In my case: *x* = 169 = 10101001 and *y* = 278 = 100010110.

Q2.

Take multiplication

*x⋅ y* = 10101001⋅100010110

= 10101001x100010110

= 100010110

100010110

100010110

100010110

= 1010000001101110

Q3

Divide by 283

1010000001101110 / 100011011

100011011

10110111101110

100011011

111010001110

100011011

11001010110

100011011

1000111010

100011011

1100

In my case: *x* = 172 = 10101100 and *y* = 254 = 11111110.

Q2.

Take multiplication *x* ⋅ *y*  = 10101100 ⋅ 11111110

= 10101100⋅11111110

= 11111110

11111110

11111110

1111111000

110010011001000

Q3

Divide by 283

110010011001000/100011011

100011011

10001001001000

100011011

100101000

100011011

110011

Q4

Compute an inverse of 51 mod 283

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Extended Euclidean Algorithm | | | | | |  | |  | |  |
| *i* | *b =* | *a \** | *q* | + | *r* | *u* | | *v* | | *w*=*u*−*vq* | | |
| 0 | 100011011 | 110011 | 1111 |  | 11010 | 0 | | 1 | | 1111 | | |
| 1 | 110011 | 11010 | 10 |  | 111 | 1 | | 1111 | | 11111 | | |
| 2 | 11010 | 111 | 101 |  | 1 | 1111 | | 11111 | | 1101100 | | |

Line 0:

Quotient 100011011/110011

1000 110011

10000011

1100 110011

1001111

1110 110011

101001

1111 110011

11010

Line 1:

Quotient 110011/11010 *w*=*u*−*vq* = 1 − 1111⋅10

10 11010 = 1 + 11110

111 = 11111

Line 2:

Quotient 11010/111 *w*=*u*−*vq* = 1111−11111⋅101

100 111 *vq* = 11111⋅101

110 = 101⋅11111

101 111 = 11111

1 11111

1100011

1111

*w*=*u*−*vq* = 1101100

Q5. To check *a*⋅*a*−1 = 1 (mod 283)

110011⋅1101100

= 1101100

1101100

1101100

1101100

101111110100

100011011

1100101100

100011011

100011010