Implementacja algorytmu sprawdzającego pierwszość liczby w czasie wielomianowym

(Implementation of polynomial time primality test)

Martyna Siejba

Praca licencjacka

Promotor: prof. Krzysztof Loryś

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

15 lutego 2019

Streszczenie

Celem niniejszej pracy jest przedstawienie algorytmu AKS w sposób przystępny dla czytelnika o podstawowej wiedzy z zakresu algebry. Praca ta jest więc rozszerzeniem artykułu M. Agrawala, N. Kayala i N. Saxeny *PRIMES is in P* o dowody pomocniczych lematów oraz wykorzystanych twierdzeń algebry abstrakcyjnej.

Początkowa część pracy poświęcona jest wprowadzeniu potrzebnych do przeprowadzenia wywodu o algorytmie AKS pojęć algebry abstrakcyjnej - zdefiniowaniu pierścienia, ciała, grupy pierwiastków z jedności oraz wielomianu cyklotomicznego. Część ta zawiera także dowody użytych w dalszych rozdziałach pracy twierdzeń algebry abstrakcyjnej. Jest ona wstępem do głównego tematu pracy, czyli prezentacji algorytmu AKS i dowodu jego poprawności. Wywód służący udowodnieniu poprawności algorytmu uzupełnia artykuł *PRIMES is in P* o dowody nieoczywistych lematów pomocniczych. Ponadto dowody wszystkich własności algebry znaleźć można w początkowej części pracy. Praca zawiera też ograniczenie złożoności algorytmu. Zaprezentowany dowód nie wykorzystuje najsilniejszego znanego ograniczenia, a służy jedynie pokazaniu, że złożoność algorytmu jest wielomianowa.

Dodatkowym celem pracy jest zaprezentowanie przykładowej implementacji algorytmu AKS w języku C++.

To samo in inglisz.

Spis treści

Rozdział 1.

Wstęp

Problem testu pierwszości, nazwany PRIMES, polega na ustaleniu dla danej liczby naturalnej n, czy jest ona liczbą pierwszą. Jako że wejście składa się z jednej liczby, a naiwny deterministyczny algorytm jest w stanie stwierdzić pierwszość w czasie $O(\sqrt{n})$, za rozmiar problemu uznaje się długość liczby na wejściu **dietz**

Przy takiej definicji problemu PRIMES nieoczywista była jego przynależność do klas złożoności P i NP. Zawieranie w klasie NP zostało po raz pierwszy udowodnione przez Vaughana Pratta w 1975 roku **pratt** Od tego momentu głównym wyzwaniem związanym z problemem było pokazanie jego zawierania lub niezawierania się w klasie P. Przesłankami sugerującymi przynależność PRIMES do klasy P były własności liczb pierwszych wykorzystywane w probablistycznych testach pierwszości. Najprostszym takim testem jest test pierwszości Fermata, opierającym się na Małym Twierdzeniu Fermata, czyli twierdzeniu, że dla liczby pierwszej p i liczby naturalnej a takiej, że $NWD(a,p) = 1$ zachodzi $a^{p-1} = 1 \ (mod\, p)$. Test Fermata polega więc na losowym wyborze a spełniającego założenia twierdzenia i sprawdzeniu, czy równość z twierdzenia zachodzi **dietz** Problemem tego podejścia jest fakt, że implikacja w drugą stronę nie zawsze jest prawdziwa. Istnieją bowiem liczby złożone p, nazywane liczbami pseudopierwszymi Fermata, dla których istnieje a takie, że równość Małego Twierdzenia Fermata jest spełniona. Z tego powodu test Fermata nie jest algorytmem deterministycznym. Innym, powszechnie wykorzystywanym w praktyce probablistycznym podejściem jest test pierwszości Millera-Rabina, który także oparty jest na Małym Twierdzeniu Fermata **dietz**

W 2002 roku Manindra Agrawal, Neeraj Kayal i Nitin Saxena zaprezentowali deterministyczny test pierwszości o wielomianowej złożoności. Chociaż algorytm AKS jest mniej powszechnie wykorzystywany w praktyce niż probablistyczny test Millera-Rabina, ma on duże znaczenie w informatyce, jako że jest pierwszym dowodem na przynależność problemu PRIMES do klasy P **dietz**

Celem niniejszej pracy jest właśnie przedstawienie czytelnikowi algorytmu AKS oraz uzasadnienie jego poprawności w zrozumiały sposób. Praca ta jest uzupełnie-

niem oryginalnej pracy Agrawala, Kayala i Saxeny o dowody nietrywialnych lematów i dodatkowe komentarze, ułatwiające zrozumienie wywodu.

Ponieważ dowód poprawności wymaga znajomości pewnych pojęć i twierdzeń algebry abstrakcyjnej, rozdział 2. poświęcony jest ich wprowadzeniu. Od czytelnika wymagana jest znajomość podstaw algebry, głównie teorii grup. Wprowadzone pojęcia i związane z nimi lematy obejmują pierścienie, ciała, pierścienie wielomianów, pierwiastki z jedności nad ciałem i wielomiany cyklotomiczne. Dla komfortu czytelnika dla zdecydowanej większości twierdzeń i lematów, nawet trywialnych, przedstawiony jest także ich dowód.

Trzeci rozdział jest poświęcony przedstawieniu i udowodnieniu poprawności algorytmu. Główna jego część ma formę serii lematów i twierdzeń, potrzebnych do uzasadnienia końcowego twierdzenia o poprawności algorytmu AKS. Wszystkie potrzebne w tej części twierdzenia algebry abstrakcyjnej są udowodnione w poprzednim rozdziale.

Rozdział czwarty poświęcony jest oszacowaniu złożoności obliczeniowej testu. Ponieważ szacowanie jest dość bezpośrednie, jest to rozdział krótki i nieskomplikowany.

Ostatni rozdział odnosi się do implementacji algorytmu AKS w języku C++. Celem zaimplementowania testu jest jest przede wszystkim pokazanie prostoty implementacji. Nie powinna ona bowiem sprawić trudności programiście z dobrą znajomością klasycznych algorytmów, w szczególności wyszukiwania binarnego i FFT.

Rozdział 2.

Podstawy algebraiczne

Aby udowodnić poprawność algorytmu AKS potrzebne nam będą podstawowe pojęcia oraz twierdzenia algebry abstrakcyjnej, w szczególności własności pierścieni ilorazowych oraz wielomianów cyklotomicznych i pierwiastków z jedności nad ciałem. Poniższy rozdział poświęcony jest więc wprowadzeniu tych pojęć oraz udowodnieniu twierdzeń przydatnych później w dowodzie poprawności algorytmu AKS.

2.1. Pierścień, ciało, pierścień ilorazowy

Zdefiniujmy najpierw podstawowe struktury algebraiczne, których własności będziemy często wykorzystywać w dowodach lematów i twierdzeń, prowadzących do udowodnienia poprawności algorytmu.

Definicja 1. Zbiór R zamknięty na dwie operacje binarne $\oplus$ (dodawanie) oraz $\odot$ (mnożenie) nazywamy ***pierścieniem*** i oznaczamy $\langle R, \oplus, \odot \rangle$, jeśli

- $\oplus$ jest przemienna ($\forall_{a,b \in R}\, a \oplus b = b \oplus a$) oraz łączna ($\forall_{a,b,c \in R}\, (a \oplus b) \oplus c = a \oplus (b \oplus c)$);
- zawiera element zerowy ($\exists_{0 \in R} \forall_{a \in R}\, a \oplus 0 = 0 \oplus a = a$);
- dla każdego elementu zawiera element przeciwny ($\forall_{a \in R} \exists_{(-a) \in R}\, a \oplus (-a) = 0$);
- $\odot$ jest łączna ($\forall_{a,b,c \in R}\, (a \odot b) \odot c = a \odot (b \odot c)$);
- $\oplus$ jest rozdzielna względem $\odot$ ($\forall_{a,b,c \in R}\, a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \wedge (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$).

Obserwacja 1. Każdy pierścień jest grupą.

Uwaga. W przypadku, gdy oczywistym jest, jaka operacja mnożenia jest rozważana, wyrażenie ab będzie skróconym zapisem operacji mnożenia argumentów a, b.

Definicja 2. Pierścień $\langle R, \oplus, \odot \rangle$ nazywamy ***przemiennym*** jeśli $\forall_{a,b \in R}\, ab = ba$.

Możemy teraz zauważyć, że pierścieniem jest na przykład zbiór liczb całkowitych z dodawaniem i mnożeniem lub zbiór wielomianów o współczynnikach całkowitych z dodawaniem i mnożeniem wielomianów.

Definicja 3. Pierścień $\langle F, \oplus, \odot \rangle$ nazywamy ***ciałem***, jeśli

- istnieje element $1 \in F$, będący elementem neutralnym mnożenia ($\forall_{a \in F}\, a1 = 1a = a$) oraz
- jeśli 0 jest elementem zerowym pierścienia $\langle F, \oplus, \odot \rangle$, to $\langle F \setminus \{0\}, \odot \rangle$ jest grupą abelową, której elementem neutralnym jest 1.

Ciało takie będziemy oznaczać $\langle F, \oplus, \odot, 0, 1 \rangle$. W dodatku ***rzędem*** ciała $\langle F, \oplus, \odot, 0, 1 \rangle$ nazywać będziemy moc zbioru F.

Innymi słowy ciało jest pierścieniem z elementem neutralnym mnożenia, w którym dla każdego niezerowego elementu istnieje element odwrotny. Przykładem ciał są zbiory reszt z dzielenia przez liczbę pierwszą z operacjami dodawania i mnożenia modulo. Jeśli rozważymy natomiast wcześniej przywołane przykłady pierścieni, możemy zauważyć, że zarówno zbiór liczb całkowitych jak i zbiór wielomianów o całkowitych współczynnikach nie jest ciałem. W obu przykładach zbiory te nie spełniają warunku na istnienie elementów odwrotnych.

Definicja 4. Niepusty zbiór $I \subseteq R$ nazywamy ***ideałem pierścienia*** $\langle R, \oplus, \odot \rangle$, jeśli

- $\langle I, \oplus \rangle$ jest podgrupą $\langle R, \oplus \rangle$ oraz
- $\forall_{i \in I, r \in R}\, ir \in I \wedge ri \in I$.

Oczywistymi przykładami ideału dla dowolnego pierścienia $\langle R, \oplus, \odot \rangle$ są zbiory R oraz $\{0\}$. Dla pierścienia $\langle \mathbb{Z}, +, \cdot \rangle$ ideałami będą też wszystkie zbiory liczb podzielnych przez pewne $n \in \mathbb{N}_+$.

Twierdzenie 1. *Jeśli $\langle R, \oplus, \odot \rangle$ jest pierścieniem przemiennym oraz $1 \in R$, to dla $a \in R$ zbiór $\langle a \rangle = \{ar \,|\, r \in R\}$ jest jego ideałem. Taki ideał nazywamy* ***ideałem głównym*** *generowanym przez element a.*

Dowód. Aby udowodnić, że $I = \langle a \rangle$ ($a \in R$) jest ideałem $\langle R, \oplus, \odot \rangle$, należy pokazać, że

1. $\langle I, \oplus \rangle$ jest podgrupą $\langle R, \oplus \rangle$ oraz
2. $\forall_{i \in I, r \in R}\, ir \in I \wedge ri \in I$.

Ad.1. Pokażemy kolejno, że

1.1. istnieje element zerowy w I,

1.2. I jest zamknięte na $\oplus$ oraz

1.3. dla każdego elementu istnieje w I element przeciwny.

Ad.1.1 Wiemy, że $0 \in R$, więc $a0 = 0 \in I$.

Ad.1.2 Weźmy dowolne $i_1, i_2 \in I$. Istnieją takie $r_1, r_2 \in R$, że $i_1 = ar_1$ oraz $i_2 = ar_2$. Stąd $i_1 \oplus i_2 = (ar_1) \oplus (ar_2)$. Z własności pierścienia $\langle R, \oplus, \odot \rangle$ mamy $(ar_1) \oplus (ar_2) = a(r_1 \oplus r_2)$, więc $i_1 \oplus i_2 \in I$, czyli I jest zamknięty na $\oplus$.

Ad.1.3 Weźmy dowolne $i = ar \in I, r \in R$. Istnieje $-r \in R$, więc $a(-r) \in I$. Wiemy, że $i \oplus a(-r) = ar \oplus a(-r) = a(r \oplus -r) = a0 = 0$, więc $a(-r) \in I$ jest elementem przeciwnym i.

Ad.2. Weźmy dowolne $i = ar_1 \in I$, $r \in R$. Wtedy $ir = ar_1 r = a(r_1 r)$, więc $ir \in I$. Z przemienności pierścienia $\langle R, \oplus, \odot \rangle$ mamy $ri = ir$, więc $ri \in I$.

□

Definicja 5. Ideał M w pierścieniu R nazywamy ***ideałem maksymalnym***, jeśli dla każdego ideału I nad R zachodzi $M \subseteq I \Rightarrow I = R$.

Dla poprzedniego przykładu ideałów w pierścieniu $\langle \mathbb{Z}, +, \cdot \rangle$ ideałami maksymalnymi będą zbiory liczb podzielnych przez liczbę pierwszą.

Przypomnijmy sobie pojęcia teorii grup potrzebne do zdefiniowania grupy ilorazowej.

