Math 580/780I Notes 4

The Euclidean Algorithm:

• Review. In grade school, we learned to compute the greatest common divisor of two numbers by factoring the numbers. For example, $(77, 119) = (7 \times 11, 7 \times 17) = 7$. Now, try $(3073531, 304313)$ this way. What's the moral?

• **Theorem 7 (The Euclidean Algorithm).** *Let a and b be positive integers. Set $r_0 = a$ and $r_1 = b$. Define $r_2, r_3, \ldots, r_{n+1}$ and n by the equations*

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 && \text{with } 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 && \text{with } 0 < r_3 < r_2 \\ &\vdots && \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n && \text{with } 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1} && \text{with } r_{n+1} = 0 \end{aligned}$$

where each q_j and r_j is in $\mathbb{Z}$. Then $(a, b) = r_n$.

• Back to examples. Compute $(3073531, 304313)$ this way. Not to be misleading, compute $(2117, 3219)$ using the Euclidean Algorithm.

• **Proof:** Let $d = (a, b)$. Then one obtains $d | r_j$ for $0 \le j \le n + 1$ inductively, and hence $d | r_n$. Thus, $d \le r_n$ (since $r_n > 0$). Similarly, one obtains r_n divides r_{n-j} for $1 \le j \le n$. It follows that r_n is a divisor of a and b. By the definition of (a, b), we deduce $r_n = (a, b)$.

• Solutions to $ax + by = m$. From Theorem 5, we need only consider $m = k(a, b)$. One can find solutions when $k = 1$ by making use of the Euclidean Algorithm (backwards). Show how the complete set of solutions for general m can be obtained from this. Also, mention the connection with the simple continued fraction for a/b.

• **Example.** Solve $3219x + 2117y = 29$. The solutions are the (x, y) of the form

$$x = 25 - t \times \frac{2117}{29} \quad \text{and} \quad y = -38 + t \times \frac{3219}{29} \qquad \text{for } t \in \mathbb{Z}.$$

• We mention the following just to give an idea of how many steps it takes to compute the greatest common divisor using the Euclidean Algorithm.

Theorem 8. *Let a and b be positive integers. The Euclidean Algorithm for calculating (a, b) takes $\le 2(\lfloor \log_2 b \rfloor + 1)$ steps (i.e, divisions), where $\lfloor x \rfloor$ denotes the largest integer $\le x$.*

Homework:

(1) For each of the following, calculate $\gcd(a, b)$ and find a pair of integers x and y for which $ax + by = \gcd(a, b)$.

(a) $a = 289$ and $b = 1003$

(b) $a = 3569$ and $b = 1333$

(2) Find the complete set of integer solutions in x and y to

$$401x + 2010y = 1.$$

(3) Find the complete set of integer solutions in x and y to

$$401x + 2010y = 43.$$

(4) Explain why the greatest common divisor of 9999999999 and 9999999993 is 3. (You should be able to give a short answer for this one.)