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 $b \in \mathrm{im} f$ 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 $b \notin \mathrm{im} f$. 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 $\mathrm{im} f = B$. 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 $b \in \mathrm{im} f$ is a single element set. Since every element of A is some preimage, $|\mathrm{im} f| = |A|$. Then since $|A| = |B|$ we see that $\mathrm{im} f = B$.
   If f is surjective then $|\mathrm{im} f| = |B|$, but $|A| \geq |\mathrm{im} f|$ (by something like the pigeonhole principle), so $|A| = |\mathrm{im} f|$ 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. Find the gcd using the Euclidean Algorithm, then lcm $= \frac{ab}{(a,b)}$.

   (a) Find the gcd first:

$$
\begin{align}
20 &= 1 \cdot 13 + 7 \tag{13}\\
13 &= 1 \cdot 7 + 6 \tag{14}\\
7 &= 1 \cdot 6 + 1 \tag{15}\\
6 &= 6 \cdot 1 \tag{16}
\end{align}
$$

   so $(20, 13) = 1$. Then the lcm is $\frac{20 \cdot 13}{1} = 260$.

   (b) Find the gcd first:

$$
\begin{align}
372 &= 5 \cdot 69 + 27 \tag{17}\\
69 &= 2 \cdot 27 + 15 \tag{18}\\
27 &= 1 \cdot 15 + 12 \tag{19}\\
15 &= 1 \cdot 12 + 3 \tag{20}\\
12 &= 4 \cdot 3 \tag{21}
\end{align}
$$

   so $(69, 372) = 3$. Then the lcm is $\frac{69 \cdot 372}{3} = 8556$.

   (c) Find the gcd first:

$$
\begin{align}
792 &= 2 \cdot 275 + 242 \tag{22}\\
275 &= 1 \cdot 242 + 33 \tag{23}\\
242 &= 7 \cdot 33 + 11 \tag{24}\\
33 &= 3 \cdot 11 \tag{25}
\end{align}
$$

   so $(792, 275) = 11$. Then the lcm is $\frac{792 \cdot 275}{11} = 19800$.

   (d) Find the gcd first:

$$
\begin{align}
11391 &= 2 \cdot 5673 + 45 \tag{26}\\
5673 &= 126 \cdot 45 + 3 \tag{27}\\
45 &= 15 \cdot 3 \tag{28}
\end{align}
$$

   so $(11391, 5673) = 3$. Then the lcm is $\frac{11391 \cdot 5673}{3} = 21540381$.

(e) Find the gcd first:

$$\begin{aligned}
1761 &= 1 \cdot 1567 + 194 && (29)\\
1567 &= 8 \cdot 194 + 15 && (30)\\
194 &= 12 \cdot 15 + 14 && (31)\\
15 &= 1 \cdot 14 + 1 && (32)\\
14 &= 14 \cdot 1 && (33)
\end{aligned}$$

so $(1761, 1567) = 1$. Then the lcm is $\frac{1761 \cdot 1567}{1} = 2759487$.

(f) Find the gcd first:

$$\begin{aligned}
507885 &= 8 \cdot 60808 + 21421 && (34)\\
60808 &= 2 \cdot 21421 + 17966 && (35)\\
21421 &= 1 \cdot 17966 + 3455 && (36)\\
17966 &= 5 \cdot 3455 + 691 && (37)\\
3455 &= 5 \cdot 691 && (38)
\end{aligned}$$

so $(507885, 60808) = 691$. Then the lcm is $\frac{507885 \cdot 60808}{691} = 44693880$.

