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.

Solution. Let n be composite. By definition we have $n = ab$ for some integers a and b with $a, b \neq \pm 1, \pm n$. Clearly $n \mid ab$. Now suppose by way of contradiction that $n \mid a$. Then we have $kn = a$ for some integer k. Now $kba = a$, so $(kb - 1)a = 0$, so $kb = 1$. Thus $b = \pm 1$, a contradiction. Hence, n does not divide a. Similarly, n does not divide b.

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 Artihmetic 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. $\square$

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. 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. Prove that if $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$. (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. By using the basic propeties of sum of classes, we have

$$\overline{a} = \overline{\sum_{i=0}^{n} a_i 10^i} = \sum_{i=0}^{n} \overline{a_i}\,\overline{10}^i = \sum_{i=0}^{n} \overline{a_i} \cdot 1,$$

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 $\overline{1}$.

Solution. Modulo 4, we have $\overline{0}^{2}=\overline{0}$,

8. Prove for any integers a and b that $a^{2}+b^{2}$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).

Solution.

9. Prove that the equation $a^{2}+b^{2}=3c^{2}$ has no solutions in nonzero integers a, b and c. [Consider the equation mod 4 as in the previous two exercises and show that a, b and c would all have to be divisible by 2 . Then each of a^{2}, b^{2} and c^{2} has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

Solution.

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

Solution.

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 $ab \equiv 0(\bmod n)$ and deduce that there cannot be an integer c such that $ac \equiv 1(\bmod n)$.

Solution.

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. $\square$

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. $\square$

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 infi nitely 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. $\square$

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 fi nite 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 fi nite 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

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

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

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

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

$$f^{-1}\left(\bigcup_{i} B_i\right) = \bigcup_{i} f^{-1}\left(B_i\right) \text{ and } f^{-1}\left(\bigcap_{i} B_i\right) = \bigcap_{i} f^{-1}\left(B_i\right).$$

(b) If $B \subseteq Y$, prove that $f^{-1}\left(B'\right) = f^{-1}(B)'$, 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 $f(x) = f\left(x'\right)$. 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. $\square$