Przypomnienie. *Podgrupę $\langle N, \odot \rangle$ grupy $\langle G, \odot \rangle$ nazywamy* ***podgrupą normalną****, jeśli $\forall_{g \in G}\, gN = Ng$, gdzie $gN = \{gn \,|\, n \in N\}$ oraz $Ng = \{ng \,|\, n \in N\}$.*

Przypomnienie. *Niech $\langle H, \odot \rangle$ będzie podgrupą grupy $\langle G, \odot \rangle$ oraz $g \in G$. Wtedy zbiór $L = gH = \{gh \,|\, h \in H\}$ nazywamy* ***warstwą lewostronną*** *oraz zbiór $R = Hg = \{hg \,|\, h \in H\}$ nazywamy* ***warstwą prawostronną*** *grupy G względem $\langle H, \odot \rangle$ wyznaczonymi przez g.*

Możemy teraz przedstawić analogię między ideałem a podgrupą normalną w sposób formalny.

Lemat 1. *Ideał I pierścienia $\langle R, \oplus, \odot \rangle$ z działaniem $\oplus$ jest podgrupą normalną grupy $\langle R, \oplus \rangle$.*

Dowód. Z definicji ideału wiemy, że $\langle I, \oplus \rangle$ jest podgrupą $\langle R, \oplus \rangle$.
Należy pokazać, że dla dowolnego $r \in R$ zachodzi $r \oplus I = I \oplus r$. Wiemy, że $\oplus$ jest przemienna, więc mamy $\{r \oplus i \,|\, i \in I, r \in R\} = \{i \oplus r \,|\, i \in I, r \in R\}$, czyli $r \oplus I = I \oplus r$. □

Zdefiniujmy więc pojęcie grupy ilorazowej, które stanie się podstawą definicji pierścienia ilorazowego.

Twierdzenie 2. *Jeśli $\langle G, \odot\rangle$ jest grupą, a $\langle N, \odot\rangle$ jej podgrupą normalną, to zbiór warstw grupy G względem N z działaniem $\otimes$ zdefiniowanym jako $(aN)\otimes(bN) = abN$ tworzy grupę. Grupę tę oznaczamy G/N i nazywamy* ***grupą ilorazową****.*

Dowód. Wystarczy pokazać, że

1. działanie jest dobrze zdefiniowane, czyli

$$\forall_{a,b,c,d\in G/N}\, a = b \wedge c = d \Rightarrow ac = bd$$

oraz

2. G/N z wyżej zdefiniowanym działaniem jest grupą.

Ad.1. Weźmy $aN = bN \in G/N$ oraz $cN = dN \in G/N$. Chcemy pokazać, że $(aN)(cN) = (bN)(dN)$. Wiemy, że, skoro $\langle N, \odot\rangle$ jest grupą, istnieje element neutralny $1 \in N$. Stąd wiemy, że $a = a1 \in aN$ oraz $b = b1 \in bN$. Z $aN = bN$ mamy $b \in aN$. Istnieje więc $n_1 \in N$ takie, że $an_1 = b$. Analogicznie, istnieje $n_2 \in N$ takie, że $cn_2 = d$.

Możemy zauważyć, że dla dowolnego $n \in N$ zachodzi $nN = N$. Własność ta wynika bezpośrednio z faktu, że N jest zamknięty na $\odot$.

Korzystając z powyższej obserwacji oraz faktu, że $\langle N, \odot\rangle$ jest podgrupą normalną mamy $(bN)(dN) = bdN = an_1cn_2N = an_1cN = an_1Nc = aNc = acN$.

Ad.2. Pokażemy kolejno

2.1. zamkniętość G/N na $\otimes$,

2.2. łączność $\otimes$,

2.3. istnienie elementu neutralnego w G/N oraz

2.4. istnienie elementów odwrotnych.

Ad.2.1. Weźmy dowolne aN, $bN \in G/N$. Mamy $(aN) \otimes (bN) = abN$. $ab \in G$, więc $abN \in G/N$.

Ad.2.2. Weźmy dowolne aN, bN, $cN \in G/N$. Korzystając z łączności $\odot$ i faktu, że N jest normalna ($cN = Nc$), mamy

$$\begin{aligned} aN \otimes ((bN) \otimes (cN)) &= aN \otimes (bcN) = a(bc)N = (ab)cN && (2.1)\\ &= (ab)Nc = (abN) \otimes cN && (2.2)\\ &= ((aN) \otimes (bN)) \otimes cN. && (2.3) \end{aligned}$$

Ad.2.3. Weźmy $1N \in G/N$, gdzie 1 jest elementem neutralnym w $\langle G, \odot \rangle$. Dla dowolnego $aN \in G/N$ mamy $(aN) \otimes (1N) = a1N = aN$, zatem $1N$ jest elementem neutralnym w G/N.

Ad.2.4. Weźmy dowolne $aN \in G/N$. Niech a^{-1} będzie elementem odwrotnym a w grupie $\langle G, \odot \rangle$. Mamy

$$(aN)(a^{-1}N) = aa^{-1}N = 1N,$$

czyli element odwrotny w G/N.

□

Znając już definicję grupy ilorazowej, możemy ją wykorzystać do zdefiniowania pierścienia ilorazowego. Jest on analogicznie zbiorem warstw względem ideału z odpowiednio zdefiniowanymi działaniami.

Twierdzenie 3. *Niech I będzie ideałem pierścienia przemiennego $\langle R, \oplus, \odot \rangle$, a operacje $+$ i $\times$ zdefiniowane będą jako:*

- $(r \oplus I) \times (s \oplus I) = (r \odot s) \oplus I$ *oraz*
- $(r \oplus I) + (s \oplus I) = (r \oplus s) \oplus I$.

Wtedy $\langle R/I, +, \times \rangle$ jest pierścieniem przemiennym. Pierścień taki nazywamy ***pierścieniem ilorazowym****.*

Dowód. $\langle I, \oplus \rangle$ jest podgrupą normalną $\langle R, \oplus \rangle$, więc z Twierdzenia **??** $\langle R/I, + \rangle$ jest grupą ilorazową. Wystarczy zatem pokazać, że

1. $\times$ jest dobrze zdefiniowana, tzn. dla $a, b, c, d \in R/I$ jeśli $a = b$ oraz $c = d$, to $a \times c = b \times d$ oraz
2. $\langle R/I, +, \times \rangle$ jest pierścieniem przemiennym.

Ad.1. Weźmy dowolne $a, b, c, d \in R$ takie, że $a \oplus I = b \oplus I$ oraz $c \oplus I = d \oplus I$. Wiemy, że $\langle I, \oplus \rangle$ jest grupą, więc zawiera element neutralny e. Stąd $a \oplus e = a \in a \oplus I = b \oplus I$. Istnieje więc $i_1 \in I$ taki, że $a = b \oplus i_1$. Analogicznie istnieje $i_2 \in I$ takie, że $c = d \oplus i_2$.
$\langle I, \oplus \rangle$ jest grupą, więc dla dowolnego $i \in I$ $i \oplus I = I$.
Mamy więc $(a \oplus I) \times (c \oplus I) = a \odot c \oplus I = (b \oplus i_1) \odot (d \oplus i_2) \oplus I$. Jako że $b, d, i_1, i_2 \in R$ oraz $\langle R, \oplus, \odot \rangle$ jest pierścieniem mamy $(b \oplus i_1) \odot (d \oplus i_2) \oplus I = b \odot d \oplus b \odot i_2 \oplus i_2 \odot d \oplus i_1 \odot i_2 \oplus I$. I jest ideałem, więc $b \odot i_2, i_1 \odot d, i_1 \odot i_2 \in I$. Stąd $b \odot d \oplus b \odot i_2 \oplus i_2 \odot d \oplus i_1 \odot i_2 \oplus I = b \odot d \oplus I = (b \oplus I) \times (d \oplus I)$.

Ad.2. Pokażemy, że $\langle R/I, +, \times \rangle$ spełnia warunki z definicji pierścienia przemiennego.

- $+$ jest przemienna. Weźmy dowolne $a \oplus I, b \oplus I \in R/I$. Z przemienności $\oplus$ w pierścieniu $\langle R, \oplus, \odot \rangle$ mamy $(a \oplus I) + (b \oplus I) = (a \oplus b) \oplus I = (b \oplus a) \oplus I = (a \oplus I) + (b \oplus I)$.
- $+$ jest łączna. Weźmy dowolne $a \oplus I, b \oplus I, c \oplus I \in R/I$. Z łączności $\oplus$ w $\langle R, \oplus, \odot \rangle$ mamy $((a \oplus I) + (b \oplus I)) + (c \oplus I) = (a \oplus b \oplus I) + (c \oplus I) = (a \oplus b) \oplus c \oplus I = a \oplus (b \oplus c) \oplus I = (a \oplus I) + (b \oplus c \oplus I) = (a \oplus I) + ((b \oplus I) + (c \oplus I))$.
- Istnieje element zerowy. Niech $0_I = 0_R \oplus I$, gdzie 0_R jest elementem zerowym pierścienia $\langle R, \oplus \rangle$. Weźmy dowolne $a \oplus I \in R/I$. Wtedy $(a \oplus I) + 0_I = a \oplus 0_R \oplus I = (a \oplus I) = 0_R \oplus a \oplus I = 0_I + (a \oplus I)$.
- Dla każdego elementu istnieje element odwrotny. Weźmy dowolne $a \oplus I \in R/I$. Istnieje $-a \in R$, będące elementem odwrotnym a. $(a \oplus I) + (-a \oplus I) = a \oplus -a \oplus I = 0_R \oplus I = 0_I = -a \oplus a \oplus I = (-a \oplus I) + (a \oplus I)$.
- $\times$ jest łączna. Weźmy dowolne $a \oplus I, b \oplus I, c \oplus I \in R/I$. Z łączności $\odot$ w pierścieniu $\langle R, \oplus, \odot \rangle$ mamy $((a \oplus I) \times (b \oplus I)) \times (c \oplus I) = (a \odot b \oplus I) \times (c \oplus I) = (a \odot b) \odot c \oplus I = a \odot (b \odot c) \oplus I = (a \oplus I) \times (b \odot c \oplus I) = (a \oplus I) \times ((b \oplus I) \times (c \oplus I))$.
- $+$ jest rozdzielna względem $\times$. Weźmy dowolne $a \oplus I, b \oplus I, c \oplus I \in R/I$. Z rozdzielności $\oplus$ względem $\odot$ w pierścieniu $\langle R, \oplus, \odot \rangle$ mamy $(a \oplus I) \times ((b \oplus I) + (c \oplus I)) = a \odot (b \oplus c) \oplus I = a \odot b \oplus a \odot c \oplus I = ((a \oplus I) \times (b \oplus I)) + ((a \oplus I) \times (c \oplus I))$ oraz $((a \oplus I) + (b \oplus I)) \times (c \oplus I) = (a \oplus b) \odot c \oplus I = a \odot c \oplus b \odot c \oplus I = ((a \oplus I) \times (c \oplus I)) + ((b \oplus I) \times (c \oplus I))$.
- $\times$ jest przemienna. Weźmy dowolne $a \oplus I, b \oplus I \in R/I$. Z przemienności $\odot$ w pierścieniu $\langle R, \oplus, \odot \rangle$ mamy $(a \oplus I) \times (b \oplus I) = a \odot b \oplus I = b \odot a \oplus I = (b \oplus I) \times (a \oplus I)$.

□

Możemy zauważyć, że ideał w teorii pierścieni odpowiada podgrupie normalnej w teorii grup. Co więcej, analogia ta aplikuje się także do konstrukcji pierścienia ilorazowego. Ideał pełni bowiem w konstrukcji pierścienia ilorazowego taką rolę, jaką w konstrukcji grupy ilorazowej pełni podgrupa normalna.

Mając już definicję pierścienia ilorazowego, możemy pokazać, że pewne pierścienie ilorazowe są ciałami. Będzie to twierdzenie, którego będziemy używać w późniejszych lematach dla pierścienia ilorazowego pierścienia wielomianów.

Twierdzenie 4. *Jeśli $\langle R, \oplus, \odot \rangle$ jest pierścieniem przemiennym z elementem neutralnym mnożenia 1, a M ideałem maksymalnym nad R, to R/M z działaniami zdefiniowanymi jak w powyższych twierdzeniach jest ciałem.*

Dowód. Wiemy, że R/M jest pierścieniem przemiennym. Wystarczy pokazać, że w R/M

1. istnieje element neutralny mnożenia oraz

2. dla każdego niezerowego elementu istnieje element odwrotny.

Ad.1. Dla dowolnego $a \oplus M \in R/M$ mamy $(a \oplus M) \times (1 \oplus M) = a \odot 1 \oplus M = a \oplus M = 1 \odot a \oplus M = (1 \oplus M) \times (a \oplus M)$. Zatem $1 \oplus M$ jest elementem neutralnym mnożenia w R/M.

Ad.2. Weźmy dowolne $a \in R$ takie, że $a \oplus M$ jest niezerowe, czyli $a \notin M$. Weźmy zbiór $J = \{ra \oplus m \,|\, r \in R, m \in M\}$. Pokażemy, że J jest ideałem nad R. W tym celu wystarczy pokazać, że

2.1. $\langle J, \oplus\rangle$ jest podgrupą $\langle R, \oplus\rangle$ oraz

2.2. $\forall_{j \in J, r \in R}\, jr \in J \wedge rj \in J$.

