Lab 2/17/12

Chapter 4

Euclid's Algorithm

gcd(a, b) = gcd(b, a(mod b))

i.e.

gcd(12, 9) = gcd(9, 12(mod9))

= gcd(9, 3)

= gcd(3, 0)

= 3

Example program:

Input: a, b (a≥b); Output: gcd(a,b)

Iterative:

```
while(r != 0)
{
        r = a%b
        a = b
}
```

Recursive:

```
gcd(a, b)
{
        if (b == 0)
                return 0;
        else
                gcd(b, a%b)
}
```

Examples:

d = gcd(m,n)

d = mx + ny

m = 62; n = 40; find d:

65 = 40*1 + 25

40 = 25*1 + 15

25 = 15*1 + 10

15 = 10*1 + 5

10 = 5*2 + 0

return 5

5 = 65x + 40y; find x, y:

5 = 15 – 10*1

= 15 – (25-15)*1

= 2*15 – 25

= 2*(40-25) – 25

= 2*40 – 3*25

= 2*40 – 3(65-40)

5 = 5*40 + (-3)*65

if 15 = 65x + 40y

3(5) = 3(5*40 + (-3)*65)

Extended Euclid's Algorithm(Theorem 4.3 from the book)

Let a, b, c, x, y ∈ $\mathbb{Z}$

ax + by = c

gcd(a, b) | c

85x + 30y = 15; find x, y:

$r_2 = r_0 - q_1r_1$; $r_3 = r_1 - q_2r_2$….etc

$s_2 = s_0 - q_1s_1$…etc

$t_2 = t_0 - q_1t_1$…etc

	$r_0 = 85$	$s_0 = 1$	$t_0 = 0$
$q_1 = 2$	$r_1 = 30$	$s_1 = 0$	$t_1 = 1$
$q_2 = 1$	$r_2 = 25$	$s_2 = 1$	$t_2 = -2$
$q_3 = 5$	**$r_3 = 5$**	**$s_3 = -1$**	**$t_3 = 3$**

Using the equation $as_i + bt_i = r_i$

Find the row where you have q_3:

$85s_3 + 30t_3 = r_3$

$85(-1) + 30(3) = 5$

$85(-1*3) + 30(3*3) = 5*3$

$85(-3) + 30(9) = 15$

$x = -3, y = 9$