Name: *Caleb McWhorter — Solutions*
MATH 308
Fall 2022
HW 14: Due 11/10

"Mathematics is the queen of the sciences and number theory is the queen of mathematics."
–Carl Friedrich Gauss

Problem 1. (10pt) For each of the following pairs (a, b), determine the quotient q and remainder r from the division algorithm and express b as $b = aq + r$:

(a) $(a, b) = (4, 17)$

(b) $(a, b) = (3, 117)$

(c) $(a, b) = (-6, 25)$

(d) $(a, b) = (9, -82)$

Solution.

(a) Because $a > 0$, we have $q = \left\lfloor \dfrac{17}{4} \right\rfloor = 4$ so that $r = 17 - 4 \cdot 4 = 17 - 16 = 1$. Therefore, $17 = 4(4) + 1$.

(b) Because $a > 0$, we have $q = \left\lfloor \dfrac{117}{3} \right\rfloor = 39$ so that $r = 117 - 3 \cdot 39 = 117 - 117 = 0$. Therefore, $117 = 3(39) + 0$.

(c) Because $a < 0$, we have $q = \left\lceil \dfrac{25}{-6} \right\rceil = -4$ so that $r = 25 - (-6)(-4) = 25 - 24 = 1$. Therefore, $25 = (-6)(-4) + 1$.

(d) Because $a > 0$, we have $q = \left\lfloor \dfrac{-82}{9} \right\rfloor = -10$ so that $r = -82 - 9(-10) = -82 + 90 = 8$. Therefore, $-82 = 9(-10) + 8$.

Problem 2. (10pt) Showing all your work and explaining all your reasoning, answer the following:

(a) Use the Euclidean algorithm to find $\gcd(220, 815)$.

(b) Do there exist integer solutions x, y to the equation $20x - 84y = 25$? Explain.

Solution.

(a) Using the Euclidean algorithm, we have...

$$\begin{aligned} 815 &= 220(3) + 155 \\ 220 &= 155(1) + 65 \\ 155 &= 65(2) + 25 \\ 65 &= 25(2) + 15 \\ 25 &= 15(1) + 10 \\ 15 &= 10(1) + 5 \\ 10 &= 5(2) \end{aligned}$$

Therefore, $\gcd(200, 815) = 5$.

(b) We know that the gcd of two integers, not both zero, divides any linear combination of the two integers; that is, if $a, b \in \mathbb{Z}$ are not both zero and $ax + by = c$, then we know that $\gcd(a, b)$ divides c. If there were integers x, y such that $20x - 84y = 25$, then $\gcd(20, 84)$ divides 25. However, $\gcd(20, 84) = 4$ does not divide 25 (for instance, because 4 is even but 25 is odd). Therefore, there can be no integer solutions x, y to $20x - 84y = 25$.

Problem 3. (10pt) Showing all your work, use the extended Euclidean algorithm to express $\gcd(350, 480)$ as a linear combination of 350 and 480.

Solution. Using the Euclidean algorithm, we have...

$$480 = 350(1) + 130$$

$$350 = 130(2) + 90$$

$$130 = 90(1) + 40$$

$$90 = 40(2) + 10$$

$$40 = 10(4)$$

Therefore, $\gcd(350, 480) = 10$. Solving for the remainders, we have...

$$\begin{aligned} 10 &= 90 - 40(2) \\ 40 &= 130 - 90(1) \\ 90 &= 350 - 130(2) \\ 130 &= 480 - 350(1) \end{aligned}$$

Now extending the Euclidean algorithm, we have...

