

Preliminaries

Exercises:

0.1 BASICS

In Exercises 1 to 4 let \mathcal{A} be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} = \{X \in \mathcal{A} \mid MX = XM\}.$$

1. Determine which of the following elements of \mathcal{A} lie in \mathcal{B} :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Solution - The elements of $\mathcal{A} \in \mathcal{B}$ are:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).

Proof. If $P, Q \in \mathcal{B}$, then $MP = PM$ and $MQ = QM$ so that $MP - PM = 0$ and $MQ - QM = 0$. Therefore, $MP - PM = MQ - QM \implies MP + QM = MQ + PM \implies M(P+Q) = (P+Q)M$. Thus, $P+Q \in \mathcal{B}$. \square

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where \cdot denotes the usual product of two matrices).

Proof. If $P, Q \in \mathcal{B}$, then $MP = PM$ and $MQ = QM$ so that $MP - PM = 0$ and $MQ - QM = 0$. Therefore, $(MP - PM) \cdot (MQ - QM) = 0 \implies 2M^2(PQ) = 2(PQ)M^2 \implies M^2(PQ) = (PQ)M^2$ after dividing both sides by 2. The matrix M is invertible as the determinant, $\det(M) = 1/(ad - bc) = 1/(1 - 0) = 1$, is

non-zero. Thus, $M^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ and we now have $M^{-1}M^2(PQ) = (PQ)M^2M^{-1} \implies M(PQ) = (PQ)M$ and therefore $P \cdot Q \in \mathcal{B}$. \square

4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

Solution - $r = 0$ and $p = s$. To find this, multiply both sides of $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ by M and set the elements of the resulting matrices equal and solve the equations.

5. Determine whether the following functions f are well-defined:

(a) $f : \mathbb{Q} \rightarrow \mathbb{Z}$ defined by $f(a/b) = a$. (b) $f : \mathbb{Q} \rightarrow \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.

Solution - Two rational numbers are considered equal when $\frac{a}{b} = \frac{c}{d} \implies ad = bc$. For example, $\frac{1}{2} = \frac{2}{4}$ since $1 \cdot 4 = 2 \cdot 2 = 4$.

(a) using $\frac{1}{2}$ and $\frac{2}{4}$ this function gives 1 and 2 respectively, which shows that this function is not well-defined.

(b) similarly, using $\frac{1}{2}$ and $\frac{2}{4}$ this function gives $\frac{1^2}{2^2} = \frac{1}{4}$ and $\frac{2^2}{4^2} = \frac{4}{16} = \frac{1}{4}$ respectively, which shows that this function is well-defined.

6. Determine whether the function $f : \mathbb{R}^+ \rightarrow \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well-defined.

f is well-defined because every real number has a unique decimal expansion therefore if we choose the first decimal digit to the right of the decimal point, it will be unique.

7. Let $f : A \rightarrow B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f .

Proof. If $f(a) = f(a)$, then $a \sim a$, thus \sim is reflexive. If $f(a) = f(b)$, then $f(b) = f(a)$ so that $a \sim b$ and $b \sim a$. Thus, \sim is symmetric. Additionally, if $f(a) = f(b)$ and $f(b) = f(c)$, then $f(a) = f(c)$ so we have that $a \sim c$ and therefore \sim is also transitive. Thus, \sim is an equivalence relation as it is reflexive, symmetric, and transitive.

If $a_1, a_2 \in f^{-1}(b)$, then $f(a_1) = b$ and $f(a_2) = b$ so that $f(a_1) = f(a_2)$ and therefore $a_1 \sim a_2$. Thus, a_1 and a_2 are in the fiber of b under f . Therefore, the equivalence classes are the fibers of f . \square

0.2 PROPERTIES OF THE INTEGERS

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) $a = 20, b = 13$. (b) $a = 69, b = 372$. (c) $a = 792, b = 275$. (d) $a = 11391, b = 5673$. (e) $a = 1761, b = 1567$. (f) $a = 507885, b = 60808$.

