Abstract Algebra 2024–I

Homework 1

Pablo Rosero & Christian Chávez

September 11, 2023

1. For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form $ax + by$ for some integers x and y.

(a) $a = 792, b = 275$

(b) $a = 507885, b = 60808$

Solution. Using the (extended) Euclidean Algorithm, we get the following. Here $[a, b]$ denotes the least common multiple of a and b.

(a) $(a, b) = 11$, $[a, b] = 19800$, $(a, b) = 8a - 23b$

(b) $(a, b) = 691$, $[a, b] = 44693880$, $(a, b) = -17a + 142b$

2. Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

Proof. Let n be composite. Recall this means n is a positive integer greater than 1. By definition, n has positive divisors other than 1 and n. Thus, $n = ab$ for some positive integers a and b with $a, b \notin \{1, n\}$. Clearly $n \mid ab$. Since $a < n$, we have $n \nmid a$. Similarly $n \nmid b$. We are done. □

3. If p is a prime, prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$. (Why this proves $\sqrt{p}$ is not a rational number.)

Proof. Suppose p is a prime number and assume for the sake of contradiction that there do exist nonzero integers a and b such that $a^2 = pb^2$. Either a and b share common factors other than 1 or not. Suppose first they do not have commont factors other than 1. Notice $a^2 = pb^2$ implies $p \mid a^2$, whence $p \mid a$ (by Euclid's lemma), and thus $pk = a$ for some $k \in \mathbb{Z}$. Thus, $p^2k^2 = pb^2$ which implies $pk^2 = b^2$. Then, $p \mid b^2$ and, as before, $p \mid b$. We have shown p divides both a and b, so p is a common factor of both, a contradiction. If a and b share common factors other than 1, we can rule them out of the equation $a^2 = pb^2$ by using the Fundamental Theorem of Arithhmetic to write a^2 and b^2 as powers of products of primes. Hence, we are led to the case above, which we proved cannot hold. In any case we arrived at a contradiction and so we conclude our main assumption was false. The proof is complete. □

Remark. Euclid's lemma states that if a prime number divides the product of two integers, then it must divide at least one of those integers. On the other hand, this proof uses basic facts about the integers. However, by writing $(a/b)^2 = p$ we see that $b = 1$ because p is an integer and the rationals that are also integers are the ones that have denominator 1. Thus $a^2 = p$ implies p is composite, a contradiction.

4. Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

Solution. The elements of $\mathbb{Z}/18\mathbb{Z}$ are

$$\begin{gathered}
\{18k \mid k \in \mathbb{Z}\}, \{1 + 18k \mid k \in \mathbb{Z}\}, \{2 + 18k \mid k \in \mathbb{Z}\} \\
\{3 + 18k \mid k \in \mathbb{Z}\}, \{4 + 18k \mid k \in \mathbb{Z}\}, \{5 + 18k \mid k \in \mathbb{Z}\} \\
\{6 + 18k \mid k \in \mathbb{Z}\}, \{7 + 18k \mid k \in \mathbb{Z}\}, \{8 + 18k \mid k \in \mathbb{Z}\} \\
\{9 + 18k \mid k \in \mathbb{Z}\}, \{10 + 18k \mid k \in \mathbb{Z}\}, \{11 + 18k \mid k \in \mathbb{Z}\} \\
\{12 + 18k \mid k \in \mathbb{Z}\}, \{13 + 18k \mid k \in \mathbb{Z}\}, \{14 + 18k \mid k \in \mathbb{Z}\} \\
\{15 + 18k \mid k \in \mathbb{Z}\}, \{16 + 18k \mid k \in \mathbb{Z}\}, \text{ and } \{17 + 18k \mid k \in \mathbb{Z}\}.
\end{gathered}$$

Note however that a more compact way to write this information is as follows:

$$\mathbb{Z}/18\mathbb{Z} = \bigcup_{i=0}^{17} \{\{i + 18k \mid k \in \mathbb{Z}\}\}.$$

5. Suppose $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer. Show that $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$. (Note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9. In particular, an integer is divisible by 9 if and only if the sum of its digits is divisible by 9).

Solution. Let $\overline{a}$ denote the residue class of a mod 9. Using modular arithmetic we have

$$\overline{a} = \overline{\sum_{k=0}^{n} a_k 10^k} = \sum_{k=0}^{n} \overline{a_k} \cdot \overline{10}^k = \sum_{k=0}^{n} \overline{a_k} \cdot 1.$$

Equivalently, this can be written as

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9,$$

and we are done.

