MATH 417, HOMEWORK 0

CHARLES ANCEL

Chapter 1.6

Exercise 1.6.4. For each of the following pairs of numbers m, n, compute $\gcd(m, n)$ and write $\gcd(m, n)$ explicitly as an integer linear combination of m and n.

(a.) $m = 60$ and $n = 8$

(b.) $m = 32242$ and $n = 42$

Proof. (a.) $m = 60$ and $n = 8$

The Euclidean Algorithm goes as follows:

(1) Divide m by n, and let the remainder be r.

(2) Replace m with n and n with r.

(3) Repeat until n becomes 0. The non-zero remainder is the gcd

60 divided by 8 gives quotient 7 and remainder 4. 8 divided by 4 gives quotient 2 and remainder 0.

Thus, $\gcd(60, 8) = 4$.

To express 4 as an integer linear combination of 60 and 8: Start from the second to the last step:

$$8 = 8(1) + 60(0)$$
$$4 = 60 - 8(7)$$

Thus, 4 can be expressed as:

$$4 = 60(1) - 8(7)$$

(b.) $m = 32242$ and $n = 42$

Using the Euclidean Algorithm:

$$32242 \div 42 = 768 \text{ remainder } 6$$
$$42 \div 6 = 7 \text{ remainder } 0$$

Thus, $\gcd(32242, 42) = 6$.

To express 6 as an integer linear combination of 32242 and 42:

$$42 = 32242(0) + 42(1)$$

$$6 = 32242 - 42(768)$$

Thus, 6 can be expressed as:

$$6 = 32242(1) - 42(768)$$

□

Exercise 1.6.9. Show that if a prime number p divides a product $a_1a_2 \dots a_r$ of nonzero integers, then p divides one of the factors.

Proof. **Base Case**: When $r = 1$, the product is just a_1. If p divides a_1, then p divides one of the factors since there's only one factor.

Inductive Step:

Assume that the statement holds for some $r = k$ such that if a prime p divides a product of k factors, then p divides at least one of these k factors. This is our inductive hypothesis.

We need to prove that it holds for $r = k + 1$.

Let's consider a product of $k + 1$ integers: $a_1a_2 \dots a_ka_{k+1}$.

Now, if p divides one of the factors $a_1, a_2, \dots, a_k$, then we are done by our inductive hypothesis.

If not, consider the product of the first k integers: $a_1a_2 \dots a_k$. Since p doesn't divide any of them individually (by our assumption), it doesn't divide their product either (by our inductive hypothesis). Let's call this product b for simplicity. So, p doesn't divide b.

Now, if p divides $b \cdot a_{k+1}$ but doesn't divide b, then p must divide a_{k+1}.

And thus, for $r = k + 1$, if p divides the product, then it divides at least one of the factors.

By induction, the statement is true for all positive integers r.

Thus, if a prime number p divides a product $a_1a_2 \dots a_r$ of nonzero integers, then p divides one of the factors. □

Exercise 1.6.11. Let n1, …, n_k be nonzero integers. Let $d = \gcd n1, \dots, n_k$, and let

$$\begin{aligned} I &= I(n1, n2, \dots, n_k) \\ &= \{m_1n_1 + m_2n_2 + \dots m_kn_k : m1, \dots, m_k \in Z\} \end{aligned}$$

(a.) Show that if $x, y \in I$, then $x + y \in I$ and $-x \in I$. Show that if $x \in Z$ and $a \in I$, then $xa \in I$.

(b.) Show that $\gcd(n1, n2, \dots, n_k)$ is the smallest element of $I \cap \mathbb{N}$.

(c.) Show that $I = \mathbb{Z}d$.

Proof. (a.) Show that if $x, y \in I$, then $x + y \in I$ and $-x \in I$. Show that if $x \in \mathbb{Z}$ and $a \in I$, then $xa \in I$. *Proof:*

1. Let $x, y \in I$. Then,

$$x = m_1n_1 + m_2n_2 + \cdots + m_kn_k$$

$$y = l_1n_1 + l_2n_2 + \cdots + l_kn_k$$

for some integers $m_1, m_2, \ldots, m_k$ and $l_1, l_2, \ldots, l_k$.

