Implementation of primality test in polynomial time

(Implementation of primality test in polynomial time)(Implementacja algorytmu, sprawdzającego pierwszość liczby w czasie wielomianowym)

Martyna Siejba

Praca licencjacka

Promotor: prof. Krzysztof Loryś

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Informatyki

19 stycznia 2019

Streszczenie

...

.....

Spis treści

Rozdział 1.

Wstęp

1.1. Przesłanki

1.2. Uwagi odnośnie notacji

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 $\oplus$ oraz $\odot$ nazywamy ***pierścieniem***, 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 ($\exists_{0\in R} \forall_{a\in R}\, a \oplus 0 = 0 \oplus a = 0$);
- dla każdego elementu zawiera element odwrotny ($\forall_{a\in R} \exists_{(-a)\in R}\, a \oplus (-a) = 0$);
- $\odot$ 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 mnożeniem i dodawaniem lub zbiór wielomianów o współczynnikach całkowitych z dodawaniem i mnożeniem wielomianów.

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

- istnieje element neutralny mnożenia ($\exists_{1 \in F} \forall_{a \in F}\, a1 = 1a = a$) oraz
- $\langle F \setminus \{0\}, \odot, 1 \rangle$ jest grupą abelową.

Innymi słowy jest to pierścień 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. ***Charakterystyką*** ciała F będziemy nazywać najmniejszą taką liczbę naturalną $char(F) = n$, że suma n jedynek równa się zeru w F.

Definicja 5. 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
- $\forall_{i \in I, r \in R}\, ir \in I \wedge ri \in I$.

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.

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 pokazać, 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) $\forall_{i \in I, r \in R}\, i \odot r \in I \wedge r \odot i \in I$.

(1) Aby udowodnić, że $\langle I, \oplus \rangle$ jest podgrupą $\langle R, \oplus \rangle$ wystarczy pokazać, że (1.1) istnieje element neutralny $e \in I$, (1.2) I jest zamknięte na $\oplus$ oraz (1.3) dla każdego elementu istnieje w I element odwrotny.

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

(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 $\oplus$.

(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 odwrotnym i.

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

□

Definicja 6. Ideał M w pierścieniu R nazywamy ***ideałem maksymalnym***, jeśli dla każdego ideału I nad R zachodzi $M \subseteq I \Rightarrow I = R$.

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

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

Lemat 1. *Ideał I pierścienia $\langle R, \oplus, \odot \rangle$ 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 $\langle G, \circ \rangle$ jest grupą, a $\langle N, \circ \rangle$ jej podgrupą normalną, to zbiór warstw grupy G względem N z działaniem $\otimes$ zdefiniowanym jako $(aN)(bN) = abN$ tworzy grupę G/N nazywaną **grupą ilorazową**.*

Dowód. Należy udowodnić, 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.

(1) Weźmy $aN = bN \in G/N$ oraz $cN = dN \in G/N$. Chcemy pokazać, że $(aN)(cN) = (bN)(dN)$. Wiemy, że, skoro $\langle N, \circ \rangle$ jest grupą, istnieje element neutralny $e \in N$. Stąd wiemy, że $a = ae \in aN$ oraz $b = be \in bN$. 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 $cn_2 = d$.

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

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

(2) Aby pokazać, że G/N jest grupą należy pokazać (2.1) zamkniętość na $\otimes$, (2.2) łączność $\otimes$, (2.3) istnienie elementu neutralnego oraz (2.4) istnienie elementów odwrotnych.

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

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

$$aN((bN)(cN)) = aN(bcN) = a(bc)N = (ab)cN \tag{2.1}$$
$$= (ab)Nc = (abN)cN = ((aN)(bN))cN. \tag{2.2}$$

(2.3) Istnieje w G/N element neutralny. Weźmy eN, gdzie e jest elementem neutralnym w G. Dla dowolnego $aN \in G/N$ mamy $(aN)(eN) = aeN = aN$.

(2.4) Dla każdego elementu istnieje element odwrotny. Weźmy dowolne $aN \in G/N$. Niech $-a$ będzie elementem odwrotnym a. Wiemy, że $-a \in G$. Mamy

$$(aN)(-aN) = a(-a)N = eN,$$

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 $\langle R, \oplus, \odot \rangle$. Jeśli zdefiniujemy operacje $+$ i $\times$ jako:*

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

to $\langle R/I, +, \times\rangle$ *jest pierścieniem przemiennym, nazywanym* ***pierścieniem ilorazowym****.*

Dowód. (1) $\langle I, \oplus\rangle$ jest podgrupą normalną $\langle R, \oplus\rangle$, więc z twierdzenia **??** $\langle R/I, +\rangle$ z jest grupą ilorazową.

Należy więc pokazać, że (2) $\times$ 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 (3) $\langle R/I, +, \times\rangle$ jest pierścieniem przemiennym.