Ad.2.1. Udowodnimy, że $\langle J, \oplus\rangle$ spełnia definicję grupy oraz zawiera się w $\langle R, \oplus\rangle$.

- Wiemy, że R jest zamknięty na $\oplus$ i $\odot$, więc $\forall_{r,a',m \in R}\, ra' \oplus m \in R$ i $J \subseteq R$.
- M jest ideałem, czyli jest grupą, więc $0 \in M$. Stąd $0a \oplus 0 = 0 \in J$, czyli J zawiera element zerowy.
- Weźmy dowolne $j = ra \oplus m \in J$. Wiemy, że $-r \in R$ oraz $-m \in M$. Stąd $-j = -ra \oplus -m \in J$. Wtedy $j \oplus -j = ra \oplus m \oplus -ra \oplus -m = ra \oplus -ra = 0a = 0$, tzn. dla każdego elementu J istnieje element przeciwny.
- Weźmy dowolne $j_1 = r_1a \oplus m_1, j_2 = r_2a \oplus m_2 \in J$. Wtedy $j_1 \oplus j_2 = r_1a \oplus m_1 \oplus r_2a \oplus m_2 = (r_1 \oplus r_2)a \oplus (m_1 \oplus m_2)$. Wiemy, że $r_1 \oplus r_2 \in R$ oraz $m_1 \oplus m_2 \in M$, więc $j_1 \oplus j_2 \in J$, czyli J jest zamknięte na $\oplus$.
- $\oplus$ jest łączne. Własność ta wynika bezpośrednio z łączności $\oplus$ w R.

Ad.2.2. Weźmy dowolne $ra \oplus m \in J$ oraz $r' \in R$. Wtedy $jr' = (ra \oplus m) \odot r' = rar' \oplus mr'$. Z przemienności mnożenia w R mamy $jr' = rr'a \oplus mr'$. Z $rr' \in R$ oraz ponieważ M jest ideałem $mr' \in M$, otrzymujemy $jr' \in J$. Analogicznie $r'j \in J$.

Wiemy, że J jest ideałem nad R. Możemy też pokazać, że $M \subset J$. Skoro $\forall_{m \in M}\, m = 0a \oplus m \in J$ oraz $1 \in R$ i $0 \in M$, to $a \in J$. Wiemy, że $a \notin M$, więc $M \subset J$.

Mamy więc ideał J nad R, który zawiera M. Z założenia, że M jest maksymalny, mamy $J = R$, więc $1 \in J$, czyli $\exists_{m \in M, r \in R}\, ra \oplus m = 1$. Wtedy $(r \oplus M) \times (a \oplus M) = ra \oplus M = ra \oplus m \oplus M = 1 \oplus M$, czyli $(a \oplus M)^{-1} = r \oplus M$.

□

2.2. Pierścień wielomianów

Następnym krokiem we wprowadzeniu pojęć algebry abstrakcyjnej będzie bliższe przyjrzenie się pierścieniom wielomianów. W dowodach będziemy korzystać z

twierdzeń i lematów z poprzedniej sekcji. Przechodząc w przestrzeń wielomianów będziemy w stanie zaaplikować twierdzenia algebry abstrakcyjnej do równości uogólnionego Małego Twierdzenia Fermata dla wielomianów, które jest bezpośrednio wykorzystane w algorytmie AKS.

Spójrzmy na pierścień liczb całkowitych modulo liczba naturalna. Na podstawie poniższego twierdzenia będziemy mogli powiązać pierwszość liczby z jego własnościami.

Twierdzenie 5. *Niech $p \in \mathbb{N}$ i $p \geq 2$ oraz $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Wówczas jeśli p jest pierwsza, to $\langle \mathbb{Z}_p, +_p, \times_p \rangle$, gdzie operacje są $+_p$ i $\times_p$ odpowiadającymi działaniami arytmetycznymi modulo p, jest ciałem.*

Dowód. Pokażemy, że jeśli p jest pierwsza, $\langle \mathbb{Z}_p, +_p, \times_p \rangle$ spełnia Definicję **??**.

1. $\langle \mathbb{Z}_p, +_p, \times_p \rangle$ z 1 jest pierścieniem. Dowód jest trywialny i korzysta z własności działań $+_p$ i $\times_p$.

2. Należy więc pokazać, że $\langle \mathbb{Z}_p \setminus \{0\}, \times_p \rangle$ jest grupą abelową. Przemienność i łączność wynikają z własności $\times_p$. Elementem neutralnym jest 1. Jedyną nietrywialną własnością jest istnienie elementu przeciwnego, tzn. należy udowodnić, że $\forall_{a \in \mathbb{Z}_p \setminus \{0\}} \exists_{a^{-1} \in \mathbb{Z}_p \setminus \{0\}} a \times_p a^{-1} = 1$.
   Weźmy dowolne $a \in \mathbb{Z}_p \setminus \{0\}$. Załóżmy nie wprost, że nie istnieje $a^{-1} \in \mathbb{Z}_p \setminus \{0\}$ takie, że $a \times_p a^{-1} = 1$. To znaczy $\forall_{b \in \mathbb{Z}_p \setminus \{0\}} a \times_p b \neq 1$. Ponieważ p jest pierwsze i wszystkie elementy $\mathbb{Z}_p \setminus \{0\}$ są mniejsze od p, wiemy, że $\forall_{b \in \mathbb{Z}_p \setminus \{0\}} a \times_p b \neq 0$. Mamy więc $p-1$ czynników b i $p-2$ możliwych wyników $a \times_p b$. Z zasady szufladkowej mamy $\exists_{b_1, b_2 \in \mathbb{Z}_p \setminus \{0\}}, b_1 \neq b_2\, a \times_p b_1 = a \times_p b_2$. Otrzymujemy $a \times_p (b_1 -_p b_2) = 0$, czyli doszliśmy do sprzeczności.

□

Twierdzenie 6. *Niech $\langle R, \oplus, \odot \rangle$ będzie pierścieniem przemiennym z 1 oraz $R[X]$ będzie zbiorem wielomianów o współczynnikach w R, a $\oplus^*$ i $\odot^*$ będą naturalnie zdefiniowanym dodawaniem i mnożeniem wielomianów z użyciem $\oplus$ i $\odot$ w operacjach na współczynnikach. Wówczas $\langle R[X], \oplus^*, \odot^* \rangle$ jest pierścieniem przemiennym z elementem neutralnym mnożenia będącym wielomianem stałym 1.*

Uwaga. Pomijamy dowód twierdzenia, ponieważ jest on standardowy. Przebiega on przez pokazanie kolejnych własności pierścienia.

Przyjrzyjmy się następnie bliżej pierścieniowi wielomianów, którego współczynniki są elementami ciała. Poniższe lematy pozwolą na ustalenie, kiedy pierścień ilorazowy takiego pierścienia jest ciałem, co stanie się podstawą dowodu algorytmu AKS.

Lemat 2. *Jeśli $\langle F, \oplus, \odot, 0, 1 \rangle$ jest ciałem, to wszystkie ideały nad $F[X]$ są ideałami głównymi.*

Dowód. Weźmy dowolny ideał I nad $F[X]$. Jeśli $I = \{0\}$, to $I = \langle 0 \rangle$. Załóżmy więc, że $I \neq \{0\}$ i weźmy $p(X) \in I$ takie, że $p(X) \neq 0$ oraz $p(X)$ jest wielomianem najmniejszego stopnia w I. Weźmy dowolny wielomian $f(X) \in I$. Jeśli w wyniku jego podzielenia przez $p(X)$ daje resztę $r(X)$, to możemy go przedstawić jako $f(X) = q(X)p(X) \oplus r(X)$, gdzie $deg(r) < deg(p)$. Zauważmy, że $r(X) \in I$, a więc i $q(X)p(X) \in I$. Z założenia o minimalnym stopniu $p(X)$ mamy $r(X) = 0$. Oznacza to, że dowolny wielomian z I da się przedstawić w postaci $q(X)p(X)$, więc $I = \langle p(X) \rangle$. □

Twierdzenie 7. *Jeśli $\langle F, \oplus, \odot, 0, 1 \rangle$ jest ciałem i wielomian $g(X)$ jest nierozkładalny w $F[X]$, to $\langle g(X) \rangle$ jest ideałem maksymalnym.*

Dowód. Weźmy dowolny ideał I nad $F[X]$. Wiemy, że jest to ideał główny, więc istnieje $f(X) \in F[X]$ takie, że $I = \langle f(X) \rangle$. Załóżmy, że $\langle g(X) \rangle \subset I$. Znaczy to, że istnieje $h(X) \in F[X]$ takie, że $g(X) = f(X)h(X)$. Z założenia $g(X)$ jest nierozkładalny, więc $f(X)$ lub $h(X)$ jest wielomianem stopnia 0. Jeśli $f(X)$ jest stopnia 0, to $\langle f(X) \rangle = F$. Jeśli $h(X)$ jest stopnia 0, to $\langle g(X) \rangle = \langle h(X) \rangle$, co jest sprzeczne z założeniem. □

Możemy w szczególności zaaplikować powyższe twierdzenia do ciała liczb całkowitych modulo liczba pierwsza.

Twierdzenie 8. *Jeśli p jest liczbą pierwszą i $h(X)$ jest nierozkładalnym w $\mathbb{Z}_p[X]$ wielomianem stopnia d, to pierścień ilorazowy $\langle \mathbb{Z}_p[X]/\langle h(X) \rangle, \oplus, \odot \rangle$, gdzie $\oplus$ i $\odot$ są naturalnie zdefiniowanymi operacjami na wielomianach, jest ciałem rzędu p^d.*

Dowód. Pokażemy kolejno, że

1. pierścień $\langle \mathbb{Z}_p[X]/\langle h(X) \rangle, \oplus, \odot \rangle$ jest ciałem oraz
2. jest ono rzędu p^d.

Ad.1. $\langle \mathbb{Z}_p, +_p, \times_p, 0, 1 \rangle$ jest ciałem, a $h(X)$ jest nierozkładalny w pierścieniu $\langle \mathbb{Z}_p[X], +^*, \times^* \rangle$, więc na mocy Twierdzenia **??** $\langle \mathbb{Z}_p[X]/\langle h(X) \rangle, \oplus, \odot \rangle$ jest ciałem.

Ad.2. Niech $M = \langle h(X) \rangle$. Pokażemy, że jeśli wielomiany $f(X), g(X) \in \mathbb{Z}_p[X]$, gdzie

$$f(X) = h(X)q_1(X) +^* r_1(X),$$
$$g(X) = h(X)q_2(X) +^* r_2(X),$$

oraz $r_1(X) = r_2(X)$, to

$$f(X) +^* M = g(X) +^* M.$$

Mamy

$$\begin{aligned} f(X) +^* M &= h(X)q_1(X) +^* r_1(X) +^* M \\ &= r_1(X) +^* h(X)q_1(X) +^* M \\ &= r_1(X) +^* M \\ &= r_2(X) +^* M \\ &= r_2(X) +^* h(X)q_2(X) +^* M \\ &= g(X) +^* M. \end{aligned}$$

Ponadto wiemy, że, ponieważ M jest ideałem głównym, dowolna para wielomianów $f(X), g(X) \in r(X) +^* M$ ma taką samą resztę z dzielenia przez $h(X)$. Mamy więc wniosek, że para wielomianów należy do tego samego elementu zbioru $\mathbb{Z}_p[X]/\langle h(X)\rangle$ wtw, gdy mają taką samą resztę z dzielenia przez $h(X)$. Mamy więc tyle elementów zbioru $\mathbb{Z}_p[X]/\langle h(X)\rangle$, ile jest różnych reszt dzielenia wielomianu przez $h(X)$, czyli też tyle, ile jest wielomianów stopnia $d-1$ w $\mathbb{Z}_p[X]$. Stąd $ord(\mathbb{Z}_p[X]/\langle h(X)\rangle) = p^d$.

□

2.3. Pierwiastki z jedności, wielomiany cyklotomiczne

Kolejną grupą twierdzeń potrzebnych do udowodnienia poprawności algorytmu AKS są twierdzenia związane z pierwiastkami jedności nad ciałem. Aby uprościć późniejsze rozważania, wprowadźmy następujące pojęcia związane z ciałami.

Uwaga. Ponieważ w tej i kolejnych sekcjach rozważane w kontekście pewnego ciała operacje i ich elementy neutralne będą oczywiste, dla uproszczenia będziemy oznaczać jako F ciało $\langle F, +, \cdot, 0, 1\rangle$.

Definicja 6. ***Charakterystyką*** ciała F będziemy nazywać najmniejszą taką liczbę naturalną $char(F) = n$, że suma n jedności równa się zeru w F.

Definicja 7. ***Podciałem*** ciała F nazywamy takie $G \subseteq F$, że G z działaniami z F ograniczonymi do elementów G jest ciałem.

Definicja 8. ***Rozszerzeniem ciała*** F nazywamy takie ciało G, że F jest podciałem G.

