Solutions to Assignment 1

1. Show that $0 = 1$ in a ring if and only if the ring consists of just one element 0 with $0 + 0 = 0$ and $0 \cdot 0 = 0$.

2. In a ring, check that $a.0 = 0 = 0.a$ for any element a of the ring.

3. Check that the axioms of a ring are satisfied by $\mathbb{Z}/n$. (Hint: One can always take remainder "at the end.")

Solution: Given integers a and b we perform division by n

$$a = cn + d \text{ and } b = en + f$$

with d and f non-negative integers less than n.

If $(e + f) = gn + h$ is the division of $e + f$ by n, then

$$a + b = (c + d)n + e + f = (c + d + g)n + h$$

is the division of $a + b$ by n. Hence, whether we take remainder modulo n before addition or after addition, the result is the same.

Similarly, if $ef = kn + m$ is the division of ef by n, then

$$ab = (cen + cf + ed)n + ef = (cen + cf + ed + k)n + m$$

is the division of ab by n. Hence, whether we take the remainder modulo n before multiplication of after multiplication, the result is the same.

Now the required identities for associative laws, distributive laws and identity hold in integers *before* taking remainder modulo n and so they will also hold *after* taking remainder modulo n. For example, given a, b and c integers, we have $a(b+c) = ab+ac$ so we also have $(a(b + c))\%n = (ab + bc)\%n$. Now, we apply the above results to get

$$(a(b + c))\%n = (a\%n)((b + c)\%n) = (a\%n)((b\%n) + (c\%n))$$

similarly,

$$(ab + ac))\%n = (((ab)\%n) + ((ac)\%n)) = ((a\%n)(b\%n) + (a\%n)(c\%n))$$

This shows that

$$(a\%n)((b\%n) + (c\%n)) = ((a\%n)(b\%n) + (a\%n)(c\%n))$$

which is the distributive law for $\mathbb{Z}/n$.

4. Check that the program below calculates the greatest common divisor of a and b. (Hint: We only need to check that the greatest common divisor is *invariant* under the above substitutions.)

```
def gcd(a,b):
    a, b = abs(a), abs(b)
    if b > a:
        a, b = b, a
    while b != 0:
        a, b = b, a%b
    return a
```

Solution: We note that the following statments hold for the greatest common divisor of two integers a and b (we use $\gcd(a, b)$ for this operation:

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(a, b) = \gcd(|a|, b)$
3. $\gcd(a, b) = \gcd(a\%b, b)$
4. $\gcd(a, 0) = a$.

It follows that at each stage of the program, we are calculating the same number. As a result of the `if` statment, we have $a \geq b$ and the result of the `while` loop keeps this inequality unchanged. At the same time, in the `while` loop, the numbers are becoming smaller since $a\%b < b$ as long as $b \neq 0$. Thus, the calculation must stop with $b = 0$.

5. Given three numbers a, b and c, we can calculate $d = \gcd(\gcd(a, b), c)$. Check that d is the greatest common divisor of a, b and c.

Solution: If d is a divisor of a, b and c, then it is also a divisor of $\gcd(a, b)$. Conversely, if d is a divisor of $\gcd(a, b)$ and of c, then d also divides a and b. We therefore have equality of the two sets

$$\{d : d \geq 0, d|a, d|b, d|c\}\{d : d \geq 0, d|\gcd(a, b), d|c\}$$

Since $\gcd(\gcd(a, b), c)$ is the maximum of the set on the right and $\gcd(a, b, c)$ is the maximum of the set on the left, these two numbers are equal.

6. If the greatest common divisor of S is d then show that any multiple of d can be written as a *finite* additive combination of multiples of elements of S.

Solution: First of all, we note that if S contains T, then the greatest common divisor S is bounded above by the greatest common divisor of T. Since the greatest common divisor is a non-negative number, we see that there is a *finite* set T such that the greatest common divisor of T is the same as the greatest common divisor of S.

Next, we note that it is enough to write the greatest common divisor of T as an additive combination of elements of T; the case of a multiple follows by multiplying the additive combination obtained and an application of the distributive law.