(2) 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 $b \odot d \oplus b \odot i_2 \oplus i_2 \odot d \oplus i_1 \odot i_2 \oplus I = b \odot d \oplus I = (b \oplus I) \times (d \oplus I)$.

(3) Pokażemy, że $\langle R/I, +, \times\rangle$ spełnia warunki z definicji pierścienia przemiennego.

(3.1) $+$ jest przemienna. Weźmy dowolne $a \oplus I, b \oplus I \in R/I$. Z przemienności $\oplus$ w pierścieniu $\langle R, \oplus, \odot\rangle$ mamy $(a \oplus I) + (b \oplus I) = a \oplus b \oplus I = b \oplus a \oplus I = (a \oplus I) + (b \oplus I)$.

(3.2) $+$ 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 $((a \oplus I) + (b \oplus I)) + (c \oplus I) = (a \oplus b \oplus I) + (c \oplus I) = (a \oplus b) \oplus c \oplus I = a \oplus (b \oplus c) \oplus I = (a \oplus I) + (b \oplus c \oplus I) = (a \oplus I) + ((b \oplus I) + (c \oplus I))$.

(3.3) Istnieje element zerowy. Niech $e = e' \oplus I$, gdzie e' jest elementem zerowym pierścienia $\langle R, \oplus\rangle$. Weźmy dowolne $a \oplus I \in R/I$. Wtedy $(a \oplus I) + e = a \oplus e' \oplus I = e' \oplus I = e = e' \oplus a \oplus I = e + (a \oplus I)$.

(3.4) Dla każdego elementu istnieje element odwrotny. Weźmy dowolne $a \oplus I \in R/I$. Istnieje $-a \in R$, będące elementem odwrotnym a. $(a \oplus I) + (-a \oplus I) = a \oplus -a \oplus I = e' \oplus I = e = -a \oplus a \oplus I = (-a \oplus I) + (a \oplus I)$.

(3.5) $\times$ 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 $((a \oplus I) \times (b \oplus I)) \times (c \oplus I) = (a \odot b \oplus I) \times (c \oplus I) = (a \odot b) \odot c \oplus I = a \odot (b \odot c) \oplus I = (a \oplus I) \times (b \odot c \oplus I) = (a \oplus I) \times ((b \oplus I) \times (c \oplus I))$.

(3.6) $+$ 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 $((a\oplus I)+(b\oplus I))\times(c\oplus I) = (a\oplus b)\odot c\oplus I = a\odot c\oplus b\odot c\oplus I = ((a\oplus I)\times(c\oplus I))+((b\oplus I)\times(c\oplus I))$.

(3.7) $\times$ jest przemienna. Weźmy dowolne $a\oplus I, b\oplus I\in R/I$. Z przemienności $\odot$ w pierścieniu $\langle R,\oplus,\odot\rangle$ mamy $(a\oplus I)\times(b\oplus I) = a\odot b\oplus I = b\odot a\oplus I = (b\oplus I)\times(a\oplus I)$.

□

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 1, a I ideałem maksymalnym nad R, to R/I z działaniami zdefiniowanymi jak w powyższych twierdzeniach jest ciałem.*

Dowód. Wiemy, że R/M jest pierścieniem przemiennym. Wystarczy pokazać, że (1) istnieje element neutralny mnożenia oraz (2) dla każdego niezerowego elementu istnieje element odwrotny.
(1) Istnieje 1 w R, więc dla dowolnego $a\oplus M\in R/M$ mamy $(a\oplus M)\times(1\oplus M) = a\odot 1\oplus M = a\oplus M = 1\odot a\oplus M = (1\oplus M)\times(a\oplus M)$.
(2) Weźmy dowolne $a\in R$ takie, że $a\oplus M$ jest niezerowe, czyli $a\notin M$. Weźmy zbiór $J = \{ra\oplus m \mid r\in R, m\in M\}$. Pokażemy, że J jest ideałem nad R. W tym celu wystarczt pokazać, że (2.1) $\langle J,\oplus\rangle$ jest podgrupą $\langle R,\oplus\rangle$ oraz (2.2)$\forall_{j\in J, r\in R}\, jr\in J\wedge rj\in J$.
(2.1.1) $J\subseteq R$. Wiemy, że R jest zamknięty na $\oplus$ i $\odot$, więc $\forall_{r,a',m\in R}\, ra'\oplus m\in R$.
(2.1.2) J zawiera element zerowy. M jest ideałem, czyli jest grupą, więc $0\in M$. Stąd $0a\oplus 0 = 0\in J$.
(2.1.3) Dla każdego elementu J istnieje element odwrotny. 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 $j\oplus -j = ra\oplus m\oplus -ra\oplus -m = ra\oplus -ra = 0a = 0$.
(2.1.4) J jest zamknięte na $\oplus$. Wexmy 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 $j_1\oplus j_2\in J$.
(2.1.5) $\oplus$ jest łączne. Własność wynika ta bezpośrednio z łączności $\oplus$ w R.
(2.2) Weźmy dowolne $ra\oplus m\in J, r'\in R$. Wtedy $jr' = (ra\oplus m)\odot r' = rar'\oplus mr'$. Z przemienności R $jr' = rr'a\oplus mr'$. $rr'\in R$ oraz, ponieważ M jest ideałem $mr'\in M$, więc $jr'\in J$. Analogicznie $r'j\in J$.
Wiemy, że J jest ideałem nad R. Możemy też pokazać, że $M\subset J$. $\forall_{m\in M}\, m = 0a\oplus m\in J$ oraz skoro $1\in R, 0\in M$, 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. *$\langle \mathbb{Z}_p, +_p, \times_p \rangle$, gdzie $p \in \mathbb{N}$ i $p \geq 2$, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ oraz operacje są odpowiadającymi działaniami arytmetycznymi modulo p, jest ciałem, jeśli p jest pierwsze.*