Zauważmy, że ciało liczb zespolonych jest rozszerzeniem ciała liczb rzeczywistych. Bardziej interesującym przykładem w dalszej części wywodu będzie jednak rozszerzenie ciał skończonego rzędu. Skorzystamy bowiem z własności, że jeśli p jest liczbą pierwszą oraz $f(X)$ jest nierozkładalny w $\mathbb{Z}_p[X]$, to $\mathbb{Z}_p[X]/\langle f(X)\rangle$ jest rozszerzeniem ciała $\mathbb{Z}_p$. Co więcej, umiemy uzasadnić, że $\mathbb{Z}_p$ jest podciałem $\mathbb{Z}_{p^{deg(g)}}$. Niech $d = deg(g)$. Zauważmy, że możemy skonstruować bijekcję między elementami

$\mathbb{Z}_p[X]/\langle f(X)\rangle$ i $\mathbb{Z}_p$ zachowującą działania, ich elementy neutralne i odwrotności. Wielomianowi $h(X) = a_0 + a_1X + \ldots + a_{d-1}X^{d-1} \in \mathbb{Z}_p[X]/\langle f(X)\rangle$ odpowiada liczba $a_0p^{d-1} + \ldots + a_{d-1} \in \mathbb{Z}_{p^d}$. Wówczas $\mathbb{Z}_p$ jest podciałem $\mathbb{Z}_{p^d}$ w taki sposób, że elementowi $k \in \mathbb{Z}_p$ odpowiada $kp^{d-1} \in \mathbb{Z}_{p^d}$.

Obserwacja 2. Jeśli ciało G jest rozszerzeniem ciała F, to $char(G) = char(F)$.

Uwaga. Jako $F(a_1, \ldots, a_n)$ będziemy oznaczać najmniejsze rozszerzenie ciała F zawierające $a_1, \ldots, a_n$.

Definicja 9. ***Ciałem rozkładu*** wielomianu $f(X) \in F[X]$ nad F nazywamy G będące rozszerzeniem F takie, że $f(X)$ można rozłożyć na czynniki liniowe w pierścieniu $G[X]$.

Jako że ciało rozkładu wielomianu będzie ważnym pojęciem w kolejnych deifnicjach, pokażmy, że takowe zawsze istnieje.

Lemat 3 (Twierdzenie Kroneckera)**.** *Dla każdego ciała F i wielomianu $f(X) \in F[X], deg(f) \geq 2$ istnieje rozszerzenie G ciała F, w którym $f(X)$ ma pierwiastek.*

Dowód. Niech $h(X) = a_0 + a_1X + \cdots + a_nX^n$ będzie nierozkładalnym w $F[X]$ czynnikiem $f(X)$. Z Twierdzenia **??** wiemy, że $F[X]/\langle h(X)\rangle$ jest ciałem, a co więcej jest rozszerzeniem F.
Niech $\alpha = X + \langle h(X)\rangle$. Ponieważ $deg(f) \geq 2$, $\alpha \in F[X]/\langle h(X)\rangle$. Mamy więc

$$\begin{aligned} h(\alpha) &= a_0 + a_1(X + \langle h(X)\rangle) + \cdots + a_n(X + \langle h(X)\rangle)^n \\ &= h(X) + \langle h(X)\rangle = 0 \end{aligned}$$

w $F[X]/\langle h(X)\rangle$, czyli α jest pierwiastkiem $f(X)$. □

Twierdzenie 9. *Dla każdego ciała F i wielomianu $f(X) \in F[X]$, $deg(f) \geq 1$ istnieje ciało rozkładu $f(X)$ nad F.*

Dowód. Dowód przebiegać będzie przez indukcję względem $n = deg(f)$. Przypadek dla $n = 1$ jest trywialny, ponieważ F spełnia warunki. Załóżmy więc $deg(f) \geq 2$ oraz, że dla wszystkich wielomianów niższego stopnia teza zachodzi. Z Lematu **??** wiemy, że istnieje ciało G będące rozszerzeniem F takie, że istnieje $\alpha \in G$, $f(\alpha) = 0$. Mamy więc w $G[X]$ równość $f(X) = (X - \alpha)g(X)$. Z założenia indukcyjnego wiemy, że dla $g(X)$ istnieje ciało rozkładu H nad G więc H jest też ciałem rozkładu $f(X)$ nad F. □

Definicja 10. Niech F będzie ciałem i $n \in \mathbb{N}_+$. Ciało rozkładu wielomianu $X^n - 1$ nad F będziemy nazywać ***n-tym ciałem cyklotomicznym*** i oznaczać $F^{(n)}$, a zbiór pierwiastków $X^n - 1$ w $F^{(n)}$ ***pierwiastkami n-tego stopnia z jedności*** i oznaczać $E^{(n)}$.

Twierdzenie 10. *Niech F będzie ciałem i $f(X) \in F[X]$. Jeśli $a \in F$ jest wielokrotnym pierwiastkiem $f(X)$, to jest też pierwiastkiem $f'(X)$.*

Dowód. Zauważmy, że, ponieważ $f(X)$ jest wielomianem, $f(X) \in F[X]$ implikuje $f'(X) \in F[X]$. Skoro $f(X)$ ma co najmniej podwójny pierwiastek w a, to istnieje $h(X) \in F[X]$ takie, że $f(X) = (X-a)(X-a)h(X)$. Wtedy $f'(X) = (X-a)((X-a)h'(X) + 2h(X))$, czyli $f'(X)$ ma pierwiastek w a. □

Przyjrzyjmy się strukturze zbioru pierwiastków n-tego stopnia z jedności nad ciałem.

Twierdzenie 11. *Niech F będzie ciałem i $p = char(F)$. Wówczas zbiór pierwiastków n-tego stopnia z jedności $E^{(n)}$, gdzie $n \in \mathbb{N}$ oraz $p \nmid n$ z operacją mnożenia w $K^{(n)}$ jest grupą cykliczną rozmiaru n.*

Dowód. Niech $\cdot$ będzie operacją mnożenia w $K^{(n)}$. Pokażemy kolejno, że

1. $|\, E^{(n)} \,| = n$,
2. $\langle E^{(n)}, \cdot \rangle$ jest grupą, a co więcej,
3. $\langle E^{(n)}, \cdot \rangle$ jest cykliczna.

Ad.1. Przypadek dla $n = 1$ jest trywialny, ponieważ zbiór $E^{(n)}$ jest wtedy zbiorem zawierającym tylko 1. Załóżmy więc, że $n \geq 2$. Z Twierdzenia **??** wiemy, że jeśli $f(X) = X^n - 1$ i $f'(X) = nX^{n-1}$ nie mają wspólnych pierwiastków w F, to nie istnieją w F wielokrotne pierwiastki wielomianu $f(X)$. Z Obserwacji **??** mamy $char(K^{(n)}) = p$. Z założenia $p \nmid n$. Możemy więc zauważyć, że jedynym pierwiastkiem $f'(X)$ w F jest 0. Dodatkowo 0 nie jest pierwiastkiem $f(X)$, więc $f(X)$ ma n różnych pierwiastków w F, skąd $|\, E^{(n)} \,| = n$.

Ad.2. Pokażemy zamkniętość $E^{(n)}$ na $\cdot$, istnienie elementu neutralnego i elementów odwrotnych w $E^{(n)}$. Weźmy dowolne $\zeta_1, \zeta_2 \in E^{(n)}$. Niech $\zeta = \zeta_1\zeta_2$. Wtedy $\zeta^n = (\zeta_1\zeta_2)^n = \zeta_1^n\zeta_2^n = 1$, czyli $\zeta_1\zeta_2 \in E^{(n)}$. Dla dowolnego $\zeta \in E^{(n)}$ istnieje element odwrotny $\zeta^{n-1} \in E^{(n)}$. Element neutralny stanowi $1_{K^{(n)}}$.

Ad.3. Pokażemy cykliczność $E^{(n)}$ poprzez znalezienie generatora grupy.

Ad.3.1. Niech n będzie liczbą pierwszą. Weźmy dowolne $\zeta \in E^{(n)}$. Załóżmy nie wprost, że istnieje $q < n, q \in \mathbb{N}$ takie, że $\zeta^q = 1$. Wtedy $q \,|\, n$, co jest sprzeczne z założeniem o pierwszości n. Skoro takie q nie istnieje, to ζ generuje $E^{(n)}$, ponieważ dla każdego $i, j < n, i, j \in \mathbb{N}\, \zeta^i \neq \zeta^j$.

Ad.3.2. Niech $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ będzie rozkładem n na czynniki pierwsze. Dla każdego $1 \leq i \leq r$ istnieje nie więcej niż $\frac{n}{p_i}$ pierwiastków wielomianu $X^{\frac{n}{p_i}} - 1$. Ponieważ $\frac{n}{p_1} < n$, istnieje ζ_i nie będąca pierwiastkiem $X^{\frac{n}{p_i}} - 1$. Niech $\alpha_i = \zeta_i^{\frac{n}{(p_i^{e_i})}}$. Wiemy, że $o_n(\alpha_i) \,|\, p_i^{e_i}$, a ponieważ p_i jest pierwsza, $o_n(\alpha_i) = p_i^s$, gdzie $s \leq e_i$. Zauważmy, że jeśli dla $k < r_i$ zachodzi $\alpha_i^{p_i^k} = 1$,

to także $(\alpha_i^{p_i^k})^{p_i} = \alpha_i^{p_i^{k+1}} = 1$. Poprzez indukcję względem k zachodzi $\alpha_i^{p_i^{e_i-1}} = 1$. Wybraliśmy α takie, że $\alpha_i^{p_i^{e_i-1}} = \zeta^{\frac{n}{p_i}} \neq 1$, więc $o_n(\alpha_i) = p_i^{e_i}$. Weźmy $\alpha = \alpha_1 \cdot \ldots \cdot \alpha_r$. Pokażemy, że $o_n(\alpha) = n$. Wiemy, że $o_n(\alpha) \mid n$. Załóżmy nie wprost, że $o_n(\alpha) \neq n$. Wynika stąd, że istnieje takie p_i, że $o_n(\alpha) \mid \frac{n}{p_i}$. Wtedy $\alpha^{\frac{n}{p_i}} = 1 = \alpha_1^{\frac{n}{p_i}} \cdot \ldots \cdot \alpha_r^{\frac{n}{p_r}}$. Dla każdego $j \neq i, 1 \leq j \leq r$ zachodzi z założenia $p_j^{e_j} \mid \frac{n}{p_i}$, a ponieważ $o_n(\alpha_j) = p_i^{e_j}$, mamy $\alpha_j^{\frac{n}{p_i}} = 1$. Mamy więc $\alpha^{\frac{n}{p_i}} = \alpha_i^{\frac{n}{p_i}} = 1$, czyli $o_n(\alpha_i) | \frac{n}{p_i}$. Mamy jednak $o_n(\alpha_i) = p_i^{e_i}$, które nie dzieli $\frac{n}{p_i}$, więc otrzymaliśmy sprzeczność. Pokazaliśmy więc, że $o_n(\alpha) = n$. Na mocy argumentu jak w przypadku, gdy n jest pierwsza, znaleźliśmy α będące generatorem $E^{(n)}$.

□

Przypomnienie. ***Funkcją Eulera*** *nazywamy taką funkcję ϕ, że dla $n \in \mathbb{N}$, $n \geq 2$ $\phi(n)$ jest równa liczbie liczb naturalnych $q < n$ takich, że $NWD(n, q) = 1$.*

Możemy teraz wprowadzić pojęcie pierwiastka pierwotnego a następnie wielomianu cyklotomicznego oraz udowodnić kilka związanych z nimi własności, które okażą się pomocne w dalszych dowodach.

Definicja 11. Pierwiastek n-tego stopnia z jedności nad ciałem F nazywamy ***pierwotnym***, jeśli jest generatorem grupy $E^{(n)}$.

Obserwacja 3. Dla każdego ciała F i $n \in \mathbb{N}$, $char(F) \nmid n$ istnieje co najmniej jeden pierwotny pierwiastek z jedności n-tego stopnia nad F.

Lemat 4. *Jeśli ζ jest pierwotnym pierwiastkiem n-tego stopnia nad ciałem $F, char(F) \nmid n$, to dowolne ζ^s, gdzie $s \in \mathbb{N}$, $NWD(s, n) = 1$ także jest pierwotnym pierwiastkiem n-tego stopnia nad F.*

Dowód. Weźmy s takie, że $NWD(s, n) = 1$. Załóżmy nie wprost, że istnieje $k < n$ takie, że $(\zeta^s)^k = 1$. Wtedy $\zeta^{sk} = 1$, więc z pierwotności ζ możemy wywnioskować, że $n \mid sk$. Ponieważ $NWD(s, n) = 1$, otrzymujemy $n \mid k$, czyli doszliśmy do sprzeczności i ζ^s jest generatorem grupy. □

Definicja 12. Niech F będzie ciałem, $n \in \mathbb{N}$, $char(F) \nmid n$ oraz ζ będzie pierwotnym pierwiastkiem z jedności n-tego stopnia nad F. Wtedy wielomian

$$Q_n(X) = \prod_{s=1, NWD(s,n)=1}^{n} (X - \zeta^s)$$

nazywamy ***n-tym wielomianem cyklotomicznym*** nad F.

Lemat 5. *Jeśli $Q_n(X)$ jest n-tym wielomianem cyklotomicznym nad ciałem F, gdzie $n \in \mathbb{N}$, to $Q_n(X) \mid X^n - 1$ w F.*

Dowód. Własność ta jest oczywista i wynika z zawierania się zbioru pierwiastków $Q_n(X)$ w zbiorze pierwiastków wielomianu $X^n - 1$. □

Obserwacja 4. $Q_n(X)$ nie zależy od wyboru ζ oraz jest stopnia $\phi(n)$. Dodatkowo z definicji $K^{(n)}$ wiemy, że współczynniki $Q_n(X)$ należą do $K^{(n)}$.

