equiv b \pmod{n}$. W szczególności mamy 455052512 liczb pierwszych mniejszych niż $10^{10}$, podczas gdy w tym samym przedziale istnieje 14884 liczb pseudopierwszych przy podstawie 2.

## Liczby silnie pseudopierwsze przy podstawie 2

Test Millera-Rabina dla tej podstawy przechodzi 16 liczb mniejszych od 100001.

$n = 2047$; $s = 1$ i $t = 1023$; $b^t \equiv 1 \pmod{n}$

$n = 3277$; $s = 2$ i $t = 819$; $b^{2t} \equiv -1 \pmod{n}$

$n = 4033$; $s = 6$ i t=63; $b^{2t} \equiv -1 \pmod{n}$

$n = 4681$; $s = 3$ i $t = 585$; $b^t \equiv 1 \pmod{n}$

$n = 8321$; $s = 7$ i $t = 65$; $b^{2t} \equiv -1 \pmod{n}$

$n = 15841$; $s = 5$ i $t = 495$; $b^t \equiv 1 \pmod{n}$

$n = 29341$; $s = 2$ i $t = 7335$; $b^{2t} \equiv -1 \pmod{n}$

$n = 42799$; $s = 1$ i $t = 21399$; $b^t \equiv 1 \pmod{n}$

$n = 49141$; $s = 2$ i $t = 12285$; $b^{2t} \equiv -1 \pmod{n}$

$n = 52633$; $s = 3$ i $t = 6579$; $b^t \equiv 1 \pmod{n}$

$n = 65281$; $s = 8$ i $t = 255$; $b^{16t} \equiv -1 \pmod{n}$

$n = 74665$; $s = 3$ i $t = 9333$; $b^{2t} \equiv -1 \pmod{n}$

$n = 80581$; $s = 2$ i $t = 20145$; $b^{2t} \equiv -1 \pmod{n}$

$n = 85489$; $s = 4$ i $t = 5343$; $b^{2t} \equiv -1 \pmod{n}$

$n = 88357$; $s = 2$ i $t = 22089$; $b^{2t} \equiv -1 \pmod{n}$

$n = 90751$; $s = 1$ i $t = 45375$; $b^{t} \equiv 1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 3

Test Millera-Rabina dla tej podstawy przechodzą 23 liczby mniejsze od 100001.