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. `https://oeis.org/A000010` lol

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. We want to find the exponent of p in the prime factorization of $n!$, call this $f(n, p)$. For now say $p = 7$, since 7 is a small prime, but still big enough where it feels like a real prime (sorry 5). Obviously $f = 0$ for $n = 1, 2, 3, 4, 5, 6$, then it jumps up to 1 when we reach $n = 7$. It stays at 1 until we reach $n = 14$, where it jumps to 2. This suggests that

$$f(n, 7) \sim \left\lfloor \frac{n}{7} \right\rfloor \ . \tag{39}$$

This form works until we hit $n = 49$, which contributes two factors of 7. In fact, every multiple of 49 contributes twice, but so far we've only counted it once. That means we have to increment f by another 1 every 49 factors:

$$f(n, 7) \sim \left\lfloor \frac{n}{7} \right\rfloor + \left\lfloor \frac{n}{49} \right\rfloor \ . \tag{40}$$

The same is true for $n = 343 = 7^3$: it's a multiple of 7, and of 49, so we've counted it twice, but we should count it three times. Then again for 7^4, etc. In total we have (the actual answer)

$$f(n, 7) = \left\lfloor \frac{n}{7} \right\rfloor + \left\lfloor \frac{n}{49} \right\rfloor + \left\lfloor \frac{n}{343} \right\rfloor + \ldots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{7^k} \right\rfloor \ . \tag{41}$$

In practice, infinitely many of the terms being summed are zero, e.g. $n = 1000$ doesn't have any contribution from multiples of 7^{1000}. The contributions stop when

$$n < 7^k \implies \log n < k \log 7 \implies \frac{\log n}{\log 7} < k \ , \tag{42}$$

so an equivalent form of the sum is

$$f(n,7) = \sum_{k=1}^{\lceil \log_7 n \rceil} \left\lfloor \frac{n}{7^k} \right\rfloor \ . \tag{43}$$

The generalization to all primes p is obvious now:

$$f(n,p) = \sum_{k=1}^{\lceil \log_p n \rceil} \left\lfloor \frac{n}{p^k} \right\rfloor \ . \tag{44}$$

9.
```python
def get_gcd(a,b):
    if b == 0:
        return 0, (0,0)

    if b>a:
        #have to swap the tuple order first
        ans = get_gcd(b,a)
        return ans[0], ans[1][::-1]

    #keep track of coefficients to get linear combination
    coeffsA = (1,0) #a = 1*a + 0*b
    coeffsB = (0,1) #b = 0*a + 1*b

    while True:
        #a = nb + r
        n = a//b
        r = a - n*b
        if r == 0:
            return b, coeffsB

        #else keep going
        tmp = coeffsB
        coeffsB = ( coeffsA[0]-n*coeffsB[0], coeffsA[1]-n*coeffsB[1] )
        coeffsA = tmp

        a = b
        b = r

print(get_gcd(20,13)) #(1, (2, -3))
print(get_gcd(69,372)) #(3, (27, -5))
print(get_gcd(792,275)) #(11, (8, -23))
print(get_gcd(11391,5673)) #(3, (-126, 253))
print(get_gcd(1761,1567)) #(1, (-105, 118))
print(get_gcd(507885,60808)) #(691, (-17, 142))
```

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

$$\begin{aligned} a \bmod 9 &= \sum_i \left(a_i 10^i\right) \bmod 9 && (45)\\ &= \sum_i \left(a_i \bmod 9\right)\left(10^i \bmod 9\right) && (46)\\ &\equiv \sum_i \left(a_i \bmod 9\right)\left(10 \bmod 9\right)^i && (47)\\ &= \sum_i \left(a_i \bmod 9\right)\left(1 \bmod 9\right)^i && (48)\\ &= \sum_i \left(a_i \bmod 9\right)\left(1 \bmod 9\right) && (49)\\ &= \sum_i a_i \bmod 9 && (50) \end{aligned}$$

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) $9^10 \equiv 1 \mod 100$. 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. $(\mathbb{Z}/n\mathbb{Z})^x = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$, 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 $\{\bar{a} \mid (a, n) = 1\} = \{\bar{a} \mid \exists c \text{ such that } \bar{a} \cdot \bar{c} \equiv 1 \mod n\}$. 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. I will be an honest person and not do this on the computer (I did 0.3.16 first):

    (a) We did this one in 0.2.1.a, now solve for the remainder in each line to find the gcd as a linear combination of a and n.
    The first line gives $7 = 20 - 13$.
    The second line gives $6 = 13 - 7 = 2 \cdot 13 - 20$.
    The third line gives $1 = 7 - 6 = -3 \cdot 13 + 2 \cdot 20$.
    Now take both sides modulo 20 to get $1 \equiv -3 \cdot 13 \equiv 17 \cdot 13$. The inverse of 13 is 17.

