

```

dat_gen(13)
We are working in F_13
~~~~~
Beginning r = 2
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 12
result = poly(1, [y], IntMod(13))
modulo = poly(y + 1, [y], IntMod(13))
result_temp = poly(6*y - 6, [y], IntMod(13))
-----
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 12
result = poly(1, [y], IntMod(13))
modulo = poly(y + 1, [y], IntMod(13))
result_temp = poly(6*y - 6, [y], IntMod(13))
-----
~~~~~
Beginning r = 3
Trying to calculate order of  $y - 1$  modulo  $y + 4$ 
-----
Order found!
order = 4
result = poly(1, [y], IntMod(13))
modulo = poly(y + 4, [y], IntMod(13))
result_temp = poly(5*y - 5, [y], IntMod(13))
-----
Trying to calculate order of  $y - 1$  modulo  $y - 3$ 
-----
Order found!
order = 12
result = poly(1, [y], IntMod(13))
modulo = poly(y - 3, [y], IntMod(13))
result_temp = poly(- 6*y + 6, [y], IntMod(13))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y + 4$ 
-----
Order found!
order = 12
result = poly(1, [y], IntMod(13))
modulo = poly(y + 4, [y], IntMod(13))
result_temp = poly(- 6*y^2 + 6, [y], IntMod(13))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y - 3$ 
-----
Order found!
order = 4
result = poly(1, [y], IntMod(13))
modulo = poly(y - 3, [y], IntMod(13))
result_temp = poly(5*y^2 - 5, [y], IntMod(13))
-----

```

```
dat_gen(17)
```

```
We are working in F_17
```

```
~~~~~
```

```
Beginning r = 2
```

```
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
```

```
-----
```

```
Order found!
```

```
order = 8
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y + 1, [y], IntMod(17))
```

```
result_temp = poly(8*y - 8, [y], IntMod(17))
```

```
-----
```

```
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
```

```
-----
```

```
Order found!
```

```
order = 8
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y + 1, [y], IntMod(17))
```

```
result_temp = poly(8*y - 8, [y], IntMod(17))
```

```
-----
```

```
~~~~~
```

```
Beginning r = 3
```

```
Trying to calculate order of  $y - 1$  modulo  $y^2 + y + 1$ 
```

```
-----
```

```
Order found!
```

```
order = 96
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y^2 + y + 1, [y], IntMod(17))
```

```
result_temp = poly(- 6*y^2 - 6*y - 5, [y], IntMod(17))
```

```
-----
```

```
Trying to calculate order of  $y^2 - 1$  modulo  $y^2 + y + 1$ 
```

```
-----
```

```
Order found!
```

```
order = 96
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y^2 + y + 1, [y], IntMod(17))
```

```
result_temp = poly(6*y^3 - 6*y^2 - 6*y + 6, [y], IntMod(17))
```

```
-----
```

```
~~~~~
```

```
Beginning r = 4
```

```
Trying to calculate order of  $y - 1$  modulo  $y + 4$ 
```

```
-----
```

```
Order found!
```

```
order = 16
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y + 4, [y], IntMod(17))
```

```
result_temp = poly(- 7*y + 7, [y], IntMod(17))
```

```
-----
```

```
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
```

```
-----
```

```
Order found!
```

```
order = 8
```

```
result = poly(1, [y], IntMod(17))
```

```
modulo = poly(y + 1, [y], IntMod(17))
```

```

result_temp = poly(8*y - 8, [y], IntMod(17))
-----
Trying to calculate order of  y - 1 modulo  y - 4
-----
Order found!
order = 16
result = poly(1, [y], IntMod(17))
modulo = poly(y - 4, [y], IntMod(17))
result_temp = poly(6*y - 6, [y], IntMod(17))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 4
-----
Order found!
order = 16
result = poly(1, [y], IntMod(17))
modulo = poly(y + 4, [y], IntMod(17))
result_temp = poly(6*y^3 - 6, [y], IntMod(17))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 1
-----
Order found!
order = 8
result = poly(1, [y], IntMod(17))
modulo = poly(y + 1, [y], IntMod(17))
result_temp = poly(8*y^3 - 8, [y], IntMod(17))
-----
Trying to calculate order of  y^3 - 1 modulo  y - 4
-----
Order found!
order = 16
result = poly(1, [y], IntMod(17))
modulo = poly(y - 4, [y], IntMod(17))
result_temp = poly(- 7*y^3 + 7, [y], IntMod(17))
-----

```

5

```

dat_gen(19)
We are working in F_19
~~~~~
Begining r = 2
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 9
result = poly(1, [y], IntMod(19))
modulo = poly(y + 1, [y], IntMod(19))
result_temp = poly(9*y - 9, [y], IntMod(19))
-----
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 9
result = poly(1, [y], IntMod(19))
modulo = poly(y + 1, [y], IntMod(19))
result_temp = poly(9*y - 9, [y], IntMod(19))
-----