Dowód. (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) $\langle \mathbb{Z}_p \setminus \{0\}, \times_p \rangle$ 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 i $p - 2$ możliwych wyników. Z zasady szufladkowej mamy $\exists b_1, b_2 \in \mathbb{Z}_p \setminus \{0\}, b_1 \neq b_2\, a \times_p b_1 = a \times_p b_2$. Wiemy, że istnieje w $\mathbb{Z}_p$ niezerowy element $-b_2$, więc $-b_2 \in \mathbb{Z}_p \setminus \{0\}$. Korzystając z własności pierścienia $\langle \mathbb{Z}_p, +_p, \times_p \rangle$ możemy przekształcić powyższe równanie do $a \times_p (b_1 +_p -b_2) = 0$. Z $b_1 \neq b_2$ mamy $b_1 +_p -b_2 \in \mathbb{Z}_p \setminus \{0\}$, czyli doszliśmy do sprzeczności. □

Twierdzenie 6. *Jeśli $\langle R, \oplus, \odot \rangle$ jest pieścieniem przemiennym z 1, to $\langle R[X], \oplus^*, \odot^* \rangle$, gdzie $R[X]$ jest zbiorem wielomianów o współczynnikach w R, a $\oplus^*$ i $\odot^*$ są naturalnie zdefiniowanym dodawaniem i mnożeniem wielomianów z użyciem $\oplus$ i $\odot$ w operacjach na współczynnikach, jest pierścieniem przemiennym z 1.*

Uwaga. Dowód twierdzenia przebiega poprzez pokazanie kolejnych własności pierścienia. Elementem zerowym jest wielomian zerowy, a elementem neutralnym mnożenia jest 1.

Przyjrzyjmy się bliżej pierścieniowi wielomianów, którego współczynniki są elementami ciała. Na podstawie poniższych lematów o ideałach w tym pierścieniu oraz twierdzeń z powyższej sekcji, będziemy mogli określić strukturę pewnych pierścieni ilorazowych, które pojawią się później w dowodzie poprawności 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 jest niezerowe i weźmy $p(x) \in I$ takie, że $p(x) \neq 0$ oraz $p(x)$ jest wielomianem najmniejszego stopnia w I. Weźmy dowolny wielomian $f(x) \in I$. Wiemy, że $\exists_{q(x),r(x)\in I}\, f(x) = q(x)p(x) \oplus r(x) \wedge deg(r(x)) < deg(p(x))$. 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* $\langle F, \oplus, \odot, 0, 1\rangle$*, to* $\langle g(x)\rangle$ *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 $g(x) = f(x)h(x)$. $g(x)$ 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 pierwsze i* $h(x)$ *jest nierozkładalnym w* $\mathbb{Z}_p[X]$ *wielomianem stopnia* d *to pierścień ilorazowy* $\langle \mathbb{Z}_p[X]/\langle h(x)\rangle, \oplus, \odot\rangle$ *jest ciałem rzędu* p^d*.*

Dowód. (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 $\mathbb{Z}_p[X]/\langle h(x)\rangle$ jest ciałem.
(2) Niech $M = \langle h(x)\rangle$ Pokażemy, że jeśli wielomiany $f(x) = h(x)q_1(x) +^* r_1(x), g(x) = h(x)q_2(x) +^* r_2(x) \in \mathbb{Z}_p[X]$, gdzie $r_1(x) = r_2(x)$, to $f(x) +^* M = g(x) +^* M$. Mamy $f(x) +^* M = h(x)q_1(x) +^* r_1(x) +^* M = r_1(x) +^* h(x)q_1(x) +^* M = r_1(x) +^* M = r_2(x) +^* M = r_2(x) +^* h(x)q_2(x) + M = g(x) + M$. 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 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 kolejne pojęcia związane z ciałami.

