MAT3 - Mały projekt 2

Jan Czechowski 337066

Zadanie 1

(a) Określić rzędy elementów w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{24}^*, \cdot_{24})$.

Rzędy elementów dla grupy 19:

In[2]:=
```
rzedyElementów19 = Table[MultiplicativeOrder[k, 19], {k, 1, 18}]
```

Out[2]=
```
{1, 18, 18, 9, 9, 9, 3, 6, 9, 18, 3, 6, 18, 18, 18, 9, 9, 2}
```

Rzędy elementów dla grupy 24 :

Wszystkie liczby naturalne względnie pierwsze z liczbą 24 na przedziale [1, 23]

In[5]:=
```
liczbyWzględniePierwszeZ24 = Select[Range[23], CoprimeQ[24, #] &]
```

Out[5]=
```
{1, 5, 7, 11, 13, 17, 19, 23}
```

Teraz dla wszystkich tych liczb szukamy najmniejszej liczby naturalnej dodatniej d, takiej, że $a^d \equiv_n 1$

In[7]:=
```
rzedyElementów24 = Table[MultiplicativeOrder[k, 24], {k, liczbyWzględniePierwszeZ24}]
```

Out[7]=
```
{1, 2, 2, 2, 2, 2, 2, 2}
```

Zadanie 2

(b) Znaleźć pierwiastki pierwotne w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{41}^*, \cdot_{41})$.

In[37]:=
```
n = 19;
grupa19 = Select[Range[1, n - 1], CoprimeQ[#, n] &];
pierwiastkiPierwotne19 = Select[grupa19, MultiplicativeOrder[#, n] == EulerPhi[n] &]
```

Out[39]=
```
{2, 3, 10, 13, 14, 15}
```

In[33]:=
```
Clear[n]
```

In[40]:=
```
n = 41;
grupa41 = Select[Range[1, n - 1], CoprimeQ[#, n] &];
pierwiastkiPierwotne41 = Select[grupa41, MultiplicativeOrder[#, n] == EulerPhi[n] &]
```

Out[42]= {6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35}

Zadanie 3

(c) Sprawdzić, czy w grupie $(Z_{2^8}^*, \cdot_{2^8})$ istnieje pierwiastek pierwotny. Czy istnieje takie $n \geq 3$, że grupa $(Z_{2^n}^*, \cdot_{2^n})$ jest cykliczna?

In[45]:=
```
pierwiastekPierwotnyWGrupieZ28 = PrimitiveRootList[2^8]
```

Out[45]= { }

Lista jest pusta co oznacza, że nie istnieje pierwastek pierwotny w tej grupie.

Funkcja sprawdzająca, czy dla danej potęgi 2^n grupa ma pierwiastki pierwotne:

In[51]:=
```
czyGrupaJestCykliczna[n_] := Module[{m, grupa, pierwiastkiPierwotne}, m = 2^n;
  grupa = Select[Range[1, m - 1], CoprimeQ[#, m] &];
  pierwiastkiPierwotne = Select[grupa, MultiplicativeOrder[#, m] == EulerPhi[m] &];
  Return[pierwiastkiPierwotne =!= {}]]
```

Teraz sprawdzamy dla n od 3 do 10

In[52]:=
```
Table[{n, czyGrupaJestCykliczna[n]}, {n, 3, 10}]
```

Out[52]=
```
{{3, False}, {4, False}, {5, False},
 {6, False}, {7, False}, {8, False}, {9, False}, {10, False}}
```

Grupa jednostek modulo 2^n dla $n \geq 3$ rozkłada się na dwa niezależne czynniki, przez co nie da się znaleźć jednego elementu, którego potęgi dawałyby wszystkie elementy tej grupy. Oznacza to, że struktura tej grupy uniemożliwia istnienie jednego generatora, który mógłby wygenerować całą grupę poprzez kolejne potęgowanie.

Zadanie 4

(d) Znaleźć elementy odwrotne do wybranych elementów w grupach $(Z_{19}^*, \cdot_{19})$ i $(Z_{24}^*, \cdot_{24})$.

Elementy odwrotne w grupie 19:

Przykładowo dla a = 3 i b = 7

In[63]:=
```
a = 3;
b = 7;
```

In[65]:=
```
n = 19;
odwrotnosc3 = PowerMod[a, -1, n]
odwrotnosc7 = PowerMod[b, -1, n]
```

Out[66]= 13

Out[67]= 11

Elementy odwrotne w grupie 24 :

Przykładowo dla c = 5 i d = 7

In[95]:=
```
c = 5;
```

In[102]:=
```
d = 7;
```

In[106]:=
```
n = 24;
odwrotnosc3 = PowerMod[c, -1, n]
odwrotnosc5 = PowerMod[d, -1, n]
```

Out[107]= 5

Out[108]= 7

Zadanie 5

(e) Zastosować test Lucasa dla wybranych dużych liczb całkowitych.

In[110]:=
```
TestLucasa[n_Integer] := Module[{pDivisors, isPrime = False},
  If[n < 2, Return[False]];
  pierwszeDzielniki = First /@ FactorInteger[n - 1];
  (*Sprawdzamy wartości b w zakresie 2 ≤ b ≤ n-1*)
  Do[If[PowerMod[b, n - 1, n] == 1 &&
     AllTrue[pierwszeDzielniki, PowerMod[b, (n - 1) / #, n] =!= 1 &], isPrime = True;
    Break[];], {b, 2, n - 1}];
  isPrime]
```

In[111]:=
```
TestLucasa[92387]
```

Out[111]= True

In[112]:=
```
TestLucasa[9123]
```

Out[112]= False

```
TestLucasa[7364]
```

Out[113]= False

Wszystko się zgadza, ponieważ 92387 jest liczbą pierwszą, 9123 NIE jest liczbą pierwszą, 7364 również

NIE jest liczbą pierwszą.