Note: Writing the greatest common divisor in terms of integers x and y is known as **Bézout's identity** – Let

a and b be integers with greatest common divisor d . Then, there exist integers x and y such that $ax + by = d$. More generally, the integers of the form $ax + by$ are exactly the multiples of d .

(a): $(20, 13) = 1$, $lcm = 2^2 \cdot 5 \cdot 13 = 260$, $20(2) + 13(-3) = 1$

(b): $(69, 372) = 3$, $lcm = 2^2 \cdot 3 \cdot 23 \cdot 31 = 8556$, $69(7) + 372(-5) = 3$

(c): $(792, 275) = 11$, $lcm = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 = 19800$, $792(8) + 275(-23) = 11$

(d): $(11391, 5673) = 3$, $lcm = 3 \cdot 31 \cdot 61 \cdot 3797 = 21540381$, $11391(-126) + 5673(253) = 3$

(e): $(1761, 1567) = 1$, $lcm = 3 \cdot 587 \cdot 1567 = 2759487$, $1761(-25) + 1567(28) = 1$

(f): $(507885, 60808) = 691$, $lcm = 2^3 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 691 = 44693880$, $507885(-17) + 60808(142) = 691$

2. Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t .

Proof. If $k \mid a$ and $k \mid b$ then $k \mid as$ and $k \mid bt$ for every pair of integers s and t . Therefore, $k \mid as + bt$. \square

3. 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. If n is composite then $n > 1$ and n is not prime. Therefore n can be constructed from multiple integers, say a, b so that $n = ab$. For example, the smallest composite number is 4, for which we can assign $a = 2$ and $b = 2$. It is easy to see that $4 \mid 4$ and $4 \nmid 2$, so that $n \mid ab$ but $n \nmid a$ or $n \nmid b$.

By the *Fundamental Theorem of Arithmetic* we know that each composite number has a unique prime factorization so we can split up this prime factorization so that a has some of the prime factors and b has the remaining. Therefore, we are always guaranteed to find an a and b such that $n = ab, n > a, n > b$ and $n \nmid a$ and $n \nmid b$. \square

4. Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b . Suppose x_o and y_o are particular solutions to $ax + by = N$ (i.e. $ax_o + by_o = N$). Prove for any integer t that the integers

$$x = x_o + \frac{b}{d}t \text{ and } y = y_o - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is in fact the general solution).

Proof. The question doesn't ask for the derivation of the above parametric equations, just the proof that they are also solutions to $ax + by = N$.

Simply plugging $x = x_o + \frac{b}{d}t$ and $y = y_o - \frac{a}{d}t$ into $ax + by = N$ gives us $a(x_o + \frac{b}{d}t) + b(y_o - \frac{a}{d}t) = N \implies ax_o + \frac{ab}{d}t + by_o - \frac{ba}{d}t = N$. Since a, b are integers they commute and $ab = ba$ so we are left with $ax_o + by_o = N$, which was given as a particular solution to $ax + by = N$. \square

5. Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ -function.

The text gave us up to $n = 6$ in (10). Continuing we have $\varphi(7) = 6, \varphi(8) = 4, \varphi(9) = 6, \varphi(10) = 4, \varphi(11) = 10, \varphi(12) = 4, \varphi(13) = 12, \varphi(14) = 6, \varphi(15) = 8, \varphi(16) = 8, \varphi(17) = 16, \varphi(18) = 6, \varphi(19) = 18, \varphi(20) =$

8, $\varphi(21) = 12$, $\varphi(22) = 10$, $\varphi(23) = 22$, $\varphi(24) = 8$, $\varphi(25) = 20$, $\varphi(26) = 12$, $\varphi(27) = 18$, $\varphi(28) = 12$, $\varphi(29) = 28$, $\varphi(30) = 8$

6. Prove the Well Ordering Property of \mathbb{Z} by induction and prove the minimal element is unique.

Proof. The text states: (1) (Well Ordering of \mathbb{Z}) If A is any nonempty subset of \mathbb{Z}^+ , there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ (m is called a *minimal element* of A).