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

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

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 zdefiniujemy pierwiastki z jedności z użyciem ciała rozkładu pewnego wielomianu nad ciałem, wprowadźmy twierdzenie Kroneckera, które pozwoli w późniejszych twierdzeniach udowodnić istnienie ciała rozkładu i pierwiastków z jedności.

Lemat 3. *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 wiemy, że $F[X]/\langle h(X)\rangle$ jest ciałem. Zauważmy, że F jest izomorficzny z $\{a + \langle h(X)\rangle \mid a \in F\} \subseteq F[X]/\langle h(X)\rangle$. Więc $F[X]/\langle h(X)\rangle$ jest rozszerzeniem F. Ponieważ $deg(f) \geq 2$, $\alpha = X + \langle h(X)\rangle \in F[X]/\langle h(X)\rangle$. Wtedy $h(\alpha) = a_0 + a_1(X + \langle h(X)\rangle) + \cdots + a_n(X + \langle h(X)\rangle)^n = h(X) + \langle h(X)\rangle = 0$ 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 **??** wiemy, że istnieje ciało G będące rozszerzeniem F takie, że istnieje $\alpha \in G$, $f(\alpha) = 0$. Mamy więc w $G[X]$ $f(X) = (X - \alpha)g(X)$. 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, a $n \geq 1, n \in \mathbb{N}$. Ciało rozkładu $F^{(n)}$ dla $X^n - 1$ nad F będziemy nazywać ***n-tym ciałem cyklotomicznym***, 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, a $f(X) \in F[X]$. 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. □

Lemat 4. *Jeśli ciało G jest rozszerzeniem ciała F, to $char(G) = char(F)$.*

Dowód. Ponieważ F i G są ciałami dla tych samych operacji $0_F = 0_G$ i $1_F = 1_G$, z definicji charakterystyki mamy $char(F) = char(G)$. □

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

Twierdzenie 11. *Dla każdego ciała $F, p = char(F)$ 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. (1) Pokażemy, że $|\, E^{(n)} \,| = n$. Przypadek dla $n = 1$ jest trywialny, ponieważ zbiór $E^(n)$ jest wtedy zbiorem zawierającym tylko 1. Załóżmy więc, że $n \geq 2$. Z **??** 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 **??** mamy $char(K^{(n)}) = p$, więc istnieje n^{-1} w $K^{(n)}$. 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 $|\, E^{(n)} \,| = n$.
(2) $E^{(n)}$ jest grupą operacją mnożenia w $K^{(n)}$. Weźmy dowolne $\zeta_1, \zeta_2 \in E^{(n)}$. Niech $\zeta = \zeta_1\zeta_2$. Wtedy $\zeta^n = (\zeta_1\zeta_2) = \zeta_1^n\zeta_2^n = 1$, czyli $\zeta_1\zeta_2 \in E^{(n)}$. Dla dowolnego $\zeta \in E^{(n)}$ istnieje element odwortny $\zeta^{n-1} \in E^{(n)}$. Element neutralny stanowi $1_{K^{(n)}}$.
(3) $E^{(n)}$ jest cykliczna.
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 $i, j < n, i, j \in \mathbb{N}\, \zeta^i \neq \zeta^j$.
Niech $n = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ będzie rozkładem n na czynniki pierwsze. Dla każdego $1 \geq i \geq r$ istnieje nie więcej niż $\frac{n}{p_i}$ pierwiastków wielomianu $x^{\frac{r}{p_i}} - 1$. n jest złożona, więc $\frac{n}{p_1} < n$ i istnieje ζ_i nie będąca pierwiastkiem $x^{\frac{r}{p_i}} - 1$. 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 $k < r_i$ $\alpha_i^{p_i^k} = 1$, to także $(\alpha_i^{p_i^k})^p = \alpha_i^{p_i^{k+1}} = 1$ i poprzez indukcję względem k $\alpha_i^{p_i^{e_i-1}} = 1$. 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 $\alpha = \alpha_1 \cdot \dots \cdot \alpha_r$. Pokażemy, że $o_n(\alpha) = n$. Wiemy, że $o_n(\alpha) \,|\, n$. Załóżmy nie wprost, że $o_n(\alpha) \neq n$. Wynika stąd, że istnieje takie p_i, że $o_n(\alpha) \,|\, \frac{n}{p_i}$. Wtedy

$\alpha^{\frac{n}{p_i}} = 1 = \alpha_1^{\frac{n}{p_i}} \cdot \dots \cdot \alpha_r^{\frac{n}{p_r}}$. Dla każdego $j \neq i, 1 \leq j \leq r$ $p_j^{e_j} \mid \frac{n}{p_i}$, a ponieważ $o_n(\alpha_j) = p_i^{e_j}$, mamy $\alpha_j^{\frac{n}{p_i}} = 1$. Mamy więc $\alpha_i^{\frac{n}{p_i}} = 1$, 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 pierwszego n 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 2. Dla każdego ciała F i $n \in \mathbb{N}$, $n \nmid char(F)$ istnieje co najmniej jeden pierwotny pierwiastek z jedności n-tego stopnia nad F.

