1. *Prove that for every integer n, $n^3 \equiv n \pmod 6$.*

   Proof. Since multiplication and addition are well-defined on the six congruence classes modulo 6, all we need to do is show that $n \cdot n \cdot n$ is congruent to n within each of the congruence classes. So,

   $$\begin{aligned}
   &\text{When } n \equiv 0 \pmod 6\text{: } n^3 \equiv 0^3 \equiv 0 \equiv n \pmod 6\\
   &\text{When } n \equiv 1 \pmod 6\text{: } n^3 \equiv 1^3 \equiv 1 \equiv n \pmod 6\\
   &\text{When } n \equiv 2 \pmod 6\text{: } n^3 \equiv 2^3 \equiv 8 \equiv 2 \equiv n \pmod 6\\
   &\text{When } n \equiv 3 \pmod 6\text{: } n^3 \equiv 3^3 \equiv 27 \equiv 3 \equiv n \pmod 6\\
   &\text{When } n \equiv 4 \pmod 6\text{: } n^3 \equiv 4^3 \equiv 64 \equiv 4 \equiv n \pmod 6\\
   &\text{When } n \equiv 5 \pmod 6\text{: } n^3 \equiv 5^3 \equiv 125 \equiv 5 \equiv n \pmod 6
   \end{aligned}$$

   So in all 6 cases, $n^3 \equiv n \pmod 6$. □

   Alternative proof. Note that $n^3 - n = n(n-1)(n+1)$. At least one of n or $n-1$ is even, so $n(n-1)(n+1)$ is even. Also, exactly one of n, $n-1$, or $n+1$ must be divisible by 3, so $n(n-1)(n+1)$ is divisible by 3. Since $n^3 - n$ is divisible by both 2 and 3, it is divisible by 6. And by definition, since $6 \mid n^3 - n$, $n^3 \equiv n \pmod 6$. □

   Another alternative proof. We can prove this for every non-negative integer by induction, and then note that for every positive n, $(-n)^3 = -n^3 \equiv -n$, so negative integers follow the same rule. Our inductive proof starts with base case 0; $0^3 \equiv 0 \pmod 6$. Now, let us assume that for a given n, $n^3 \equiv n \pmod 6$, and proceed to prove that $(n+1)^3 \equiv n+1 \pmod 6$. We can prove that $n^2 + n$ is even by noting that it is always a sum of two numbers of the same parity. Thus, $3(n^2+n) \equiv 0 \pmod 6$, so adding this to both sides of our inductive assumption:

   $$\begin{aligned}
   n^3 &\equiv n \pmod 6\\
   n^3 + 3(n^2+n) &\equiv n + 0 \pmod 6\\
   n^3 + 3n^2 + 3n + 1 &\equiv n + 1 \pmod 6\\
   (n+1)^3 &\equiv n + 1 \pmod 6
   \end{aligned}$$

   □

2. *Let us say that, for nonzero rational numbers a and b, $a \simeq b$ if a and b have the same denominator when written in lowest terms. Explain why $\simeq$ is an equivalence relation and describe its equivalence classes.*

   To prove reflexivity, let us consider an arbitrary nonzero rational number x which has the form $\frac{p}{q}$ when written in lowest terms. Since x has the same denominator as itself (specifically: q), $x \simeq x$.

   To prove symmetry, let us consider nonzero rationals x and y such that $x \simeq y$. Let x have the form $\frac{p}{q}$ when written in lowest terms. Since $x \simeq y$, y has the same denominator, so in lowest terms y has the form $\frac{p'}{q}$ for some (possibly different) p'. Since y has the same denominator as x (specifically: q), $y \simeq x$.

   To prove transitivity, let us consider nonzero rationals x, y, and z such that $x \simeq y$ and $y \simeq z$. Let x have the form $\frac{p_1}{q}$ when written in lowest terms. Since $x \simeq y$, y has the same denominator as x, so in lowest terms y has the form $\frac{p_2}{q}$. Since $y \simeq z$, z has the same denominator as y, so y has the form $\frac{p_3}{q}$. Since x has the same denominator as z (specifically: q), $x \simeq z$.

The equivalence classes group together all numbers with the same denominator in lowest terms. For instance, the equivalence class [1] contains only nonzero integers:

$$[1] = \{\cdots, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, \cdots\}$$

while the equivalence class $[\frac{1}{2}]$ contains half-integers only:

$$[\tfrac{1}{2}] = \{\cdots, \tfrac{-9}{2}, \tfrac{-7}{2}, \tfrac{-5}{2}, \tfrac{-3}{2}, \tfrac{-1}{2}, \tfrac{1}{2}, \tfrac{3}{2}, \tfrac{5}{2}, \tfrac{7}{2}, \tfrac{9}{2}, \cdots\}$$

and so forth; note that certain equivalence classes are a bit sparse:

$$[\tfrac{1}{6}] = \{\cdots, \tfrac{-13}{6}, \tfrac{-11}{6}, \tfrac{-7}{6}, \tfrac{-5}{6}, \tfrac{-1}{6}, \tfrac{1}{6}, \tfrac{5}{6}, \tfrac{7}{6}, \tfrac{11}{6}, \tfrac{13}{6}, \cdots\}$$

In general, an archtypical equivalence class might have representative element $\frac{1}{k}$ for any positive integer k, and have elements given by the following rule:

$$[\tfrac{1}{k}] = \{\tfrac{n}{k} : n \in \mathbb{Z}, n \neq 0, \gcd(n, k) = 1\}$$

3. *Prove that for every number k there is a number N such that all of the numbers $N+1, N+2, N+3, \cdots, N+k$ are composite.*

Proof. We shall prove specifically that any $N > 1$ such that $N \equiv 1 \pmod{(k+1)!}$ satisfies this rule; we shall do this by induction on k.