(base case - $n = 1$): Suppose we have a subset $\{a\}$ for $a \in \mathbb{Z}^+$. Any singleton subset of \mathbb{Z}^+ meets the minimal element criterion because $a \leq a$ and obviously this a is unique as it is the only element in the subset.

(induction hypothesis $n = k$): Assume a subset of \mathbb{Z}^+ with order k , where k is an integer and $k > 1$, meets the minimal element criterion and that this minimal element is unique.

(show $n = k + 1$ holds): Suppose that we have a subset A of \mathbb{Z}^+ with order $k + 1$, and let us partition it into two other subsets B and C such that $A = B \cup C$, where order of B is k and order of C is 1. We know that B has a minimal element that is unique (induction hypothesis), which we will denote as m . Additionally, let us denote the element of the singleton set C as c , which is trivially the minimal and unique element. c is either greater than or less than m as they both are elements of A and therefore must be distinct. If $c > m$, then m is still the minimal and unique element of A . If $c < m$, then c is the new minimal and unique element of A . Therefore, A has a minimal element that is unique. \square

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

Proof. Suppose that p is prime and that \sqrt{p} is a rational number. That is, $\sqrt{p} = \frac{a}{b}$, where a, b are integers without any common factors (i.e. in reduced form). $\sqrt{p} = \frac{a}{b} \implies p = \frac{a^2}{b^2} \implies pb^2 = a^2$, which means that $p \mid a$ and therefore we can write a as pn , where $n \in \mathbb{Z}^+$. Therefore, $(pn)^2 = pb^2 \implies pn^2 = b^2$, which means that $p \mid b$ but this is a contradiction because a and b were hypothesized to not have any common factors. Thus, there do not exist nonzero integers a and b such that $a^2 = pb^2$. \square

8. Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2) \dots 2 \cdot 1$ (it involves the greatest integer function).

Since p is prime and $p < n$, where $n \in \mathbb{Z}^+$ it must show up as one of the factors of $n! = n(n-1)(n-2) \dots 2 \cdot 1$, therefore, we can re-write this as $n! = p[n(n-1)(n-2) \dots 2 \cdot 1]$. But we forgot to also factor out all the multiples of p up to or less than n so the last expression would actually be something like $n! = p(2 \cdot p)(3 \cdot p) \dots [n(n-1)(n-2) \dots 2 \cdot 1] = p(p)(p) \dots [2 \cdot 3 \dots n(n-1)(n-2) \dots 2 \cdot 1]$. We also need to continue this process of pulling out factors that are higher powers of p up to the point where p^i is less than or equal to n . The best way to see how many multiples of powers of p are less than or equal to n is by using the greatest integer function or what is commonly known in computer science as the *floor* function. This function will let us know how many factors of each powers of prime there are up to n .

For example, suppose $p = 2$ and $n = 27$:

$$\left\lfloor \frac{27}{2} \right\rfloor = 13, \left\lfloor \frac{27}{2^2} \right\rfloor = 6, \left\lfloor \frac{27}{2^3} \right\rfloor = 3, \left\lfloor \frac{27}{2^4} \right\rfloor = 1, \left\lfloor \frac{27}{2^5} \right\rfloor = 0$$

As we can see, the reason that 2^5 gave us 0 is because $2^5 > 27$. If we add up all these factors, this is the power that p divides $n!$. Therefore, a general formula for the largest power of p which divides $n!$ is:

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

This formula is called *Legendre's formula*.

9. Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y .

Left to the reader.

10. Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes Euler's φ -function. Conclude in particular that φ tends to infinity as n tends to infinity.

Proof. Suppose we are given a positive integer N such that $\varphi(n) = N$.