$n = 121$; $s = 3$ i $t = 15$; $b^{t} \equiv 1 \pmod{n}$

$n = 703$; $s = 1$ i $t = 351$; $b^{t} \equiv -1 \pmod{n}$

$n = 1891$; $s = 1$ i $t = 945$; $b^{2t} \equiv -1 \pmod{n}$

$n = 3281$; $s = 4$ i $t = 205$; $b^{t} \equiv -1 \pmod{n}$

$n = 8401$; $s = 4$ i $t = 525$; $b^{t} \equiv -1 \pmod{n}$

$n = 8911$; $s = 1$ i $t = 4455$; $b^{t} \equiv -1 \pmod{n}$

$n = 10585$; $s = 3$ i $t = 1323$; $b^{2t} \equiv -1 \pmod{n}$

$n = 12403$; $s = 1$ i $t = 6201$; $b^{t} \equiv -1 \pmod{n}$

$n = 16531$; $s = 1$ i $t = 8265$; $b^{t} \equiv -1 \pmod{n}$

$n = 18721$; $s = 5$ i $t = 585$; $b^{16t} \equiv -1 \pmod{n}$

$n = 19345$; $s = 4$ i $t = 1209$; $b^{2t} \equiv -1 \pmod{n}$

$n = 23521$; $s = 5$ i $t = 735$; $b^{t} \equiv -1 \pmod{n}$

$n = 31621$; $s = 2$ i $t = 7905$; $b^{t} \equiv -1 \pmod{n}$

$n = 44287$; $s = 1$ i $t = 22143$; $b^{t} \equiv -1 \pmod{n}$

$n = 47197$; $s = 2$ i $t = 11799$; $b^{t} \equiv 1 \pmod{n}$

$n = 55969$; $s = 5$ i $t = 1749$; $b^{16t} \equiv -1 \pmod{n}$

$n = 63139$; $s = 1$ i $t = 31569$; $b^{t} \equiv -1 \pmod{n}$

$n = 74593$; $s = 5$ i $t = 2331$; $b^{16t} \equiv -1 \pmod{n}$

$n = 79003$; $s = 1$ i $t = 39501$; $b^{t} \equiv -1 \pmod{n}$

$n = 82513$; $s = 4$ i $t = 5157$; $b^{t} \equiv 1 \pmod{n}$

$n = 87913$; $s = 3$ i $t = 10989$; $b^{t} \equiv 1 \pmod{n}$

$n = 88573$; $s = 2$ i $t = 22143$; $b^{t} \equiv 1 \pmod{n}$

$n = 97567$; $s = 1$ i $t = 48783$; $b^{t} \equiv -1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 5

Test Millera-Rabina dla tej podstawy przechodzi 16 liczb mniejszych od 100001.

$n = 781$; $s = 2$ i $t = 195$; $b^{t} \equiv 1 \pmod{n}$

$n = 1541$; $s = 2$ i $t = 385$; $b^{t} \equiv -1 \pmod{n}$

$n = 5461$; $s = 2$ i $t = 1365$; $b^{t} \equiv -1 \pmod{n}$

$n = 5611$; $s = 1$ i $t = 2805$; $b^{t} \equiv 1 \pmod{n}$

$n = 7813$; $s = 2$ i $t = 1953$; $b^{2t} \equiv -1 \pmod{n}$

$n = 13021$; $s = 2$ i $t = 3255$; $b^{t} \equiv -1 \pmod{n}$

$n = 14981$; $s = 2$ i $t = 3745$; $b^{t} \equiv 1 \pmod{n}$

$n = 15751$; $s = 1$ i $t = 7875$; $b^{t} \equiv 1 \pmod{n}$

$n = 24211$; $s = 1$ i $t = 12105$; $b^{t} \equiv 1 \pmod{n}$

$n = 25351$; $s = 1$ i $t = 12675$; $b^{t} \equiv 1 \pmod{n}$

$n = 29539$; $s = 1$ i $t = 14769$; $b^{t} \equiv 1 \pmod{n}$

$n = 38081$; $s = 6$ i $t = 595$; $b^{16t} \equiv -1 \pmod{n}$

$n = 40501$; $s = 2$ i $t = 10125$; $b^t \equiv 1 \pmod{n}$

$n = 44801$; $s = 8$ i $t = 175$; $b^t \equiv 1 \pmod{n}$

$n = 53971$; $s = 1$ i $t = 26985$; $b^t \equiv 1 \pmod{n}$

$n = 79381$; $s = 2$ i $t = 19845$; $b^t \equiv -1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 7

Test Millera-Rabina dla tej podstawy przechodzi 21 liczb mniejszych od 100001.

