HOMEWORK 1: SOLUTIONS

1. (Divisibility is transitive) Prove directly from the definition of divisibility that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Solution. Suppose that $a \mid b$ and $b \mid c$. There are $m, n \in \mathbb{Z}$ such that $b = am$ and $c = bn$. So $c = bn = (am)n = a(mn)$. By definition, $a \mid c$.

2. (Division algorithm) The division algorithm asserts that for any integers $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that

$$a = qb + r, \qquad 0 \leq r < |b|.$$

(1) Let x be a real number. Denote by m and n the greatest integer not exceeding x and the least integer no less than x, respectively. Show that

$$x - 1 < m \leq x \leq n < x + 1.$$

Solution. The inequalities $m \leq x$ and $n \geq x$ are immediate. Since m and n are the greatest and least such integers, respectively, we have $m + 1 > x$ and $n - 1 < x$. Putting these inequalities together gives $x - 1 < m \leq x \leq n < x + 1$.

(2) Prove the existence part of the division algorithm.

Solution. Suppose first that $b > 0$. Let q be the greatest integer not exceeding a/b and write $r = a - qb$. By Part (1), we have

$$\frac{a}{b} - 1 < q \leq \frac{a}{b}.$$

Multiplying both sides by b, we get $a - b < qb \leq a$, which is equivalent to $0 \leq r < b = |b|$.

Now consider the case $b < 0$. Let q be the least integer no less than a/b and put $r = a - qb$. By Part (1) again,

$$\frac{a}{b} \leq q < \frac{a}{b} + 1.$$

Multiplying both sides by b and keeping in mind $b < 0$, we get $a + b < qb \leq a$. Since $b = -|b|$, this is equivalent to $0 \leq r < |b|$.

(3) Prove the uniqueness part of the division algorithm: if there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < |b|,$$
$$a = q_2 b + r_2, \qquad 0 \leq r_2 < |b|,$$

then $q_1 = q_2$ and $r_1 = r_2$.

Solution. Equating the right-hand sides of the above two equations, we get

$$q_1 b + r_1 = q_2 b + r_2, \tag{1}$$

i.e.,

$$r_1 - r_2 = (q_2 - q_1)b.$$

In particular, $b \mid r_1 - r_2$. But $0 \leq r_1, r_2 < |b|$ implies $|r_1 - r_2| < |b|$. So $r_1 = r_2$. Combining this with Equation (1) leads to $q_1 = q_2$.

3. (Definition of ideal) Show that for any $a, b \in \mathbb{Z}$, the set

$$I_{a,b} = \{ax + by : x, y \in \mathbb{Z}\}$$

is an ideal of $\mathbb{Z}$.

Solution. We verify the definition of ideal as follows.

(a) $0 \in I_{a,b}$: This is clear as $0 = a \cdot 0 + b \cdot 0 \in I_{a,b}$.

(b) If $z, w \in I_{a,b}$, then $z + w \in I_{a,b}$: if $z = ax + by$ and $w = ax' + by'$, then

$$z + w = (ax + by) + (ax' + by') = a(x + x') + b(y + y') \in I_{a,b}.$$

(c) If $n \in \mathbb{Z}$ and $z \in I_{a,b}$, then $nz \in I_{a,b}$: writing $z = ax + by$, we have

$$nz = n(ax + by) = a(nx) + b(ny) \in I_{a,b}.$$

Therefore, $I_{a,b}$ is an ideal of $\mathbb{Z}$.

4. (Multiplying congruences) Use the definition of congruence to show that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Solution. By definition of congruence, $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ mean $m \mid a_1 - b_1$ and $m \mid a_2 - b_2$, respectively. Since

$$a_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + (a_2 - b_2)b_1,$$

linearity yields $m \mid a_1 a_2 - b_1 b_2$, which is equivalent to $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

5. (A divisibility test) Prove that a nonzero integer is divisible by 3 if and only if the sum of its base-10 decimal digits is divisible by 3. What can you say about divisibility by 11?

Solution. Suppose that $n \in \mathbb{Z} \setminus \{0\}$ with base-10 decimal expansion given by

$$n = \epsilon \sum_{k=0}^{m} a_k 10^k,$$

where $\epsilon \in \{-1, 1\}$ and $a_k \in \{0, 1, ..., 9\}$ for each $0 \leq k \leq m$. Since $10 \equiv 1 \pmod{3}$, we have $10^k \equiv 1 \pmod{3}$ for each $0 \leq k \leq m$. It follows that

$$n \equiv \epsilon \sum_{k=0}^{m} a_k \pmod{3}.$$

Consequently, $n \equiv 0 \pmod{3}$ if and only if

$$\sum_{k=0}^{m} a_k \equiv 0 \pmod{3}.$$

So n is divisible by 3 if and only if the sum of its base-10 decimal digits is divisible by 3.

Similarly, since $10 \equiv -1 \pmod{11}$, we have $10^k \equiv (-1)^k \pmod{11}$ for each $0 \leq k \leq m$. Hence

$$n \equiv \epsilon \sum_{k=0}^{m} a_k(-1)^k \pmod{11}.$$

As a result, $n \equiv 0 \pmod{11}$ if and only if

$$\sum_{k=0}^{m} a_k(-1)^k \equiv 0 \pmod{11}.$$

In other words, n is divisible by 11 if and only if the alternating sum of its base-10 decimal digits is divisible by 11.

6. (Euclidean algorithm)

(1) Use Euclidean algorithm to compute $\gcd(2026, 748)$.