Note that $n = p^\alpha \cdot k$ from some prime divisor p of n , where $k \in \mathbb{Z}^+$ and $p^\alpha \nmid k$. Therefore, $\varphi(n) = p^{\alpha-1}(p-1)\varphi(k) \implies \varphi(n) \geq p-1$ and $\varphi(n) > p^{\alpha-1} \implies N \geq p-1$ and $N > p^{\alpha-1}$ for any prime divisor of n . As n grows there will be a point that these last inequalities will not hold because $p-1 \geq N$ or $p^{\alpha-1} > N$. To demonstrate this, we can find an n where all integers above this value would give $\varphi(n) \neq N$.

Let's look for a number n that would satisfy this. Since $n = p^\alpha \cdot k$ let $k = 1$ so that $n = p^\alpha$. Then, $\varphi(n) = \varphi(p^\alpha) \implies N = p^{\alpha-1}(p-1)$ The smallest prime factor that an integer can have is 2. Therefore, let $p = 2$ such that $N = 2^{\alpha-1}(2-1) = 2^{\alpha-1} \implies 2N = 2^\alpha \implies \alpha = \log_2(2N)$. This gives us a lower bound for the value of alpha needed.

Now we need to find the base p of $n = p^\alpha$. We saw that $N = p^{\alpha-1}(p-1)$ and if $\alpha = 1$ we have $N = p-1 \implies p = N+1$. Therefore, $n > (N+1)^{\log_2(2N)}$ will give us an n that will suffice. Thus, for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$.

□

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1) \dots p_s^{\alpha_s-1}(p_s-1) \\ &= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \dots p_s^{\alpha_s}\left(1-\frac{1}{p_s}\right) \\ &= p_1^{\alpha_1}p_2^{\alpha_2} \dots p_s^{\alpha_s}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \dots \left(1-\frac{1}{p_s}\right) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \dots \left(1-\frac{1}{p_s}\right) \end{aligned}$$

From this last equation it is easy to see that φ tends to infinity as n tends to infinity.

11. Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ -function.

Proof. If $d \mid n$ then $n = dc$ for some $c \in \mathbb{Z}^+$. Therefore, $\varphi(n) = \varphi(dc) \implies \varphi(n) = \varphi(d)\varphi(c) \implies \varphi(d) \mid \varphi(n)$. □

0.3 $\mathbb{Z}/n\mathbb{Z}$: THE INTEGERS MODULO n

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

The residue classes of $\mathbb{Z}/18\mathbb{Z}$ are $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{15}, \bar{16}, \bar{17}\}$ of which these elements have the representatives:

$$\begin{aligned}
\bar{0} &= \{0, 0 \pm 18, 0 \pm 36, \dots\} \\
\bar{1} &= \{1, 1 \pm 18, 1 \pm 36, \dots\} \\
\bar{2} &= \{2, 2 \pm 18, 2 \pm 36, \dots\} \\
\bar{3} &= \{3, 3 \pm 18, 3 \pm 36, \dots\} \\
\bar{4} &= \{4, 4 \pm 18, 4 \pm 36, \dots\} \\
\bar{5} &= \{5, 5 \pm 18, 5 \pm 36, \dots\} \\
\bar{6} &= \{6, 6 \pm 18, 6 \pm 36, \dots\} \\
\bar{7} &= \{7, 7 \pm 18, 7 \pm 36, \dots\} \\
\bar{8} &= \{8, 8 \pm 18, 8 \pm 36, \dots\} \\
\bar{9} &= \{9, 9 \pm 18, 9 \pm 36, \dots\} \\
\bar{10} &= \{10, 10 \pm 18, 10 \pm 36, \dots\} \\
\bar{11} &= \{11, 11 \pm 18, 11 \pm 36, \dots\} \\
\bar{12} &= \{12, 12 \pm 18, 12 \pm 36, \dots\} \\
\bar{13} &= \{13, 13 \pm 18, 13 \pm 36, \dots\} \\
\bar{14} &= \{14, 14 \pm 18, 14 \pm 36, \dots\} \\
\bar{15} &= \{15, 15 \pm 18, 15 \pm 36, \dots\} \\
\bar{16} &= \{16, 16 \pm 18, 16 \pm 36, \dots\} \\
\bar{17} &= \{17, 17 \pm 18, 17 \pm 36, \dots\}
\end{aligned}$$

2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ (use the Division Algorithm).

