

CSCI 124 and CSCI 297 - Discrete Structures II - Fall 2006
Modular Inverse Practice Problems and Solutions

Find the modular inverse of the following numbers using the euclidean algorithm. You may use a calculator to compute remainders.

1. $12^{-1} \pmod{25}$

Answer:

a	b	q	s	t
25	12	2	1	-2
12	1	12	0	1
1	0			

$$25(1) - (12)(2) = 1 \Rightarrow 12^{-1} \pmod{25} = -2 \pmod{25} = 23 \pmod{25}$$

2. $17^{-1} \pmod{20}$

Answer:

a	b	q	s	t
20	17	1	6	-7
17	3	5	-1	6
3	2	1	1	-1
2	1	2	0	1
1	0			

$$20(6) + 17(-7) = 1 \Rightarrow -7 = 17^{-1} \pmod{20} = 13.$$

3. $9^{-1} \pmod{25}$

Answer:

a	b	q	s	t
25	9	2	4	-11
9	7	1	-3	4
7	2	3	1	-3
2	1	2	0	1
1	0			

$$25(4) + 9(-11) = 1 \Rightarrow -11 = 9^{-1} \pmod{25} = 14.$$

4. $15^{-1} \pmod{32}$

Answer:

a	b	q	s	t
32	15	2	-7	15
15	2	7	1	-7
2	1	2	0	1
1	0			

$$32(-7) + 15(15) = 1 \Rightarrow 15 = 15^{-1} \text{ MOD } 32.$$

$$5. 3^{-1} \text{ mod } 32$$

Answer:

a	b	q	s	t
32	3	10	-1	11
3	2	1	1	-1
2	1	2	0	1
1	0			

$$32(-1) + 3(11) = 1 \Rightarrow 11 = 3^{-1} \text{ MOD } 32.$$