$n = 25$; $s = 3$ i $t = 3$; $b^{2t} \equiv -1 \pmod{n}$

$n = 325$; $s = 2$ i $t = 81$; $b^{2t} \equiv -1 \pmod{n}$

$n = 703$; $s = 1$ i $t = 351$; $b^t \equiv 1 \pmod{n}$

$n = 2101$; $s = 2$ i $t = 525$; $b^t \equiv -1 \pmod{n}$

$n = 2353$; $s = 4$ i $t = 147$; $b^{2t} \equiv -1 \pmod{n}$

$n = 4525$; $s = 2$ i $t = 1131$; $b^{2t} \equiv -1 \pmod{n}$

$n = 11041$; $s = 5$ i $t = 345$; $b^{2t} \equiv -1 \pmod{n}$

$n = 14089$; $s = 3$ i $t = 1761$; $b^{4t} \equiv -1 \pmod{n}$

$n = 20197$; $s = 2$ i $t = 5049$; $b^t \equiv 1 \pmod{n}$

$n = 29857$; $s = 5$ i $t = 933$; $b^{4t} \equiv -1 \pmod{n}$

$n = 29891$; $s = 1$ i $t = 14945$; $b^t \equiv -1 \pmod{n}$

$n = 39331$; $s = 1$ i $t = 19665$; $b^t \equiv 1 \pmod{n}$

$n = 49241$; $s = 3$ i $t = 6155$; $b^{4t} \equiv -1 \pmod{n}$

$n = 58825$; $s = 3$ i $t = 7353$; $b^{2t} \equiv -1 \pmod{n}$

$n = 64681$; $s = 3$ i $t = 8085$; $b^t \equiv -1 \pmod{n}$

$n = 76627$; $s = 1$ i $t = 38313$; $b^t \equiv 1 \pmod{n}$

$n = 78937$; $s = 3$ i $t = 9867$; $b^{4t} \equiv -1 \pmod{n}$

$n = 79381$; $s = 2$ i $t = 19845$; $b^{t} \equiv -1 \pmod{n}$

$n = 87673$; $s = 3$ i $t = 10959$; $b^{4t} \equiv -1 \pmod{n}$

$n = 88399$; $s = 1$ i $t = 44199$; $b^{t} \equiv 1 \pmod{n}$

$n = 88831$; $s = 1$ i $t = 44415$; $b^{t} \equiv -1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 2, 3

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw. Otrzymano je dzięki programowi, który sprawdzał liczby począwszy od najmniejszej znanej liczby silnie pseudopierwszej dla dwóch podstaw.

$n = 1373653$; $s = 2$ i $t = 343413$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{t} \equiv 1 \pmod{n}$

$n = 1373717$; $s = 2$ i $t = 343429$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1373761$; $s = 6$ i $t = 21465$; $b_1^{16t} \equiv -1 \pmod{n}$; $b_2^{64t} \equiv -1 \pmod{n}$

$n = 1373819$; $s = 1$ i $t = 686909$; $b_1^{t} \equiv -1 \pmod{n}$; $b_2^{t} \equiv 1 \pmod{n}$

$n = 1400821$; $s = 2$ i $t = 350205$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{t} \equiv 1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 2, 5

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw.

$n = 1373677$; $s = 2$ i $t = 343419$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377031$; $s = 1$ i $t = 68851$; $b_1^{t} \equiv 1 \pmod{n}$; $b_2^{t} \equiv 1 \pmod{n}$

$n = 1377037$; $s = 2$ i $t = 344259$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377847$; $s = 1$ i $t = 688923$; $b_1^{t} \equiv 1 \pmod{n}$; $b_2^{t} \equiv -1 \pmod{n}$

$n = 1377853$; $s = 2$ i $t = 344463$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 2, 7

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw.

$n = 1373683$; $s = 1$ i $t = 686841$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

$n = 1377811$; $s = 1$ i $t = 688905$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

$n = 1377829$; $s = 2$ i $t = 344457$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377043$; $s = 1$ i $t = 688521$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

$n = 1377853$; $s = 2$ i $t = 344463$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 3, 5

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw.

$n = 1373683$; $s = 1$ i $t = 686841$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

$n = 1373717$; $s = 2$ i $t = 343429$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377037$; $s = 2$ i $t = 344259$; $b_1^t \equiv 1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377791$; $s = 1$ i $t = 688895$; $b_1^t \equiv 1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

$n = 1377821$; $s = 2$ i $t = 344455$; $b_1^{2t} \equiv -1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 3, 7

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw.

$n = 1373689$; $s = 3$ i $t = 171711$; $b_1^t \equiv -1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1373761$; $s = 6$ i $t = 21465$; $b_1^{64t} \equiv -1 \pmod{n}$; $b_2^{64t} \equiv -1 \pmod{n}$

$n = 1373777$; $s = 4$ i $t = 85861$; $b_1^{16t} \equiv -1 \pmod{n}$; $b_2^{16t} \equiv -1 \pmod{n}$

$n = 1377781$; $s = 2$ i $t = 344445$; $b_1^t \equiv 1 \pmod{n}$; $b_2^{2t} \equiv -1 \pmod{n}$

$n = 1377787$; $s = 1$ i $t = 688893$; $b_1^t \equiv 1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

## Liczby silnie pseudopierwsze przy podstawie 5, 7

Podajemy kilka przykładów liczb silnie pseudopierwszych dla tych podstaw.

