Pergunta 3

February 20, 2019

1 Jupyter + SageMath HelloWorld

1.1 Para o corpo finito primo $\mathbb{F}_{37}$:

1.1.1 Criação do corpo finito:

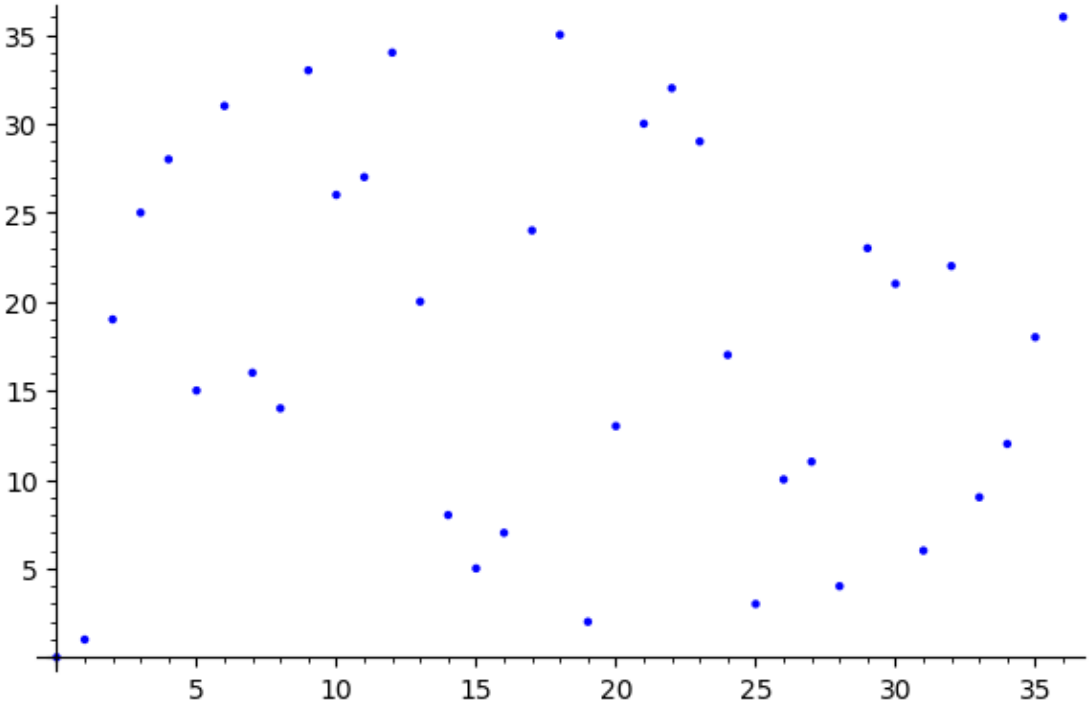
```
In [59]: p = 37;
         Fp = FiniteField(p);Fp
```

```
Out[59]: Finite Field of size 37
```

1.1.2 Criação do *plot* da função $x \mapsto x^{35}$:

```
In [60]: list_plot([x^(p-2) for x in Fp])
```

Out[60]:



1.1.3 Determinação do menor primo elemento primitivo de $\mathbb{F}_{37}$:

```
In [61]: g = Fp.primitive_element(); g
```

```
Out[61]: 2
```

1.1.4 Testar, por amostragem, que: se g é elemento primitivo, então, para todo o expoente n, verifica-se $g^n = 1$ sse $n \equiv 0 \; mod \; (p-1)$

Note-se que: $p \iff q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

```
In [62]: n = ZZ.random_element(0,p); n
```

```
Out[62]: 15
```

```
In [63]: (g^(n) == 1 and n == power_mod(0,1,p-1)) or (not(g^(n) == 1)
                                                      and not(n == power_mod(0,1,p-1)))
```

```
Out[63]: True
```

