TUGAS KULIAH

ELLIPTIC CURVE

Disusun sebagai salah satu tugas

mata kuliah Kriptografi



Patricia Joanne

140810160065

Dikumpulkan tanggal

11 Oktober 2018

PROGRAM STUDI S-1 TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PADJADJARAN

2018

**SOAL**

Diberikan persamaan ellips y2 = x3 + x + 6 melewati z29.

Jika diketahui: p = 29, a = 1, dan b = 6.

Cari anggota yang menjadi QR dan berapa saja pembangkitnya?

**JAWAB**

Anggota yang menjadi QRnya adalah:

|  |  |  |  |
| --- | --- | --- | --- |
| x | 𝑅(𝑝−1)/2 ≡1 (𝑚𝑜𝑑 𝑝) | Ya/tidak | Anggota kuadrat residu |
| 0 | 0 | Tidak |  |
| 1 | 1 | Ya | 1 |
| 2 | 28 | Tidak |  |
| 3 | 28 | Tidak |  |
| 4 | 1 | Ya | 4 |
| 5 | 1 | Ya | 5 |
| 6 | 1 | Ya | 6 |
| 7 | 1 | Ya | 7 |
| 8 | 28 | Tidak |  |
| 9 | 1 | Ya | 9 |
| 10 | 28 | Tidak |  |
| 11 | 28 | Tidak |  |
| 12 | 28 | Tidak |  |
| 13 | 1 | Ya | 13 |
| 14 | 28 | Tidak |  |
| 15 | 28 | Tidak |  |
| 16 | 1 | Ya | 16 |
| 17 | 28 | Tidak |  |
| 18 | 28 | Tidak |  |
| 19 | 28 | Tidak |  |
| 20 | 1 | Ya | 20 |
| 21 | 28 | Tidak |  |
| 22 | 1 | Ya | 22 |
| 23 | 1 | Ya | 23 |
| 24 | 1 | Ya | 24 |
| 25 | 1 | Ya | 25 |
| 26 | 28 | Tidak |  |
| 27 | 28 | Tidak |  |
| 28 | 1 | Ya | 28 |

Jadi **anggota QRnya**: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

Titik yang melewati Z29 pada persamaan ellips y2 = x3 + x + 6 adalah:

|  |  |  |  |
| --- | --- | --- | --- |
| x | x3 + x + 6 mod 29 | Pada QR(29)? | y |
| 0 | 6 | Ya | (8,21) |
| 1 | 8 | Tidak |  |
| 2 | 16 | Ya | (4,25) |
| 3 | 7 | Ya | (6,23) |
| 4 | 16 | Ya | (4,25) |
| 5 | 20 | Ya | (7,22) |
| 6 | 25 | Ya | (5,24) |
| 7 | 8 | Tidak |  |
| 8 | 4 | Ya | (2,27) |
| 9 | 19 | Tidak |  |
| 10 | 1 | Ya | (1,28) |
| 11 | 14 | Tidak |  |
| 12 | 6 | Ya | (8,21) |
| 13 | 12 | Tidak |  |
| 14 | 9 | Ya | (3,26) |
| 15 | 3 | Tidak |  |
| 16 | 0 | Tidak |  |
| 17 | 6 | Ya | (8,21) |
| 18 | 27 | Tidak |  |
| 19 | 11 | Tidak |  |
| 20 | 22 | Tidak |  |
| 21 | 8 | Tidak |  |
| 22 | 4 | Ya | (2,27) |
| 23 | 16 | Ya | (4,25) |
| 24 | 21 | Tidak |  |
| 25 | 25 | Ya | (5,24) |
| 26 | 5 | Ya | (11,18) |
| 27 | 25 | Ya | (5,24) |
| 28 | 4 | Ya | (2,27) |

Jadi **pembangkitnya** adalah (6, 8), (6, 21), (16, 4), (16, 25), (7, 6), (7, 23), (20, 7), (20, 22), (25, 5), (25, 24), (4, 2), (4, 27), (1,1), (1, 28), (9, 3), (9, 26), (5, 11), (5, 18).