2, 134 52

r_1	r_2	q	r

$134 = 52 \times 2 + 30$

$52 = 30 \times 1 + 22$

$30 = 22 \times 1 + 8$

$22 = 8 \times 2 + 6$

$8 = 6 \times 1 + 2$

$6 = 2 \times 3 + 0$

2 0

$\gcd(134, 52) = 2$

3,

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	134	52		1	0		0	1	
2	52	30	30	0	1	1	1	-2	-2
1	30	22	22	1	-1	-1	-2	3	3
1	22	8	8	-1	2	2	3	-5	-5
2	8	6	6	2	-5	-5	-5	13	13
1	6	2	2	-5	7	7	13	-18	-18
3	2	0	0	7	-26	-26	-18	67	67

$\gcd(134, 52) = 2, \; S = 7, \; t = -18$

INT202 Complexity of Algorithms

1. Exercises of modular arithmetic

a) 12+18 (mod 9) $= 30 \pmod 9 = 3$

b) 3*7(mod 11) $= 21 \pmod{11} = 10$

c) 103*42 (mod 17) $= [103 \pmod{17} \times 42 \pmod{17}] \pmod{17} = [1 \times 8] \pmod{17} = 8$

d) ~~7^2 (mod 13)~~ $7^2 \pmod{13} = (7 \bmod 13)^2 \bmod 13 = 49 \pmod{13} = 10$

e) ~~7^3 (mod 13)~~ $7^3 \pmod{13} = 7^2 \cdot 7 \pmod{13} = [7^2 \pmod{13} \times 7 \pmod{13}] \bmod 13 = 70 \pmod{13} = 5$

f) ~~7^4 (mod 13)~~ $7^4 \pmod{13} = 7^3 \cdot 7 \pmod{13} = 35 \pmod{13} = 9$

g) ~~7^5 (mod 13)~~ $7^5 \pmod{13} = 7^4 \cdot 7 \pmod{13} = 63 \pmod{13} = 11$

h) ~~7^6 (mod 13)~~ $7^6 \pmod{13} = 7^5 \cdot 7 \pmod{13} = 77 \pmod{13} = 12$

2. Use Euclidean Algorithm to find GCD of 134 and 52

3. Given two integers 134 and 52, find two integers, s and t, such that s*a+t*b=gcd(a,b)

4. Find the multiplicative inverse of 8 mod 11.

5. Let n > ~~0~~ 0 be an integer. Prove that n is divisible by 9 if and only if the sum of its digits is divisible by 9.

6. Let us consider Z_{28} the set of integers modulo 28.

   1) Give the necessary and sufficient condition required for an element of Z_{28} to have an inverse in Z_{28}.

   2) Determine all the elements of Z_{28} that have an inverse in Z_{28}.

   3) Evaluate φ(28) wherein φ is the Euler totient function.

   4) Evaluate 4^{-1} and 5^{-1} if they exist.

4,

q	r_1	r_2	r	t_1	t_2	t
	11	8		0	1	
1	8	3	3	1	-1	-1
2	3	2	2	-1	3	3
1	2	1	1	3	-4	-4
2	1	0	0	-4	11	11

$8^{-1} = t_1 = -4 \notin Z_{11}^*$,

so, $-4 + 11 = 7$

5, $n \bmod 9 = (n_k \times 10^k + \cdots + n_1 \times 10^1 + n_0 \times 10^0) \bmod 9$

$= [(n_k \times 10^k) \bmod 9 + \cdots + (n_0 \times 10^0) \bmod 9] \bmod 9$

$= \{[(n_k \bmod 9) \times (10^k \bmod 9)] \bmod 9 + \cdots + [(n_0 \bmod 9) \times (10^0 \bmod 9)] \bmod 9\} \bmod 9$

$= \{(n_k \bmod 9) \bmod 9 + \cdots + (n_0 \bmod 9) \bmod 9\} \bmod 9$

$= (n_k + \cdots + n_0) \bmod 9 \bmod 9 \bmod 9 = (n_k + \cdots + n_0) \bmod 9$