Math 4400 Homework 2

Due: Wednesday, May 31st, 2017 (Quiz on Friday)

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. Let $a_1, \dots, a_n$ be nonzero integers, with $n \geq 2$. We define the greatest common denominator of this n-tuple recursively:
$$\gcd(a_1, \dots, a_n) = \gcd\left(\gcd(a_1, \dots, a_{n-1}), a_n\right)$$
and $\gcd(a_1, a_2)$ is the usual gcd. Prove the following generalization of Bezout's lemma: the equation
$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$
has a solution with $x_1, \dots, x_n \in \mathbb{Z}$ if and only if b is divisible by $\gcd(x_1, \dots, x_n)$.

Solution: (The problem statement should say $\gcd(a_1, \dots, a_n)$, not $\gcd(x_1, \dots, x_n)$)

We proceed by induction on n. The base case, $n = 2$, is just Bezout's lemma. Now let $k \geq 2$ and suppose that, for arbitrary integers $a_1, a_2, \dots, a_k, b \in \mathbb{Z}$, the equation $a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$ has an integer solution if and only if $\gcd(a_1, \dots, a_k) \mid b$. Let $a_1, \dots, a_{k+1}, b \in \mathbb{Z}$ be arbitrary. We wish to show that $a_1x_1 + \cdots + a_{k+1}x_{k+1} = b$ has a solution if and only if $\gcd\left(a_1, \dots, a_{k+1}\right) \mid b$.

So, suppose $a_1x_1 + \cdots + a_{k+1}x_{k+1} = b$ has a solution $x_1^0, x_2^0, \cdots, x_{k+1}^0$. By definition,
$$\gcd(a_1, \cdots, a_{k+1}) = \gcd(\gcd(a_1, \cdots, a_k), a_{k+1})$$
which means $\gcd(a_1, \cdots, a_{k+1})$ divides $\gcd(a_1, \cdots, a_k)$ and a_{k+1}. By induction, $\gcd(a_1, \cdots, a_k)$ divides $a_1x_1^0 + \cdots + a_kx_k^0$, and so
$$\gcd(a_1, \cdots, a_{k+1}) \mid a_1x_1^0 + \cdots + a_kx_k^0$$
but since $\gcd(a_1, \cdots, a_{k+1}) \mid a_{k+1}$, we see that
$$\gcd(a_1, \cdots, a_{k+1}) \mid a_1x_1^0 + \cdots + a_{k+1}x_{k+1}^0$$
and thus $\gcd(a_1, \cdots, a_{k+1}) \mid b$, as desired.

Conversely, suppose that $\gcd(a_1, \cdots, a_{k+1}) \mid b$. Then by Bezout's lemma, there exist some $x, y \in \mathbb{Z}$ such that
$$\gcd(a_1, \cdots, a_k)x + a_{k+1}y = b.$$
By the induction hypothesis, since $\gcd(a_1, \cdots, a_k)$ divides $\gcd(a_1, \cdots, a_k)x$, there exist some $x_1^0, \cdots, x_k^0$ in $\mathbb{Z}$ such that $a_1x_1^0 + \cdots + a_kx_k^0 = \gcd(a_1, \cdots, a_k)x$. But then
$$a_1x_1^0 + \cdots + a_kx_k^0 + a_{k+1}y = b,$$
as desired.

2. Prove the theorem we mentioned in class about how to get continued fractions expansions from the Euclidean algorithm. Namely, suppose $a, b \in \mathbb{Z}$ are integers with $a, b \geq 1$. Suppose the Euclidean

algorithm applied to a and b goes as

$$\begin{aligned} b =& q_1 a + r_1 \\ a =& q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} =& q_{n+1} r_n \end{aligned}$$

for some $n \geq 0$. Show that $\frac{b}{a} = [q_1; q_2, \ldots, q_{n+1}]$

Solution: We proceed by induction on n. If $n = 0$, then the Euclidean algorithm is just one step: $b = q_1 a$, so $b/a = q_1$, whose continued fraction expansion is just $[q_1]$, as desired.

Now suppose the result is true for $n = k$. We wish to prove the result when $n = k + 1$. So suppose that $a, b \in \mathbb{Z}$ and that the Euclidean algorithm has $k + 2$ steps:

$$\begin{aligned} b =& q_1 a + r_1 \\ a =& q_2 r_1 + r_2 \\ &\vdots \\ r_k =& q_{k+2} r_{k+1} \end{aligned}$$

By the induction hypothesis, we know that $a/r_1 = [q_2; q_3, \cdots, q_{k+2}]$. Further, $b/a = q_1 + r_1/a$. But this means that $b/a = q_1 + 1/[q_2; q_3, \cdots, q_{k+2}] = [q_1; q_2, \cdots, q_{k+2}]$, as desired.