Lemat 5. *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 $NWD(s, n) = 1$. Niech $k = o_n(\zeta^s)$. Mamy więc $k \mid n$. Ponieważ $\zeta^n = 1$ mamy $(\zeta^s)^k = \zeta^n$. $(\zeta^s)^k \in E^{(n)}$, więc, jako że $E^{(n)}$ jest grupą, $(\zeta^s)^- k \in E^{(n)}$. Otrzymujemy $\zeta^s = \zeta^{fracnk}$. Z $NWD(s, n) = 1$ mamy $n = k$ i ostatecznie $o_n(\zeta^s) = n$, czyli ζ^s jest generatorem grupy. □

Definicja 12. Niech F będzie ciałem, $n \in \mathbb{N}$, $n \nmid char(F)$ 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 6. *Jeśli $Q_n(X)$ jest wielomianem cyklotomicznym n-tego stopnia 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 $X^n - 1$. □

Obserwacja 3. $Q_n(X)$ 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. *Jeśli G jest rozszerzeniem ciała F oraz istnieje, to dla każdego $g \in G$, jeśli istnieje niezerowy $f(X) \in F[X]$, $f(g) = 0$, to istnieje niezerowy wielomian minimalny w $F[X]$.*

Dowód. Niech $I = f \,|\, f \in F, f(g) = 0$. Zauważmy, że I jest ideałem nad $F[X]$. Co więcej ponieważ F jest ciałem, to 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 nie jest ideałem zerowym, $m(X)$ nie jest wielomianem zerowym. Jeśli $m(X)$ jest moniczny, to jest wielomianem minimalnym, w przeciwnym przypadku współczynnik a przy najwyższej potędze X nie jest jedynką. Ponieważ każdy element niezerowy ma odwrotność w F, to istnieje też moniczny wielomian będący wielomianem minimalnym. □

Lemat 7. *Jeśli G jest rozszerzeniem ciała F oraz $m(X) \in F[X]$ wielomianem minimalnym dla $g \in G$, to dla każdego $f(X) \in F[X]$ $f(g) = 0 \Rightarrow m(X) \,|\, f(X)$.*

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

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

Dowód. Niech ζ będzie pierwotnym pierwiastkiem n-tego stopnia nad $\mathbb{F}_q$. Dowód przebiegał będzie w dwóch krokach: (1) pokażemy, że dla dowolnego $k > 1$ $\zeta^{q^k} = \zeta$ wtw, gdy $\zeta \in \mathbb{F}_{q^k}$ oraz, że (2) jeśli $\zeta \in \mathbb{F}_{q^d}$ jest pierwiastkiem wielomianu $f(X) \in \mathbb{F}_q$, to istnieje $h(X) \in \mathbb{F}_q$ takie, że $h(X) \,|\, f(X)$ oraz $deg(h(X)) = d$.
(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 niewięcej niż q^k pierwiastków, a skoro wszystkie elementy $\mathbb{F}_{q^k}$ są jego pierwiastkami, to wszystkie pierwiastki są elementami $\mathbb{F}_{q^k}$.
Możemy zauważyć, że powyższą równoważność można zaaplikować do ζ otrzumując $\zeta \in \mathbb{F}_{q^k}$ wtw, gdy $\zeta^{q^k} = \zeta$ a więc i $q^k = 1 \,(mod\, n)$.
Weźmy $d = o_n(q)$. Wtedy $\mathbb{F}_{q^d}$ będzie najmniejszym ciałem, zawierającym wszystkie pierwiastki n-tego stopnia nad $\mathbb{F}_{||}$.
(2) Niech $m(X) \in \mathbb{F}_q$ będzie minimalnym wielomianem dla ζ. Wiemy, że taki istnieje i jest niezerowy, ponieważ istnieje $f(X) = X^n - 1 \in \mathbb{F}_q[X]$ i $f(\zeta) = 0$. Ponieważ $\mathbb{F}_q/\langle m(X) \rangle$ jest izomorficzne z $\mathbb{F}_{p^d}$, to $deg(m) = d$. Z własności wielomianu minimalnego mamy $m(X) | Q_n(X)$ oraz $m(X)$ jest nierozkładalny w $\mathbb{F}_q$.
Ponieważ $m(X)$ dzieli dowolny wielomian, którego pierwiastkiem jest ζ oraz wszystkie pierwiastki $Q_n(X)$ są pierwiastkami pierwotnymi z jedynki n-tego stopnia, możemy wywnioskować, że $Q_n(X)$ można rozłożyć na nierozkładalne wielomiany stopnia $o_n(q)$ w $\mathbb{F}_q$. □

Rozdział 3.

