Preliminaries

0.1: Basics

Proposition 1

1. For (not injective) $\to$ (no left inverse): if f is not injective then there exist $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, call this element $b \in B$. If a left inverse $g : B \to A$ existed it would be the case that $g(b) = a_1$ but also $g(b) = a_2$. This is not a function.
   For (injective) $\to$ (left inverse): we want to construct a $g : B \to A$ such that $g(f(a)) = a$ holds for all $a \in A$. The definition of injective given is that if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$. The contrapositive is that if $f(a_1) = f(a_2)$, then $a_1 = a_2$, meaning that the preimage of any $b \in \text{im}f$ is a one-element set $\{a\}$. Defining $g(b) = a$ means $g(f(a)) = g(b) = a$ as required.

2. For (not surjective) $\to$ (no right inverse): if f is not surjective then there exists $b \in B$ such that $b \notin \text{im}f$. Then, $f \circ g$ (for some $g : B \to A$) cannot be the identity map because $(f \circ g)(b)$ cannot be b.
   For (surjective) $\to$ (right inverse): we want to construct $g : B \to A$ such that $f(g(b)) = b$ holds for all $b \in B$. For a given $b \in B$, choose an a such that $f(a) = b$. This is always possible since $\text{im}f = B$. Define $g(b) = a$, then $f(g(b)) = f(a) = b$ as required.

3. For (bijective) $\to$ (inverse exist): if f is bijective then it is injective and surjective. From the above we see that f has a left inverse g and right inverse h, now we need to show $g = h$.

$$f = f \tag{1}$$
$$I \circ f = f \circ I \tag{2}$$
$$(f \circ h) \circ f = f \circ (g \circ f) \tag{3}$$
$$f \circ h \circ f = f \circ g \circ f \tag{4}$$
$$g \circ f \circ h \circ f = g \circ f \circ g \circ f \tag{5}$$
$$I \circ h \circ f = I \circ g \circ f \tag{6}$$
$$I \circ h \circ f \circ h = I \circ g \circ f \circ h \tag{7}$$
$$I \circ h \circ I = I \circ g \circ I \tag{8}$$
$$h = g \tag{9}$$

4. It suffices to show (injective) $\leftrightarrow$ (surjective). If f is injective then (from part 1) the preimage of every $b \in \text{im}f$ is a single element set. Since every element of A is some preimage, $|\text{im}f| = |A|$. Then since $|A| = |B|$ we see that $\text{im}f = B$. If f is surjective then $|\text{im}f| = |B|$, but $|A| \geq |\text{im}f|$ (by something like the pigeonhole principle), so $|A| = |\text{im}f|$ and we have a bijection between the two sets.

Exercises

1. Instead of checking these just work out the general case first. Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

$$MX = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} \tag{10}$$
$$XM = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix} \tag{11}$$

   The equality of the diagonal elements means $c = 0$, the equality of the top right entries means $a = d$. The general form of X is

$$X = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} . \tag{12}$$

   So in order, the answers are: yes, no, yes, no, yes, no.

2. If $P, Q \in \mathcal{B}$, $(P+Q)M = PM + QM = MP + MQ = M(P+Q)$.

3. $(PQ)M = P(QM) = P(MQ) = (PM)Q = (MP)Q = M(PQ)$.

4. See (12).

5. (a) No: then $1 = f\left(\frac{1}{2}\right) = f\left(\frac{2}{4}\right) = 2$.

   (b) Yes: $f\left(\frac{mx}{my}\right) = \frac{m^2x^2}{m^2y^2} = \frac{x^2}{y^2} = f\left(\frac{x}{y}\right)$ (anyway, this is just $x \mapsto x^2$).

6. No: then $0 = f(1.0) = f(0.\bar{9}) = 9$.

7. Reflexivity: $f(a) = f(a)$ so $a \sim a$. Symmetry: $a \sim b \implies f(a) = f(b) \implies f(b) = f(a) \implies b \sim a$. Transitivity: equality is transitive so if $a \sim b$ and $b \sim c$ then $f(a) = f(b) = f(c)$ so $a \sim c$.

0.2: Properties of the Integers

Exercises

1. Future Eric promises to do this boring computation: find GCD using the Euclidean Algorithm, then LCM = product/GCD

2. If $k|a$ and $k|b$ then $a = mk$ and $b = nk$ for some $m, n \in \mathbb{Z}$. Then $as + bt = mks + nkt = k(ms + nt)$.

3. If n is composite then it is either a power of a prime p^n or its prime factorization $\prod_i p_i^{n_i}$ contains multiple primes. In the first case, $a = p$ and $b = p^{n-1}$. In the second case, $a = p_1^{n_1}$ and $b = \prod_{i>1} p_i^{n_i}$.

4. $ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + a\frac{b}{d}t - b\frac{a}{d}t = N$

5. Future Eric does not promise to do this boring computation

6. Call the set A. If $|A| = 1$, trivially that element m is the minimal element. For $|A| = n > 1$ elements, choose one element a (finite choice) and make the set $A^* = \{b | b \in A, b \neq a\}$. Then A^* has a minimal element, call it m_{n-1}. Since A is a set, $a \neq m_{n-1}$. Then one of them is smaller, and is the unique minimal element of A.

