Lecture 21

Instructor's Comments: This should be the lecture you give on the day of the midterm. It is a very light computational lecture.

Definition: For $x \in \mathbb{R}$, define the floor function $\lfloor x \rfloor$ to be the greatest integers less than or equal to x.

Example:

(i) $\lfloor 2.5 \rfloor = 2 = \lfloor 2 \rfloor$

(ii) $\lfloor \pi \rfloor = 3$

(iii) $\lfloor 0 \rfloor = 0$

(iv) $\lfloor -2.5 \rfloor = -3$

Example: Find $\gcd(56, 35)$

$$\begin{aligned}
56(1) + 35(0) &= 56 && \text{Eqn [1]} \\
56(0) + 35(1) &= 35 && \text{Eqn [2]} \\
56(1) + 35(-1) &= 21 && q_1 = \lfloor \tfrac{56}{35} \rfloor = 1 \text{ Eqn [3]} = [1] - q_1[2] \\
56(-1) + 35(2) &= 14 && q_2 = \lfloor \tfrac{35}{21} \rfloor = 1 \text{ Eqn [4]} = [2] - q_2[3] \\
56(2) + 35(-3) &= 7 && q_3 = \lfloor \tfrac{21}{14} \rfloor = 1 \text{ Eqn [5]} = [3] - q_3[4] \\
56(-5) + 35(8) &= 0 && q_4 = \lfloor \tfrac{14}{7} \rfloor = 2 \text{ Eqn [6]} = [4] - q_4[5]
\end{aligned}$$

Therefore $\gcd(56, 35) = 7 = 56(2) + 35(-3)$. This process gives rise to the Extended Euclidean Algorithm.

Example: Find $x, y \in \mathbb{Z}$ such that $506x + 391y = \gcd(506, 391)$.

x	y	r	q
1	0	506	0
0	1	391	0
1	-1	115	$\lfloor \frac{506}{391} \rfloor = 1$
-3	4	46	$\lfloor \frac{391}{115} \rfloor = 3$
7	-9	23	$\lfloor \frac{115}{46} \rfloor = 2$
-17	22	0	$\lfloor \frac{46}{23} \rfloor = 2$

Therefore, $506(7) + 391(-9) = 23 = \gcd(506, 391)$. ∎

Note: This process is known as the Extended Euclidean Algorithm.

Handout or Document Camera or Class Exercise

Use the Extended Euclidean Algorithm to find integers x and y such that $408x+170y = \gcd(408, 170)$.

Solution:

x	y	r	q
1	0	408	0
0	1	170	0
1	-2	68	$\lfloor \frac{408}{170} \rfloor = 2$
-2	5	34	$\lfloor \frac{170}{68} \rfloor = 2$
5	-12	0	$\lfloor \frac{68}{34} \rfloor = 2$

Therefore, $408(-2) + 170(5) = 34 = \gcd(408, 170)$. ■

Note:

(i) Bézout's Lemma is the Extended Euclidean Algorithm in the textbook.

(ii) With $\gcd(a, b)$, what if

1. $b > a$? Then swap a and b. This works since $\gcd(a, b) = \gcd(b, a)$.
2. $a < 0$ or $b < 0$? Solution is to make all the terms positive. This works since

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

(iii) In practice, one can accomplish these goals by changing the headings then accounting for this in the final steps.

Handout or Document Camera or Class Exercise

Use the Extended Euclidean Algorithm to find integers x and y such that $399x - 2145y = \gcd(399, -2145)$.

Solution:

x	$-y$	r	q
0	1	2145	0
1	0	399	0
-5	1	150	$\lfloor \frac{2145}{399} \rfloor = 5$
11	-2	99	$\lfloor \frac{399}{150} \rfloor = 2$
-16	3	51	$\lfloor \frac{150}{99} \rfloor = 1$
27	-5	48	$\lfloor \frac{99}{51} \rfloor = 1$
-43	8	3	$\lfloor \frac{51}{48} \rfloor = 1$
27-(16)(-43)	-5-16(8)	0	$\lfloor \frac{48}{3} \rfloor = 1$

Therefore, $x = -43$, $-y = 8$ and so $y = -8$, $\gcd(399, -2145) = 3$. Hence

$$399(-43) - 2145(-8) = 3 = \gcd(399, -2145)$$