3. (a) Find all integer solutions of $13853x + 6951y = \gcd(13853, 6951)$.

Solution: We start by performing the Euclidean algorithm:

$$\begin{aligned} 13853 &= 1 \cdot 6951 + 6902 \\ 6951 &= 1 \cdot 6902 + 49 \\ 6902 &= 140 \cdot 49 + 42 \\ 49 &= 1 \cdot 42 + 7 \\ 42 &= 6 \cdot 7 \end{aligned}$$

So $\gcd(13853, 6951) = 7$. From the work we did for the Euclidean algorithm, we get an initial solution to the equation:

$$\begin{aligned} 49 - 42 &= 7 \\ 49 - (6902 - 140 \cdot 49) &= 7 \\ 141 \cdot 49 - 6902 &= 7 \\ 141 \cdot (6951 - 6902) - 6902 &= 7 \\ 141 \cdot 6951 - 142 \cdot 6902 &= 7 \\ 141 \cdot 6951 - 142 \cdot (13853 - 6951) &= 7 \\ 283 \cdot 6951 - 142 \cdot 13853 &= 7 \end{aligned}$$

So we get an initial solution $x_0 = -142$ and $y_0 = 283$. Thus every solution to the equation is given by

$$(x, y) = \left(-142 + k\frac{6951}{7}, 283 - k\frac{13853}{7}\right), k \in \mathbb{Z}$$

We simplify: the set of solutions is

$$\{(-142 + 993k, 283 - 1979k) \mid k \in \mathbb{Z}\}$$

(b) Show that $427x + 259y = 13$ has no integer solutions

Solution: By the Euclidean algorithm, $\gcd(427, 259) = 7$

$$\begin{aligned}
427 &= 1 \cdot 259 + 168 \\
259 &= 1 \cdot 168 + 91 \\
168 &= 1 \cdot 91 + 77 \\
91 &= 1 \cdot 77 + 14 \\
77 &= 5 \cdot 14 + 7 \\
14 &= 2 \cdot 7
\end{aligned}$$

But 7 does not divide 13, so by Bezout's lemma, $427x + 259y = 13$ has no integer solutions.

4. Suppose $a, b, c \in \mathbb{Z}$, $a \neq 0$. Suppose also that $c \mid a$ and $c \mid b$. Show that $c \mid \gcd(a, b)$.

Solution: By Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b)$$

Since $c \mid a$ and $c \mid b$, we see that c divides the left hand side above. But that means c divides $\gcd(a, b)$. (We know that the greatest common divisor of a and b exists because $a \neq 0$)

5. Suppose $\gcd(a, b) = 1$, $a \mid c$, and $b \mid c$. Show $ab \mid c$.

Solution: By definition, there exist $j, k \in \mathbb{Z}$ such that $aj = c$ and $bk = c$. By Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Then $axc + byc = c$. But then $axbk + byaj = c$. We see that ab divides the left-hand side, and so ab must divide c.

6. Suppose $\gcd(a, b) = 1$ and $a \mid bc$. Show that $a \mid c$.

Solution: We can factor a, b, and c into primes:

$$\begin{aligned}
a &= p_1 p_2 \cdots p_s \\
b &= q_1 q_2 \cdots q_t \\
c &= r_1 r_2 \cdots r_u
\end{aligned}$$

and so

$$bc = q_1 \cdots q_t r_1 \cdots r_u$$

First, let's discuss the idea of the proof: since $a \mid bc$, we have $p_s \mid bc$. Since p_s is prime, this means p_s divides one of the q's or one of the r's. But since $\gcd(a, b) = 1$, we can't have $p_s \mid q_i$ for any i. Thus

$p_s \mid r_j$ for some j, which means $p_s = r_j$ for some j. We can relabel the r's so that $p_s = r_u$. Now we have $p_1 p_2 \cdots p_{s-1} \mid q_1 \cdots q_t r_1 \cdots r_{u-1}$. We can repeat the process above to show that $p_{s-1} = r_{u-1}$, $p_{s-2} = r_{u-2}$, and so on, until we get

$$r_1 r_2 \cdots r_{u-s} a = r_1 r_2 \cdots r_{u-s} p_1 p_2 \cdots p_s = r_1 r_2 \cdots r_u = c$$

Note how I wrote "we can repeat the process above to show…"; this suggests that a truly rigorous proof would use induction. Here's how that would go:

We proceed by induction on s, the number of primes appearing in the factorization of a. If $s = 1$, then we have $a = p_1$ is prime. Then, since $a \mid bc$ we know a has to divide b or c. But a can't divide b since $\gcd(a, b) = 1$. Thus $a \mid c$, as desired.