1.2 Para o corpo finito primo $\mathbb{F}_{163}$:

1.2.1 Criação do corpo finito:

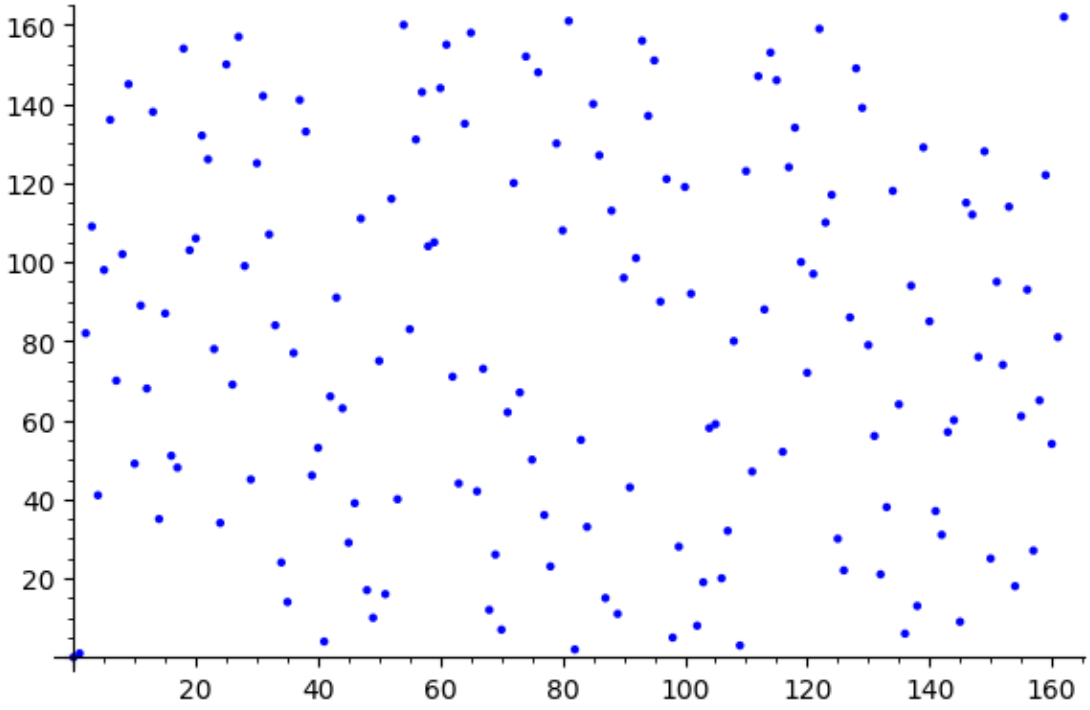
```
In [64]: p = 163;
         Fp = FiniteField(p);Fp
```

```
Out[64]: Finite Field of size 163
```

1.2.2 Criação do *plot* da função $x \mapsto x^{161}$:

```
In [65]: list_plot([x^(p-2) for x in Fp])
```

```
Out[65]:
```



1.2.3 Determinação do menor primo elemento primitivo de $\mathbb{F}_{163}$:

```
In [66]: g = Fp.primitive_element(); g
```

```
Out[66]: 2
```

1.2.4 Testar, por amostragem, que: se g é elemento primitivo, então, para todo o expoente n, verifica-se $g^n = 1$ sse $n \equiv 0 \ mod \ (p-1)$

```
In [67]: n = ZZ.random_element(0,p); n
```

```
Out[67]: 52
```

```
In [68]: (g^(n) == 1 and n == power_mod(0,1,p-1)) or (not(g^(n) == 1)
                                                      and not(n == power_mod(0,1,p-1)))
```

```
Out[68]: True
```

1.3 Para o corpo finito primo $\mathbb{F}_{263}$:

1.3.1 Criação do corpo finito:

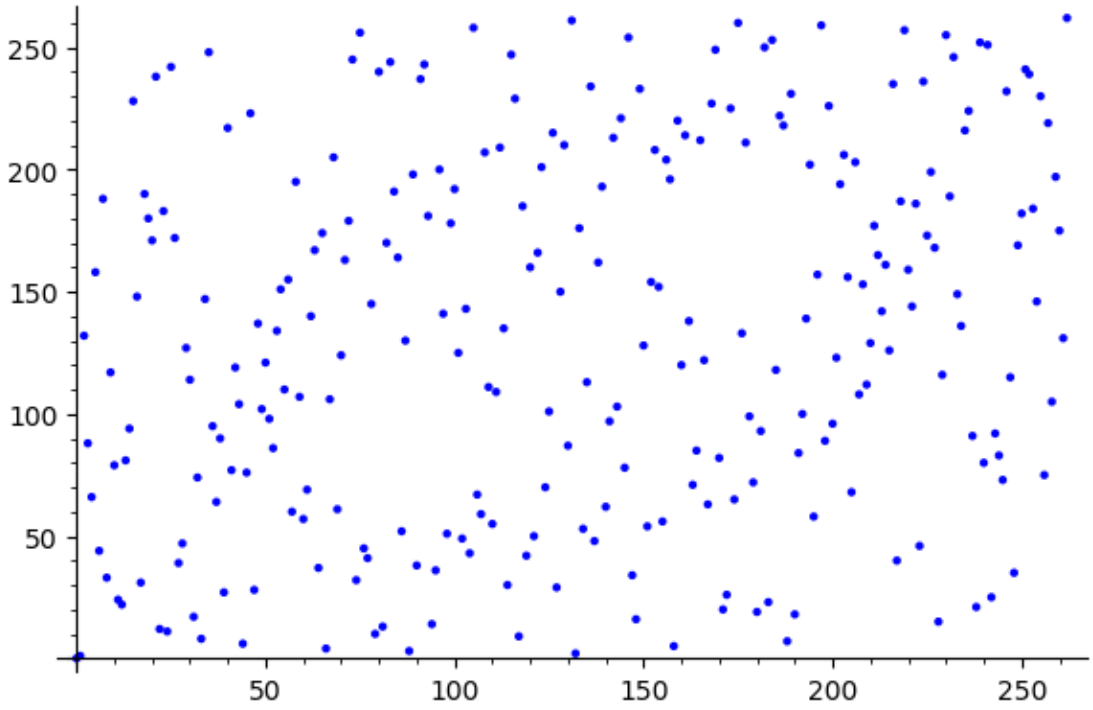
```
In [69]: p = 263;
         Fp = FiniteField(p);Fp
```

```
Out[69]: Finite Field of size 263
```

