Tp0e3

February 26, 2020

Exercício 3 - Corpos finitos primos

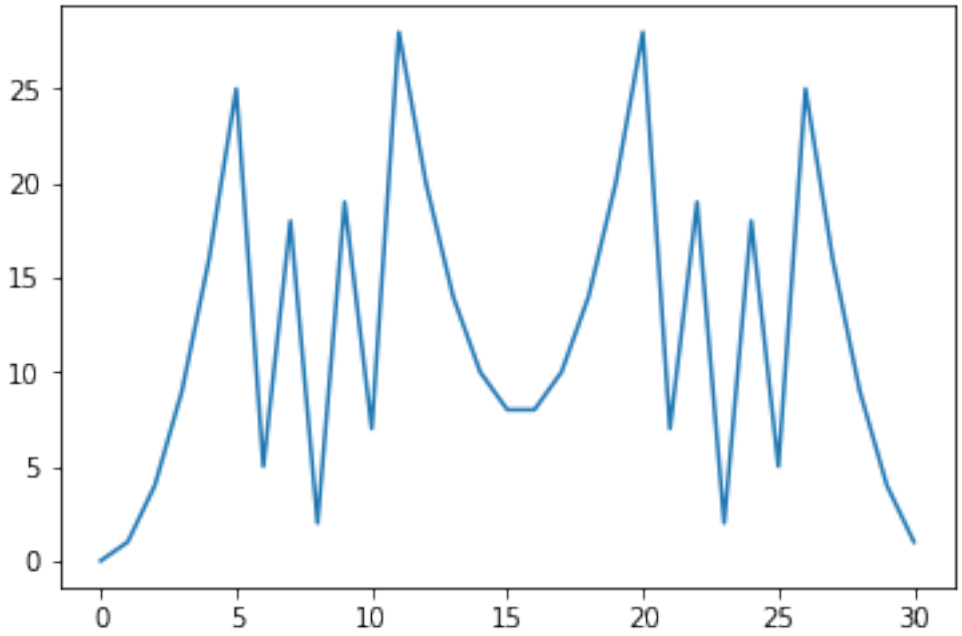
De forma a resolver o exercício foi necessário tomar conhecimento do conceito de corpos finitos. Após ter realmente percebido o que eram corpos finitos, numa primeira fase deste exercício tivemos de criar quatro corpos finitos sendo eles P = 31,127,8191,131071. Para tal efeito, recorremos à função do SageMath GF(p), em que p é um número primo.

[10]:
```
p1 = 31
corpo1 = GF(31)
print(corpo1)

p2 = 127
corpo2 = GF(p2)
print(corpo2)

p3 = 8191
corpo3 = GF(p3)
print(corpo3)

p4 = 131071
corpo4 = GF(p4)
print(corpo4)
```

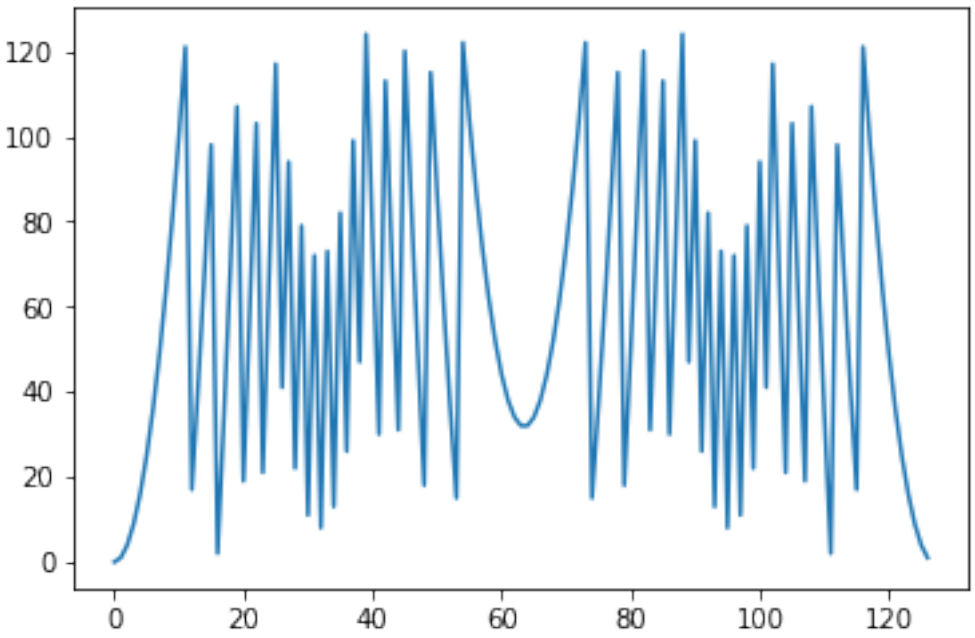
```
Finite Field of size 31
Finite Field of size 127
Finite Field of size 8191
Finite Field of size 131071
```

Uma vez criados os corpos, foi criado um gráfico para cada corpo criado através da função plot da ferramenta do SageMath. Assim, de forma a tornar o gráfico visível, utilizamos a função plot.show():