Suppose we prove that for any integers a and b, for suitable integers A and B, we have $\gcd(a, b) = aA+bB$. We can write $T = T_! \cup \{c\}$ and apply this to $\gcd(\gcd(T_1), c)$ to get (using the previous exercise inductively!)

$$\gcd(T) = \gcd(\gcd(T_1), c) = \gcd(T_1)D + cC$$

for suitable integers D and C. Since we can assume that T_1 is a *smaller* finite set than T, we can assume the result for T_1 and write $\gcd(T_1)$ as a combination of elements of T_1. The result would then follow. Thus, we are reduced to the case where T has two elements a and b.

Now we use the program that calculates $\gcd(a, b)$ and note that $a\%b = a - b \cdot (a//b)$ is an additive combination of a and b and so is $b = a \cdot 0 + b \cdot 1$. Thus, at each stage the new pair consists of additive combinations of the old pair. Moreover, if e is an additive combination of c and d where c and d are additive combinations of a and b, then e is an additive combination of a and b. Since the final answer is one element of the pair, we see that $\gcd(a, b)$ is an additive combination of a and b.

7. Consider the set R of real numbers of the form $a + b\sqrt{5}$ where a and b are *integers* with the usual operations of addition and multiplication of real numbers. Check that R as defined above is a ring.

Solution: Since the collection of real numbers is a ring, we only need to check that R is closed under addition and multiplication, and that it contains 0 and 1.

1. We have $0 = 0 + 0 \cdot \sqrt{5}$ and $1 = 1 + 0\sqrt{5}$.
2. We have
$$a + b\sqrt{5} + c + d\sqrt{5} = (a + c) + (b + d)\sqrt{5}$$

3. We have
$$(a + b\sqrt{5})(c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5}$$

This completes the check.

8. Show that $(m\mathbb{Z}) \cdot (n\mathbb{Z}) = (mn) \cdot \mathbb{Z}$ and $(m\mathbb{Z}) + (n\mathbb{Z}) = \gcd(m, n)\mathbb{Z}$.

Solution: We note that $(ma)(nb) = (mn)(ab)$ by associativity and commutativity of multiplication. Hence, the left-hand side of the first identity is contained the right-hand side of the first identity. Conversely, $(mn)a = (ma)(n \cdot 1)$ so that the right-hand side is contained in the left-hand side as well. This proves the first identity.

We have seen earlier that every multiple of the gcd of a pair of numbers m and n is an additive combination of m and n. This proves that the right-hand side of the second identity is contained in the left-hand side of this identity. Conversely $ma+nb$ is divisible by any divisor of m and n, hence it is a multiple of $\gcd(m, n)$.; this proves that the left-hand side is contained in the right-hand side.

9. More generally, for any ring R and ideals I and J in R, show that $I \cdot J$ and $I + J$ are ideals in R.

Solution: Recall that $I + J$ consists of elements of the form $a + b$ with a in I and b in J. By the associativity and commutativity of addition, we have $(a+b)+(c+d) = (a + c) + (b + d)$. Hence, if a and c lie in I and b and d lie in J, then the right hand side lies in $I + J$. This shows that $I + J$ is closed under addition. Similarly, the distributive law says that $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$. Now, if a lies in I, which is an ideal, then so does $c \cdot a$. Similarly, J is an ideal and b lies in J means that $c \cdot b$ lies in J. Hence, the right-hand side lies in $I + J$ showing that $I + J$ is closed under left multiplication by c in R. A similar argument can be used for right multiplication. (Note that if I and J are *only* closed under left multiplication by elements of R, then the same applies to $I + J$.)

Recall that $I \cdot J$ consists of finite sums of the form $\sum_i a_i \cdot b_i$ where a_i are in I and b_i are in J. This is clearly closed under addition. If c is any element of R, then
$$c \cdot (\sum_i a_i \cdot b_i) = \sum_i c \cdot (a_i \cdot b_i) = \sum_i (c \cdot a_i) \cdot b_i$$
where we have applied the distributive law and the associative law. Now I is an ideal, so a_i lies in I implies that $c \cdot a_i$ lies in I. This shows that the right-hand side lies in $I \cdot J$. Similarly, on multiplication by c on the right, we use the fact that $b_i \cdot c$ lies in J when b_i lies in J. (Note that we only use that I is closed under left multiplication ahd J is closed under right multiplication!)