    (b) From scratch, sadly

    $$89 = 1 \cdot 69 + 20 \qquad \Longrightarrow 20 = 1 \cdot 89 - 1 \cdot 69 \tag{51}$$
    $$69 = 3 \cdot 20 + 9 \qquad \Longrightarrow 9 = 69 - 3 \cdot 20 = -3 \cdot 89 + 4 \cdot 69 \tag{52}$$
    $$20 = 2 \cdot 9 + 2 \qquad \Longrightarrow 2 = 20 - 2 \cdot 9 = 7 \cdot 89 - 9 \cdot 69 \tag{53}$$
    $$9 = 4 \cdot 2 + 1 \qquad \Longrightarrow 1 = 9 - 4 \cdot 2 = -31 \cdot 89 + 40 \cdot 69 \tag{54}$$
    $$2 = 2 \cdot 1 \tag{55}$$

    The inverse of 69 is 40.

    (c) Why don't they reuse numbers man

    $$3797 = 2 \cdot 1891 + 15 \qquad \Longrightarrow 15 = 1 \cdot 3797 - 2 \cdot 1891 \tag{56}$$
    $$1891 = 126 \cdot 15 + 1 \qquad \Longrightarrow 1 = 1891 - 126 \cdot 15 = -126 \cdot 3797 + 253 \cdot 1891 \tag{57}$$
    $$15 = 15 \cdot 1 \tag{58}$$

    The inverse of 1891 is 253.

    (d) I refuse to write these numbers more than once so, $n = 77695236973$, $a = 6003722857$.

    $$n = 12 \cdot a + 5650562689 \text{ (why)} \qquad \Longrightarrow 5650562689 = n - 12a \tag{59}$$
    $$a = 1 \cdot 5650562689 + 353160168 \qquad \Longrightarrow 353160168 = a - 5650562689 = -n + 13a \tag{60}$$
    $$5650562689 = 16 \cdot 353160168 + 1 \qquad \Longrightarrow 1 = 5650562689 - 16 \cdot 353160168 = 17n - 220a \tag{61}$$
    $$353160168 = 353160168 \cdot 1 \tag{62}$$

    The inverse of a is $-220 = n - 220 = 77695236753$.

16. Reuse the gcd code from 0.2.9 to get inverses: if $(a, n) = 1$, then $1 = ax + by$ for some $x, y \in \mathbb{Z}$, then taking both sides modulo n gives x as the inverse of a.

```
def get_gcd(a,b):
    if b == 0:
        return 0, (0,0)

    if b>a:
        #have to swap the tuple order first
        ans = get_gcd(b,a)
        return ans[0], ans[1][::-1]

    coeffsA = (1,0) #a = 1*a + 0*b
    coeffsB = (0,1) #b = 0*a + 1*b

    while True:
        #a = nb + r
        n = a//b
        r = a - n*b
        if r == 0:
            return b, coeffsB

        #else keep going
        tmp = coeffsB
        coeffsB = ( coeffsA[0]-n*coeffsB[0], coeffsA[1]-n*coeffsB[1] )
        coeffsA = tmp

        a = b
        b = r
```

```

def get_inv(a,n):
    gcd, coeffs = get_gcd(a,n)
    if gcd == 1:
        #then coeffs[0]*a + coeffs[1]*n = 1
        #take mod n, coeffs[0]*a = 1
        return modn(coeffs[0],n)
    else:
        return None

def modn(a,n):
    q = a//n
    return a - n*q

def addmodn(a,b,n):
    return modn(a+b,n)
def multmodn(a,b,n):
    return modn(a*b,n)

print(modn(-11,12)) #1
print(addmodn(13,5,12)) #6
print(multmodn(7,7,12)) #1
print()
#verify the solution for 0.3.14:
for i in range(24):
    print(i, get_inv(i,12)) #None other than 1,5,7,11, which are their own inverses
print()
#verify the solution for 0.3.15:
print(get_inv(13,20)) #17
print(get_inv(69,40)) #29
print(get_inv(1891,3797)) #253
print(get_inv(6003722857,77695236973)) #77695236753
```