Algorytm

3.1. Schemat algorytmu

noend 1 Algorytm ASK

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: $r \leftarrow$ najmniejsze takie q, że $o_q(n) > log^2 n$ ▷ Krok 2.
4: **if** istnieje $a \leq r$ takie, że $1 < NWD(a, n) < n$ **then** ▷ Krok 3.
5: **return** ZŁOŻONA
6: **if** $n \leq r$ **then** ▷ Krok 4.
7: **return** PIERWSZA
8: **for** $a \leftarrow 1$ **to** $\lfloor \sqrt{\phi(r)}\, log\, n \rfloor$ **do** ▷ Krok 5.
9: **if** $(X + a)^n \neq X^n + a\, (mod\, X^r - 1,\, n)$ **then** ▷ Krok 6.
10: **return** ZŁOŻONA
11: **return** PIERWSZA ▷ Krok 7.

3.2. Dowód poprawności

Dowód poprawności algorytmu przeprowadzimy poprzez udowodnienie serii lematów i ostatecznie wykorzystanie ich do udowodnienia twierdzenia, że algorytm zwróci *PIERWSZA* wtw, gdy liczba n na wejściu jest pierwsza. Lematy prowadzące do końcowego twierdzenia będą często udowodnione z użyciem twierdzeń i lematów z poprzedniego rozdziału. Sam dowód twierdzenia o poprawności będzie opierał się na założeniu nie wprost, że n jest złożona, a algorytm zwróci *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. Następujące lematy przyjmują bowiem założenia, jakie te liczby spełniają w ostatnim kroku algorytmu.

Lemat 8. *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

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

skąd teza. □

Lemat 9. *Jeśli $a, n \in \mathbb{N}$, $n \geq 2$ i $NWD(a, n) = 1$, to n jest pierwsza wtw, gdy $(X + a)^n = X^n + a \,(mod\, n)$.*

Dowód. Rozpatrzmy współczynniki przy x^i w wielomianie $p(x) = (X+a)^n - (X^n+a)$. Wystarczy pokazać, że $p(x) = 0 \,(mod\, n)$ wtw, gdy n jest pierwsza.
(1) Załóżmy, że n jest pierwsza. Wtedy współczynnik przy x^i $(1 \leq i \leq n)$ w wielomianie $p(x)$ jest równy $\binom{n}{i}a^{n-i} = \frac{n!}{i!(n-i)!} \cdot a^{n-1}$. Z $\binom{n}{i} \in \mathbb{Z}$ oraz pierwszości n wiemy, że nie istnieje q takie, że $q \,|\, i! \cdot (n-i)! \wedge q \nmid (n-1)!$, więc $\frac{(n-1)!}{i!\cdot(n-i)!} \in \mathbb{Z}$ oraz $\binom{n}{i}$ jest podzielne przez n. Stąd $n \,|\, p(x)$.
(2) Załóżmy, że n jest złożona. Niech q będzie pewnym dzielnikiem pierwszym n oraz $q^k \parallel n$. Współczynnik przy x^q jest równy $\binom{n}{q}a^{n-q}$. Można 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 $q \,|\, n$, to $q \nmid (n-1) \cdot \ldots \cdot (n-q+1)$, czyli $q^k \parallel n \cdot (n-1) \cdot \ldots \cdot (n-q+1)$. 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 10. *Niech $a, n, r \in \mathbb{N}$, $n \geq 2$, $r \geq 1$ i $NWD(a, n) = 1$, wtedy 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 $(X + a)^n - (X^n + a) = 0 \,(mod\, X^r - 1,\, n)$. □

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

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

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 $1 \leq i \leq p-1$ zachodzi $p \,|\, \binom{p}{i}$, skąd wynika teza. □

Lemat 12. *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.
(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 $m \cdot \binom{n}{m} \,|\, \ell_n$.
(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 13. *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. (1) Przypadek, gdy $n = 2$ jest trywialny, ponieważ teza zachodzi dla $r = 3$. Podobnie dla $n = 3$, warunki spełnia $r = 4$.
(2) 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 $r \leq l \leq B$. □

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 14. *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 $g(X) \in \mathbb{F}_p[X]$ takie, że

$$f(X^{m'}) - f(X)^{m'} = g(X)(X^r - 1)$$
$$f(X^{mm'}) - f(X^m)^{m'} = g(X)(X^{mr} - 1).$$

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 15. *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 $f(X)g(X)$.*

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

Lemat 16. *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 $a^i a^{j-i} = a^j\,(mod\, r)$, a ponieważ a^i i a^j są niezerowe, to $a^{j-i} = 1\,(mod\, r)$ i ostatecznie $a \cdot a^{j-i-1} = 1\,(mod\, r)$, więc znaleźliśmy a^{-1}. □

Definicja 15. Na potrzeby kolejnych lematów ustalmy $n, r, p \in \mathbb{N}$, $n \geq 2$, $r < \lceil log^5 n \rceil$ 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 dla każdego $0 \leq a \leq \ell$ zachodzi