Proof. The distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are:

$$a \equiv r \pmod{n}$$

$$\text{for } n \in \mathbb{Z}^+ \text{ and } a \in \mathbb{Z} \text{ where } r \in \{0, 1, 2, \dots, n-1\}$$

Thus, $a \equiv r \pmod{n} \implies n \mid (a-r) \implies a-r = nq \implies a = nq + r$, which by the Division Algorithm and $r \in \{0, 1, 2, \dots, n-1\}$ give us the equations:

$$\begin{aligned}
a_0 &= nq + 0 \\
a_1 &= nq + 1 \\
a_2 &= nq + 2 \\
&\dots \\
a_{n-1} &= nq + (n-1)
\end{aligned}$$

Letting q iterate over \mathbb{Z} we can write these n equations as $\bar{r} = \{r + qn \mid q \in \mathbb{Z}\}$ which are precisely $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$. \square

3. Prove that if $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod{9}$ (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) [note that $10 \equiv 1 \pmod{9}$].

Proof. Since $10 \equiv 1 \pmod{9}$, then $10^2 \equiv 1^2 \pmod{9}, 10^3 \equiv 1^3 \pmod{9}, \dots, 10^n \equiv 1^n \pmod{9}$. Therefore if we take each component of $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ and seeing that in general $a_n 10^n \equiv a_n \pmod{9}$ we have that:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0 \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod{9} \quad \square$$

4. Compute the remainder when 37^{100} is divisible by 29.

Noting that $37^{14} \equiv -1 \pmod{29}$ we see that $37^{100} = 37^{14}37^{14}37^{14}37^{14}37^{14}37^{14}37^{14}37^2 \equiv (-1)^7 6 \pmod{29} \implies 37^{100} \equiv -6 \pmod{29} \implies 23 \pmod{29}$. Therefore, the remainder is 23. Note that we could have also used *Fermat's Little Theorem* here since 29 is prime.

5. Compute the last two digits of 9^{1500} .

To compute the last two decimal digits of 9^{1500} we can take the mod of 100.

Since $9^{10} \equiv 1 \pmod{100}$, $9^{20} \equiv 1 \pmod{100}$, $9^{30} \equiv 1 \pmod{100}$, ... etc., we have that $9^{1500} \equiv 1 \pmod{100}$ and therefore the last two digits are 01.

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

Proof. The squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are the squares of representatives of $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

Let's take a closer look:

$$\begin{aligned}0^2 &\equiv 0 \pmod{4} \\1^2 &\equiv 1 \pmod{4} \\2^2 &\equiv 0 \pmod{4} \\3^2 &\equiv 1 \pmod{4} \\4^2 &\equiv 0 \pmod{4} \\5^2 &\equiv 1 \pmod{4} \\6^2 &\equiv 0 \pmod{4} \\7^2 &\equiv 1 \pmod{4} \dots\end{aligned}$$

Which shows us that the squares are getting mapped to $\bar{0}$ and $\bar{1}$.

To make this more general, note that by definition $\bar{0} = \{0, 0 \pm 4, 0 \pm 8, \dots\}$ and it is easy to see that if we take any multiple of 4 and square it, it will also be a multiple of 4 and therefore will have a remainder of 0 when divided by 4. A similar argument for $\bar{1}$ shows that the remainder will always be 1. For representatives from $\bar{2} = \{2, 2 \pm 4, 2 \pm 8, \dots\}$, if squared we have $(2 + 4n)(2 + 4n) = 4 + 16n + 16n^2 = 4(1 + 4n + 4n^2)$ which is divisible by 4 so will have a remainder of 0. A similar argument for the squares of representatives from $\bar{3}$ shows that they will have a remainder of 1. Therefore, the square elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$. \square

7. 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).