Definicja 13. Jeśli G jest rozszerzeniem ciała F, to ***wielomianem minimalnym*** dla $g \in G$ nazywamy nierozkładalny moniczny wielomian $m(X) \in F[X]$ taki, że $m(g) = 0$.

Twierdzenie 12. *Niech G będzie rozszerzeniem ciała F i dla $g \in G$, istnieje niezerowy $f(X) \in F[X]$ taki, że $f(g) = 0$. Wówczas istnieje niezerowy wielomian minimalny dla g w $F[X]$.*

Dowód. Niech $I = \{f(X) \mid f(X) \in F[X], f(g) = 0\}$. Zauważmy, że I jest ideałem nad $F[X]$. Ponieważ F jest ciałem, to na mocy Lematu **??** I jest ideałem głównym. Istnieje wiec $m(X) \in F[X]$ takie, że $I = \langle m(X) \rangle$ oraz $m(X)$ ma minimalny stopień w I. Dodatkowo ponieważ z założenia $I \neq \{0\}$, istnieje niezerowy wielomian $f(X)$ mający pierwiastek w g. Stąd także $m(X)$ nie jest wielomianem zerowym. Jeśli $m(X)$ jest moniczny, to jest wielomianem minimalnym, w przeciwnym przypadku współczynnik przy najwyższej potędze X nie jest jedynką. Ponieważ każdy element niezerowy ma odwrotność w F, to istnieje też moniczny wielomian będący wielomianem minimalnym. □

Lemat 6. *Niech G będzie rozszerzeniem ciała F oraz $m(X) \in F[X]$ będzie wielomianem minimalnym dla $g \in G$. Wówczas dla każdego $f(X) \in F[X]$ zachodzi implikacja $f(g) = 0 \Rightarrow m(X) \mid f(X)$.*

Dowód. Własność ta wynika z poprzedniego dowodu. Jeśli $m(X)$ jest wielomianem minimalnym dla g nad F i $f(X) \in F[X]$ oraz $f(g) = 0$, to $f(X)$ należy do ideału głównego generowanego przez $m(X)$. Istnieje zatem $h(X) \in F[X]$ takie, że $f(X) = h(X)m(X)$. □

Twierdzenie 13. *Dla $n, q \in \mathbb{N}$ takich, że $NWD(n, q) = 1$, wielomian cyklotomiczny $Q_n(X)$ nad $\mathbb{Z}_q$ jest rozkładalny na nierozkładalne czynniki stopnia $o_n(q)$ w $\mathbb{Z}_q[X]$.*

Dowód. Niech ζ będzie pierwotnym pierwiastkiem n-tego stopnia nad $\mathbb{Z}_q$. Wprowadźmy oznaczenie $\mathbb{F}_{q^k}$ na zbiór będący ciałem rzędu q^k. Zauważmy, że takie ciało istnieje, ponieważ zbiór wielomianów o współczynnikach ze zbioru $\mathbb{Z}_q$ stopnia mniejszego niż k jest ciałem rzędu q^k.

Dowód przebiegał będzie w trzech krokach.

1. Pokażemy, że dla dowolnego $k > 1$ zachodzi $\zeta^{q^k} = \zeta$ wtw, gdy $\zeta \in \mathbb{F}_{q^k}$.

2. Niech d będzie najmniejszą liczbą taką, że $\zeta \in \mathbb{F}_{q^d}$ oraz $f(X) \in \mathbb{Z}_q[X]$ będzie wielomianem o pierwiastku w ζ takim, że $deg(f) > 0$. Wówczas istnieje w $\mathbb{Z}_q[X]$ wielomian $h(X)$ taki, że $h(X) \mid f(X)$ i $deg(h) = d$.

3. Wywnioskujemy tezę.

Ad.1. Zauważmy, że jeśli dowolne $a \in \mathbb{F}_{q^k}$, to z twierdzenia Lagrange'a mamy $a^{q^k-1} = 1$, stąd $a^{q^k} = a$. Zauważmy, że równanie $a^{q^k} = a$ ma nie więcej niż q^k pierwiastków, a skoro wszystkie elementy $\mathbb{F}_{q^k}$ są jego pierwiastkami, to wszystkie pierwiastki są elementami $\mathbb{F}_{q^k}$.

Ad.2. Niech $m(X) \in \mathbb{Z}_q[X]$ będzie minimalnym wielomianem dla ζ. Wiemy, że taki istnieje z Twierdzenia **??** oraz ponieważ istnieje niezerowe $Q_n(X) \in \mathbb{Z}_q[X]$. Założyliśmy, że $\zeta \in \mathbb{F}_{q^d}$. Wiemy także, że $\zeta \in \mathbb{Z}_q/\langle m(X)\rangle$, tzn. $\zeta \in \mathbb{F}_{q^{deg(m)}}$. Ponieważ $m(X)$ jest wielomianem minimalnym oraz d jest najmniejszą liczbą spełniającą założenie, otrzymujemy $deg(m) = d$. Na mocy Lematu **??** otrzymujemy dodatkowo, że $m(X)$ dzieli dowolny wielomian $f(X) \in \mathbb{Z}_q[X]$, mający pierwiastek w ζ.

Ad.3. Wiemy, że zachodzi $\zeta^{q^{o_n(q)}} = \zeta$, więc także $\zeta \in \mathbb{F}_{q^{o_n(q)}}$. Ponieważ ζ jest pierwiastkiem pierwotnym wiemy, że jest to najmniejsza liczba, spełniająca tę własność. Możemy więc skorzystać z faktu udowodnionego w drugim kroku i wywnioskować, że każdy wielomian o pierwiastku w ζ można podzielić przez pewien inny wielomian należący do $\mathbb{Z}_q[X]$ stopnia $o_n(q)$. Stosując to rozumowanie indukcyjnie możemy wywnioskować tezę.

□

Rozdział 3.

Algorytm

3.1. Idea algorytmu

Algorytm AKS opiera się na uogólnieniu Małego Twierdzenia Fermata dla wielomianów, czyli twierdzeniu, że pierwszość liczby n, $n > 2$ jest równoważna z zachodzeniem równości $(X+a)^n = X^n+a(modn)$, gdzie $NWD(a, n) = 1$. Jest to własność przydatna bardziej niż podstawowe Małe Twierdzenie Fermata, ponieważ występuje w nim równoważność a nie jednostronna implikacja, która była niewystarczająca, aby zapewnić determinizm w teście pierwszości Fermata. Naiwne sprawdzenie tego twierdzenia skutkowałoby jednak złożonością obliczeniową $O(nlog^2n)$, ponieważ wymagałaby mnożenia wielomianów n-tego stopnia. W kontekście problemu PRIMES jest to złożoność niesatysfakcjonująca, ponieważ względem rozmiaru problemu, czyli długości n, jest to złożoność wykładnicza. Problem ten rozwiązany został w algorytmie AKS poprzez sprawdzenie równości uogólnionego Małego Twierdzenia Fermata nie w pierścieniu $\mathbb{Z}_n[X]$ a w zawartym w nim pierścieniu ilorazowym zdefiniowanym tak, że długość wielomianów, na których wykonane jest mnożenie, jest wielomianowa względem długości liczby n. Poprawność tego podejścia wynika z nietrywialnego twierdzenia, że w odpowiednio wybranym pierścieniu ilorazowym pierścienia $\mathbb{Z}_n[X]$ jeśli równanie $(X + a)^n = X^n + a$ zachodzi dla odpowieniej liczby różnych a, to n nie może być liczbą złożoną.

3.2. Schemat algorytmu

Algorithm 1 Algorytm AKS

Dane wejściowe: liczba całkowita $n > 1$

Wynik: **PIERWSZA** - jeśli n jest pierwsza; **ZŁOŻONA** - jeśli n jest złożona

1: **if** istnieje takie $a \in \mathbb{N}, b > 1$, że $a^b = n$ **then** ▷ Krok 1.
2: **return** ZŁOŻONA
3: **end if**

4: $r \leftarrow$ najmniejsza liczba taka, że zachodzi $o_r(n) > log^2 n$ ▷ Krok 2.
5: **if** istnieje $a \leq r$ takie, że $1 < NWD(a, n) < n$ **then** ▷ Krok 3.
6: **return** ZŁOŻONA
7: **end if**
8: **if** $n \leq r$ **then** ▷ Krok 4.
9: **return** PIERWSZA
10: **end if**
11: **for** $a \leftarrow 1$ **to** $\lfloor \sqrt{\phi(r)} \log n \rfloor$ **do** ▷ Krok 5.
12: **if** $(X + a)^n \neq X^n + a \,(mod\, X^r - 1,\, n)$ **then** ▷ Krok 6.
13: **return** ZŁOŻONA
14: **end if**
15: **end for**
16: **return** PIERWSZA ▷ Krok 7.

3.3. Dowód poprawności

Dowód poprawności algorytmu przeprowadzimy poprzez udowodnienie serii lematów i ostatecznie wykorzystanie ich do udowodnienia twierdzenia, że algorytm zwróci *PIERWSZA* wtedy i tylko wtedy, gdy liczba n na wejściu jest pierwsza. Lematy prowadzące do końcowego twierdzenia będą często udowodnione z użyciem twierdzeń i lematów z poprzedniego rozdziału. Kluczowym fragmentem dowodu będzie znalezienie sprzeczności w twierdzeniu, że jeśli n jest złożona, to algorytm może zwócić *PIERWSZA* w kroku 7. Zdefiniujemy bowiem na podstawie n, jej pierwszego dzielnika p oraz wybranego w trakcie wykonania algorytmu r zbiór, który, korzystając z założeń wynikających z przebiegu algorytmu, będziemy mogli ograniczyć z dwóch stron, doprowadzając do sprzeczności.

Równoważność między pierwszością liczby n oraz zwróceniem *PIERWSZA* przez algorytm pokażemy poprzez udowodnienie implikacji w dwie strony. Zacznijmy od pokazania, że jeśli n jest liczbą pierwszą, to algorytm zwróci *PIERWSZA*. Aby udowodnić to twierdzenie wykorzystamy dwa lematy, z których będziemy w stanie wywnioskować, że algorytm nie zakończy się zwróceniem *ZŁOŻONA* w 5. kroku.

Lemat 7. *Niech a, $n \in \mathbb{N}$, $n \geq 2$ i $NWD(a, n) = 1$. Wtedy n jest pierwsza wtw, gdy $(X + a)^n = X^n + a \,(mod\, n)$.*

Dowód. Rozpatrując współczynniki przy X^i w wielomianie

$$p(X) = (X + a)^n - (X^n + a)$$

pokażemy, że $p(X) = 0 \,(mod\, n)$ wtw, gdy n jest pierwsza.

1. Załóżmy, że n jest pierwsza. Wtedy współczynnik przy X^i $(1 \leq i < n)$ w wielomianie $p(X)$ jest równy $\binom{n}{i} a^{n-i} = \frac{n!}{i!(n-i)!} \cdot a^{n-i}$. Z $\binom{n}{i} \in \mathbb{Z}$ oraz pierwszości

n wiemy, że nie istnieje q takie, że $q \mid i! \cdot (n-i)! \wedge q \nmid (n-1)!$, więc $\frac{(n-1)!}{i! \cdot (n-i)!} \in \mathbb{Z}$ oraz $n \mid \binom{n}{i}$. Stąd $n \mid p(X)$.

2. Załóżmy, że n jest złożona. Niech q będzie pewnym dzielnikiem pierwszym n oraz $q^k \parallel n$. Współczynnik przy X^q jest równy $\binom{n}{q}a^{n-q}$. Możemy zauważyć, że q^k nie dzieli $\binom{n}{q}$, ponieważ $\binom{n}{q} = \frac{n!}{q!(n-q)!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-q+1)}{q!}$. Wiemy, że skoro q jest pierwsze i $q \mid n$, to

$$q \nmid (n-1) \cdot \ldots \cdot (n-q+1),$$

skąd możemy wywnioskować, że

$$q^k \parallel n \cdot (n-1) \cdot \ldots \cdot (n-q+1).$$

Mamy więc $q^k \nmid \binom{n}{q}$. Ponieważ a jest względnie pierwsze z n, to $q \nmid a^{n-q}$, więc $q^k \nmid \binom{n}{q}a^{n-q}$. Stąd mamy $p(X) \neq 0 \, (mod\, n)$.

□

Lemat 8. *Niech a, n, $r \in \mathbb{N}$, $n \geq 2$, $r \geq 1$ i $NWD(a,n) = 1$. Wówczas jeśli n jest pierwsza, to $(X+a)^n = X^n + a \, (mod\, X^r - 1,\, n)$.*

Dowód. Dowód wynika bezpośrednio z Lematu **??**. Wiemy, że

$$(X+a)^n - (X^n + a) = 0 \, (mod\, n),$$

więc także

$$(X+a)^n - (X^n + a) = 0 \, (mod\, X^r - 1,\, n).$$

□

Twierdzenie 14. *Niech $n \in \mathbb{N}$, $n \geq 2$ będzie liczbą podaną na wejściu algorytmu. Jeśli n jest liczbą pierwszą algorytm zwróci PIERWSZA.*

Dowód. Ponieważ n jest liczbą pierwszą, algorytm nie zwróci *ZŁOŻONA* w kroku 1. i 3. Z Lematu **??** wiemy, że dla każdego $1 \leq a < n$ zachodzi

$$(X+a)^n = X^n + a \, (mod\, X^r - 1,\, n),$$

więc algorytm się nie zakończy w kroku 5. Ostatecznie algorytm zwróci *PIERWSZA* w kroku 4 lub 7. □

Zacznijmy dowód odwrotnej implikacji od wprowadzenia pojęcia introspektywności oraz udowodnienia związanych z nim własności.