```

```

~~~~~
Beginning r = 3
Trying to calculate order of  $y - 1$  modulo  $y - 7$ 
-----
Order found!
order = 9
result = poly(1, [y], IntMod(19))
modulo = poly(y - 7, [y], IntMod(19))
result_temp = poly(- 3*y + 3, [y], IntMod(19))
-----
Trying to calculate order of  $y - 1$  modulo  $y + 8$ 
-----
Order found!
order = 18
result = poly(1, [y], IntMod(19))
modulo = poly(y + 8, [y], IntMod(19))
result_temp = poly(2*y - 2, [y], IntMod(19))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y - 7$ 
-----
Order found!
order = 18
result = poly(1, [y], IntMod(19))
modulo = poly(y - 7, [y], IntMod(19))
result_temp = poly(2*y^2 - 2, [y], IntMod(19))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y + 8$ 
-----
Order found!
order = 9
result = poly(1, [y], IntMod(19))
modulo = poly(y + 8, [y], IntMod(19))
result_temp = poly(- 3*y^2 + 3, [y], IntMod(19))
-----
~~~~~
Beginning r = 4
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 9
result = poly(1, [y], IntMod(19))
modulo = poly(y + 1, [y], IntMod(19))
result_temp = poly(9*y - 9, [y], IntMod(19))
-----
Trying to calculate order of  $y - 1$  modulo  $y^2 + 1$ 
-----
Order found!
order = 72
result = poly(1, [y], IntMod(19))
modulo = poly(y^2 + 1, [y], IntMod(19))
result_temp = poly(9*y^2 - 9, [y], IntMod(19))
-----
Trying to calculate order of  $y^3 - 1$  modulo  $y + 1$ 
-----
Order found!
order = 9

```

```

result = poly(1, [y], IntMod(19))
modulo = poly(y + 1, [y], IntMod(19))
result_temp = poly(9*y^3 - 9, [y], IntMod(19))
-----
Trying to calculate order of  $y^3 - 1$  modulo  $y^2 + 1$ 
-----
Order found!
order = 72
result = poly(1, [y], IntMod(19))
modulo = poly(y^2 + 1, [y], IntMod(19))
result_temp = poly(- 9*y^4 + 9*y^3 + 9*y - 9, [y], IntMod(19))
-----
5

```

dat_gen(23)

We are working in F_{23}

```

~~~~~
Beginning r = 2
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 22
result = poly(1, [y], IntMod(23))
modulo = poly(y + 1, [y], IntMod(23))
result_temp = poly(11*y - 11, [y], IntMod(23))
-----
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 22
result = poly(1, [y], IntMod(23))
modulo = poly(y + 1, [y], IntMod(23))
result_temp = poly(11*y - 11, [y], IntMod(23))
-----
~~~~~
Beginning r = 3
Trying to calculate order of  $y - 1$  modulo  $y^2 + y + 1$ 
-----
Order found!
order = 132
result = poly(1, [y], IntMod(23))
modulo = poly(y^2 + y + 1, [y], IntMod(23))
result_temp = poly(- 8*y^2 - 8*y - 7, [y], IntMod(23))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y^2 + y + 1$ 
-----
Order found!
order = 132
result = poly(1, [y], IntMod(23))
modulo = poly(y^2 + y + 1, [y], IntMod(23))
result_temp = poly(8*y^3 - 8*y^2 - 8*y + 8, [y], IntMod(23))
-----
~~~~~
Beginning r = 4
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----

```

```

Order found!
order = 22
result = poly(1, [y], IntMod(23))
modulo = poly(y + 1, [y], IntMod(23))
result_temp = poly(11*y - 11, [y], IntMod(23))
-----
Trying to calculate order of  y - 1 modulo  y^2 + 1
-----
Order found!
order = 88
result = poly(1, [y], IntMod(23))
modulo = poly(y^2 + 1, [y], IntMod(23))
result_temp = poly(11*y^2 - 11, [y], IntMod(23))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 1
-----
Order found!
order = 22
result = poly(1, [y], IntMod(23))
modulo = poly(y + 1, [y], IntMod(23))
result_temp = poly(11*y^3 - 11, [y], IntMod(23))
-----
Trying to calculate order of  y^3 - 1 modulo  y^2 + 1
-----
Order found!
order = 88
result = poly(1, [y], IntMod(23))
modulo = poly(y^2 + 1, [y], IntMod(23))
result_temp = poly(- 11*y^4 + 11*y^3 + 11*y - 11, [y], IntMod(23))
-----
5

```

dat_gen(29)

We are working in F₂₉