Adding the two:

$$x + y = (m_1 + l_1)n_1 + (m_2 + l_2)n_2 + \cdots + (m_k + l_k)n_k$$

The right side is an integer linear combination of $n_1, n_2, \ldots, n_k$. Thus, $x + y \in I$.

2. For $-x$:

$$-x = -m_1n_1 - m_2n_2 - \cdots - m_kn_k$$

This is again an integer linear combination of $n_1, n_2, \ldots, n_k$. Thus, $-x \in I$.

3. Let $x \in \mathbb{Z}$ and $a \in I$. Then, a can be written as:

$$a = m_1n_1 + m_2n_2 + \cdots + m_kn_k$$

Multiplying by x:

$$xa = xm_1n_1 + xm_2n_2 + \cdots + xm_kn_k$$

This is still an integer linear combination of $n_1, n_2, \ldots, n_k$. Thus, $xa \in I$.

(b.) Show that $\gcd(n_1, n_2, \ldots, n_k)$ is the smallest element of $I \cap \mathbb{N}$.

Proof:

By definition of the gcd, for each n_i, there exists integers m_i such that:

$$d = m_1n_1 + m_2n_2 + \cdots + m_kn_k$$

This means $d \in I$. Moreover, d is positive by definition of the gcd.

If there exists another positive element $d' \in I$ such that $d' < d$, then d' would also be a common divisor of $n_1, n_2, \ldots, n_k$ which is larger than the gcd, a contradiction.

Thus, d is the smallest positive element in I.

(c.) Show that $I = \mathbb{Z}d$.

Proof:

From part (b), d is the smallest positive element in I.

1. $I \subseteq \mathbb{Z}d$: Any element $x \in I$ can be written as:

$$x = m_1n_1 + m_2n_2 + \cdots + m_kn_k$$

Since d divides each n_i, it divides their integer combination. Therefore, x is an integer multiple of d, so $x \in \mathbb{Z}d$.

2. $\mathbb{Z}d \subseteq I$: Any element $x = kd$ (for some $k \in \mathbb{Z}$) can be written using the integer combination of $n_1, n_2, \ldots, n_k$ since d is in I. So, $x \in I$.

Combining these, $I = \mathbb{Z}d$. □

Exercise 1.6.12. Let $n_1, \ldots, n_k$ be nonzero integers.

(a.) Is it true that the integers $n_1, \ldots, n_k$ are relatively prime if and only if they are pairwise relatively prime?

(b.) Show that $n_1, \ldots, n_k$ are relatively prime if and only if $1 \in I(n_1, \ldots, n_k)$.

Proof. Exercise 1.6.12

(a) Is it true that the integers $n_1, \ldots, n_k$ are relatively prime if and only if they are pairwise relatively prime?

Proof:

($\Rightarrow$) Suppose the integers $n_1, \ldots, n_k$ are relatively prime. This means that their greatest common divisor (gcd) is 1. If any pair of them, say n_i and n_j, were not relatively prime, then their gcd would be some integer greater than 1. This would then also be a divisor of the set of numbers $n_1, \ldots, n_k$, contradicting our assumption that they are relatively prime. Hence, they must be pairwise relatively prime.

($\Leftarrow$) Suppose $n_1, \ldots, n_k$ are pairwise relatively prime. This means that for any pair n_i and n_j, the $\gcd(n_i, n_j) = 1$. Suppose, for the sake of contradiction, that the numbers $n_1, \ldots, n_k$ are not relatively prime. Then their gcd is some integer greater than 1. This gcd would be a common divisor for some pair n_i and n_j, contradicting our assumption that they are pairwise relatively prime. Hence, the numbers must be relatively prime.

So, the integers $n_1, \ldots, n_k$ are relatively prime if and only if they are pairwise relatively prime.

(b) Show that $n_1, \ldots, n_k$ are relatively prime if and only if $1 \in I(n_1, \ldots, n_k)$.