Solution. We run the Euclidean algorithm as follows:

$$\begin{aligned} 2026 &= 748 \cdot 2 + 530 \\ 748 &= 530 \cdot 1 + 218 \\ 530 &= 218 \cdot 2 + 94 \\ 218 &= 94 \cdot 2 + 30 \\ 94 &= 30 \cdot 3 + 4 \\ 30 &= 4 \cdot 7 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

So $\gcd(2026, 748) = 2$.

(2) Express the gcd as $2026x + 748y$ for integers x, y.

Solution. By our calculations in Part (1),

$$\begin{aligned} 2 = 30 - 4 \cdot 7 &= 30 - (94 - 30 \cdot 3) \cdot 7 \\ &= 30 \cdot 22 - 94 \cdot 7 = (218 - 94 \cdot 2) \cdot 22 - 94 \cdot 7 \\ &= 218 \cdot 22 - 94 \cdot 51 = 218 \cdot 22 - (530 - 218 \cdot 2) \cdot 51 \\ &= 218 \cdot 124 - 530 \cdot 51 = (748 - 530 \cdot 1) \cdot 124 - 530 \cdot 51 \\ &= 748 \cdot 124 - 530 \cdot 175 = 748 \cdot 124 - (2026 - 748 \cdot 2) \cdot 175 \\ &= 748 \cdot 474 - 2026 \cdot 175. \end{aligned}$$

So we may take $x = -175$ and $y = 474$.

(3) (multiplicative inverse) Given nonzero integers a and m, a *multiplicative inverse* of a modulo m is an integer x such that $ax \equiv 1 \pmod{m}$. Such an inverse exists if and only if $\gcd(a, m) = 1$. Find the least nonnegative multiplicative inverse of 37 modulo 101.

Solution. We first perform the Euclidean algorithm to find $\gcd(37, 101)$:

$$\begin{aligned} 101 &= 37 \cdot 2 + 27 \\ 37 &= 27 \cdot 1 + 10 \\ 27 &= 10 \cdot 2 + 7 \\ 10 &= 7 \cdot 1 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

So $\gcd(37, 101) = 1$. Next, we do backward substitution:

$$\begin{aligned} 1 = 7 - 3 \cdot 2 &= 7 - (10 - 7 \cdot 1) \cdot 2 \\ &= 7 \cdot 3 - 10 \cdot 2 = (27 - 10 \cdot 2) \cdot 3 - 10 \cdot 2 \\ &= 27 \cdot 3 - 10 \cdot 8 = 27 \cdot 3 - (37 - 27 \cdot 1) \cdot 8 \\ &= 27 \cdot 11 - 37 \cdot 8 = (101 - 37 \cdot 2) \cdot 11 - 37 \cdot 8 \\ &= 101 \cdot 11 - 37 \cdot 30. \end{aligned}$$

So $101 \cdot 11 - 37 \cdot 30 = 1$. Reducing it modulo 101, we get $37 \cdot (-30) \equiv 1 \pmod{101}$. Thus -30 is a multiplicative inverse of 37 modulo 101. To find the least nonnegative multiplicative inverse, we add 101 to -30 to get $-30 + 101 = 71$.

7. (Linear equations) Determine whether $84x + 126y = 30$ has an integer solution $(x, y) \in \mathbb{Z}^2$. If it does, find all integer solutions; if it does not, prove impossibility.

Solution. The equation is insolvable because $84 = 42 \cdot 2$ and $126 = 42 \cdot 3$ imply $\gcd(84, 126) = 42$, which does not divide 30.

8. (A structural gcd identity) Let $m, n \in \mathbb{Z}$, not both equal to zero. Prove that for every integer k we have

$$\gcd(m, n + km) = \gcd(m, n).$$

This identity can be used to compute the greatest common divisors via successive subtraction until the numbers become manageable. For instance,

$$\gcd(531, 225) = \gcd(306, 225) = \gcd(81, 225) = \gcd(81, 144) = \gcd(81, 63) = 9.$$

The idea involved here is the same as in Euclidean algorithm.

Solution. Let $a = \gcd(m, n + km)$ and $b = \gcd(m, n)$.

Since $a \mid m$ and $a \mid n + km$, we have $a \mid n$ by linearity. So $a \mid b$ by definition of gcd.

Similarly, since $b \mid m$ and $b \mid n$, we have $b \mid n + km$. So $b \mid a$.

Hence, $a = b$.

Optional challenge

9. (Modulo powers of 2)

(1) Show that the square of every odd integer is congruent to 1 modulo 8.

Solution. Let $n = 2k + 1$ be an odd integer. Then

$$n^2 = (2k+1)^2 = 4k(k+1) + 1 \equiv 1 \pmod{8},$$

since exactly one of k and $k+1$ is even.

(2) Show by induction that for any odd integer a and any integer $n \geq 3$, we have

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

Solution. We induct on $n \geq 3$. The base case $n = 3$ is proved in Part (1). Suppose that

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

for some $n \geq 3$ and every odd a. Then there is some $k \in \mathbb{Z}$ such that

$$a^{2^{n-2}} = 1 + 2^n k.$$

Squaring both sides gives

$$a^{2^{n-1}} = (1 + 2^n k)^2 = 1 + 2^{n+1}k + 2^{2n}k^2.$$

Since $2n \geq n + 1$, the second and third terms on the right-hand side are divisible by 2^{n+1}. We deduce

$$a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$$

for every odd a. This concludes the induction.