Definicja 14. Dla ustalonych r, $p \in \mathbb{N}$, gdzie p jest pierwsza, liczbę $m \in \mathbb{N}$ nazywamy ***introspektywną*** modulo $X^r - 1$, p dla wielomianu $f(X)$, jeśli zachodzi

$$(f(X))^m = f(X^m) \, (mod\, X^r - 1,\, p).$$

Lemat 9. *Niech r, $p \in \mathbb{N}$ oraz p jest pierwsza. Jeśli m i m' są introspektywne modulo $X^r - 1$, p dla $f(X)$, to mm' także jest introspektywna modulo $X^r - 1$, p dla $f(X)$.*

Dowód. Z introspektywności m mamy $(f(X))^{mm'} = (f(X^m))^{m'} \, (mod\, X^r - 1,\, p)$. Z introspektywności m' wiemy, że istnieje $g(X) \in \mathbb{Z}_p[X]$ takie, że

$$f(X^{m'}) - f(X)^{m'} = g(X) \cdot (X^r - 1) \, (mod\, p)$$
$$f(X^{mm'}) - f(X^m)^{m'} = g(X^m) \cdot (X^{mr} - 1) \, (mod\, p).$$

Mamy więc

$$(f(X^m))^{m'} = f(X^{mm'}) \, (mod\, (X^m)^r - 1,\, p),$$

a, ponieważ $X^r - 1$ dzieli $X^{mr} - 1$, także

$$(f(X^m))^{m'} = f(X^{mm'}) \, (mod\, X^r - 1,\, p).$$

Otrzymujemy więc

$$(f(X))^{mm'} = f(X^{mm'}) \, (mod\, X^r - 1,\, p).$$

□

Lemat 10. *Niech r, $p \in \mathbb{N}$ oraz p jest pierwsza. Jeśli m jest introspektywna modulo $X^r - 1$, p dla $f(X)$ i $g(X)$, to jest także introspektywna modulo $X^r - 1$, p dla $f(X) \cdot g(X)$.*

Dowód. Mamy

$$(f(X))^m = f(X^m) \, (mod\, X^r - 1,\, p)$$

oraz

$$(g(X))^m = g(X^m) \, (mod\, X^r - 1,\, p).$$

Mnożąc stronami otrzymujemy

$$(f(X) \cdot g(X))^m = f(X^m) \cdot g(X^m) \, (mod\, X^r - 1,\, p).$$

□

Lemat 11. *Jeśli p jest liczbą pierwszą, to dla dowolnych $f(X), g(X) \in \mathbb{Z}_p[X]$ zachodzi w $\mathbb{Z}_p[X]$*

$$(f(X) + g(X))^p = (f(X))^p + (g(X))^p.$$

Dowód. Mamy

$$(f(X) + g(X))^p = (f(X))^p + (g(X))^p + \sum_{i=1}^{i<p} \binom{p}{i} (f(X))^i \cdot (g(X))^{p-i}.$$

Na mocy argumentu użytego w dowodzie Lematu **??** otrzymujemy wniosek, że dla $1 \leq i < p$ zachodzi $p \,|\, \binom{p}{i}$, skąd wynika teza. □

Uwaga. Na potrzeby kolejnych lematów ustalmy n, r, $p \in \mathbb{N}$, $n \geq 2$ oraz

$$\ell = \lfloor \sqrt{\phi(r)}\, log\, n \rfloor$$

takie, że p jest pierwszym dzielnikiem n, $o_r(n) > log^2 n$, $NWD(r, n) = 1$, więc i $NWD(r, p) = 1$. Ponadto niech dla każdego $0 \leq a \leq \ell$ zachodzi

$$(X + a)^n = X^n + a\ (mod\, X^r - 1,\, n).$$

Możemy teraz zdefiniować

$$I = \{(\frac{n}{p})^i \cdot p^j \mid i,\, j \geq 0\},$$

$$P = \{\prod_{a=0}^{\ell} (X + a)^{e_a} \mid e_a \geq 0\}.$$

Niech G będzie zbiorem reszt z dzielenia elementów I przez r oraz niech $t = |\, G\, |$. Niech $Q_r(X)$ będzie r-tym wielomianem cyklotomicznym nad $\mathbb{Z}_p$ ($r \nmid p = char(\mathbb{Z}_p)$). Weźmy nierozkładalny w $\mathbb{Z}_p[X]$ wielomian $h(X) \in \mathbb{Z}_p[X]$ taki, że $h(X)\, |Q_r(X)$ i $deg(h) = o_r(p)$. Z Twierdzenia **??** wiemy, że taki wielomian istnieje. Zdefiniujmy następnie $F = \mathbb{Z}_p/\langle h(X)\rangle$ oraz $\mathcal{G}$ będący zbiorem elementów P w F.

Zauważmy, że ustalone powyżej liczby n, r spełniają założenia, jakie spełniają odpowiednio zmienne n i r w 7. kroku algorytmu. Jeśli dodatkowo założymy, że n jest złożona, to istnieje p spełniające wszystkie założenia.

Na podstawie zdefiniowanej wcześniej introspektywności oraz jej własności możemy udowodnić następujące twierdzenie.

Lemat 12. *Dowolny element $i \in I$ jest introspektywny modulo $X^r - 1$, p dla dowolnego wielomianu $p(X) \in P$.*

Dowód. Pokażemy, że

1. dla dowolnego $0 \leq a \leq \ell$ liczby $\frac{n}{p}$ i p są introspektywne dla $X + a$, a następnie
2. wywnioskujemy tezę.

Ad.1. Niech $0 \leq a \leq \ell$. Liczba p jest pierwsza, więc z Lematu **??** otrzymujemy

$$(X + a)^p = X^p + a\ (mod\, X^r - 1,\, p),$$

więc p jest introspektywne dla $(X + a)$. Z założenia w Uwadze **??** mamy też

$$(X + a)^n = X^n + a\ (mod\, X^r - 1,\, n).$$

Weźmy $f_1(X) = (X + a)^{\frac{n}{p}}$, $f_2(X) = X^{\frac{n}{p}} + a \in \mathbb{Z}_p[X]$. Zauważmy, że

$$(f_1(X))^p = X^n + a = (f_2(X))^p\ (mod\, X^r - 1,\, p)$$
$$(f_1(X))^p - (f_2(X))^p = 0\ (mod\, X^r - 1,\, p).$$

Z Lematu **??** mamy

$$(f_1(X) - f_2(X))^p = 0 \ (mod\, X^r - 1,\, p)$$
$$f_1(X) = f_2(X) \ (mod\, X^r - 1,\, p).$$

Więc $\frac{n}{p}$ także jest introspektywne modulo $X^r - 1$, p dla $X + a$.

Ad.2. Ponieważ elementy zbioru I są iloczynami liczb $\frac{n}{p}$ i p, a elementy zbioru P są iloczynami wielomianów $X + a$, $0 \leq a \leq \ell$, z Lematów **??** i **??** możemy wywnioskować tezę.

□

Żeby ograniczyć z dołu rozmiar zbioru $\mathcal{G}$ wprowadzimy i udowodnimy dwa pomocnicze lematy. Udowodnimy, że X jest pierwotnym pierwiastkiem r-tego stopnia z jedności w F, dzięki czemu będziemy ostatecznie w stanie stwierdzić, że w $\mathcal{G}$ jest co najmniej tyle elementów, ile różnych wielomianów stopnia mniejszego niż t w P. Drugi lemat pozwoli nam natomiast oszacować dokładniej ich liczbę.

Lemat 13. *X jest pierwotnym pierwiastkiem r-tego stopnia z jedności w F.*

Dowód. Z Lematu **??** oraz ponieważ $h(X) \,|\, Q_r(X)$, mamy $h(X) \,|\, X^r - 1$, więc $X^r = 1$ w F, czyli X jest pierwiastkiem r-tego stopnia z jedności w F. Załóżmy nie wprost, że X nie jest pierwotnym pierwiastkiem. Oznacza to, że istnieje $k < r$ takie, że $X^k = 1$ w F. Implikuje to, że $h(X) \,|\, X^k - 1$ w $\mathbb{Z}_p[X]$. Rozważmy pierwiastki $h(X)$ i $X^k - 1$ w r-tym ciele cyklotomicznym nad $\mathbb{Z}_p$. Istnieje w nim pierwiastek pierwotny r-tego stopnia ζ, który jest pierwiastkiem $h(X)$. Mamy więc $h(\zeta) = 0 \ (mod\, p)$ w $\mathbb{Z}_p^{(r)}$, a ponieważ istnieje pewne $p(X) \in \mathbb{Z}_p[X]$ takie, że $(X^k - 1) = p(X) \cdot h(X) \ (mod\, p)$, to także $\zeta^k - 1 = 0 \ (mod\, p)$ w $\mathbb{Z}_p^{(r)}$. Wynika stąd, że ζ jest też pierwiastkiem z jedności k-tego stopnia w $\mathbb{Z}_p$, a ponieważ $k < r$, mamy sprzeczność z założeniem o pierwotności ζ. □

Lemat 14. *Dla $k + 1$ wielomianów pierwszego stopnia o różnych pierwiastkach $f_1(X), \ldots, f_{k+1}(X)$ istnieje co najmniej $\binom{k+d}{k+1}$ różnych wielomianów $f(X)$ stopnia mniejszego niż d, które można przedstawić jako $f(X) = \prod_{i=1}^{k+1}(f_i(X))^e$, gdzie $e \in \mathbb{N}$.*

Dowód. Przedstawimy, w jaki sposób mozna skonstruować bijekcję między sposobem wyboru $k+1$ z $k+d$ elementów ciągu a różnymi wielomianami $f(X)$. Spójrzmy na ciąg $k + d$ elementów z $k + 1$ elementami wyróżnionymi. Jeśli spojrzymy na liczbę elementów między elementami wyróżnionymi otrzymamy ciąg $a_1, \ldots, a_{k+2}$ taki, że $\sum_{i=1}^{k+2} a_i = d - 1$. Powiemy, że takiemu ciągowi odpowiada wielomian $f(X) \in G$, jeśli $f(X) = \prod_{i=1}^{k+1}(f_i(X))^{a_i}$. Łatwo zauważyć, że jednemu takiemu wyróżnieniu elementów ciągu odpowiada dokładnie jeden wielomian oraz dla różnych wyróżnień elementów, odpowiadające wielomiany są różne. Stąd otrzymujemy tezę, że różnych wielomianów stopnia mniejszego niż d w F jest co najmniej $\binom{k+d}{k+1}$. □

Mając już pomocnicze lematy, możemy przejść do znalezienia ograniczenia dolnego rozmiaru zbioru $\mathcal{G}$.

Lemat 15. $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$.

Dowód. Pokażemy, że

1. dowolne dwa różne wielomiany stopnia mniejszego niż t w P są różne także w $\mathcal{G}$ oraz
2. w P jest co najmniej $\binom{t+\ell}{t-1}$ różnych wielomianów stopnia mniejszego niż t.

Ad.1. Niech $f(X) \neq g(X) \in P$, $deg(f), deg(g) < t$. Załóżmy nie wprost, że $f(X) = g(X)$ w F. Niech $Q(Y) = f(Y) - g(Y)$, gdzie Y jest elementem F, czyli także wielomianem. Zauważmy, że oczywistym pierwiastkiem $Q(Y)$ jest X. Wiemy, że $f(X) \neq g(X)$, więc $Q(Y)$ nie jest wielomianem zerowym. Weźmy dowolne $i \in I$. Z Lematu **??** wiemy, że i jest introspektywne modulo $X^r - 1, p$ dla dowolnego wielomianu z P, więc też dla dowolnego wielomianu w $\mathcal{G}$. Mamy więc w F

$$(f(X))^i = (g(X))^i \text{ i } f(X^i) = g(X^i).$$

Oznacza to, że dla każdego $i \in I$ X^i jest pierwiastkiem $Q(Y)$ w F, czyli też dla każdego $i' \in G$ $X^{i'}$ jest pierwiastkiem $Q(Y)$ w F. Załóżmy nie wprost, że istnieją $i < i' \in G$ takie, że $X^i = X^{i'}$ w F. Mamy więc $h(X) \mid X^i$ w $\mathbb{Z}_p[X]$ lub $X^{i-i'} = 1$. Pierwszy argument tej dysjunkcji jest w oczywisty sposób nieprawdziwy, ponieważ $h(X)$ nie ma pierwiastka w zerze, a drugi jest sprzeczny z Lematem **??**. Znaleźliśmy więc $|G| = t$ pierwiastków $Q(Y)$ w F więc $Q(Y)$ jest wielomianem zerowym w F lub $deg(Q) \geq t$, zatem doszliśmy do sprzeczności z założeniem.