In the base case $k = 1$, we are asserting that whenever $N \equiv 1 \pmod 2$ and $N > 1$, it is the case that $N + 1$ is composite. This is trivial because if $N \equiv 1 \pmod 2$ then $N + 1$ is even; since $N > 1$, $N + 1 > 2$, and thus $N + 1$ is composite, as it is divisible by 2.

For our inductive step, we assume that for $N \equiv 1 \pmod{k!}$ and $N > 1$, all of $N+1, N+2, \ldots, N+(k-1)$ are composite. Now we want to take some subset of this family of values of N and show that on them, $N + k$ is also composite. Let us specifically try to engineer it to be the case that $N + k$ is divisible by $k + 1$ (and since $N > 1$, it is not equal to $k + 1$). In particular, we want values of N such that $N + k \equiv 0 \pmod{k+1}$, or in other words, $N \equiv 1 \pmod{k+1}$.

We thus can satisfy our desired rule on N by simultaneously satisfying the two congruences:

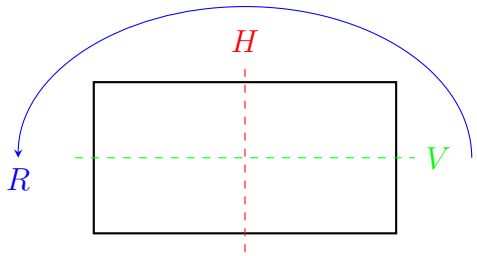
$$\begin{aligned} N &\equiv 1 \pmod{k!} \\ N &\equiv 1 \pmod{k+1} \end{aligned}$$

which is in fact true whenever $N \equiv 1 \pmod{(k+1)!}$, completing our inductive step. □

Alternative proof. An easy way to prove this result by example would be to let $N = (k+1)! + 1$. Then, note that for each $i \leq k$, $N + i = (k+1)! + i + 1$, and since $(k+1)!$ is divisible by $i + 1$, $(k+1)! + i + 1$ is also divisible by $i + 1$, so $N + i$ is divisible by $i + 1$ and thus nonprime. □

4. *Determine the symmetries of a rectangle which is not a square; give each symmetry a name and produce a Cayley table.*

A nonsquare rectangle is *not* symmetric when rotated clockwise or counterclockwise by 90°, or when reflected across a diagonal, but will be symmetric under an 180-degree rotation or a reflection across an axis bisecting an opposite pair of sides. There are thus four symmetries. including the identity transformation I, which is not pictured below, the vertical flip V, the horizontal flip H, and the rotation R.

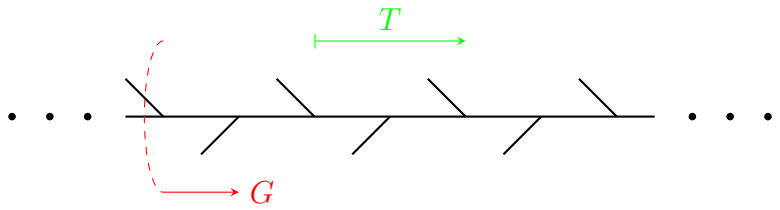


Now, to build a Cayley table, we will consider what results when we perform the various actions in sequence; obviously any action together with the identity transformation is unaffected, while performing any action twice returns things to their original state. Less obviously, performing both flips (in any order) results in the same action as the rotation, and a flip with a rotation is identical to the other flip. So our Cayley table is:

	I	V	H	R
I	I	V	H	R
V	V	I	R	H
H	H	R	I	V
R	R	H	V	I

Incidentally, this is actually an Abelian group.

5. *Describe the infinite group of symmetries of the following infinitely long figure. Determine as many rules as you can for multiplying the symmetries, and determine whether this group is Abelian.*



This shape has two fundamental transformations: a translation mapping each "quill" onto the next neighbor on the same side, denoted in the image above by T, and a glide reflection mapping each quill onto the next quill on the opposite side, denoted in the image by G. Note that there is in fact an *infinite* family of transformations so described: not only is there the transformation T, but also the result of performing T twice, called T^2, or three times, called T^3, etc. In addition we could reverse T and call it T^{-1}, or perform its reverse several times, and so forth.

Note that G can be combined with T or with itself, but performing G twice maps a quill by simple transformation, so $G^2 = T$. We could thus say that every transfromation in here is either T^k or GT^k for integer k, and we have the following compositional rules:

$$\begin{aligned} T^a T^b &= T^{a+b} \\ (GT^a)(T^b) &= GT^{a+b} \\ (T^a)(GT^b) &= GT^{a+b} \\ (GT^a)(GT^b) &= T^{a+b+1} \end{aligned}$$

And note that this group *is* Abelian.