Network and Information Security
Lecture 3

B.Tech. Computer Engineering
Sem. VI.

M. T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

- Euclidian Algorithm for finding GCD of two positive integers
- Fact 1: gcd(a,0) = a
- Fact 2: gcd(a,b) = gcd(b,r) where r is the remainder of dividing a by b
- Find gcd(36,10)

- gcd(36,10)
- =gcd(10,6)
- =gcd(6,4)
- =gcd(4,2)
- =gcd(2,0)
- =2

Euclidian algorithm

```
r1  =   a;            // Initialization
r2  =   b;
while(r2 > 0)
 {
     q =  r1/r2;
     r   = r1 – q x r2;
     r1  = r2;
     r2 = r;
}
gcd(a,b) =r1;
```

Example 4

Find the greatest common divisor of 2740 and 1760.

r1=2740, r2=1760

q	r1	r2	r
1	2740	1760	980

Example 4

Find the greatest common divisor of 2740 and 1760.

r1=2740, r2=1760

q	r1	r2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	20

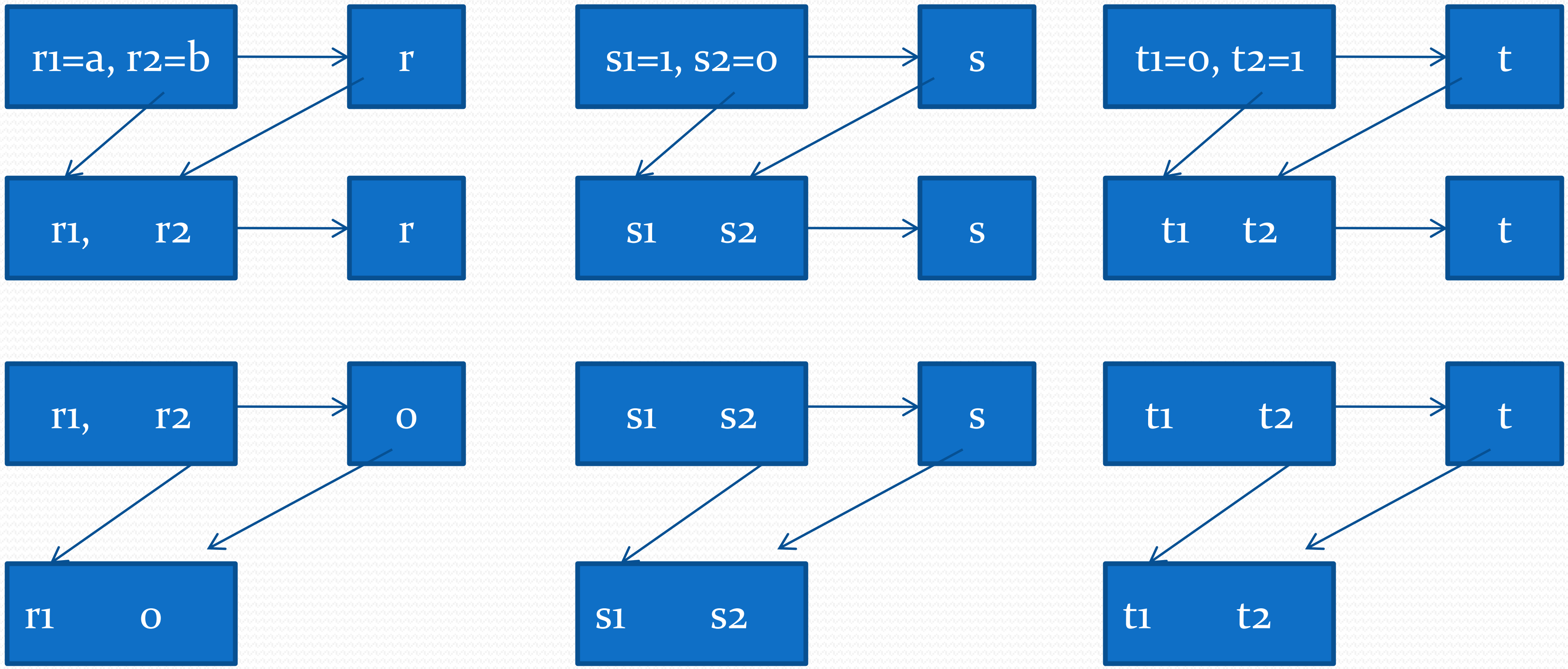
The Extended Euclidean Algorithm

- Given two integers, a and b, we often need to find other two integers, s and t such that
- s x a + t x b = gcd(a,b)
- Example 5
- Given a=161 and b=28, find gcd(161,28) and the values of s and t.

- r1=a, r2=b, s1=1, s2=0, t1=0, t2=1
- For r1, r2,

  q= r1/r2; (quotient)

  r = r1/r2; (reminder)



r1=a, r2=b → r

r1, r2 → r

s1=1, s2=0 → s

s1 s2 → s

t1=0, t2=1 → t

t1 t2 → t

r1, r2 → 0

r1 0

s1 s2 → s

s1 s2

t1 t2 → t

t1 t2

gcd(a,b)=r1

s=s1 s=s1 -qx s2

t=t1 t=t1 – q x t2

- r= r1- q x r2, s= s1 – q x s2, t= t1 – q x t2

q	r1	r2	r	s1	s2	s	t1	t2	t
5	161	28	21	1	0	1	0	1	-5
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

- $r = r1 - q \times r2$, $s = s1 - q \times s2$, $t = t1 - q \times t2$

q	r1	r2	r	s1	s2	s	t1	t2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

r1=7, s=-1, t=6

s x a + t x b = (-1) x 161 + (6) x 28

= -161 + 168

= 7 = gcd(161,28)

Algorithm:

```
r1=a, r2=b, s1=1, s2=0, t1=0, t2=1
while( r2>0)
{
    q = r1/r2;
    r = r1 – q x r2;
    r1 = r2;
    r2= r;
    s= s1 – q x s2;
    s1 = s2;
    s2= s;
    t = t1 – q x t2;
    t1 = t2;
    t2 = t;
}
gcd(a,b) =r1; s=s1; t= t1;
```