Now suppose the result is true when $s = k$ and suppose $a = p_1 p_2 \cdots p_{k+1}$. Then $p_{k+1} \mid bc$. As I argued above, this means $p_{k+1} = r_i$ for some i. Without loss of generality, we may assume $p_{k+1} = r_u$. Then

$$a/p_{k+1} = p_1 p_2 \cdots p_k \mid q_1 \cdots q_t r_1 \cdots r_{u-1} = b \cdot c/p_{k+1}$$

Note that we still have $\gcd(a/p_{k+1}, b) = 1$, since any divisor of a/p_{k+1} is certainly a divisor of a. Thus, by the induction hypothesis, this means $a/p_{k+1} \mid c/p_{k+1}$. But this means $a \mid c$, as desired.

7. Let a and b be two positive integers. Let $S = \left\{ c \in \mathbb{N} \middle| a \mid c, b \mid c \right\}$. Then S is nonempty, since it contains ab, so it has a minimal element. This minimal element is called the *lowest common multiple* of a and b and denoted $\operatorname{lcm}(a, b)$. Show that $\operatorname{lcm}(a, b)$ divides every other element of S. Hint: use the division algorithm.

Solution: (The problem statement should really say $S = \left\{ c \in \mathbb{N} \middle| a \mid c, b \mid c, c \neq 0 \right\}$, so that $\operatorname{lcm}(a, b)$ isn't always 0)

Let $m = \operatorname{lcm}(a, b)$. Then there exist $x, y \in \mathbb{Z}$ such that $ax = by = m$. Further, let n be any common multiple of a and b, so that $at = n$ and $bu = n$ for some $t, u \in \mathbb{N}$. The division algorithm tells us that there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < m$, such that $n = qm + r$. We wish to show that $r = 0$. If $r \neq 0$, then $r = n - qm$ is a nonzero common multiple of a; indeed, $n - qm = at - qax = a(t - qx)$ and $n - qm = bu - qby = b(u - qy)$. But this contradicts the fact that $m = \operatorname{lcm}(a, b)$, since $r < m$.

8. Find a formula for all the points on the hyperbola

$$x^2 - y^2 = 1$$

whose coordinates are rational numbers

Solution: This is a lot like what we did in class to find a formula for all the pythagorean triples. Start with any point on the hyperbola with rational coordinates, such as $(1, 0)$. Suppose (x_0, y_0) is some point on the hyperbola with $x_0, y_0 \in \mathbb{Q}$. Then the line going through $(1, 0)$ and (x_0, y_0) has rational slope. Let m be the slope of this line. We're going to compute x_0 and y_0 in terms of m.

Then the equation of the line going through $(1, 0)$ and (x_0, y_0) is $y = m(x - 1)$, by the point-slope formula. Thus the intersection of our line and our hyperbola is the set of solutions to the following two equations:

$$\begin{aligned} y &= m(x-1) \\ x^2 - y^2 &= 1 \end{aligned}$$

Substituting the first equation into the second one, we see that

$$x^2 - (m(x-1))^2 = 1$$

In other words,

$$(1-m^2)x^2 + 2m^2x - m^2 - 1 = 0$$

Now, we know that $(1,0)$ is one of the points where our line intersects our hyperbola. Thus $x = 1$ is a solution to the above equation, but it's not the solution we're looking for. So we can divide the above polynomial by $x - 1$:

$$\frac{(1-m^2)x^2 + 2m^2x - m^2 - 1}{x-1} = (1-m^2)x + m^2 + 1$$

so we must have $(1-m^2)x_0 + m^2 + 1 = 0$. Thus, we must have $m \neq 1$ (or else our equation says $2 = 0$), so

$$x_0 = \frac{m^2+1}{m^2-1}$$

and

$$y_0 = mx - m = \frac{m^3+m}{m^2-1} + \frac{-m^3+m}{m^2-1} = \frac{2m}{m^2-1}$$

We have shown that every point with rational coordinates (usually just called a *rational point*) on our hyperbola $x^2 - y^2 = 1$ is of the form

$$\left(\frac{m^2+1}{m^2-1}, \frac{2m}{m^2-1}\right)$$

for some $m \in \mathbb{Q}$ with $m \neq 1$. Now we have to check: is this point actually on the hyperbola for all $m \in \mathbb{Q} \setminus \{1\}$? The answer is yes:

$$\left(\frac{m^2+1}{m^2-1}\right)^2 - \left(\frac{2m}{m^2-1}\right)^2 = \frac{m^4 + 2m^2 + 1 - 4m^2}{m^4 - 2m^2 + 1} = 1$$

for all $m \in \mathbb{Q}$ with $m \neq 1$.