Ad.2. Z założeń o ℓ i $o_r(n)$ mamy $\ell = \lfloor \sqrt{\phi(r)}\, log\, n \rfloor < \sqrt{r}\, log\, n$ oraz $o_r(n) > log^2 n$. Ponieważ $r > o_r(n)$, otrzymujemy

$$\ell < \sqrt{r}\, log\, n < \sqrt{r \cdot o_r(n)} < r < p.$$

W połączeniu z $deg(h) > 1$ mamy wniosek że dla dowolnych $0 \leq i < j \leq \ell$ $X + i \neq X + j$ w F oraz $X + i$ i $X + j$ są niezerowe.
Z Lematu **??** otrzymujemy wniosek, że w P, a co za tym idzie także w $\mathcal{G}$, jest co najmniej $\binom{t+\ell}{\ell+1} = \binom{t+\ell}{t-1}$ różnych wielomianów stopnia mniejszego niż t. Stąd $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$.

□

Następnym krokiem będzie znalezienie ograniczenia górnego dla rozmiaru zbioru $\mathcal{G}$. Wykorzystamy do tego wiedzę o introspektywności elementów zbioru I dla elementów zbioru $\mathcal{G}$.

Lemat 16. *Jeśli* $n \neq p^e$, $e \in \mathbb{N}$, *to* $|\,\mathcal{G}\,| \leq n^{\sqrt{t}}$.

Dowód. Weźmy

$$I' = \{(\frac{n}{p})^i \cdot p^j \,|\, 0 \leq i,\, j \leq \lfloor\sqrt{t}\rfloor\} \subset I.$$

Ponieważ n nie jest potęgą p,

$$i \neq i' \vee\ j \neq j' \Rightarrow (\frac{n}{p})^i \cdot p^j \neq (\frac{n}{p})^{i'} \cdot p^{j'}.$$

Mamy więc $|\,I'\,| = (\lfloor\sqrt{t}\rfloor + 1)^2 > t$. Ponieważ $|\,G\,| = t$, istnieją takie $i_1 < i_2 \in I'$, że $i_1 = i_2 \,(mod\, r)$. W połączeniu z $X^r = 1 \,(mod\, X^r - 1)$ otrzymujemy

$$X^{i_1} = X^{i_2} \,(mod\, X^r - 1),$$

a więc i

$$X^{i_1} = X^{i_2} \,(mod\, X^r - 1,\, p).$$

Weźmy dowolny wielomian $f(X) \in P$. Z Lematu **??** mamy

$$(f(X))^{i_1} = f(X^{i_1}) = f(X^{i_2}) = (f(X))^{i_2} \ (mod\, X^r - 1,\, p).$$

Oznacza to, że dowolny $f(X) \in \mathcal{G}$ jest pierwiastkiem wielomianu $Q(Y) = Y^{i_1} - Y^{i_2}$ w F. Skoro $\mathcal{G} \subset F$, to $Q(Y)$ ma co najmniej $|\,\mathcal{G}\,|$ różnych pierwiastków w F oraz

$$deg(Q) = i_2 \leq (\frac{n}{p} \cdot p)^{\lfloor\sqrt{t}\rfloor} \leq n^{\sqrt{t}}.$$

Otrzymujemy więc $|\,\mathcal{G}\,| \leq deg(Q) \leq n^{\sqrt{t}}$. □

Mając już ograniczenia z dwóch stron zbioru $\mathcal{G}$ możemy je ze sobą porównać, czym będziemy chcieli ostatecznie dojść do sprzeczności. W tym celu skorzystamy z dodatkowych dwóch ograniczeń dolnych mocy zbioru G, wprowadzonych w kolejnych lematach.

Lemat 17. *Jeśli* $a, r \in N$, $NWD(a,r) = 1$, *to istnieje* a^{-1} *takie, że* $aa^{-1} = 1 \,(mod\, r)$.

Dowód. Spójrzmy na ciąg $a, a^2, \ldots, a^{r+1}$. Istnieją w nim $1 \leq i < j \leq r+1$ takie, że $a^i = a^j \,(mod\, r)$, Ponieważ $NWD(a,r) = 1$, to także $NWD(a^i, r) = NWD(a^j, r) = 1$. Mamy $a^i a^{j-i} = a^i \,(mod\, r)$, a ponieważ a^i jest niezerowe, to $a^{j-i} = 1 \,(mod\, r)$ i ostatecznie $a \cdot a^{j-i-1} = 1 \,(mod\, r)$, więc znaleźliśmy a^{-1}. □

Lemat 18. $t = |\,G\,| \geq \phi(r)$.

Dowód. Weźmy zbiór A różnych a_i takich, że $a_i < r$ oraz $NWD(a_i, r) = 1$ dla $1 \leq i \leq k$. Z definicji funkcji Eulera mamy $|\,A\,| = \phi(r)$. Niech

$$B = \{b \,|\, b = p \cdot a_i \,(mod\, r),\, b < r,\, a_i \in A\}.$$

Zauważmy, że dla wszystkich $b \in B$ zachodzi $NWD(b, r) = 1$, więc $B \subseteq A$. Pokażemy, że $A = B$. Załóżmy nie wprost $p \cdot a_i = p \cdot a_j \,(mod\, r), 1 \leq i < j \leq \phi(r)$. Z Lematu **??** wiemy, że istnieje $p^{-1} \in \mathbb{Z}_p$. Więc mnożąc stronami przez p^{-1} otrzymujemy sprzeczność.
Mamy $A = B$, możemy więc wywnioskować równanie

$$p^{\phi(r)} \cdot a_1 \cdot \cdots \cdot a_{\phi(r)} = a_1 \cdot \cdots \cdot a_{\phi(r)} \,(mod\, r)$$
$$p^{\phi(r)} = 1 \,(mod\, r) \qquad \text{(Dla każdego } a_i \text{ istnieje } a_i^{-1}.)$$

Z twierdzenia Lagrange'a mamy wniosek, że $\phi(r)$ dzieli moc grupy, generowanej przez p modulo r, czyli zawartej w G, skąd wynika teza. □

Lemat 19. *$\langle G, \cdot \rangle$ jest podgrupą $\mathbb{Z}_r^*$ oraz $|\, G \,| > log^2 n$.*

Dowód. Dowód przebiegać będzie w dwóch krokach.

1. Udowodnimy, że $\langle G, \cdot \rangle$ spełnia definicję grupy i zawiera się w $\mathbb{Z}_r^*$.

   1.1. Oczywistym jest, że $G \subseteq \mathbb{Z}_r$. Wiemy, że $NWD(n,\, r) = 1$ oraz $p \,|\, n$, więc $NWD(p,\, r) = 1$. Wynika stąd, że nie istnieje w I element podzielny przez r, więc $0 \notin G$. Mamy więc $G \subseteq \mathbb{Z}_r^*$.

   1.2. $(\frac{n}{p})^0 \cdot p^0 = 1 \in G$, czyli istnieje element neutralny w G.

   1.3. Mnożenie spełnia własności działania w grupie, co wynika z własności mnożenia.

   1.4. Żeby pokazać zamkniętość na mnożenie, weźmy dowolne

   $$g_1 = (\frac{n}{p})^{i_1} \cdot p^{j_1} \,(mod\, r),\; g_2 = (\frac{n}{p})^{i_2} \cdot p^{j_2} \,(mod\, r) \in G,$$

   gdzie $i_1,\, i_2,\, j_1,\, j_2 \geq 0$. Wtedy

   $$g_1 g_2 = (\frac{n}{p})^{i_1 + i_2} \cdot p^{j_1 + j_2} \,(mod\, r)$$

   . Więc $g_1 g_2 \in G$.

   1.5. Weźmy dowolne $g \in G$. Wiemy, że istnieją $1 \leq i < j \leq |\, G \,| + 1$ takie, że $g^i = g^j$. Ponieważ $g \neq 0$ mamy $g^{j-i} = 1$, więc mamy $g^{j-i-1} \in G$, będące odwrotnością g.

2. Pokażemy, że $|\, G \,| > log^2 n$. Załóżmy nie wprost, że $|\, G \,| \leq log^2 n$. Spójrzmy na ciąg $1,\, n,\, \ldots\, , n^{|G|}$ modulo r. Jest to ciąg $|G| + 1$ liczb, należących do G. Wynika stąd, że istnieją $k, l \in \mathbb{N}, 0 \leq k < l \leq |\, G \,|$ takie, że $n^k = n^l \,(mod\, r)$. Mamy więc $n^{l-k} = 1 \,(mod\, r)$. $l - k \leq |\, G \,| \leq log^2 n$, co jest sprzeczne z założeniem, że $o_r(n) > log^2 n$.

□

Dodatkowo w rozwijaniu nierówności w ostatecznym ciągu przekształceń skorzystamy z następującego lematu.

Lemat 20. *Dla $n \in \mathbb{N}$, $n \geq 2$ zachodzi $\binom{2n+1}{n} \geq 2^{n+1}$.*

Dowód. Dowód przebiegał będzie przez indukcję. Przypadek dla $n = 2$ jest trywialny. Mamy $\binom{5}{2} = 10 > 2^3 = 8$.
Przyjmijmy założenie indukcyjne $\binom{2n+1}{n} > 2^{n+1}$. Pokażemy, że $\binom{2n+3}{n+1} > 2^{n+2}$. Mamy

$$\begin{aligned}\binom{2n+3}{n+1} &= \binom{2n+2}{n} + \binom{2n+2}{n+1} \\ &= \binom{2n+2}{n} + \binom{2n+1}{n+1} + \binom{2n+1}{n} \\ &= \binom{2n+2}{n} + 2\binom{2n+1}{n} \qquad (\text{Z założenia } \binom{2n+1}{n} > 2^{n+1}) \\ &> 2^{n+2},\end{aligned}$$

skąd teza. □

Mając już ograniczenie górne i dolne mocy $\mathcal{G}$ oraz dodatkowe pomocnicze nierówności, możemy udowodnić docelową implikację, że jeśli algorytm zróci *PIERWSZA* to n jest liczbą pierwszą.

Twierdzenie 15. *Niech $n \in \mathbb{N}$, $n \geq 2$ będzie liczbą podaną na wejściu algorytmu. Jeśli algorytm zwróci PIERWSZA, to n jest pierwsza.*

Dowód. Algorytm może zwrócić *PIERWSZA* tylko w kroku 4. i 7.

1. Jeśli algorytm zakończył wykonanie w kroku 4., to $r \geq n$, oraz

   $$\forall_{2 \leq a < r}\, NWD(a, n) = n \vee NWD(a, n) = 1.$$

   Oznacza to, że nie istnieje $2 \leq a < n$ będące właściwym dzielnikiem n, więc n jest pierwsze.

2. Załóżmy nie wprost, że algorytm zakończył wykonanie w kroku 7., zwracając *PIERWSZA* i n jest złożona. Ponieważ algorytm nie zakończył się w kroku 1., wiemy, że n nie jest potęgą żadnej liczby naturalnej, w szczególności nie istnieją takie $p < n, k \in \mathbb{N}$, gdzie p jest pierwsze, że $n = p^k$. W kroku 2. zostaje wybrane najmniejsze takie r, że $o_r(n) > log^2 n$. Ponadto z niespełnionego warunku w kroku 3. wiemy, że dla $1 \leq a \leq r$ zachodzi $NWD(a, n) = 1$, w szczególności $NWD(r, n) = 1$. Z kroków 4. i 5. mamy $n > r$ oraz $\forall_{1 \leq a \leq \lfloor \sqrt{\phi(r)}\, log\, n \rfloor} (X + a)^n = X^n + a\ (mod\, X^r - 1,\, n)$. Z założenia, że n jest liczbą złożoną wiemy, że istnieje p, będące pierwszym dzielnikiem n. Mamy więc $n, r, p \in \mathbb{N}$, spełniające założenia w Uwadze **??**. Weźmy zdefiniowany w niej zbiór $\mathcal{G}$. Na mocy Lematu **??** mamy nierówność $|\,\mathcal{G}\,| \geq \binom{t+\ell}{t-1}$ oraz

z Lematu **??** oraz Uwagi **??** zachodzi $t > log^2 n$, $\ell = \lfloor \sqrt{\phi(r)} log\, n \rfloor$. Możemy więc wywnioskować nierówność

$$
\begin{aligned}
|\,\mathcal{G}\,| &\geq \binom{t+\ell}{t-1} \\
&\geq \binom{\lfloor \sqrt{t}\, log\, n \rfloor + 1 + \ell}{\ell + 1} && \text{Z } t > log^2 n \text{ mamy } t \geq \lfloor \sqrt{t}\, log\, n \rfloor + 1. \\
&= \binom{\lfloor \sqrt{t}\, log\, n \rfloor + 1 + \ell}{\lfloor \sqrt{t}\, log\, n \rfloor} \\
&\geq \binom{2\lfloor \sqrt{t}\, log\, n \rfloor + 1}{\lfloor \sqrt{t}\, log\, n \rfloor} && \text{Z } \ell = \lfloor \sqrt{\phi(r)} log\, n \rfloor \text{ oraz Lematu ?? otrzymujemy } \ell \geq \lfloor \sqrt{t}\, log\, n \rfloor. \\
&> 2^{\lfloor \sqrt{t}\, log\, n \rfloor + 1} && \text{Z Lematu ??.} \\
&\geq 2^{\sqrt{t}\, log\, n} \\
&= n^{\sqrt{t}}.
\end{aligned}
$$

Mamy więc $|\,\mathcal{G}\,| > n^{\sqrt{t}}$ oraz, ponieważ n nie jest potęgą liczby pierwszej, z lematu **??** $|\,\mathcal{G}\,| \leq n^{\sqrt{t}}$. Otrzymaliśmy sprzeczność, więc n nie jest liczbą złożoną.