6. Compute the remainder when 37^{100} is divided by 29.

Solution. Performing all arithmetic mod 29, we have $37^{100} = 8^{100}$. Moreover, note that

$$\begin{aligned} 8^{28} &= \left(8^2\right)^2 \cdot \left(\left(8^2\right)^2\right)^2 \cdot \left(\left(\left(8^2\right)^2\right)^2\right)^2 \\ &= 6^2 \cdot \left(6^2\right)^2 \cdot \left(\left(6^2\right)^2\right)^2 \\ &= 7 \cdot 7^2 \cdot \left(7^2\right)^2 \\ &= 7 \cdot 20 \cdot 20^2 \\ &= 140 \cdot 23 \\ &= 24 \cdot 23 \\ &= 552 \\ &= 1. \end{aligned}$$

So we have $8^{100} = 8^{28} \cdot 8^{28} \cdot 8^{28} \cdot 8^{16} = 8^{16} = 23$, as computed above.

7. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.

Proof. We have $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Modulo 4, we have $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4} = \overline{0}$, and $\overline{3}^2 = \overline{9} = \overline{1}$. □

8. Let $a, b \in \mathbb{Z}$. Prove that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4. (Hint: use the previous exercise.)

Proof. Suppose $a^2 + b^2$ can be divided by 4 (so, it is not zero). By the division algorithm, there are unique integers q and r such that $a^2 + b^2 = 4q + r$ with $0 \leq r < 4$. Then $\overline{a^2 + b^2} \equiv \overline{r}$, taking congruence classes mod 4. By the previous exercise, $\overline{a^2 + b^2} = \overline{a}^2 + \overline{b}^2$ can only be $\overline{0}$, $\overline{1}$ or $\overline{2}$. Thus $\overline{r} \neq \overline{3}$, whence $r \neq 3$. □

9. Prove that the equation $x^2 + y^2 = 3z^2$ has no solutions for positive integers x, y and z.

Proof. Suppose, to the contrary, there are are nonzero integers x, y, and z such that $x^2 + y^2 = 3z^2$. Either these integers have factors in common or not. If they do, we can factor them out of the equation $x^2 + y^2 = 3z^2$ to get a new equation $\hat{x}^2 + \hat{y}^2 = 3\hat{z}^2$ where $\hat{x}$, $\hat{y}$ and $\hat{z}$ do not share common factors. This situation lead us to the second case, so we only need to prove such a case is imposible. Suppose x, y, and z do not share common factors. Taking residue classes modulo 3, we have $\overline{x}^2 + \overline{y}^2 = \overline{0}$. This equation is satisfied (if and) only if x and y are multiples of 3. Indeed, if k is any integer, then $\overline{k}$ can only be $\overline{0}$, $\overline{1}$ or $\overline{2}$; thus $\overline{k}^2$ can only be $\overline{0}$ or $\overline{1}$. Since $\overline{1} + \overline{0} = \overline{0} + \overline{1} = \overline{1}$ and $\overline{1} + \overline{1} = \overline{2}$, the only possible case is $\overline{x}^2 = \overline{y}^2 = \overline{0}$. In other words, $3 \mid x^2$ and $3 \mid y^2$.

Euclid's lemma implies 3 divides both x and y. Finally, notice this implies the left side of $x^2 + y^2 = 3z^2$ is a multiple of 9 and by dividing by 3 we get z^2 is a multiple of 3, whence z is also a multiple of 3. We have shown that x, y, and z have 3 as common factor, which is a contradiction. The proof is complete. □

10. Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Proof. Suppose $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Then there are $\overline{x}, \overline{y} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ such that $\overline{a} \cdot \overline{x} = \overline{1}$ and $\overline{b} \cdot \overline{y} = \overline{1}$. Thus

$$(\overline{a} \cdot \overline{b}) \cdot (\overline{x} \cdot \overline{y}) = (\overline{a} \cdot \overline{x}) \cdot (\overline{b} \cdot \overline{y}) = \overline{1},$$

whence the result follows. □

11. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

Proof. Suppose $d = (a, n) > 1$. By definition, $a = dx$ and $dy = n$ for some positive integers x and y. Thus $ay = dxy = nx$, whence $ay \equiv 0 \pmod{n}$. Since $d > 1$, we have $y < n$. Take $b = y$. If there were an integer c such that $ac \equiv 1 \pmod{n}$, then $abc \equiv b \pmod{n}$, whence $0 \equiv b \pmod{n}$. This is a contradiction since $1 \leq b < n$. □

12. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$. (Use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers.)

Proof. Suppose a and n are relatively prime, which means $(a, n) = 1$. We know there are integers x and y such that $1 = ax + ny$. Thus $1 \equiv ax \pmod{n}$. Take $c = x$ and conclude. □

13. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^{\times}$is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4 . Verify this directly in the case $n = 12$.

