18.095 **IAP 2016**
Problem Set 1 Part 1 **Due: 01/8/2016**

Problem 1. Let a and b be positive integers. The *Euclidean quotient* is the greatest integer less than a/b, which we denote $\lfloor a/b \rfloor$. The *Euclidean remainder* is the integer $r = a - qb$. The nonnegative integers q and r evidently satisfy

$$a = qb + r \qquad \text{and} \qquad r \equiv a \bmod b.$$

The *greatest common divisor* $\gcd(a, b)$ is the largest integer that divides both a and b.

(a) Prove that $0 \le r < b$ and $\gcd(a, b) = \gcd(b, r)$.

Assuming $a \ge b$ (swap them if not), this gives an algorithm to compute $\gcd(a, b)$.

1. While $b > 0$:
   a. Compute $q = \lfloor a/b \rfloor$ and $r = a - qb$.
   b. Replace a by b and then replace b by r.
2. Output a.

This is known as the *Euclidean algorithm*.

(b) Use the Euclidean algorithm to compute $\gcd(n, 9699690)$, where n is your MIT ID. In your answer list the sequence of Euclidean remainders r computed by the algorithm.

(c) Prove that the length of the sequence of remainders is bounded by $2 \log_2 \max(a, b)$.

The *extended Euclidean algorithm* augments the Euclidean algorithm as follows.

1. Let
$$R = \begin{bmatrix} a \\ b \end{bmatrix}, \quad S = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad T = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$
and let R_1 and R_2 denote the top and bottom entries of R, respectively.
2. While $R_2 > 0$:
   a. Compute $q = \lfloor R_1/R_2 \rfloor$ and let $Q = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix}$.
   b. Replace R by QR, replace S by QS, and replace T by QT.
3. Output R, S, T.

(d) Prove that after each iteration of step 2 of the extended Euclidean algorithm we have

$$R = aS + bT.$$

Conclude that $\gcd(a, b)$ is an integer linear combination of a and b. More precisely, $\gcd(a, b) = as + bt$, where s and t are the top entries in the final outputs S and T.

(e) Prove that every integer linear combination of a and b is a multiple of $\gcd(a, b)$. Conclude that $\gcd(a, b)$ is the unique positive integer that is both a divisor of a and b, and an integer linear combination of a and b.

(f) Let $p = 10^9 + 7$ and let n be your MIT ID. Use the extended Euclidean algorithm to compute the inverse of n modulo p, that is, an integer m such that $mn = kp + 1$ for some integer k (hint: note that 1 must be an integer linear combination of p and n).