$n = 1373789$; $s = 2$ i $t = 343447$; $b_1^t \equiv 1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

$n = 1373803$; $s = 1$ i $t = 686901$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

$n = 1377023$; $s = 1$ i $t = 688511$; $b_1^t \equiv -1 \pmod{n}$; $b_2^t \equiv -1 \pmod{n}$

$n = 1377031$; $s = 1$ i $t = 688515$; $b_1^t \equiv 1 \pmod{n}$; $b_2^t \equiv 1 \pmod{n}$

$n = 1377041$; $s = 4$ i $t = 688515$; $b_1^t \equiv -1 \pmod{n}$; $b_2^{4t} \equiv 1 \pmod{n}$

## Informacje dodatkowe

Test Millera-Rabina jest stosunkowo dobrym testem sprawdzającym pierwszość, szczególnie gdy posiadamy następujące informacje. Najmniejsza liczba silnie pseudopierwsza złożona dla podstawy 2 to 2047, więc wszystkie liczby mniejsze od niej, które pozytywnie przejdą test Millera-Rabina, są pierwsze. Podobnie 1373653 to najmniejsza liczba silnie pseudopierwsza złożona dla podstaw 2 i 3, 25326001 – dla podstaw 2, 3 i 5, a 3215031751 – dla podstaw 2, 3, 5 i 7. Co więcej, istnieje tylko jedna liczba złożona silnie pseudopierwsza dla podstaw 2, 3, 5 i 7, która jest mniejsza niż $25 \cdot 10^9$, a jest nią 3251031751.

# ROZDZIAŁ 4

# WIADOMOŚCI TEORETYCZNE O LICZBACH BARDZO SILNIE PSEUDOPIERWSZYCH

## Definicja liczb bardzo silnie pseudopierwszych

Niech $n$ będzie liczbą nieparzystą złożoną, $p$ liczbą pierwszą dzielącą $n - 1$, a $b_1$, …, $b_k$ liczbami naturalnymi względnie pierwszymi z $n$. Niech $n - 1 = p^r m$, gdzie $p$ nie dzieli $m$. Mówimy że $n$ jes*t bardzo silnie pseudopierwsza* ze względu na liczbę pierwszą $p$ i podstawy $b_1$, $b_2$, …, $b_k$, ($n$ jes*t* bspp($p$; $b_1$, …, $b_k$)), jeśli dla każdego $a$ pojawiającego się w sekwencji:

(*) $\quad b_i^m,\ b_i^{pm},\ b_i^{p^2 m},\ \ldots,\ b_i^{p^{r-1} m},\ b_i^{p^r m}, \quad i = 1,2,\ldots,k.$

Zbiór $S(a)$ (czyli zbiór wszystkich resz*t* modulo $n$ pojawiających się we wszystkich sekwencjach (*) przed $a$) ma następujące własności (II):

1. Ostatnim wyrazem w sekwencji (*) modulo $n$ jest 1.
2. Dla każdych trzech różnych elementów $y_1$, $y_2$, $y_3 \in S(a)$, $y_3/y_1$ jest potęgą $y_2/y_1$ modulo $n$. W szczególności zbiór $S(a)$ ma co najwyżej $p$ elementów.
3. Dla $p = 2$ mamy $S(1) \subset \{1, -1\}$.

## Liczby pierwsze w obliczu definicji liczb pseudopierwszych

Załóżmy że $n$ jest liczbą pierwszą. W takim przypadku $p^r m = n - 1 = \varphi(n)$ (gdzie $\varphi(n)$ to funkcja Eulera – patrz *Definicja 7*; dla liczby pierwszej $n$ ma ona własność $\varphi(n) = n - 1$). Stąd ostatnim wyrazem w sekwencji (*) jest 1 (mod $n$) (z twierdzenie Eulera – patrz *Twierdzenie 3*). Jeśli w sekwencji (*) pojawi się $a$ (mod $n$) oraz

$$a \equiv b_i^{p^s m} \pmod{n},\ 0 < s < r,\ b > a,\ b \equiv b_i^{p^{s-1} m} \pmod{n},\ 0 < s < r,$$

to $b^p \equiv a \pmod{n}$, tzn. $b$ jest rozwiązaniem kongruencji $x^p \equiv a \pmod{n}$, a ta kongruencja z *Twierdzenia 13* ma dokładnie $p$ rozwiązań. Niech $x_1$, $x_2$, …, $x_p$ będą tymi rozwiązaniami. W takim przypadku grupa $\{1, x_2/x_1, \ldots, x_p/x_1\}$ jest cykliczna

rzędu $p$, gdyż każda grupa o rzędzie równym liczbie pierwszej jest cykliczna (jest to wniosek z twierdzenia Lagrange'a (1) - patrz *Wniosek 2* do *Twierdzenia 1*). Ponieważ zaś $S(a) = \{y_1, y_2, \ldots, y_l\}$ jest podzbiorem $\{x_1, x_2, \ldots, x_p\}$ możemy stwierdzić, że w zbiorze $\{y_2/y_1, \ldots, y_l/y_1\}$ każdy element jest potęgą jakiegoś innego.