1.3.2 Criação do *plot* da função $x \mapsto x^{261}$:

```
In [70]: list_plot([x^(p-2) for x in Fp])
```

Out[70]:



1.3.3 Determinação do menor primo elemento primitivo de $\mathbb{F}_{263}$:

```
In [71]: g = Fp.primitive_element(); g
```

```
Out[71]: 5
```

1.3.4 Testar, por amostragem, que: se g é elemento primitivo, então, para todo o expoente n, verifica-se $g^n = 1$ sse $n \equiv 0 \ mod \ (p-1)$

```
In [72]: n = ZZ.random_element(0,p); n
```

```
Out[72]: 167
```

```
In [73]: (g^(n) == 1 and n == power_mod(0,1,p-1)) or (not(g^(n) == 1)
                                                      and not(n == power_mod(0,1,p-1)))
```

```
Out[73]: True
```

1.4 Para o corpo finito primo $\mathbb{F}_{1009}$:

1.4.1 Criação do corpo finito:

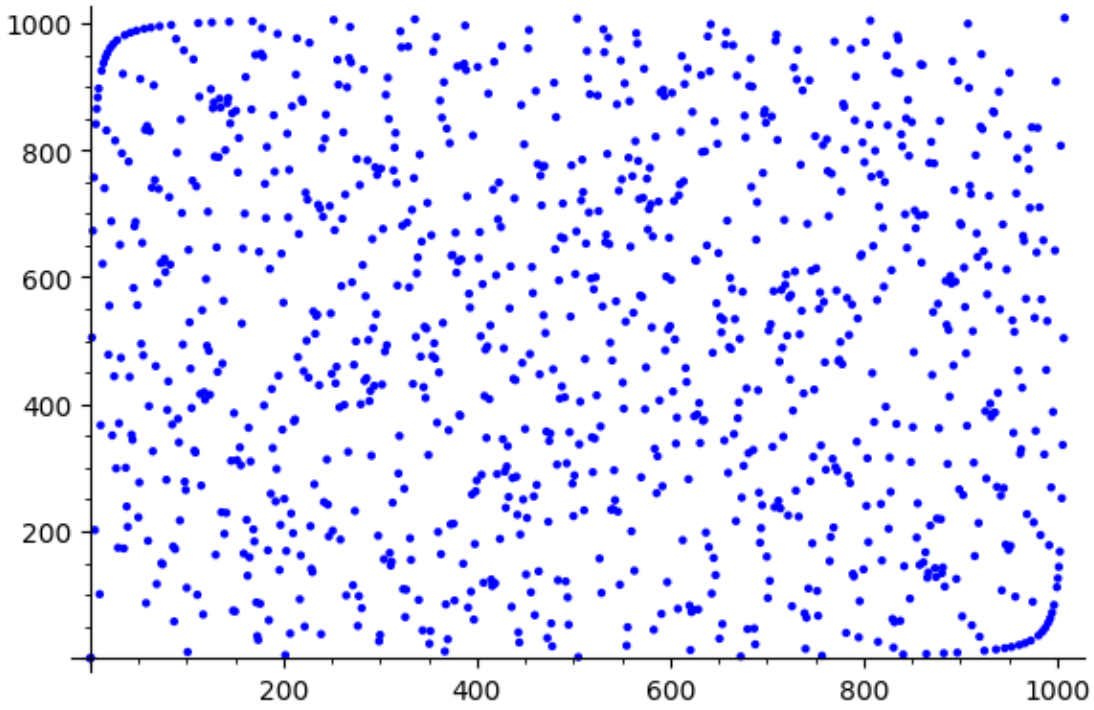
```
In [74]: p = 1009;
         Fp = FiniteField(p);Fp
```

```
Out[74]: Finite Field of size 1009
```

1.4.2 Criação do *plot* da função $x \mapsto x^{1007}$:

```
In [75]: list_plot([x^(p-2) for x in Fp])
```

Out[75]:



1.4.3 Determinação do menor primo elemento primitivo de $\mathbb{F}_{1009}$:

```
In [76]: g = Fp.primitive_element(); g
```

```
Out[76]: 11
```

1.4.4 Testar, por amostragem, que: se g é elemento primitivo, então, para todo o expoente n, verifica-se $g^n = 1$ sse $n \equiv 0 \ mod \ (p-1)$

```
In [77]: n = ZZ.random_element(0,p); n
```

```
Out[77]: 377

In [78]: (g^(n) == 1 and n == power_mod(0,1,p-1)) or (not(g^(n) == 1)
                                                      and not(n == power_mod(0,1,p-1)))

Out[78]: True
```