- Konstantinos Filippou
- ics23044

Exercise 1

Να δείξετε ότι η συνθήκη $4a^3 + 27b^2 \neq 0 \bmod p$ ικανοποιείται για την καμπύλη $y^2 \equiv x^3 + 5x + 1 \bmod 97$.

Solution

Για την καμπύλη έχουμε ότι α = 5 και b = 1.

Επομένως, 4a^3 = 4x5^3 = 4x125 = 500 και 27b^2= 27x1 = 27

4a^3+27b^2 = 527 mod 97 = 527 − 5x97= 527 − 485 = 42 διάφορο του 0

Επομένως η συνθήκη ικανοποιείται.

Exercise 2

Εκτελέστε τις προσθέσεις:

- (3,25)+(6,21) και
- (10,9)+(10,9)

στην ομάδα που ορίζει η καμπύλη της παραπάνω άσκησης, δηλ. $y^2 \equiv x^3 + 5x + 1 \bmod 97$. Να λύσετε την άσκηση στο χαρτί με τη βοήθεια του αλγορίθμου πρόσθεσης (διαφάνεια 22) και να επαληθεύσετε τα αποτελέσματα με ανάπτυξη κώδικα που θα συνοδεύει την λύση σας.

Solution

- P1 = (3,25) και P2 = (6,21)

  P1 διάφορο του P2:

  λ = (y2-y1) / (x2-x1) = (21-25) / (6-3) = -4/3

  Βρίσκουμε το αντίστροφο του 3 στο mod 97.

  97 = 3x32 + 1

  1 = 97 - 3x32

  Επομένως είναι -32 , άρα 97-32 = 65.

  λ = -4x65 = -260

  97x2 = 194 , 260 - 194 = 66

  Άρα 260 ≡ 66 (mod 97)

  Επομένως 97 - 66 = 31.

  Άρα λ = 31.

  x3 = λ^2 - x1 - x2 = 31^2 -2-6 = 961-9=952

  Βρίσκω το 952 mod 97.

97x9 = 873

952-873 = 79

Άρα x3 = 79

y3 = λ(x1-x3) - y1 = 31(3-79) - 25 = 31x-76 - 25 = -2356-25 = -2381

Βρίσκω το 2381 mod 97:

97x24 = 2328

2381 - 2328 = 53

Άρα το -2381 είναι το 97-53 = 44.

Επομένως P3 = (79,44)

- P1 = P2 = (10,9)

  Επομένως παίρνω τον άλλον τύπο για λ:

  λ = (3x1^2 + A)/(2y1) = (3x10^2 + 5) / (2x9) = 305/18

  305 mod 97 = 14

  Βρίσκω τον αντίστροφο του 18 στο mod 97.

  97 = 18x5 + 7

  18 = 7x2 + 4

  7 = 4x1 + 3

  4 = 3x1 + 1

  3 = 3x1 + 0

  Από το τελευταίο μη μηδενικό υπόλοιπο:

  1 = 4-3x1

  Από το προηγούμενο εκφράζουμε το 3:

  3 = 7−4x1: 1 = 4−(7−4x1) = 4−7+4 = 2x4−7

  Ομοίως για το 4:

  4=18−7x2:1 = 2x(18−7x2)−7 = 2x18−4x7−7 = 2x18−5x7

  Και από το πρώτο για το 7:

  7 = 97−18x5:1 = 2x18−5x(97−18x5) = 2x18−5x97+25x18

  1 = (2+25)x18−5x97 = 27x18−5x97

  27·18 ≡ 1 (mod 97)

  Άρα ο αντίστροφος είναι 27.

  λ = 14x27 = 378 mod 97 = 87

  x3 = λ^2 - x1 - x2 = 87^2 - 10-10 = 7569 -20 = 7549 mod 97 = 80

  y3 = λ(x1-x3) - y1 = 80(10-80) - 9 = 87(-70) - 9 = -6090-9 = -6099

  6099 mod 97 = 85

  Άρα για το -6099 είναι 97-85 = 12

Άρα το P3 = (80,12)

Και επαλυθεύουμε προγραμματιστικά:

```
K = GF(97)
E = EllipticCurve(K, [0,0,0,5,1])

P1 = E(3,25)
P2 = E(6,21)
P3 = P1 + P2
print("P1 + P2 =", P3)
P1 = E(10,9)
P2 = E(10,9)
P3 = P1 + P2
print("P1 + P2 =", P3)
```

```
P1 + P2 = (79 : 44 : 1)
P1 + P2 = (80 : 12 : 1)
```

Exercise 3

Έστω $E : y^2 = x^3 + 3x + 2$ μια ελλειπτική καμπύλη που ορίζεται στο $\mathbf{Z}_7$:

- Υπολογίστε όλα τα σημεία της E στο $\mathbf{Z}_7$
- Ποια είναι η τάξη της ομάδας?
- Δοθέντος του στοιχείου $a = (2, 4)$, καθορίστε την τάξη του a. Είναι το a γεννήτορας?
- Βρείτε ένα σημείο της καμπύλης με τάξη διαφορετική από αυτήν της καμπύλης.