Tak więc liczby pierwsze spełniałyby założenia definicji liczb bardzo silnie pseudopierwszych, gdyby nie fakt, że $n$ ma być liczbą nieparzystą złożoną.

## Twierdzenie 17

Jeśli $n$ jest liczbą bardzo silnie psuedopierwszą przy podstawie $b$ i $p = 2$, to jest silnie pseudopierwsza przy podstawie $b$ (bspp(2; $b$) jes*t* spp($b$)).

**Dowód:** Dane są $n$ i $b$ spełniające warunek (II). Musimy wykazać, że spełniają one warunek (I). Niech $n - 1 = p^r m$, gdzie $p$ nie dzieli $m$. Dla $p = 2$ $m$ musi być liczbą nieparzystą, a więc pełni rolę $t$. Mamy więc rozkład analogiczny jak w przypadku liczb silnie pseudopiewszych: $n - 1 = 2^r m$. Dla $p = 2$ wiemy, że zbiór $S(1)$ składa się wyłącznie z 1 i –1, a więc w sekwencji (*) może pojawić się –1, tzn. będzie istniała liczba $h$ z przedziału [0, $r$), taka że $b^{2^h t} \equiv -1 \pmod{n}$, dzięki czemu liczba $n$ spełnia warunek (I). W przypadku, gdy w sekwencji (*) mamy same 1, to spełniony jest warunek $b^t \equiv 1 \pmod{n}$, co kończy dowód.

# ROZDZIAŁ 5

# PRZYKŁADY I WYNIKI OBLICZEŃ DOTYCZĄCE LICZB BARDZO SILNIE PSEUDOPIERWSZYCH

## Informacje wstępne

Poniższe danych została opracowana przez autora pracy w oparciu o wyniki otrzymane dzięki specjalnie do tego celu napisanemu programowi.

## Przykłady liczb bardzo silnie pseudopierwszych przy podstawie 2

$n$ = 29341, $p$ = 163, $r$ = 1, $m$ = 180, (*) modulo $n$: 1 1

$n$ = 30121, $p$ = 251, $r$ = 1, $m$ = 120, (*) modulo $n$: 1 1

$n$ = 30889, $p$ = 13, $r$ = 1, $m$ = 2376, (*) modulo $n$: 22288 1

$n$ = 31417, $p$ = 17, $r$ = 1, $m$ = 1848, (*) modulo $n$: 1 1

$n$ = 31609, $p$ = 439, $r$ = 1, $m$ = 72, (*) modulo $n$: 1 1

$n$ = 31621, $p$ = 31, $r$ = 1, $m$ = 1020, (*) modulo $n$: 1 1

**Uwaga:** Z powyższych liczb jedynie 29341 przechodzi test Millera-Rabina.

## Przykłady liczb bardzo silnie pseudopierwszych przy podstawach 2, 3, 5

W wierszach podano kolejne wyrazy sekwencji (*) modulo $n$ dla kolejnych podstaw, czyli pierwszy wiersz to kolejne wyrazy sekwencji (*) modulo $n$ dla podstawy 2, drugi – dla podstawy 3, a trzeci – 5.

