Euclidean Algorithm

1. Motivation

   (a) Number Systems:
   $\mathbb{N}$ Natural Numbers :={0,1,2,3, ...} ← This interests us
   $\mathbb{Z}$ Integers :={... ,-2,-1,0,1,2, ...}
   $\mathbb{R}$ Reals

   (b) Prime Numbers: A prime number is one that cannot be factored any further. All numbers can be factorized uniquely into the product of powers of primes. Ex: $12 = 2^2 \times 3^1$ and in general $N = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \cdots \times p_k^{e_k}$ where p_i is a prime and e_i is the power of that prime. Prime numbers are the building blocks of all whole numbers, like atoms are the building blocks of all matter.

   What are some primes?:

   What is the prime factorization of 180?:

   (c) Greatest Common Divisor (GCD): This is the greatest number that will divide both of two given numbers. Ex: $12 = 2^2 \times 3^1$ and $18 = 2^1 \times 3^2$ and gcd(12,18) $= 2^1 \times 3^1$ since this shows up in both factorizations.

2. Euclidean Algorithm: Given two whole numbers, a and b where a $\geq$ b, this algorithm will produce the gcd(a,b).

$$a = b \times q_1 + r_1$$

$$b = r_1 \times q_2 + r_2$$

$$r_1 = r_2 \times q_3 + r_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \times q_{n-1} + r_n$$

$$r_{n-1} = r_n \times q_n$$

where $0 \leq r_i < r_{i-1}$

and r_n = gcd(a,b)

Ex: Find gcd(252,198):

$$252 = 1 \times 198 + 54$$

$$198 = 3 \times 54 + 36$$

$$54 = 1 \times 36 + 18$$

$$36 = 2 \times 18$$

$$\Rightarrow gcd(252, 198) = 18$$

3. Homework:

   (a) List the first 15 prime numbers:

   (b) Factorize 836:

   (c) Factorize 1092:

   (d) Use Euclidean Algorithm and find gcd(55,34):

   (e) Use Euclidean Algorithm and find gcd(102,222):

   (f) Use Euclidean Algorithm and find gcd(51,87):