$$\begin{aligned} 10 &= 90 - 40(2) \\ &= 90 - 2(130 - 1 \cdot 90) = 90 - 2 \cdot 130 + 2 \cdot 90 = 3 \cdot 90 - 2 \cdot 130 \\ &= 3 \cdot 90 - 2 \cdot 130 = 3(350 - 2 \cdot 130) - 2 \cdot 130 = 3 \cdot 350 - 6 \cdot 130 - 2 \cdot 130 = 3 \cdot 350 - 8 \cdot 130 \\ &= 3 \cdot 350 - 8 \cdot 130 = 3 \cdot 350 - 8(480 - 1 \cdot 350) = 3 \cdot 350 - 8 \cdot 480 + 8 \cdot 350 = -8 \cdot 480 + 11 \cdot 350 \end{aligned}$$

Therefore, we have...

$$-8 \cdot 480 + 11 \cdot 350 = 10$$

Problem 4. (10pt) Recall that a rational number is a real number of the form $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. A real number which is not rational is called irrational. All integers are rational numbers: if $n \in \mathbb{Z}$, we have $n = \frac{n}{1}$. Some real numbers are rational, e.g. $0.26 = \frac{26}{100} = \frac{13}{50}$ and $0.\overline{3} = \frac{1}{3}$. However, not all real numbers are rational. Write a proof that $\sqrt{2}$ is not rational by completing the following:

(a) We know that $\sqrt{2}$ is either rational or irrational. If $\sqrt{2}$ is not irrational, what do we know about $\sqrt{2}$?

(b) Explain why we can write $\sqrt{2}$ as $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b \neq 0$, and $\gcd(a, b) = 1$.

(c) Show that (b) implies that $a^2 = 2b^2$.

(d) Use Euclid's Theorem to show that $2|a$.

(e) Explain why (d) implies that $b^2 = 2k^2$ for some $k \in \mathbb{Z}$.

(f) Explain why (e) implies that $2|b$.

(g) Explain why (f) contradicts (b). What does this imply about $\sqrt{2}$?

Solution.

(a) Because $\sqrt{2}$ is either rational or irrational, if $\sqrt{2}$ is not irrational, then it must be rational, i.e. $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$.

(b) By (a), if $\sqrt{2}$ were rational, then by definition, we know that $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. Of course, $\frac{a}{b}$ need not be 'reduced', i.e. it could be that $\gcd(a, b) > 1$. By multiplying by $1 = \frac{1/\gcd(a,b)}{1/\gcd(a,b)}$, we obtain new integers a', b' with $\frac{a}{b} = \frac{a'}{b'}$ and $\gcd(a', b') = 1$. But we could have simply chosen this representation to begin with, i.e. simply define $a = a'$ and $b = b'$. Therefore, we may assume that we have already done that, i.e. $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b \neq 0$, and $\gcd(a, b) = 1$.

(c) If $\sqrt{2} = \frac{a}{b}$, then $a = b\sqrt{2}$. Squaring both sides, we obtain $a^2 = (b\sqrt{2})^2 = 2b^2$.

(d) Clearly, $2 \mid (2b^2)$. But then 2 divides a^2 because $a^2 = 2b^2$. But because $a^2 = a \cdot a$, by Euclid's Theorem, we know that $2 \mid a$ or $2 \mid a$, i.e. 2 divides a.

(e) By (d), we know that $2 \mid a$, i.e. a is a multiple of 2. But then $a = 2k$ for some $k \in \mathbb{Z}$. Then we know that $2b^2 = a^2 = (2k)^2 = 4k^2$, i.e. $2b^2 = 4k^2$. Dividing both sides by 2, we obtain $b^2 = 2k^2$.

(f) By (e), we know that $b^2 = 2k^2$. But because $2 \mid (2k^2)$, we know that 2 divides b^2 because $b^2 = 2k^2$. Because $b^2 = b \cdot b$, by Euclid's Theorem, we know that $2 \mid b$ or $2 \mid b$, i.e. 2 divides b.

(g) By (d) and (f), we know that $2 \mid a$ and $2 \mid b$. But then $\gcd(a, b) \geq 2$. This contradicts the assumption in (b) that we have chosen a, b such that $\gcd(a, b) = 1$. Therefore, it cannot be that $\sqrt{2}$ is rational. This shows that $\sqrt{2}$ must be irrational.