7. If $a^2 = pb^2$ then $p = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$. Any prime factor on the right-hand side shows up an even number of times; the only prime factor on the left-hand side shows up once (an odd number of times).

8. ?

9. programming

10. ?

11. Write the prime factorization of n as $\prod_i p_i^{n_i}$. Then $\phi(n) = \prod_i (p_i - 1)p_i^{n_i - 1}$. If $d|n$ then all the prime factors of d are prime factors of n; the prime factorization of d is $p_{i_1}^{m_1} \dots p_{i_j}^{m_j}$ where $i_1 \dots i_j$ are some labels of prime factors of n and all m_i are at most the corresponding n_i. Then $\phi(d) = \prod_k (p_{i_k} - 1)p_k^{m_k - 1}$. Comparing to $\phi(n)$, we see $(p_{i_k} - 1)p_k^{m_k - 1} | (p_k - 1)p_k^{n_k - 1}$ since $n_k \geq m_k$. This is true for each prime factor of d.

0.3: $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Exercises

1. $\bar{0} : \{\dots, -36, -18, 0, 18, 36, \dots\}$
   $\bar{1} : \{\dots, -35, -17, 1, 19, 37, \dots\}$
   $\bar{n} : \{\dots, -36 + n, -18 + n, n, 18 + n, 36 + n, \dots\}$

2. For $a \in \mathbb{Z}$, there exists unique $q, r \in \mathbb{Z}$ with $r \in [0, n)$ such that $a = qn + r$. Then a and r are in the same equivalence class modulo n.

3. Write $a = \sum_i a_i 10^i$. Then

$$a \bmod 9 = \sum_i \left(a_i 10^i\right) \bmod 9 \tag{13}$$

$$= \sum_i (a_i) \bmod 9 \left(10^i\right) \bmod 9 \tag{14}$$

$$\equiv \sum_i (a_i) \bmod 9 \,(10 \bmod 9)^i \tag{15}$$

$$= \sum_i (a_i) \bmod 9 \,(1 \bmod 9)^i \tag{16}$$

$$= \sum_i (a_i) \bmod 9 \,(1 \bmod 9) \tag{17}$$

$$= \sum_i a_i \bmod 9 \tag{18}$$

4. $37 \equiv 8 \mod 29$, so we want $8^{100} \mod 29$. Notice that $8^2 = 64 = 58 + 8 \equiv 8 \mod 29$ so you can keep multiplying by 8 to find $8 \equiv 8^2 \equiv 8^3 \equiv \ldots \equiv 8^{100}$.

5. We want $9^{1500} \mod 100$. Note that (trial and error) $9^1 0 \equiv 1 \mod 100$. Then $9^{1500} = (9^{10})^{150} \equiv 1^{150} \mod 100 = 1 \mod 100$.

6. $0^2 = 0$; $1^2 = 1$; $2^2 = 4 \equiv 0$; $3^2 = 9 \equiv 1$

7. Both a^2 and b^2 are 0 or 1 mod 4, so their sum is 0, 1 or 2 mod 4 (not 3).

8. The left-hand side of $a^2 + b^2 = 3c^2$ is, from above, in one of $\bar{0}, \bar{1}, \bar{2}$. Since c^2 is in $\bar{0}$ or $\bar{1}$, the right-hand side is in $\bar{0}$ or $\bar{3}$. For equality the only option is that c^2 is in $\bar{0}$ while a^2 and b^2 are either both in $\bar{0}$ or $\bar{2}$. In either case all are even; being squares, this means that a^2, b^2, c^2 are all divisible by 4 and in $\bar{0}$, so we can divide both sides by 4. This can be repeated ad infinitum, even though $a^2, b^2, c^2 > 0$ and there is a minimal positive integer 1.

9. $1^2 = 1$; $3^3 = 9 \equiv 1$; $5^2 = 25 \equiv 1$; $7^2 = 49 \equiv 1$; any higher odd integer is equivalent to one of these.

10. $(\mathbb{Z}/n\mathbb{Z})^x = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\}$, and $\phi(n)$ is the number of a on $[1, n]$ (equivalent to $[0, n-1]$ modulo n) such that $(a, n) = 1$.

11. If $(a, n) = 1$ and $(b, n) = 1$, then, taking the prime factorizations of all three, we see that a and n have no prime factors in common (likewise for b and n). Then ab has no prime factors in common with n, so $(ab, n) = 1$. Take everything modulo n to complete the proof.

12.

13. If $(a, n) = 1$ then there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Take both sides modulo n to get $(a \mod n)(x \mod n) \equiv 1 \mod n$. Then $c = x$, or any equivalent.

14. Exercise 12 shows that if $(a, n) \neq 1$, then there is no c such that $ac \equiv 1 \mod n$. Exercise 13 shows that if $(a, n) = 1$, then there is such a c. We can take c to be on $[0, n-1)$ without loss of generality. Then $\{\bar{a} | (a, n) = 1\} = \{\bar{a} | \exists c \text{ such that } \bar{a} \cdot \bar{c} \equiv 1 \mod n\}$. For $n = 12$, the first set is $\{1, 5, 7, 11\}$. To see which elements aren't invertible we have to make a times table:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

15. Future Eric does not promise to do this boring computation
16. programming