Proof. We have seen above that any integer squared and divided by 4 will either leave a remainder of 1 or 0. Therefore, given two integers a and b , if we square them the remainders when divided by 4 can be 0 or 1. Therefore, when summed together we can get 0, 1, or 2. Therefore, $a^2 + b^2$ never leaves a remainder of 3 when divided by 4. \square

8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b, 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.]

Proof. Suppose that the equation $a^2 + b^2 = 3c^2$ has solutions in nonzero integers. Using the above exercise we know that $a^2 + b^2$ can only have a remainder of 0, 1, or 2 when divided by 4.

Therefore, $a^2 + b^2 \equiv 0, 1, 2 \pmod{4} \implies 3c^2 \equiv 0, 1, 2 \pmod{4}$ but since the integer solutions were considered nonzero $c \neq 0$. Additionally, we know that $c \neq 1$ as that would imply that $a^2 + b^2 = 3$ but if a and b are both 1 that would equal 2 and if any of them were larger than 1 then $a^2 + b^2$ would be 5 or greater. Thus, $3c^2 \equiv 2 \pmod{4} \implies a^2 + b^2 \equiv 2 \pmod{4}$. Since both sides of $a^2 + b^2 = 3c^2$ are divisible by 4 the squares must have a factor of 2.

Thus, we can write $a^2 + b^2 = 3c^2$ as $4(k^2 + t^2) = 3(4)s^2$, where k, t, s are nonzero integers. Dividing the out the 4 from both sides we are left with $k^2 + t^2 = 3s^2$ but we can use the same argument for this equation as we did for the last and this process could be repeated indefinitely, which is absurd. Therefore the equation $a^2 + b^2 = 3c^2$ does not have nonzero integer solutions. (Note that this method of proof is called *proof by infinite descent* or *Fermat's method of descent*). \square

9. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Proof. An odd integer can be represented by $2n + 1, n \in \mathbb{Z}$. Therefore, $(2n + 1)^2 = (2n + 1)(2n + 1) = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$. n itself will either be an odd or even integer so we can represent this with:

$$\begin{aligned} 4((2k)^2 + 2k) + 1 &= 16k^2 + 8k + 1 = 8(2k^2 + k) + 1 \\ &\text{(for } n \text{ an even integer with } k \in \mathbb{Z}) \\ 4((2t + 1)^2 + 2t + 1) + 1 &= 16t^2 + 24t + 8 + 1 = 8(2t^2 + 3t + 1) + 1 \\ &\text{(for } n \text{ an odd integer with } t \in \mathbb{Z}) \end{aligned}$$

Therefore, we have shown that the square of any odd integer always leaves a remainder of 1 when divided by 8 as the two above equations are $(2n + 1)^2 \equiv 1 \pmod{8}$. \square

10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ -function.

Proof. The residue classes of $\mathbb{Z}/n\mathbb{Z}$ are $\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$. Additionally, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}$.

Therefore, $\bar{a} \cdot \bar{c} = \bar{1} \implies (a + kn)(c + gn) = 1 + sn$ for integers k, g, s .

$(a + kn)(c + gn) = 1 + sn \implies ac + agn + ckn + kgn^2 = 1 + sn \implies n(kng + ck + ag) + ac = 1 + sn$ so that:

$$ac + n(kng + ck + ag - s) = 1 \implies (a, n) = 1 \text{ and } (c, n) = 1$$

This shows us that representatives of the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are relatively prime with n . Therefore, the amount of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ will be equal to the number of elements that have representatives relatively prime to n which is equal to $\varphi(n)$ by definition. \square

