Extended Euclidean Algorithm and Fermat's Little Theorem

CSE 468 Fall 2025 – jedimaestro@asu.edu

gcd(888,54) == ???

$888 = 54 \times 16 + 24$

$54 = 24 \times 2 + 6$

$24 = 6 \times 4 + 0$

gcd(888,54) $==$ 6

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5
3	4	6	-4	21
4	1	4	5	-26
5	1	2	-9	47
6	2	0	23	-120

egcd(240,46) $==$ 2 in 6 steps

2 $==$ -9 $\times$ 240 $+$ 47 $\times$ 46

egcd(240,46) $==$???

i	q	r	s	t
0	—	240	1	0

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5
3	4	6	-4	21

egcd(240,46) $==$???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5
3	4	6	-4	21
4	1	4	5	-26

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5
3	4	6	-4	21
4	1	4	5	-26
5	1	2	-9	47

egcd(240,46) == ???

i	q	r	s	t
0	—	240	1	0
1	—	46	0	1
2	5	10	1	-5
3	4	6	-4	21
4	1	4	5	-26
5	1	2	-9	47
6	2	0	23	-120

egcd(240,46) $==$ 2

2 $==$ -9 $\times$ 240 $+$ 47 $\times$ 46

How to calculate $49^{-1} \bmod 239$?

Fermat's little theorem: $49^{-1} = 49^{239-2} = 49^{237} = 200 \pmod{239}$

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1
2	4	43	1	-4
3	1	6	-1	5
4	7	1	8	-39
5	6	0	-49	239

egcd(239,49) $==$ 1 in 5 steps

$1 == 8 \times 239 + \text{-}39 \times 49$

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1
2	4	43	1	-4

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1
2	4	43	1	-4
3	1	6	-1	5

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1
2	4	43	1	-4
3	1	6	-1	5
4	7	1	8	-39

egcd(239,49) == ???

i	q	r	s	t
0	—	239	1	0
1	—	49	0	1
2	4	43	1	-4
3	1	6	-1	5
4	7	1	8	-39
5	6	0	-49	239

egcd(239,49) $==1$

$1 == 8 \times 239 + \text{-39} \times 49$

$49^{-1} = 239 - 39 = 200$