# Tymon Zadara - 337086 - Mały Projekt Mat 3

## Zadanie 1: określić rzędy elementów w grupach, w których numery elementów są względnie pierwsze z numerem grupy

In[13]:=
```
(*Grupa Z19*)
rzedyGrupy19 =
 Table[{k, MultiplicativeOrder[k, 19]}, {k, Select[Range[18], CoprimeQ[19, #] &]}]
```
Out[13]=
```
{{1, 1}, {2, 18}, {3, 18}, {4, 9}, {5, 9}, {6, 9}, {7, 3}, {8, 6}, {9, 9},
 {10, 18}, {11, 3}, {12, 6}, {13, 18}, {14, 18}, {15, 18}, {16, 9}, {17, 9}, {18, 2}}
```
In[14]:=
```
rzedyGrupy24 =
 Table[{k, MultiplicativeOrder[k, 24]}, {k, Select[Range[23], CoprimeQ[24, #] &]}]
```
Out[14]=
```
{{1, 1}, {5, 2}, {7, 2}, {11, 2}, {13, 2}, {17, 2}, {19, 2}, {23, 2}}
```

## Zadanie 2: Znaleźć pierwiastki pierwotne dla grup

In[17]:=
```
(*Wzór na ilość peirwiastków pierwotnych w Grupie Zn*)

iloscpierw[n_] := EulerPhi[EulerPhi[n]];
iloscpierw[19]
iloscpierw[41]
```
Out[18]=
```
6
```
Out[19]=
```
16
```
In[20]:=
```
pierwiastkiPierwotne19 = PrimitiveRootList[19]
```
Out[20]=
```
{2, 3, 10, 13, 14, 15}
```
```
(*zgadza się - jest 6 pierwiastków pierwotnych*)
```
In[21]:=
```
pierwiastkiPierwotne41 = PrimitiveRootList[41]
```
Out[21]=
```
{6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35}
```
```
(*zgadza się - jest 16 pierwiastków pierwotnych*)
```

## Zadanie 3:Sprawdzić czy w grupie Z2^8 istnieje pierwiastek pierwotny, czy istnieje n > 3 gdzie grupa Z2^n jest cykliczna

In[22]:=
```
pierwiastkiPierwotne2do8 = PrimitiveRootList[2^8]
```
Out[22]=
```
{}
```

```
(*jak widać nie ma pierwiastków pierwotnych w grupie Z2^8*)

(*grupa jest cykliczna jeżeli rząd grupy jest liczbą
 pierwszą czyli jeżeli liczba elementów grupy jest liczbą pierwszą*)

(* Zgodnie z twierdzeniem 2 w pliku. Czyli Jeżeli
grupa posiada pierwiastek pierwotny to jest cykliczna*)
```

Zgodnie z twierdzeniem 2 z pliku wiemy, że nie istnieje takie n>3 które wygeneruje grupę Z2^n cykliczną. Jest to spowodowane tym, że grupy te dla każdego n będą rzędu parzystego(czyli zawsze podzielne przez 2 - czyli nigdy pierwsze), nie będą posiadały pierwiastków pierwotnych i tym samym nie będą spełniały wymaganych warunków aby były cykliczne.

## Zadanie 4: Znaleźć elementy odwrotne do wybranych elementów grup z zadania 1

In[27]:=
```
odwrotnosci19 = Table[{k, PowerMod[k, -1, 19]}, {k, Select[Range[18], CoprimeQ[#, 19] &]}]
```
Out[27]=
```
{{1, 1}, {2, 10}, {3, 13}, {4, 5}, {5, 4}, {6, 16}, {7, 11}, {8, 12}, {9, 17},
 {10, 2}, {11, 7}, {12, 8}, {13, 3}, {14, 15}, {15, 14}, {16, 6}, {17, 9}, {18, 18}}
```
In[28]:=
```
odwrotnosci24 = Table[{k, PowerMod[k, -1, 24]}, {k, Select[Range[23], CoprimeQ[#, 24] &]}]
```
Out[28]=
```
{{1, 1}, {5, 5}, {7, 7}, {11, 11}, {13, 13}, {17, 17}, {19, 19}, {23, 23}}
```
```
(* to samo co w zadaniu 1 tylko należy zamienic MultiplicativeOrder na PowerMod  -
 czyli do potęgi i modulo*)
```

## Zadanie 5:
## Funkcja sprawdzająca czy n jest pierwsze iterując po b od 2 do n-1, gdy spełnia oba warunki to prawda

In[83]:=
```
testPierwszościLucasa[n_] := Module[{dzielniki, isPrime = False},
dzielniki = FactorInteger[n - 1][[All, 1]];
Do[If[(PowerMod[b, n - 1, n] == 1) && (AllTrue[dzielniki, PowerMod[b, (n - 1)/#, n] ≠ 1 &]),
    isPrime = True;
    Break[];], {b, 2, n - 1}];
isPrime]
```

In[84]:=
```
testPierwszościLucasa[1009]
```

Out[84]=
```
True
```

In[85]:=
```
testPierwszościLucasa[1012]
```

Out[85]=
```
False
```

In[86]:=
```
testPierwszościLucasa[1 000 000 007]
```

Out[86]=
```
True
```

In[87]:=
```
testPierwszościLucasa[123 452]
```

Out[87]=
```
False
```