

CSCI 124 and CSCI 297 - Discrete Structures II - Fall 2006
GCD and Exponentiation Practice Problems Solutions

Find the GCD of the following numbers using the euclidean algorithm. In cases where the numbers are relatively prime, find the inverse of the smaller number modulo the larger one. You may use a calculator to compute remainders.

1. 70, 120

(120, 70) (70, 50) (50, 20) (20, 10) (10, 0)

GCD=10

2. 168, 504

(504, 168) (168, 0)

GCD = 168

3. 180, 600

(600, 180) (180, 60) (60, 0)

GCD=60

4. 260, 455

(455, 260) (260, 195) (195, 65), (65, 0)

GCD=65

5. 60, 84

(84, 60) (60, 24) (24, 12) (12, 0)

GCD=12

6. 234, 470

(470, 234) (234, 2) (2, 0)

GCD=2

7. 480, 1800

(1800, 480) (480, 360) (360, 120) (120, 0)

GCD = 120

8. 84, 180

(180, 84) (84, 12) (12, 0)

GCD = 12

9. 120, 144

(144, 120) (120, 24) (24, 0)

GCD = 24

10. 292, 244

(292, 244) (244, 48) (48, 4) (4, 0)

GCD=4

11. 210, 861

(861, 210) (210, 21) (21, 0)

GCD=21

12. 64, 160

(160, 64) (64, 32) (32, 0)

GCD=32

13. 308, 504

(504, 308) (308, 196) (196, 112) (112, 84) (84, 28) (28, 0)

GCD=28

14. 1386, 1170

(1386, 1170) (1170, 216) (216, 90) (90, 36) (36, 18) (18, 0)

GCD=18

15. 1890, 450

(1890, 450) (450, 90) (90, 0)

GCD=90

16. 696, 432

(696, 432) (432, 264) (264, 168) (168, 96) (96, 72) (72, 24) (24, 0)

GCD = 24

17. 105, 231

(231, 105) (105, 21) (21, 0)

GCD=21

18. 273, 595

(595, 273) (273, 49) (49, 28) (28, 21) (21, 7) (7, 0)

GCD = 7

19. 910, 1155

(1155, 910) (910, 245) (245, 175) (175, 70) (70, 45) (45, 25) (25, 20) (20, 5) (5, 0)

GCD=5

Compute the following exponentiations using the fast algorithm, square and multiply.

20. $39^{215} \bmod 121$

$215 = 11010111$

i	b_i	z_{first}	z_{second}
7	1	1	39
6	1	69	29
5	0	115	115
4	1	36	73
3	0	5	5
2	1	25	7
1	1	49	96
0	1	20	54

$$39^{215} \bmod 121 = 54$$

$$21. 52^{21} \bmod 63$$

$$21 = 10101$$

i	b_i	z_{first}	z_{second}
4	1	1	52
3	0	58	58
2	1	25	40
1	0	25	25
0	1	58	55

$$52^{21} \bmod 63 = 55$$

$$22. 111^{67} \bmod 129$$

$$67 = 1000011$$

i	b_i	z_{first}	z_{second}
6	1	1	111
5	0	66	66
4	0	99	99
3	0	126	126
2	0	9	9
1	1	81	90
0	1	102	99

$$111^{67} \bmod 129 = 99$$