Ejercicio6

March 13, 2022

[1]:
```python
from math import gcd

n=13250459

def f(x):
    return x*x+1

def rho_de_polard(n,imprime=False):
    x=1
    y=1
    contador=0
    resultado=1

    if imprime:
        print("Iteracion ", contador)
        print("x: ",x," y:",y , " mcd: ", resultado)

    while resultado==1 or resultado == n:
        x=f(x)%n
        y=f(f(y))%n
        resultado=gcd(x-y,n)
        contador+=1

        if imprime:
            print("Iteracion ", contador)
            print("x: ",x," y:",y , " mcd: ", resultado)
        if 1<resultado<n:
            return resultado

    return "No hay divisores"
```

[2]:
```python
def ParteEntera(n):
    if n%2==0:
        a=n//2
    else:
```

```
        a=(n+1)//2

    contador=1
    b=0
    c=0
    encontrado=False

    while encontrado==False:
        b=a*a+n
        contador+=1
        c=b//(2*a)

        if c>=a:
            encontrado=True
        else:
            a=c

    return a
```

1 Ejercicio 6

Dado p=4987, el primo de mayor periodo del ejercicio anterior

1. **Calcula los convergentes de** $\sqrt{p}$.
2. **Calcula las soluciones de las ecuaciones de Pell,** $x^2 - py^2 = \pm 1$

En primer lugar vamos a añadir unas mejoras a la función para que calcule los convergentes y las soluciones de las ecuaciones de Pell.

[3]:
```
def FCS_convergentes_(n):
    alpha=n
    q_fijo=ParteEntera(alpha)
    fcs=[]
    convergentes=[]
    soluciones=[]
    A=[1,q_fijo]
    B=[0,1]
    i=1 #Contador de posición para A y B
    q=q_fijo
    P_sig=0
    P_act=0
    Q_act=1
    Q_sig=1

    entra=False
```

```python
    fcs.append(q)
    convergentes.append(A[i]/B[i])
    while 2*q_fijo!=q:
        if Q_act==4:
            soluciones.append((A_act,B_act))
            entra=True

        P_sig=q*Q_act-P_act
        Q_sig=(n-P_sig*P_sig)//Q_act
        q=(P_sig+q_fijo)//Q_sig

        fcs.append(q)
        P_act=P_sig
        Q_act=Q_sig
        A.append(q*A[i]+A[i-1])
        B.append(q*B[i]+B[i-1])
        i+=1
        convergentes.append(A[i]/B[i])

    if entra==False:
        soluciones.append((A[len(fcs)],B[len(fcs)]))


    return fcs,convergentes,soluciones
```

Recordemos que las soluciones positivas de la ecuación de Pell, por lo visto en clase, son los A_{n-1} y los B_{n-1} de $\sqrt{p}$ tales que n es un múltiplo de la longitud de periodo.

Con esta modificación la sucesión de convergentes y los pares A_i y B_i que son soluciones de la ecuación de Pell son los siguientes:

[4]:
```python
a,b,c=FCS_convergentes_(4987)
print("FCS:",a)
print()
print("Convergentes:",b)
print()
print("Soluciones: ", c)
```

```
FCS: [70, 1, 1, 1, 1, 1, 1, 1, 5, 1, 4, 46, 1, 6, 1, 6, 1, 1, 3, 1, 2, 1, 14, 1,
22, 1, 1, 1, 1, 12, 4, 4, 1, 69, 1, 4, 4, 12, 1, 1, 1, 1, 22, 1, 14, 1, 2, 1, 3,
1, 1, 6, 1, 6, 1, 46, 4, 1, 5, 1, 1, 1, 1, 1, 1, 1, 140]

Convergentes: [70.0, 71.0, 70.5, 70.66666666666667, 70.6, 70.625,
70.61538461538461, 70.61904761904762, 70.61864406779661, 70.61870503597122,
70.6186943620178, 70.61869440965867, 70.61869440864946, 70.61869440879101,
70.61869440877327, 70.61869440877553, 70.61869440877524, 70.61869440877537,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
```

```
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535, 70.61869440877535, 70.61869440877535, 70.61869440877535,
70.61869440877535]

Soluciones:  [(719704422302267113395432178632101,
10191415011671948990992687640732)]
```

Como vemos las convergentes se calculan correctamente y convergen al irracional *sqrtp*. Por otro lado, la menor solución positiva de la ecuación de Pell se obtiene en la última iteración para $A = 719704422302267113395432178632101$ y $B = 10191415011671948990992687640732$ que además es par.

[5]:
```
(719704422302267113395432178632101^2-4987*10191415011671948990992687640732^2)%4
```

[5]:
```
1
```

3. Calcula las unidades del anillo de enteros cuadráticos $Z[\sqrt{p}]$.

4. ¿Es $Z[\sqrt{p}]$ el anillo de enteros del cuerpo $Q[\sqrt{p}]$?.

Como sabemos, las soluciones de la ecuación de Pell son unidades del anillo $Z[\sqrt{p}]$ con $p = 4987$ en nuestro caso. Por lo tanto cualquier unidad del anillo es una potencia salvo signo $(A + B\sqrt{p})^n$ con $n \in Z$.

Finalmente queda ver si $Z[\sqrt{p}]$ es anillo de enteros de $Q[\sqrt(p)]$. Como $p \equiv 3 \ mod \ 4$ se tiene que $Z[\sqrt{p}]$ es anillo de enteros del cuerpo $Q[\sqrt(p)]$.