Math 2001 - Assignment 8

Due October 23, 2020

(1) Compute $\gcd(a, b)$ and its Bezout coefficients using the Euclidean algorithm for the following numbers. Then find $\operatorname{lcm}(a, b)$.

(a) $a = 85, b = 25$ (b) $a = 57, b = 24$

Solution.

(a)

$$\begin{array}{rrrl} & 85 & 25 & \\ 85 & 1 & 0 & \\ 25 & 0 & 1 & /\cdot(-3) \\ 10 & 1 & -3 & /\cdot(-2) \\ 5 & -2 & 7 & /\cdot(-2) \\ 0 & & & \end{array}$$

Hence $\gcd(85, 25) = 5 = -2 \cdot 85 + 5 \cdot 25$.
$\operatorname{lcm}(85, 25) = \frac{85 \cdot 25}{\gcd(85,25)} = 85 \cdot 5 = 425$.

(b)

$$\begin{array}{rrrl} & 57 & 24 & \\ 57 & 1 & 0 & \\ 24 & 0 & 1 & /\cdot(-2) \\ 9 & 1 & -2 & /\cdot(-2) \\ 6 & -2 & 5 & /\cdot(-1) \\ 3 & 3 & -7 & /\cdot(-2) \\ 0 & & & \end{array}$$

Hence $\gcd(57, 24) = 3 = 3 \cdot 57 - 7 \cdot 24$.

(2) Solve the following for $u, v \in \mathbb{Z}$:

(a) $33u + 10v = -5$ (b) $44u + 10v = 5$

Solution. (a) Find the Bezout coefficients for $\gcd(33, 10)$:

$$\begin{array}{rrrl} 33 & 1 & 0 & \\ 10 & 0 & 1 & /\cdot 3 \\ 3 & 1 & -3 & /\cdot 3 \\ 1 & -3 & 10 & \\ 0 & & & \end{array}$$

Hence $33(-3) + 10 \cdot 10 = 1$. Multiplication with -5 yields

$$33 \cdot \underbrace{15}_{u} + 10 \cdot \underbrace{(-50)}_{v} = -5$$

(b) Since $\gcd(44, 10) = 2$ and 2 does not divide 5, this equation has no solution.

(3) Let $a, b, c \in \mathbb{Z}$ with a, b not both 0. Show that

$$\exists x, y \in \mathbb{Z}\colon x \cdot a + y \cdot b = c \text{ iff } \gcd(a, b)|c.$$

Hint: There are 2 implications to show:

(a) If $x \cdot a + y \cdot b = c$, then $\gcd(a, b)|c$.

Proof (direct). Assume $x \cdot a + y \cdot b = c$. Let $d = \gcd(a, b)$. Since d divides a and b, we have $m, n \in \mathbb{Z}$ such that $a = md, b = nd$. Then

$$c = x \cdot a + y \cdot b = (xm + yn)d$$

is a multiple of d. Hence d divides c. □

(b) If $\gcd(a, b)|c$, then there are $x, y \in \mathbb{Z}$ such that $x \cdot a + y \cdot b = c$.
Hint: Use Bezout's identity!

Proof (direct). Assume $\gcd(a, b)|c$, that is $c = n \gcd(a, b)$ for $n \in \mathbb{Z}$. By Bezout's identity we have $u, v \in \mathbb{Z}$ such that

$$ua + vb = \gcd(a, b).$$

Multiplication by n yields

$$\underbrace{nu}_{x} a + \underbrace{nv}_{y} b = n \gcd(a, b) = c.$$

Hence we have found integers $x = nu, y = nv$ such that $x \cdot a + y \cdot b = c$. □

(4) Two integers have the *same parity* if both are even or both are odd. Otherwise they have *opposite parity*.

Let $a, b \in \mathbb{Z}$. Show that if $a + b$ is even, then a, b have the same parity.
Hint: Use a contrapositive proof.

Proof (contrapositive). We show that if a, b have different parity, then $a + b$ is odd.

Assume that a, b have different parity (i.e., one is even, the other odd).

Case a even, b odd: Then $a = 2m$ and $b = 2n + 1$ for some $m, n \in \mathbb{Z}$. Hence $a + b = 2(m + n) + 1$ is odd.

Case a odd, b even: Similar to the previous case. □

(5) Show for all $a \in \mathbb{Z}$: If a^2 is even, then a is even.
Hint: Which type of proof is the best to use?

Solution. Using a contrapositive proof allows us to start with an assumption on a. So that's what we choose.

Proof (contrapositive). Show: if a is odd, then a^2 is odd.

Assume a is odd, that is, $a = 2n + 1$ for some $n \in \mathbb{Z}$. Then

$$a^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$$

is odd. □

(6) Complete the following proof of **Euclid's Lemma:**
Let p be a prime, $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

Proof: Assume $\underline{p|ab}$ but $p \nmid a$. We will show $p|b$.
By Bezout's identity we have $u, v \in \mathbb{Z}$ such that

$$\underline{ua + vp} = \gcd(a, p).$$

Since p is <u>prime</u> and $p \nmid a$, we have $\gcd(a, p) = \underline{1}$. Hence

$$ua + vp = \underline{1}.$$

Multiplying this equation by <u>b</u> yields

$$\underline{uab + vpb} = b$$

Since $p|\underline{uab}$ and $p|\underline{vpb}$, we have a multiple of p on the left hand side of this equation. Thus $\underline{p|b}$. □