Algoritmi u teoriji brojeva

Zadaća 3

Mihael Petrinjak

Zadatak 1.

Pišem algoritam za računanje jacobijeva simbola $(\frac{a}{m})$.

In [1]:

```
def Jacobi(a, m) :
    a = a % m
    t = 1
    while a != 0 :
        while a % 2 == 0 :
            a = a / 2
            if m % 8 == 3 or m % 8 == 5 : t = -t
        a, m = m, a
        if a % 4 == 3 and m % 4 == 3 : t = -t
        a = a % m
    if m == 1 : return t
    return 0
```

In [2]:

```
for i in range(1,10):
    print(f"{i} : {Jacobi(i,1753)}")
```

```
1 : 1
2 : 1
3 : 1
4 : 1
5 : -1
6 : 1
7 : -1
8 : 1
9 : 1
```

Najmanji kvadratni neostatak modulo 1753 je 5 jer je Jacobijev simbol $(\frac{5}{1753})$ jednak -1.

Zadatak 2.

Pišem algoritam za računanje kvadratnih korijena modulo p.

In [4]:

```
def korijeni(a, p) :
    for x in range(1,p) :
        if pow(x,2,p) == a : # funkcija pow potencira modularno
            yield x
```

In [5]:

```
{x for x in korijeni(1367,1753)}
```

Out[5]:

```
{321, 1432}
```

Zadatak 3.

Iz $q < 2^{1/2}Q^2 < 6 \cdot 10^8$ slijedi da možemo uzeti $Q = 17000$.

Provodim račun u [browser verziji PARI/GP (https://pari.math.u-bordeaux.fr/gp.html)](https://pari.math.u-bordeaux.fr/gp.html).

```
?
a = sqrt(2)
b = sqrt(38)
Q = 17000
C = Q^3
B = [1, 0, 0; -round(C*a), C, 0; -round(C*b), 0, C]
R = qflll(B)
print("q = ", R[1,1], ", p1 = ", R[2,1], ", p2 = " , R[3,1])
q = 72048778, p1 = 101892359, p2 = 444138496
```

Provjera uvjeta:

In [84]:

```
a = np.sqrt(2)
b = np.sqrt(38)
q = 72048778
p1 = 101892359
p2 = 444138496
```

In [86]:

```
10**5 < q and q < 6*10**8
```

Out[86]:

```
True
```

In [85]:

```
max(abs(a-p1/q),abs(b-p2/q)) < q**(-3/2)
```

Out[85]:

```
True
```

Dakle, $q = 72\ 048\ 778$, $p_1 = 101\ 892\ 359$, $p_2 = 444\ 138\ 496$ su traženi brojevi.