□

Twierdzenie 16. *Algorytm zwróci PIERWSZA wtw, gdy n jest liczbą pierwszą.*

Dowód. W Twierdzeniach **??** i **??** udowodniliśmy implikacje w dwie strony, skąd wynika teza. □

3.4. Złożoność obliczeniowa

Oszacowanie złożoności obliczeniowej algorytmu jest o wiele prostsze niż udowodnienie poprawności i wymagać będzie tylko odpowiedniego ograniczenia wartości r. Aby to osiągnąć pokażmy najpierw pomocniczy lemat o dolnym ograniczeniu namniejszej wspólnej wielokrotności n kolejnych liczb.

Lemat 21. *Niech $\ell_n = NWW(1, \ldots, n)$. Wtedy dla $n \geq 9$ zachodzi $\ell_n \geq 2^n$.*

Dowód. Pokażemy, że

1. dla dowolnego $m \leq n$, $m \in \mathbb{N}$ zachodzi $m \cdot \binom{n}{m} \,|\, \ell_n$, a następnie
2. wywnioskujemy tezę.

Ad.1. Weźmy dowolne $m \leq n$, $m \in \mathbb{N}$. Niech q będzie dowolną liczbą pierwszą taką, że $q \,|\, \ell_n$. Z własności ℓ_n i monotoniczności funkcji $log_q\, x$ możemy wywnioskować, że $q^{\lfloor log_q n \rfloor} \parallel \ell_n$. Niech $q^l \parallel m$. Zauważmy, że

$$q^{\sum_{i=1}^{i \leq \lfloor log_q n \rfloor} \lfloor \frac{n}{q^i} \rfloor} \parallel n!.$$

Analogicznie $q^{\sum_{i=1}^{i\leq\lfloor log_q m\rfloor}\lfloor\frac{m}{q^i}\rfloor} \parallel m!$ i $q^{\sum_{i=1}^{i\leq\lfloor log_q (n-m)\rfloor}\lfloor\frac{n-m}{q^i}\rfloor} \parallel (n-m)!$. Ponieważ $m,\, n-m \leq n$ zachodzi $q^{\sum_{i=1}^{i\leq\lfloor log_q n\rfloor}\lfloor\frac{m}{q^i}\rfloor} \parallel m!$ i $q^{\sum_{i=1}^{i\leq\lfloor log_q n\rfloor}\lfloor\frac{n-m}{q^i}\rfloor} \parallel (n-m)!$. Otrzymujemy

$$q^{\sum_{i=1}^{i\leq\lfloor log_q n\rfloor}\lfloor\frac{n}{q^i}\rfloor-(\lfloor\frac{m}{q^i}\rfloor+\lfloor\frac{n-m}{q^i}\rfloor)} \parallel \binom{n}{m}.$$

Zauważmy, że jeśli $q^i \,|\, m$, to $\lfloor\frac{n}{q^i}\rfloor - (\lfloor\frac{m}{q^i}\rfloor + \lfloor\frac{n-m}{q^i}\rfloor) = 0$, a w przeciwnym wypadku $\lfloor\frac{n}{q^i}\rfloor - (\lfloor\frac{m}{q^i}\rfloor + \lfloor\frac{n-m}{q^i}\rfloor) \leq 1$. Stąd mamy

$$\sum_{i=1}^{i\leq\lfloor log_q n\rfloor} \lfloor\frac{n}{q^i}\rfloor - (\lfloor\frac{m}{q^i}\rfloor + \lfloor\frac{n-m}{q^i}\rfloor) \leq \lfloor log_q n\rfloor - l,$$

a ponieważ $q^l \parallel m$, otrzymujemy wniosek, że jeśli $q^i \,|\, m \cdot \binom{n}{m}$, to $i \leq \lfloor log_q n\rfloor$. Ponieważ nierówność ta zachodzi dla każdego pierwszego dzielnika, możemy wywnioskować, że $m \cdot \binom{n}{m} \,|\, \ell_n$.

Ad.2. W szczególności mamy

$$n \cdot \binom{2n}{n} \,|\, \ell_{2n}$$

oraz

$$(n+1)\binom{2n+1}{n+1} = (2n+1)\binom{2n}{n} \,|\, \ell_{2n+1}.$$

Wiemy, że $NWD(n,\, 2n+1) = 1$ oraz $\ell_{2n} \,|\, \ell_{2n+1}$, więc

$$n(2n+1)\binom{2n}{n} \,|\, \ell_{2n+1}.$$

Możemy stąd przejść do nierówności

$$\ell_{2n+1} \geq n(2n+1)\binom{2n}{n} \geq n\sum_{i=0}^{i\leq 2n}\binom{2n}{n} \geq n\sum_{i=0}^{i\leq 2n}\binom{2n}{i} = n(1+1)^{2n} = n\,4^n.$$

Mamy więc dla $n \geq 4$ nierówność $\ell_{2n+2} \geq \ell_{2n+1} \geq 2^{2n+2}$, skąd bezpośrednio możemy wywnioskować $\ell_n \geq 2^n$ dla $n \geq 9$.

□

Lemat 22. *Niech $n \in \mathbb{N}$, $n \geq 2$, wtedy istnieje takie $r \leq \max\{3, \lceil \log^5 n\rceil\}$, $r \in \mathbb{N}$, że $o_r(n) > log^2 n$.*

Dowód. Przypadek, gdy $n = 2$ jest trywialny, ponieważ teza zachodzi dla $r = 3$. Podobnie dla $n = 3$, warunki spełnia $r = 4$.
Załóżmy więc, że $n \geq 4$. Niech $B = \lceil log^5 n\rceil$. Wtedy $B > 10$.
Spójrzmy na najmniejsze takie r, że

$$r \nmid n^{\lfloor logB\rfloor}\prod_{i=1}^{i\leq\lfloor log^2 n\rfloor}(n^i - 1).$$

Niech $P = n^{\lfloor logB \rfloor} \prod_{i=1}^{i \leq \lfloor log^2 n \rfloor} (n^i - 1)$. Istnieje więc pewne q takie, że $q \mid r$ i $q \nmid P$. $\lfloor logB \rfloor \geq 1$, więc możemy wywnioskować, że $q \nmid n$. Wynika stąd, że $q \nmid NWD(r, n)$, więc $\frac{r}{NWD(r,n)} \nmid P$. Znaleźliśmy więc liczbę $\frac{r}{NWD(r,n)} \leq r$, która nie dzieli P. Z założenia, że r jest najmniejsze takie, że $r \nmid P$ mamy $NWD(r, n) = 1$.
Dodatkowo wiemy, że $\forall_{1 \leq i \leq \lfloor log^2 n \rfloor} r \nmid (n^i - 1)$, więc nie istnieje takie $1 \leq i \leq \lfloor log^2 n \rfloor$, że $n^i = 1 \,(mod\, r)$. Oznacza to, że $o_r(n) > log^2 n$. Możemy też ograniczyć P z góry:

$$n^{\lfloor logB \rfloor} \prod_{i=1}^{i \leq \lfloor log^2 n \rfloor} (n^i - 1) < n^{\lfloor logB \rfloor} \prod_{i=1}^{i \leq \lfloor log^2 n \rfloor} n^i < n^{\lfloor logB \rfloor} n^{\frac{log^2 n (log^2 n + 1)}{2}} \leq n^{\lfloor logB \rfloor + \frac{log^4 n + log^2 n}{2}}.$$

Dla $n \geq 4$ mamy

$$n^{\lfloor logB \rfloor + \frac{log^4 n + log^2 n}{2}} \leq n^{log^4 n} \leq 2^{log^5 n} \leq 2^B.$$

Wiemy, że $B > 10$, więc z Lematu **??** mamy $\ell_B \geq 2^B > P$. Oznacza to, że istnieje $l \in \{1, \ldots, B\}$ takie, że $l \nmid P$. Z założenia o r mamy, że $r \leq l \leq B$. □

Ograniczenie r pozwala nam już bezpośrednio ograniczyć złożoność obliczeniową algorytmu.

Twierdzenie 17. *Złożoność obliczeniową algorytmu można ograniczyć asymptotycznie poprzez* $O(log^{\frac{21}{2}} n \cdot log\, log\, n)$.

Dowód. Przeanalizujmy kolejne kroki algorytmu pod kątem złożoności obliczeniowej.

(krok 1.) W kroku 1. algorytm sprawdzi dla wszystkich możliwych wartości b, których jest nie więcej niż $log\, n$, czy dla pewnego a zachodzi $a^b = n$. Do znalezienia możliwego wykładnika a użyć można wyszukiwania binarnego dla wartości od 2 do n. Sprawdzenie możliwego a wykonane w wyszukiwaniu binarnym będzie wymagało $log\, b$ operacji na liczbach długości nie większej niż $log\, n$. Mamy więc ograniczenie złożoności kroku pierwszego

$$O(log\, n \cdot (log\, n \cdot (log\, b \cdot log\, n))) = O(log^n \cdot log\, log\, n).$$

(krok 2.) Z Lematu **??** wiemy, że istnieje $r \leq max\{3, \lceil log^5 n \rceil\}$. Dla potencjalnych $O(log^5 n)$ wartości r, algorytm sprawdzi $O(log^2 n)$ kolejnych potęg n i przyrówna je do 1 modulo r. Dla kroku 2. otrzymujemy więc ograniczenie złożoności

$$O(log^5 n \cdot (log^2 n \cdot log\, r)) = O(log^7 n \cdot log\, log\, n).$$

(krok 3.) Dla możliwych $O(r)$ wartości a wystarczy obliczyć $NWD(a, n)$. Algorytm Euklidesa pozwala znaleźć $NWD(a, n)$ w czasie $O(log\, n + log^2 r)$, gdzie pierwszy składnik sumy odpowiada pierwszej operacji policzenia a modulo n, po czym algorytm będzie wykonywał się na liczbach nie większych niż r. Mamy więc złożoność kroku 3. ograniczoną przez

$$O(r \cdot (log\, n + log^2 r)) = O(log^2 n + log\, n \cdot log^2 log\, n)).$$

(krok 4.) W kroku 4. zostaje wykonane tylko jedno porównanie na liczbach długości nie większej niż n, więc ogólnym ograniczeniem złożoności kroku jest $O(log\, n)$.

(krok 6.) Dla danego a algorytm obliczy wartość $(X+a)^n - X^n + a$ modulo $X^r - 1$, p. Obliczenie $(X+a)^n$ modulo X^r-1, p wykonane być może za pomocą wykorzystania szybkiej transformaty Fouriera w czasie $O(r \cdot log\, n \cdot log\, n)$, gdzie ostatni czynnik $log\, n$ odpowiada za złożoność wykonania operacji na współczynnikach długości $log\, n$. Mamy więc ograniczenie kroku 6. jako $O(log^7 n)$.

(krok 5.) W kroku 5. wykonany zostanie krok 6. $\lfloor \sqrt{\phi(n)}\, log\, n \rfloor$. Mamy więc złożoność obliczeniową kroku 5.

$$O(\sqrt{\phi(r)}\, log\, n \cdot log^7 n) \subseteq O(\sqrt{r}\, log\, n \cdot log^7 n) \subseteq O(log^{\frac{5}{2}} n \cdot log^8 n) \subseteq O(log^{\frac{21}{2}} n).$$

Suma złożoności wszystkich kroków jest zdominowana przez złożoność kroku 5., więc złożoność całego algorytmu można ograniczyć przez $O(log^{\frac{21}{2}} n)$. □

Rozdział 4.

Implementacja

Algorytm AKS zaimplementowałam w języku C++ (standard C++11) z użyciem biblioteki NTL w wersji 11.3.2. Wykorzystałam zaimplementowane w niej operacje na długich liczbach oraz efektywne mnożenie wielomianów.

4.1. Kompilacja i sposób użycia

Aby skompilować program `aks.cpp` należy najpierw zainstalować bibliotekę NTL dostępną do ściągnięcia wraz z instrukcją na stronie `https://www.shoup.net/ntl/` w odpowiednim folderze. Następnie wystarczy skompilować program poleceniem:

```
$ g++ -g -O2 -std=c++11 -pthread -march=native aks.cpp \
 -o aks -lntl -lgmp -lm
```

Kompilacja zakończy się stworzeniem pliku wykonywalnego `aks`. Po jego uruchomieniu należy na standardowym wejściu podać liczbę naturalną, a program wypisze na standardowe wyjście napis *PIERWSZA* lub *ZŁOŻONA*.

4.2. Testowanie

Testy poprawnościowe znajdują się w pliku `corr.in`, a poprawne wyniki w pliku `corr.out`. Do skorzystania z nich można użyć skryptu w pliku `test.sh`, który kompiluje program, a następnie uruchamia go podając na wejściu liczby z kolejnych linii pliku `corr.in`. Po wykonaniu programu dla wszystkich testów z pliku, program zwróci wynik skryptu `diff`, który porównuje otrzymane wyniki z oczekiwanymi.