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

Możemy teraz zdefiniować, $I = \{n^i \cdot p^j \mid i, j \geq 0\}$, $P = \{\prod_{a=0}^{\ell} (X+a)^{e_a} \mid e_a \geq 0\}$ oraz G będące zbiorem reszt z dzielenia elementów I przez r. Niech $Q_r(X)$ będzie r-tym wielomianem cyklotomicznym nad $\mathbb{F}_p$ ($r \nmid p = char(\mathbb{F}_p)$). Weźmy $h(X) \in \mathbb{F}_p[X]$. Z twierdzenia **??** wiemy, że taki wielomian istnieje, jest nierozkładalny w $\mathbb{F}_p[X]$ oraz $deg(h) = o_r(p)$. Zdefiniujmy $F = \mathbb{F}_p / \langle h(X) \rangle$ oraz $\mathcal{G}$ będący zbiorem elementów P w F.

Lemat 17. *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 $0 \leq a \leq \ell$ n oraz p są introspektywne dla $X + a$, a następnie (2) wywnioskujemy tezę.
(1) Niech $0 \leq a \leq \ell$. p jest pierwsze, więc z lematu **??** otrzymujemy

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

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

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

Weźmy $f_1(X) = (X + a)^{\frac{n}{p}}$, $f_2(X) = X^{\frac{n}{p}} + a \in \mathbb{F}_p[X]$. 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 $X + a, 0 \leq a \leq \ell$.
(2) Ponieważ elementy zbioru I są iloczynami liczb n i p, a elementy zbioru P są iloczynami wielomianów $X+a$, $0 \leq a \leq \ell$, z lematów **??** i **??** możemy wywnioskować tezę. □

Lemat 18. *$\langle G, \cdot \rangle$ jest podgrupą $\mathbb{Z}_r^*$ oraz $|\,G\,| > log^2 n$.*

Dowód. (1) Pokażemy, że $\langle G, \cdot \rangle$ jest podgrupą $\mathbb{Z}_r^*$. 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 $G \subseteq \mathbb{Z}_r^*$. Mamy też $(\frac{n}{p})^0 \cdot p^0 = 1 \in G$, czyli istnienie elementu neutralnego w G. Mnożenie spełnia własności działania w grupie, więc wystarczy jeszcze tylko pokazać, że G jest (1.1) zamknięta na $\cdot$ i (1.2) dla każdego elementu istnieje element odwrotny.
(1.1) Weźmy dowolne $g_1 = (\frac{n}{p})^{i_1} \cdot p^{j_1} \,(mod\, r)$, $g_2 = (\frac{n}{p})^{i_2} \cdot p^{j_2} \,(mod\, r) \in G$, $i_1, i_2, j_1, j_2 \geq 0$. Wtedy $g_1 g_2 = (\frac{n}{p})^{i_1+i_2} \cdot p^{j_1+j_2} \,(mod\, r)$. $(\frac{n}{p})^{i_1+i_2} \cdot p^{j_1+j_2} \in I$, więc $g_1 g_2 \in G$.
(1.2) 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 $o_r(n) > log^2 n$. □

Lemat 19. *$|\,G\,| \geq \phi(r)$.*

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 zbiór $B = \{b \,|\, b = p \cdot a_i \,(mod\, r),\ b < r,\ a_i \in A\}$. 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 $p^{-1} \in \mathbb{F}_p$. Więc mnożąc stronami przez p^{-1} otrzymujemy sprzeczność.
Mamy $A = B$, możemy więc wywnioskować równanie

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

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 20. *$\mathcal{G}$ jest grupą z mnożeniem, generowaną przez zbiór $\mathcal{G}_{gen} = \{X, X + 1, \ldots, X + \ell\}$ w ciele F.*

Obserwacja 4. *$\mathcal{G} \subset F$.*

Dowód. (1) $\mathcal{G}$ jest grupą. Łatwo można zauważyć, że $\mathcal{G}$ zawiera element neutralny i jest zamknięty na mnożenie. Wystarczy więc pokazać, że dla każdego $g \in \mathcal{G}$ istnieje element odwrotny. Wykorzystamy argument z dowodu lematu **??**, tzn. ponieważ $\mathcal{G}$ jest skończonego rozmiaru, dla dowolnego $g \in \mathcal{G}$ także $g^2, \ldots, g^{|\mathcal{G}|+1} \in \mathcal{G}$. Istnieje $g^i \in \mathcal{G}$, $0 \leq i$, będące odwrotnością g.
(2) Zbiór $\mathcal{G}_{gen}$ generuje $\mathcal{G}$. Dla $g \in \mathcal{G}$, $g \neq 1$ oczywistym jest, że g można przedstawić jako iloczyn elementów $\mathcal{G}_{gen}$. Wiemy, że $h(X)$ dzieli $Q_r(X)$, czyli też, na mocy lematu **??**, $X^r - 1$. Mamy więc $X^r = 1$ w $\mathcal{G}$, czyli 1 także jest generowana przez $\mathcal{G}_{gen}$. Odwrotny wniosek, że każdy element generowany przez $\mathcal{G}_{gen}$ należy do $\mathcal{G}$ jest oczywisty. □