Solution.

14. (a) Prove that if n is squarefree (i.e., $n > 1$ and n is not divisible by the square of any prime), then $\sqrt{n}$ is irrational.

(b) Prove that $\sqrt[3]{2}$ is irrational.

Solution.

15. Let a and b be nonzero integers and let $d = (a, b)$. Prove that a/d and b/d are relatively prime.

Proof. Let $d' = (a/d, b/d)$. There are integers x and y such that $d = ax + by$. Thus

$$1 = \frac{a}{d}x + \frac{b}{d}y.$$

Because d' divides any linear combination of a/d and b/d, it follows $d' \mid 1$. Hence $d' = 1$ and the proof is complete. □

16. Prove that if $(r, m) = 1 = (r', m)$, then $(rr', m) = 1$.

Solution.

17. Assume that $d = sa + tb$ is a linear combination of integers a and b. Find infinitely many pairs of integers (s_k, t_k) with

$$d = s_k a + t_k b$$

Solution.

18. If a and b are relatively prime and if each divides an integer n, then their product ab also divides n.

Proof. Let $d = (a, b)$ and $l = [a, b]$. Suppose a and b are relatively prime and that each one divides an integer n. Since n is a common multiple of a and b, then n must be divisible by l. Notice $l = ab$ because $dl = ab$ and $d = 1$. Thus $ab \mid n$, as desired. □

19. If $a > 0$, prove that $a(b, c) = (ab, ac)$. [One must assume that $a > 0$ lest $a(b, c)$ be negative.]

Solution.

20. A Pythagorean triple is a triple (a, b, c) of positive integers for which

$$a^2 + b^2 = c^2$$

it is called primitive if the $\gcd(a, b, c) = 1$.

(a) Consider a complex number $z = q + ip$, where $q > p$ are positive integers. Prove that

$$\left(q^2 - p^2, 2qp, q^2 + p^2\right)$$

is a Pythagorean triple by showing that $|z^2| = |z|^2$. [One can prove that every primitive Pythagorean triple (a, b, c) is of this type.]

(b) Show that the Pythagorean triple $(9, 12, 15)$ (which is not primitive) is not of the type given in part (i).

Solution.

21. Let $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_n\}$ be finite sets, where the x_i are distinct and the y_j are distinct. Show that there is a bijection $f : X \to Y$ if and only if $|X| = |Y|$; that is, $m = n$.

Solution.

22. (Pigeonhole Principle points) If X and Y are finite sets with the same number of elements, show that the following conditions are equivalent for a function $f : X \to Y$.

(a) f is injective;

(b) f is bijective;

(c) f is surjective.

Solution.

23. (a) Let $f : X \to Y$ be a function, and let $\{S_i : i \in I\}$ be a family of subsets of X. Prove that

$$f\left(\bigcup_{i \in I} S_i\right) = \bigcup_{i \in I} f(S_i)$$

(b) If S_1 and S_2 are subsets of a set X, and if $f : X \to Y$ is a function, prove that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. Give an example in which $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

(c) If S_1 and S_2 are subsets of a set X, and if $f : X \to Y$ is an injection, prove that $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$.

Solution.

24. Let $f : X \to Y$ be a function.

(a) If $B_i \subseteq Y$ is a family of subsets of Y, prove that

$$f^{-1}\left(\bigcup_i B_i\right) = \bigcup_i f^{-1}(B_i) \text{ and } f^{-1}\left(\bigcap_i B_i\right) = \bigcap_i f^{-1}(B_i).$$

(b) If $B \subseteq Y$, prove that $f^{-1}(B') = f^{-1}(B)'$, where B' denotes the complement of B.

Solution.

25. Let $f : X \to Y$ be a function. Define a relation on X by $x \equiv x'$ if $f(x) = f(x')$. Prove that $\equiv$ is an equivalence relation. (If $x \in X$ and $f(x) = y$, the equivalence class $[x]$ is usually denoted by $f^{-1}(y)$, the inverse image of $\{y\}$.)

Proof. We prove the defining properties of an equivalence relation. Let $x, y, z \in X$.

(i) (Reflexity) Because $f(x) = f(x)$, we have $x \equiv x$.

(ii) (Symmetry) Suppose $x \equiv y$, which means $f(x) = f(y)$. Clearly $f(y) = f(x)$, which, by definition, is equivalent to $y \equiv x$.

(iii) (Transitivity) Suppose $x \equiv y$ and $y \equiv z$. Then $f(x) = f(y)$ and $f(y) = f(z)$, whence $f(x) = f(z)$. Therefore $x \equiv z$.

The proof is finished. □