10. Given a ring R, we can define a set map $r : \mathbb{Z} \to R$ by defining the image of 0 as 0 (in R), the image of a positive integer n is the sum of n copies of 1 (in R), the image of a negative integer $-n$ is the sum of n copies of -1 (in R).

    Check that the above map r has the property that $r(m+n) = r(m)+r(n)$ and $r(m\cdot n) = r(m) \cdot r(n)$.

Solution: If m is positive and $n = -k$ is negative, then there are three cases to consider $m > k$ and $m = k$ and $m < k$. In the first case, we have $m+n = m-k > 0$. In this case $r(m + n)$ is a sum of $m - k$ copies of 1. On the other hand $r(m)$ is the sum of m copies of 1 in R and $r(n)$ is a sum of k copies of -1 in R. Since addition is commutative and associative in R, we can re-group this into $m - k$ copies of 1 in R, and k copies of pairs of 1 and -1 in R. As -1 is the additive inverse of 1 in R, the latter pairs add up to 0 in R. Making use of the additive identity property of R we see that the result is just the sum of $m - k$ copies of 1 in R as required. The remaining cases are similar.

The remaining cases for addition are similar to the one above.

The case of multiplication can be done in a similar fashion using the distributive law and the associative law for addition, together with the fact that 1 is the additive identity. However, we need one further ingredient as follows.

$$1+(-1) = 0 = (-1)\cdot 0 = (-1)\cdot((-1)+1) = (-1)\cdot(-1)+(-1)\cdot 1 = (-1)\cdot(-1)+(-1)$$

Adding 1 to both sides ("on the right"!), we see that

$$\begin{aligned} 1 = 1 + 0 = \\ &1 + ((-1) + 1) = (1 + (-1)) + 1 = ((-1) \cdot (-1) + (-1)) + 1 = \\ &\qquad (-1) \cdot (-1) + ((-1) + 1) = (-1) \cdot (-1) + 0 = (-1) \cdot (-1) \end{aligned}$$

In other words, we derive the ("obvious") identity $1 = (-1) \cdot (-1)$. This is required in the proof that $r(mn) = r(m)r(n)$ when m and n are negative.

11. If $f : R \to S$ is a homomorphism of rings then define the set I to consist of elements a such that $f(a) = 0$. Check that I is an ideal.

Solution: If a and b lie in I and c lies in R, then we have

$$\begin{aligned} f(a + b) = f(a) + f(b) = 0 + 0 = 0 \text{ and} \\ &f(c \cdot a) = f(c) \cdot f(a) = f(c) \cdot 0 = 0 \text{ and} \\ &\qquad f(a \cdot c) = f(a) \cdot f(c) = 0 \cdot f(c) = 0 \end{aligned}$$

This shows that $a + b$, $c \cdot a$ and $a \cdot c$ lie in I. Hence, I is an ideal.

12. What are the elements a and a' of R such that $a + I = a' + I$?

> **Solution:** Given that $a + I = a' + I$, we see that a' is an element of the right-hand side. Hence, it is an element of the left-hand side and so $a' = a + b$ for some b in I. It follows that $a' - a = b$ lies in I. So the condition $a + I = a' + I$ can be also written as $(a' - a) \in I$.

13. Check that R/I with the operations $\oplus$ and $\odot$ as addition and multiplication forms a ring with $0 + I$ and $1 + I$ as additive and multiplicative identity respectively.

> **Solution:** One only needs that $(a + I) \oplus (b + I)$ is $(a + b) + I$ and $(a + I) \odot (b + I) = (a \cdot b) + I$. Since, addition and multiplication satisfy the necessary axioms in R, the same axioms follow automatically! (See the proof for the ring properties for $\mathbb{Z}/n$.)

14. **Starred** Look for other examples of rings that you have already learned about so far.

> **Solution:** Various collections of functions are rings. For example, the ring of continuous functions, the ring of differentiable functions and so on.