Lemat 21. *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 $\mathbb{F}_p[X]$. Rozważmy $h(X)$ i $X^k - 1$ w r-tym ciele cyklotomicznym nad $\mathbb{F}_p$. Istnieje w nim pierwiastek pierwotny r-tego stopnia ζ, który jest pierwiastkiem $h(X)$. Ponieważ $h(X)|X^k - 1$ także w rozszerzeniu ciała $\mathbb{F}_p$, to $\zeta^k - 1 = 0$ w $\mathbb{F}_p^{(r)}$. Otrzymaliśmy sprzeczność z założeniem, że ζ jest pierwiastkiem pierwotnym, ponieważ $k < r$.

□

Lemat 22. *Jeśli w grupie G istnieje co najmniej $k+1$ różnych wielomianów $f_1(X), \ldots, f_{k+1}(X)$ pierwszego stopnia, to istnieje co najmniej $\binom{k+d}{k+1}$ różnych wielomianów stopnia mniejszego niż d.*

Dowód. Uzasadnimy, że jesteśmy w stanie skonstruować bijekcję między $\binom{k+d}{d-1}$ elementami a różnymi wielomianami stopnia mniejszego niż d w F. 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 $\binom{k+d}{k+1}$. □

Lemat 23. $|\mathcal{G}| \geq \binom{t+\ell}{t-1}$.

Dowód. Pokażemy, że (1) dowolne dwa różne wielomiany stopnia mniejszego niż t w P są różne także w $\mathcal{G}$ oraz, że w (2) P jest co najmniej $\binom{t+\ell}{t-1}$ różnych wielomianów stopnia mniejszego niż t.
(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 $Q(Y) = f(Y) - g(Y)$. 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 dla dowolnego wielomianu z P, więc też dla dowolnego wielomianu w $\mathcal{G}$. Mamy więc $(f(X))^i = (g(X))^i$ i $f(X^i) = g(X^i)$ w F. 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 $h(X)|X^i$ w $\mathbb{F}_p$ lub $X^{i-i'} = 1$. Pierwszy argument tej dysjunkcji jest w oczywisty sposób nieprawdziwy, a drugi jest sprzeczny z lematem **??**. Znaleźliśmy więc $|\,G\,| = t$ pierwiastków $Q(Y)$ w F więc $Q(Y)$ jest wielomianem zerowym w F lub $deg(Q) > t$, zatem doszliśmy do sprzeczności z założeniem.
(2) Z założeń 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

$$\ell < \sqrt{r}\log n < r < p.$$

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 $|\,\mathcal{G}\,| \geq \binom{t+\ell}{t-1}$. □

Lemat 24. *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, $i \neq i'$, $j \neq j' \Rightarrow (\frac{n}{p})^i \cdot p^j \neq (\frac{n}{p})^{i'} \cdot p^{j'}$. 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 $(f(X))^{i_1} = f(X^{i_1}) = f(X^{i_2}) = f(X)^{i_2} \,(mod\, X^r - 1, p)$. Czyli dowolny $f(X) \in \mathcal{G}$ jest pierwiastkiem wielomianu $Q(X) = Y^{i_1} - Y^{i_2}$ w F. Skoro $\mathcal{G} \subset F$, to $Q(X)$ 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 $|\,\mathcal{G}\,| \leq n^{\sqrt{t}}$. □

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 I i III. 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 V. Ostatecznie algorytm zwróci *PIERWSZA* w kroku IV lub VII. □

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 IV i VII.
(1) Jeśli algorytm zakończył wykonanie w kroku IV, 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 VII, zwracając *PIERWSZA* i n jest złożona. Ponieważ algorytm nie zakończył się w kroku I, 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 II zostaje wybrane najmniejsze takie r, że $o_r(n) > log^2 n$. Ponadto z niespełnionego warunku w kroku III wiemy, że dla $1 \leq a \leq r$ zachodzi $NWD(a,\, n) = 1$, w szczególności $NWD(r,\, n) = 1$. Z warunku w kroku IV i V 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 definicji **??**. Weźmy zdefiniowany w niej zbiór $\mathcal{G}$. Na mocy lematu **??** mamy nierówność $|\,\mathcal{G}\,| \geq \binom{t+\ell}{t-1}$ oraz z lematu **??** oraz definicji **??** zachodzi $t > log^2 n$, $\ell = \lfloor \sqrt{\phi(r)} log\, n \rfloor$. Możemy więc wywnioskować nierówność

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

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. □

3.3. Złożoność obliczeniowa

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