Math 25 — Assignment 2

Due Tuesday, October 4th, *beginning of class*.

1. For each pair $(a, b) = (45, 75), (101, 42)$, express $\gcd(a, b)$ as an integer linear combination of a and b.

   Solution: We consider the transcript of the XGCD algorithm for $(45, 75)$.

q_j	r_j	$q_j r_j$	x_j	y_j
	75	—	1	0
1	45	45	0	1
1	30	15	1	-1
1	15	15	-1	2
	0			

   Therefore, we see $75 \cdot (-1) + 30 \cdot (2) = 15 = \gcd(75, 45)$.

   Similarly, we consider the transcript of the XGCD algorithm for $(101, 42)$.

q_j	r_j	$q_j r_j$	x_j	y_j
	101	—	1	0
2	42	84	0	1
2	17	34	1	-2
2	8	16	-2	5
8	1	8	5	-12
	0			

   Therefore, we see $101 \cdot (5) + 42 \cdot (-12) = 1 = \gcd(101, 42)$.

2. Let k be a positive integer. Use Bezout's identity to show that $3k + 2$ and $5k + 3$ are relatively prime (i.e., their $\gcd$ is 1).

   Solution: Observe that
   $$5 \cdot (3k + 2) - 3 \cdot (5k + 3) = 1.$$
   Thus, from Bezout's identity we see that $\gcd(5k + 3, 3k + 2) = 1$ for all integers k.

3. Let $a = \prod_{i=1}^{k} p_i^{a_i}$ and $b = \prod_{i=1}^{k} p_i^{b_i}$ be prime factorizations where $a_i, b_i \geq 0$ (as opposed to ≥ 1 – this lets us use a common base $p_1, \ldots, p_k$ of primes). Express the prime factorization of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of the prime factorizations above. (Prove your formula holds of course.)

   Solution: We claim that
   $$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}, \qquad \operatorname{lcm}(a, b) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}.$$
   We prove the first equality. Let q be a prime and let q^e be the largest power of q dividing $\gcd(a, b)$. Then $p^e \mid a$ and $p^e \mid b$. We may assume $e > 0$, since otherwise $q^e = 1$ and there is nothing to do.

   Since q divides a, we have that q divides one of the primes p_i for some unique i, (the p_i are distinct primes). Thus $q = p_i$ (because these are primes). Then
   $$q^e \mid p^{a_i} \iff e \leq a_i.$$

Similarly, $q^e \mid b$, so $e \le b_i$ (we had ensured a common base of primes at the outset). Therefore $e \le \min(a_i, b_i)$. Conversely, if $q = p_i$ and $e \le \min(a_i, b_i)$, then $q^e \mid a$ and $q^e \mid b$.

If d is a common divisor of both a and b, then any prime dividing d must be one of the p_i. We write the unique factorization of d as

$$d = \prod_{i=1}^{k} p_i^{e_i}$$

where $e_i \ge 0$. The prior argument shows that $e_i \le \min(a_i, b_i)$, and that any such choice of exponents begets a common divisor of a and b. The largest common divisor of a and b one can construct is with the choice $e_i = \min(a_i, b_i)$, so

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}.$$

We now examine the least common multiple $m = \operatorname{lcm}(a, b)$. We can use the identity

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

(This is Theorem 1.12 from the book. One can do things in the other order – first establish the prime factorization of the lcm, and then prove this identity. See below.)

Because $\max(x, y) + \min(x, y) = x + y$, we see that

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)} = \prod_{i=1}^{k} p_i^{a_i + b_i - \min(a_i, b_i)} = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}.$$

This proves the claim.

For the interested student, we prove Theorem 1.12 via prime factorizations. Let $m = \operatorname{lcm}(a, b)$ and write as its prime factorization

$$m = \prod_{i=1}^{k} p_i^{e_i} \cdot \lambda$$

where $\lambda \in \mathbb{Z}$ is coprime to the p_i. Since $a \mid m$, we have that $p_i^{a_i}$ divides $p_i^{e_i}$ as before, or in other words $a_i \le e_i$. Similarly, $b_i \le e_i$. Thus $\max(a_i, b_i) \le e_i$. We then need only show that

$$\prod_{i=1}^{k} p_i^{\max(a_i, b_i)}$$

is a common multiple of a and b, whence minimality follows. But of course

$$\prod_{i=1}^{k} p_i^{\max(a_i, b_i)} = a \cdot \prod_{i=1}^{k} p_i^{\max(a_i, b_i) - a_i} = b \cdot \prod_{i=1}^{k} p_i^{\max(a_i, b_i) - b_i}$$

(the exponents necessarily being non-negative) so indeed this is the case.

4. (Euclid's Lemma) Let a, b, d be integers. Prove that if $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$. (Hint: Bezout's identity gives that

$$ax + dy = 1$$

for some integers x, y.)

Solution: From Bezout's lemma we have that $ax + dy = 1$ for some $x, y \in \mathbb{Z}$. Now

$$abx + dby = b.$$

Because $d \mid ab$ and $d \mid d$, we have $d \mid b$.