$n$ = 2821, $p$ = 5, $r$ = 1, $m$ = 564,

(*) modulo $n$: 729 1

1366 1

1 1

$(1366/1)^4 \pmod{2821} = (729/1)$

$n$ = 6601, $p$ = 3, $r$ = 1, $m$ = 2200,

(*) modulo $n$: 2830 1

1887 1

2830 1

$(2830/1)^2 \pmod{6601} = (1887/1)$

$n$ = 29341, $p$ = 3, $r$ = 1, $m$ = 5868,

(*) modulo $n$: 1925 1

1925 1

8659 1

$(8659/1)^3 \pmod{29341} = (1925/1)$

$n$ = 41041, $p$ = 3, $r$ = 3, $m$ = 1520,

(*) modulo $n$: 22551 1 1 1

40140 1 1 1

35179 1 1 1

$(40140/22551)^1 \pmod{41041} = (35179/22551)$

$n$ = 46657, $p$ = 3, $r$ = 6, $m$ = 64,

(*) modulo $n$: 20140 41614 1 1 1 1 1

13835 3784 1 1 1 1 1

41965 3784 1 1 1 1 1

$(13835/1)^3 \pmod{46657} = (3784/1)$

$(20140/1)^3 \pmod{46657} = (3784/1)$

$(41695/1)^3 \pmod{46657} = (3784/1)$

$(41695/1)^3 \pmod{46657} = (3784/1)$

$n$ = 75361, $p$ = 5, $r$ = 1, $m$ = 15072,

(*) modulo $n$: 39560 1

26079 1

68511 1

$(68511/26079)^{120} \pmod{7531} = (39560/26079)$

Dla porównania, z powyższych liczb jedynie 29341 i 75361 przechodzą test Millera-Rabina i to tylko dla $b = 2$. Dla pozostałych dwóch podstaw nie przechodzą.

## Garść danych

W przedziale od 1 do 100001 (oczywiście wyłączając z tego przedziału wszystkie liczby pierwsze, jako że liczby bardzo silnie pseudopierwsze są naturalne złożone) mamy 78 liczb bardzo silnie pseudopierwszych dla $b = 2$, w tym najmniejszą jest 341. Dla porównania test Millera-Rabina przechodzi 16 liczb z tego przedziału.

W przedziale od 1 do 100001 (oczywiście wyłączając z tego przedziału wszystkie liczby pierwsze, jako że liczby bardzo silnie pseudopierwsze są naturalne złożone) mamy 9 liczb bardzo silnie pseudopierwszych dla $b_1 = 2$, $b_2 = 3$ i $b_3 = 5$ w tym najmniejszą jest 2821.

## Porównanie liczb silnie pseudopierwszych i bardzo silnie pseudopierwszych

Najmniejszą liczbą silnie pseudopierwszą przy podstawach 2, 3 i 5 jest 25326001. Liczba ta jest jednocześnie bardzo silnie pseudopierwsza tylko dla dwóch podstaw: 2 i 3.

$n = 25326001$, $p = 2$, $r = 4$, $m = 1582875$; podstawy $b_1 = 2$, $b_2 = 3$

(*) modulo $n$: 2532600 1 1 1 1

2532600 1 1 1 1

$n = 25326001$, $p = 2$, $r = 4$, $m = 1582875$; podstawy $b_1 = 2$, $b_2 = 5$

(*) modulo $n$: 2532600 1 1 1 1

1 1 1 1 1

$n$ = 25326001, $p$ = 2, $r$ = 4, $m$ = 1582875; podstawy $b_1$ = 3, $b_2$ = 5

(*) modulo $n$: 2532600 1 1 1 1

1 1 1 1 1

Podobnie dzieje się i dla innych liczb.

$n$ = 25326023, $p$ = 2, $r$ = 1, $m$ = 12663011, $b_1$ = 2, $b_2$ = 3

(*) modulo $n$: 1 1

1 1

$n$ = 25326047, $p$ = 2, $r$ = 1, $m$ = 12663026, $b_1$ = 2, $b_2$ = 3

(*) modulo $n$: 1 1

1 1

# BIBLIOGRAFIA

1. Jerzy Browkin *Teoria ciał*, PWN, 1977
2. Jerzy Browkin *On very strong pseudoprimes*, maszynopis
3. Neal Koblitz *Wykład z teorii liczb i kryptografii*, Wydawnictwa Naukowo--Techniczne, 1994
4. Ivan Niven i Herbert S. Zuckerman *An Introduction to the Theory of Numbers (second edition)*, John Wiley & Sons, Inc., 1966
5. Kenneth H. Rosen *Elementary Number Theory and its Applicatopns (third edition)*, Adison-Wesley Publishing Company, 1993
6. Wacław Sierpiński *Arytmetyka teoretyczna*, PWN, 1955