```

~~~~~
Beginning r = 2
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y + 1, [y], IntMod(29))
result_temp = poly(14*y - 14, [y], IntMod(29))
-----
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y + 1, [y], IntMod(29))
result_temp = poly(14*y - 14, [y], IntMod(29))
-----
~~~~~
Beginning r = 3
Trying to calculate order of  y - 1 modulo  y^2 + y + 1
-----

```

```

Order found!
order = 168
result = poly(1, [y], IntMod(29))
modulo = poly(y^2 + y + 1, [y], IntMod(29))
result_temp = poly(- 10*y^2 - 10*y - 9, [y], IntMod(29))
-----
Trying to calculate order of  y^2 - 1 modulo  y^2 + y + 1
-----
Order found!
order = 168
result = poly(1, [y], IntMod(29))
modulo = poly(y^2 + y + 1, [y], IntMod(29))
result_temp = poly(10*y^3 - 10*y^2 - 10*y + 10, [y], IntMod(29))
-----
~~~~~
Beginning r = 4
Trying to calculate order of  y - 1 modulo  y + 12
-----
Order found!
order = 7
result = poly(1, [y], IntMod(29))
modulo = poly(y + 12, [y], IntMod(29))
result_temp = poly(- 9*y + 9, [y], IntMod(29))
-----
Trying to calculate order of  y - 1 modulo  y - 12
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y - 12, [y], IntMod(29))
result_temp = poly(8*y - 8, [y], IntMod(29))
-----
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y + 1, [y], IntMod(29))
result_temp = poly(14*y - 14, [y], IntMod(29))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 12
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y + 12, [y], IntMod(29))
result_temp = poly(8*y^3 - 8, [y], IntMod(29))
-----
Trying to calculate order of  y^3 - 1 modulo  y - 12
-----
Order found!
order = 7
result = poly(1, [y], IntMod(29))
modulo = poly(y - 12, [y], IntMod(29))
result_temp = poly(- 9*y^3 + 9, [y], IntMod(29))
-----

```

```

Trying to calculate order of  $y^3 - 1$  modulo  $y + 1$ 
-----
Order found!
order = 28
result = poly(1, [y], IntMod(29))
modulo = poly(y + 1, [y], IntMod(29))
result_temp = poly(14*y^3 - 14, [y], IntMod(29))
-----
5

```

```

dat_gen(31)
We are working in F_31
~~~~~
Begining r = 2
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 10
result = poly(1, [y], IntMod(31))
modulo = poly(y + 1, [y], IntMod(31))
result_temp = poly(15*y - 15, [y], IntMod(31))
-----
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 10
result = poly(1, [y], IntMod(31))
modulo = poly(y + 1, [y], IntMod(31))
result_temp = poly(15*y - 15, [y], IntMod(31))
-----
~~~~~
Begining r = 3
Trying to calculate order of  $y - 1$  modulo  $y + 6$ 
-----
Order found!
order = 30
result = poly(1, [y], IntMod(31))
modulo = poly(y + 6, [y], IntMod(31))
result_temp = poly(- 9*y + 9, [y], IntMod(31))
-----
Trying to calculate order of  $y - 1$  modulo  $y - 5$ 
-----
Order found!
order = 5
result = poly(1, [y], IntMod(31))
modulo = poly(y - 5, [y], IntMod(31))
result_temp = poly(8*y - 8, [y], IntMod(31))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y + 6$ 
-----
Order found!
order = 5
result = poly(1, [y], IntMod(31))
modulo = poly(y + 6, [y], IntMod(31))
result_temp = poly(8*y^2 - 8, [y], IntMod(31))
-----

```



```

Trying to calculate order of  $y^2 - 1$  modulo  $y - 5$ 
-----
Order found!
order = 30
result = poly(1, [y], IntMod(31))
modulo = poly(y - 5, [y], IntMod(31))
result_temp = poly(- 9*y^2 + 9, [y], IntMod(31))
-----
~~~~~
Beginning r = 4
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 10
result = poly(1, [y], IntMod(31))
modulo = poly(y + 1, [y], IntMod(31))
result_temp = poly(15*y - 15, [y], IntMod(31))
-----
Trying to calculate order of  $y - 1$  modulo  $y^2 + 1$ 
-----
Order found!
order = 40
result = poly(1, [y], IntMod(31))
modulo = poly(y^2 + 1, [y], IntMod(31))
result_temp = poly(15*y^2 - 15, [y], IntMod(31))
-----
Trying to calculate order of  $y^3 - 1$  modulo  $y + 1$ 
-----
Order found!
order = 10
result = poly(1, [y], IntMod(31))
modulo = poly(y + 1, [y], IntMod(31))
result_temp = poly(15*y^3 - 15, [y], IntMod(31))
-----
Trying to calculate order of  $y^3 - 1$  modulo  $y^2 + 1$ 
-----
Order found!
order = 40
result = poly(1, [y], IntMod(31))
modulo = poly(y^2 + 1, [y], IntMod(31))
result_temp = poly(- 15*y^4 + 15*y^3 + 15*y - 15, [y], IntMod(31))
-----
5

```

