Sveučilište u Zagrebu

Prirodoslovno - matematički fakultet

Matematički odsjek

Eliptičke krivulje u kriptografiji

4. domaća zadaća

Student:
Antonio Kovačić

Nastavnik:
Doc. dr. sc. Filip Najman

Zagreb, 12. lipnja 2014.

Sadržaj

1 Problem

1. Zadana je točka $P = (0, 2)$ na eliptičkoj krivulji $y^2 = x^3 + 2x + 4$ nad poljem $\mathbb{F}_{211}$. Odredite NAF prikaz broja 106. Izračunajte $106P$.

2. Pronađite jednu eliptičku krivulju E nad $\mathbb{F}_{17}$ sa svojstvom da je red grupe $E(\mathbb{F}_{17})$ jednak 20.

3. Zadana je eliptička krivulja

$$E\ :\ y^2 = x^3 + x + 4$$

nad poljem $\mathbb{F}_{191}$. Odredite red grupe $E(\mathbb{F}_{191})$ Shanks-Mestreovom metodom, koristeći točku $P = (24, 10)$.

2 Rješenje

2.1 1. zadatak

Za prvi zadatak sam koristio *Sage* i *Python*. Rješenje je isprogramirano u *Sageu*. U [2, s. 58-59] su navedeni algoritmi za traženje zadanih informacija. No kako bi se sve poklopilo s indeksima, na binarni zapis sam dodao još 2 nule (jer u algoritmu za NAF prikaz petlja ide od 0 do d, pa fale još dvije znamenke ispred jer n_d i n_{d+1} nisu definirani bili. U konačnici, implementacija je dana sa:

```
import math
E=EllipticCurve(GF(211),[2,4])
E
c=[]
s=[]
bini=106
bini=bin(bini)
bini=bini[2:len(bini)]
bini='00'+bini
bini=list(bini)
c.append(0)
d=len(bini)
bini=list(reversed(bini))
for i in range(d-1):
    c.append(math.floor((int(bini[i])+int(bini[i+1])+c[i])/2))
    s.append(int(bini[i])+c[i]-2*c[i+1])
s
P=E([0,2])
Q=P
for i in reversed(range(len(s)-1)):
    Q=2*Q
    if(s[i]==1): Q=Q+P
    if(s[i]==-1): Q=Q-P
Q
Elliptic Curve defined by y^2 = x^3 + 2*x + 4 over Finite Field of size 211
[0.0, 1.0, 0.0, 1.0, 0.0, -1.0, 0.0, 1.0]
(2 : 4 : 1)
```

U zadnje dvije linije vidimo ispis rješenja. Rješenja su:

NAF prikaz je $s = (0, 1, 0, 1, 0, -1, 0, 1)$, a $106P = (2, 4)$

2.2 2. zadatak

Ovaj zadatak sam riješio primjenom tehnike *brute forcea.* U *sageu* sam kreirao krivulje oblika $y^2 = x^3 + ax + b$ čija je diskriminanta različita od 0, $a, b \in \mathbb{F}_{17}$ su proizvoljni. Zatim sam samo provjeravao je li $|E(\mathbb{F}_{17})| = 20$. Druga je opcija bila da iz formule za računanje ranga:

$$|E(\mathbb{F}_{17})| = 17 + 1 + \sum_{x \in \mathbb{F}_{17}} \left(\frac{x^3 + ax + b}{17} \right) = 20$$

nađem a i b takve da je $\sum_{x \in \mathbb{F}_{17}} \left(\frac{x^3+ax+b}{17} \right) = 2$ što se na kraju svodi na isto.[1] Implementacija izrečenog algoritma slijedi:

```
krivulje=[]
for i in range (17):
    for j in range(17):
        if ((4*(i**3)+27*(j**2)) % 17 != 0):
            E=EllipticCurve(GF(17), [i,j])
            if (E.order()==20):
                if (E not in krivulje): krivulje.append(E)
for i in range(len(krivulje)):
    krivulje[i]
```

Program je kao riješenja dao dole navedene krivulje:

$$y^2 = x^3 + x + 6$$

$$y^2 = x^3 + x + 11$$

$$y^2 = x^3 + 2x$$

$$y^2 = x^3 + 3x + 4$$

$$y^2 = x^3 + 3x + 13$$

$$y^2 = x^3 + 4x + 3$$

$$y^2 = x^3 + 4x + 14$$

[1] Izraz $\left(\frac{x^3+ax+b}{17} \right)$ je Legendreov simbol definiran u [1, s. 29]

$$y^2 = x^3 + 5x + 8$$

$$y^2 = x^3 + 5x + 9$$

$$y^2 = x^3 + 6x + 7$$

$$y^2 = x^3 + 6x + 10$$

$$y^2 = x^3 + 7x + 5$$

$$y^2 = x^3 + 7x + 12$$

$$y^2 = x^3 + 8x$$

$$y^2 = x^3 + 9x$$

$$y^2 = x^3 + 10x + 3$$

$$y^2 = x^3 + 10x + 14$$

$$y^2 = x^3 + 11x + 6$$

$$y^2 = x^3 + 11x + 11$$

$$y^2 = x^3 + 12x + 2$$

$$y^2 = x^3 + 12x + 15$$

$$y^2 = x^3 + 13x + 5$$

$$y^2 = x^3 + 13x + 12$$

$$y^2 = x^3 + 14x + 1$$

$$y^2 = x^3 + 14x + 16$$

$$y^2 = x^3 + 15x$$

$$y^2 = x^3 + 16x + 7$$

$$y^2 = x^3 + 16x + 10$$

Pa kao riješenje mogu uzeti bilo koju od tih krivulja, na primjer $E\ :\ y^2 = x^3 + x + 6$.

2.3 3. zadatak

U trećem zadatku sam koristio algoritam naveden u [2, s. 60]. Implementirao sam ga također pomoću *Sagea* i *Phytona* te je njegova implementacija navedena:

```
import math
p=191
m=int(math.ceil(2*(p**0.25)))
E=EllipticCurve(GF(p), [1,4])
P=E([24,10])
Q=int((p+1+math.floor(2*math.sqrt(p))))*P
listaAdicija=[]
for j in range(m):
    listaAdicija.append(j*P)
for i in range(m):
    if (listaAdicija.count(Q-i*(m*P))):
        m
        i
        listaAdicija.index(Q-i*(m*P))
        int(math.floor(2*math.sqrt(p)))
        t=i*m+listaAdicija.index(Q-i*(m*P))-int(math.floor(2*math.sqrt(p)))
t
order=p+1-t
order
8
1
3
27
-16
208
```

Pa vrijedi da je $|E(\mathbb{F}_{191})| = 208$.

Literatura

[1] A. Dujella. *Uvod u teoriju brojeva.* http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[2] A. Dujella. *Eliptičke krivulje u kriptografiji.* http://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf, 2013.