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

Proof. If $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then we know that there exists \bar{c} and \bar{d} such that $\bar{a} \cdot \bar{c} = \bar{1}$ and $\bar{b} \cdot \bar{d} = \bar{1}$ so that:

$$(\bar{a} \cdot \bar{c})(\bar{b} \cdot \bar{d}) = \bar{1} \cdot \bar{1} \implies (\bar{a} \cdot \bar{b})(\bar{c} \cdot \bar{d}) = \bar{1} \cdot \bar{1}$$

Therefore, if we can show that $\bar{1} \cdot \bar{1} = \bar{1}$, then by definition $\bar{a} \cdot \bar{b}$ and $\bar{c} \cdot \bar{d}$ will be elements in $(\mathbb{Z}/n\mathbb{Z})^\times$.

$$\begin{aligned}\bar{1} \cdot \bar{1} &= (1 + kn)(1 + sn) \text{ for some } k, s \in \mathbb{Z} \implies \\ 1 + sn + kn + skn^2 &\implies 1 + n(s + k + skn) \implies \bar{1} \cdot \bar{1} \in \bar{1}\end{aligned}$$

Thus we have shown that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

12. 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. Since a and n are relatively prime, they have a common divisor. Therefore, $a = mx$ and $n = bx$, with $b, m, x \in \mathbb{Z}$. Thus, $ba = bmx = mn \implies ab \equiv 0 \pmod{n}$

Suppose there is a $c \in \mathbb{Z}$ such that $ac \equiv 1 \pmod{n}$. Then this means $ac = 1 + kn$ for some $k \in \mathbb{Z}$. $ac = 1 + kn \implies bac = b(1 + kn) \implies b = mnc - bkn \implies b = n(mc - bk)$, which implies that b is a multiply of n which is a contradiction with $1 \leq b < n$. Therefore, there cannot be an integer c such that $ac \equiv 1 \pmod{n}$. □

13. 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 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. Since $(a, n) = 1 \implies ac + nb = 1$ for $b, c \in \mathbb{Z}$. Thus, $ac + nb = 1 \implies ac - 1 = n(-b) \implies ac \equiv 1 \pmod{n}$. □

14. 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 $n = 12$.

Proof. From the previous two exercises the only way we can have $ac \equiv 1 \pmod{n}$ is if a and n are relatively prime (exercise 13) because when they are not relatively prime we showed that there cannot be a c that meets this criteria. Therefore, the representatives of \bar{a} and \bar{c} in the definition of $(\mathbb{Z}/n\mathbb{Z})^\times$ must be relatively prime to n so that we arrive at Proposition 4. □

15. For each of the following pairs of integers a and n , show that a is relatively prime to n and determine the multiplicative inverse of \bar{a} in $\mathbb{Z}/n\mathbb{Z}$.

(a) $a = 13, n = 20$.

$$\begin{aligned}20 &= 13(1) + 7 \\ 13 &= 7(1) + 6 \\ 7 &= 6(1) + 1 \\ \hline 17\end{aligned}$$

(b) $a = 69, n = 89$.

$$\begin{aligned}89 &= 69(1) + 20 \\ 69 &= 20(3) + 9 \\ 20 &= 9(2) + 2\end{aligned}$$

$$9 = 2(4) + 1$$

(c) $a = 1891, n = 3797. 3797 = 1891(2) + 15$
 $1891 = 15(126) + 1$

(d) $a = 6003722857, n = 77695236973.$

$$77695236973 = 6003722857(12) + 5650562689$$
$$6003722857 = 5650562689(1) + 353160168$$
$$5650562689 = 353160168(16) + 1$$

16. Write a computer program to add and multiply mod n , for any n given as input. The output of these operations should be the least residues of the sums and products of the two integers. Also include the feature that if $(a, n) = 1$, an integer c between 1 and $n - 1$ such that $\bar{a} \cdot \bar{c} = \bar{1}$ may be printed on request. (Your program should not, of course, simply quote “mod” functions already built into many systems).

Left to the reader.