```

dat_gen(37)

```

```

We are working in F_37

```

```

~~~~~
Beginning r = 2
Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 36
result = poly(1, [y], IntMod(37))
modulo = poly(y + 1, [y], IntMod(37))
result_temp = poly(18*y - 18, [y], IntMod(37))
-----

```

```

Trying to calculate order of  $y - 1$  modulo  $y + 1$ 
-----
Order found!
order = 36
result = poly(1, [y], IntMod(37))
modulo = poly(y + 1, [y], IntMod(37))
result_temp = poly(18*y - 18, [y], IntMod(37))
-----
~~~~~
Beginning r = 3
Trying to calculate order of  $y - 1$  modulo  $y + 11$ 
-----
Order found!
order = 18
result = poly(1, [y], IntMod(37))
modulo = poly(y + 11, [y], IntMod(37))
result_temp = poly(3*y - 3, [y], IntMod(37))
-----
Trying to calculate order of  $y - 1$  modulo  $y - 10$ 
-----
Order found!
order = 9
result = poly(1, [y], IntMod(37))
modulo = poly(y - 10, [y], IntMod(37))
result_temp = poly(- 4*y + 4, [y], IntMod(37))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y + 11$ 
-----
Order found!
order = 9
result = poly(1, [y], IntMod(37))
modulo = poly(y + 11, [y], IntMod(37))
result_temp = poly(- 4*y^2 + 4, [y], IntMod(37))
-----
Trying to calculate order of  $y^2 - 1$  modulo  $y - 10$ 
-----
Order found!
order = 18
result = poly(1, [y], IntMod(37))
modulo = poly(y - 10, [y], IntMod(37))
result_temp = poly(3*y^2 - 3, [y], IntMod(37))
-----
~~~~~
Beginning r = 4
Trying to calculate order of  $y - 1$  modulo  $y + 6$ 
-----
Order found!
order = 18
result = poly(1, [y], IntMod(37))
modulo = poly(y + 6, [y], IntMod(37))
result_temp = poly(- 16*y + 16, [y], IntMod(37))
-----
Trying to calculate order of  $y - 1$  modulo  $y - 6$ 
-----
Order found!
order = 36

```

```

result = poly(1, [y], IntMod(37))
modulo = poly(y - 6, [y], IntMod(37))
result_temp = poly(15*y - 15, [y], IntMod(37))
-----
Trying to calculate order of  y - 1 modulo  y + 1
-----
Order found!
order = 36
result = poly(1, [y], IntMod(37))
modulo = poly(y + 1, [y], IntMod(37))
result_temp = poly(18*y - 18, [y], IntMod(37))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 6
-----
Order found!
order = 36
result = poly(1, [y], IntMod(37))
modulo = poly(y + 6, [y], IntMod(37))
result_temp = poly(15*y^3 - 15, [y], IntMod(37))
-----
Trying to calculate order of  y^3 - 1 modulo  y - 6
-----
Order found!
order = 18
result = poly(1, [y], IntMod(37))
modulo = poly(y - 6, [y], IntMod(37))
result_temp = poly(- 16*y^3 + 16, [y], IntMod(37))
-----
Trying to calculate order of  y^3 - 1 modulo  y + 1
-----
Order found!
order = 36
result = poly(1, [y], IntMod(37))
modulo = poly(y + 1, [y], IntMod(37))
result_temp = poly(18*y^3 - 18, [y], IntMod(37))
-----
~~~~~
Beginning r = 5
Trying to calculate order of  y - 1 modulo  y^4 + y^3 + y^2 + y + 1
-----
Order found!
order = 13680
result = poly(1, [y], IntMod(37))
modulo = poly(y^4 + y^3 + y^2 + y + 1, [y], IntMod(37))
result_temp = poly(- 15*y^4 - 15*y^3 - 15*y^2 - 15*y - 14, [y], IntMod(37))
-----
Trying to calculate order of  y^4 - 1 modulo  y^4 + y^3 + y^2 + y + 1
-----
Order found!
order = 13680
result = poly(1, [y], IntMod(37))
modulo = poly(y^4 + y^3 + y^2 + y + 1, [y], IntMod(37))
result_temp = poly(15*y^7 - 7*y^6 + 8*y^5 - 15*y^4 - 15*y^3 + 7*y^2 - 8*y
[y], IntMod(37))
-----

```