Solution

```
K = GF(7)
E = EllipticCurve(K, [0,0,0,3,2])

print(E)
print(E.points())
print(E.order())
a = E(2,4)
print(a.order())
print(a.order() == E.order())
for P in E.points():
    if P != E(0) and P.order() != a.order():
        print(P, P.order())
        break
```

```
Elliptic Curve defined by y^2 = x^3 + 3*x + 2 over Finite Field of size 7
[(0 : 1 : 0), (0 : 3 : 1), (0 : 4 : 1), (2 : 3 : 1), (2 : 4 : 1), (4 : 1 : 1), (4 : 6 : 1), (5 : 3 : 1), (5 : 4 : 1)]
9
9
True
(5 : 3 : 1) 3
```

Exercise 4

Υπολογίστε το κλειδί συνεδρίας στο πρωτόκολλο ECDH (ελλειπτικός DH). Το ιδιωτικό κλειδί σας είναι $a = 9$ και έχετε λάβει το δημόσιο κλειδί του Bob $B = (5, 2)$. Η ελλειπτική καμπύλη που χρησιμοποιήθηκε είναι $E : y^2 \equiv x^3 + x + 6 \bmod 11$.

- Να λύσετε την άσκηση στο χαρτί με τη βοήθεια του αλγορίθμου πρόσθεσης (διαφάνεια 22) και να επαληθεύσετε το αποτέλεσμα με ανάπτυξη κώδικα που θα συνοδεύει την λύση σας.
- Πόσες πράξεις απαιτήθηκαν συνολικά από τον αλγόριθμο διπλασίασε και πρόσθεσε; Πόσες από αυτές ήταν πράξεις πρόσθεσης και πόσες πράξεις διπλασιασμού?

Solution

- Αρχικοποίηση R = 0, P = (5,2)

  Bit 1:
  R = R + P = O + P = P = (5, 2)
  R = 2R (διπλασιασμός): R = 2 x (5, 2)
  → m = (3 x 5^2 + 1) / (2 x 2) = (3 x 25 + 1) / 4 = 76 / 4
  76 ≡ 10 (mod 11), 4^{-1} = 3 (αφού 4 x 3 = 12 ≡ 1)
  m = 10 x 3 = 30 ≡ 8
  x_3 = 8^2 − 2 x 5 = 64 − 10 = 54 ≡ 10
  y_3 = 8 x (5 − 10) − 2 = 8 x (−5) − 2
  −5 ≡ 6
  8 x 6 = 48 ≡ 4
  4 − 2 = 2
  → R = (10, 2)

  Bit 0:
  R = 2R (διπλασιασμός): R = 2 x (10, 2)
  m = (3 x 10^2 + 1) / (2 x 2) = (3 x 100 + 1) / 4 = 301 / 4
  301 mod 11 = 301 − 27 x 11 = 301 − 297 = 4
  4/4 = 1 (αφού 4 x 3 = 12 ≡ 1 ⇒ 4^{-1} = 3)
  m = 4 x 3 = 12 ≡ 1
  x_3 = 1^2 − 2 x 10 = 1 − 20 = −19 ≡ 3
  y_3 = 1 x (10 − 3) − 2 = 7 − 2 = 5
  → R = (3, 5)

  Bit 0:
  R = 2R (διπλασιασμός): R = 2 x (3, 5)
  m = (3 x 9 + 1) / 10 = (27 + 1) / 10 = 28 / 10
  28 mod 11 = 6
  10^{-1} mod 11 = 10
  m = 6 x 10 = 60 ≡ 5
  x_3 = 25 − 6 = 19 ≡ 8
  y_3 = 5 x (3 − 8) − 5 = 5 x (−5) − 5 = −25 − 5
  −25 ≡ −3 ≡ 8
  8 − 5 = 3
  → R = (8, 3)

  Bit 1:
  R = R + P (πρόσθεση): (8, 3) + (5, 2)
  m = (2 − 3) / (5 − 8) = (−1) / (−3) = 10 / 8
  10 x 8^{-1} = 10 x 7 = 70 ≡ 4

$x_3 = 16 - 8 - 5 = 3$

$y_3 = 4 \times (8 - 3) - 3 = 4 \times 5 - 3 = 20 - 3 = 17 \equiv 6$

$\rightarrow R = (3, 6)$

Αποτέλεσμα: S = (3,6)

```
K = GF(11)
E = EllipticCurve(K, [0,0,0,1,6])

B = E(5, 2)

a = 9

S = a * B
print("S = a * B =", S)
```

```
S = a * B = (3 : 6 : 1)
```

- Πέρα από την αρχικοποίηση συμβαίνουν 3 πολλαπλασιασμοί και 1 πρόσθεση, επομένως 4 πράξεις.