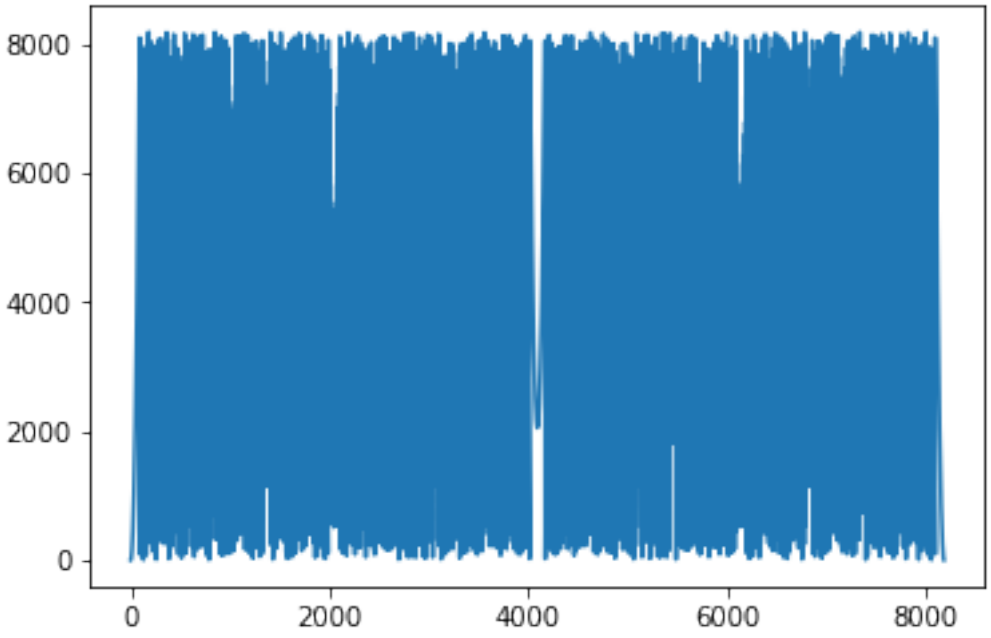
[11]:
```
import matplotlib.pyplot as plt
graph=plt.plot([x**2 for x in corpo1])
plt.show(graph)
```



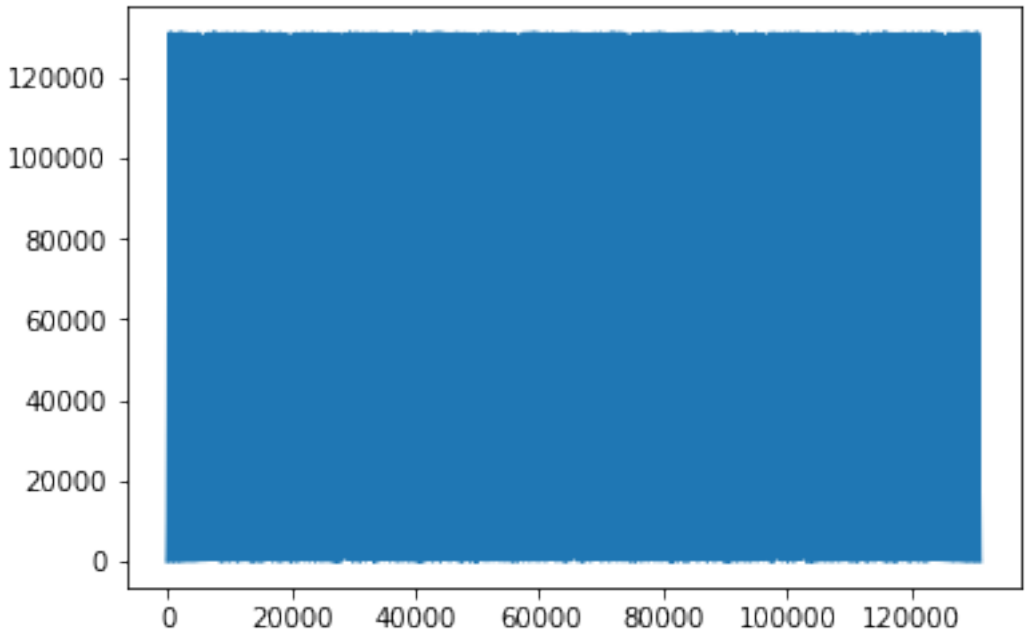
[12]:
```
graph=plt.plot([x**2 for x in corpo2])
plt.show(graph)
```



[13]:
```
graph=plt.plot([x**2 for x in corpo3])
plt.show(graph)
```



[14]:
```
graph=plt.plot([x**2 for x in corpo4])
plt.show(graph)
```



Com a análise dos resultados obtidos nos fim das suas execuções, concluimos que as representações correspondem ao que era esperado. No caso de por exemplo x ser igual a 5, obtemos o valor 25. Caso seja 6 e o valor execede o número primo em questão, no gráfico iremos obter a diferença entre o que seria de esperar e esse número, desta forma quando x é igual a 6, obtemos o valor 5, como podemos observar.

Por último, determina-se um elemento primitivo para cada um dos corpos finitos primos. Posto isto, verifica-se a proposição exposta cada cada um dos elementos primitivos e é sempre apresentada como verdadeira.

[16]:
```
e1 = corpo1.primitive_element()
print(e1)
n = mod(0,p1-1)
e1^n == 1
```

```
3
```

[16]: True

[17]:
```
e2 = corpo2.primitive_element()
print(e2)
n = mod(0,p2-1)
e2^n == 1
```

```
3
```

[17]: True

[18]:
```
e3 = corpo3.primitive_element()
print(e3)
n = mod(0,p3-1)
e3^n == 1
```

```
17
```

[18]: True

[19]:
```
e4 = corpo4.primitive_element()
print(e4)
n = mod(0,p4-1)
e4^n == 1
```

```
3
```

[19]: True