EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 4W-S

1. **Euclid's Algorithm** Euclid's algorithm is a fast algorithm for computing the greatest common divisor of two integers. Here is an example. To compute $gcd(16,10)$:

$$16 = 10 \times 1 + 6 \quad (1)$$
$$10 = 6 \times 1 + 4 \quad \text{(notice this is a recursive call of } gcd(10,6)) \quad (2)$$
$$6 = 4 \times 1 + 2 \quad \text{(notice this is a recursive call of } gcd(6,4)) \quad (3)$$
$$4 = 2 \times 2 + 0 \quad \text{(notice this is a recursive call of } gcd(4,2)) \quad (4)$$

So $gcd(16,10) = 2$, the last non-zero remainder. We can also back substitute to find x, y such that

$$2 = 16x + 10y = gcd(16,10).$$

Here is how:

Rearrange (3) to get an expression for gcd(16,10): $2 = 6 - 4 \times 1$

rearrange (2) to get $4 = (10 - 6 \times 1)$

and substitute: $2 = 6 - (10 - 6 \times 1) \times 1$

simplify: $2 = -10 + 6 \times 2$

now rearrange (1) to get $6 = (16 - 10 \times 1)$ and substitute: $2 = -10 + (16 - 10 \times 1) \times 2$

simplify: $2 = 16 \times 2 - 10 \times 3$

So $x = 2$ and $y = -3$.

Run Euclid's algorithm for to determine the greatest common divisor for the following:

1. $a = 8, b = 22$

2. $a = 13, b = 21$

3. $a = 140, b = 38$