Proof:

Recall the definition of $I(n_1, \ldots, n_k)$:

$$I = \{m_1 n_1 + m_2 n_2 + \cdots + m_k n_k : m_1, \ldots, m_k \in \mathbb{Z}\}$$

($\Rightarrow$) Suppose $n_1, \ldots, n_k$ are relatively prime. By the property of the gcd, there exist integers $m_1, \ldots, m_k$ such that:

$$m_1 n_1 + m_2 n_2 + \cdots + m_k n_k = \gcd(n_1, \ldots, n_k)$$

Given they're relatively prime, this means:

$$m_1 n_1 + m_2 n_2 + \cdots + m_k n_k = 1$$

This shows that $1 \in I(n_1, \ldots, n_k)$.

($\Leftarrow$) Conversely, suppose $1 \in I(n_1, \ldots, n_k)$. This means that there exist integers $m_1, \ldots, m_k$ such that:

$$m_1 n_1 + m_2 n_2 + \cdots + m_k n_k = 1$$

Any common divisor of $n_1, \ldots, n_k$ would also be a divisor of the left side of the equation, which is 1. Hence, the only common divisor is 1. This implies that $n_1, \ldots, n_k$ are relatively prime.

Thus, $n_1, \ldots, n_k$ are relatively prime if and only if $1 \in I(n_1, \ldots, n_k)$.

$\square$

Chapter 1.7

Exercise 1.7.4. Compute the congruence class modulo 12 of 4^{237}.

Proof. To compute the congruence class modulo 12 of 4^{237}, we want to determine 4^{237} mod 12.

Proof:

Let's calculate powers of 4 modulo 12 to find a pattern:

$4^1 \equiv 4 \mod 12$

$4^2 \equiv 16 \equiv 4 \mod 12$

$4^3 \equiv 64 \equiv 4 \mod 12$

And so on...

We can see that higher powers of 4 are always congruent to 4 modulo 12. Therefore:

$$4^{237} \equiv 4 \mod 12$$

Thus, the congruence class modulo 12 of 4^{237} is 4. □

Exercise 1.7.5. Can an element of $\mathbb{Z}_n$ be both invertible and a zero divisor?

Proof. No, an element of $\mathbb{Z}_n$ cannot be both invertible and a zero divisor.

Let's break down the definitions:

1. An element a in $\mathbb{Z}_n$ is *invertible* if there exists an element b in $\mathbb{Z}_n$ such that:

$$a \cdot b \equiv 1 \mod n$$

That is, a has a multiplicative inverse modulo n.

2. An element a in $\mathbb{Z}_n$ is a *zero divisor* if $a \neq 0$ and there exists a nonzero element b in $\mathbb{Z}_n$ such that:

$$a \cdot b \equiv 0 \mod n$$

Let's suppose, for contradiction, that there exists an element a in $\mathbb{Z}_n$ which is both invertible and a zero divisor.

Then, by definition, there exist elements b and c (with $c \neq 0$) in $\mathbb{Z}_n$ such that:

$$a \cdot b \equiv 1 \mod n$$
$$a \cdot c \equiv 0 \mod n$$

Now, let's multiply the second equation by b:

$$a \cdot c \cdot b \equiv 0 \mod n$$

Given that $a \cdot b \equiv 1 \mod n$, this gives:

$$c \equiv 0 \mod n$$

But this contradicts our definition of a zero divisor, where c is supposed to be nonzero.

Thus, our initial assumption that an element could be both invertible and a zero divisor is incorrect. An element of $\mathbb{Z}_n$ cannot be both invertible and a zero divisor. □

Exercise 1.7.11.

Proof.

(1) If a and n are relatively prime, by Bezout's Lemma, there are integers s and t such that:

$$as + nt = 1$$

(2) Considering this equation in the modular context, taking both sides modulo n yields:

$$as \equiv 1 \mod n$$

This means that, within the modular arithmetic system modulo n, multiplying a by s results in a remainder of 1 when divided by n.

(1) In $\mathbb{Z}_n$, this congruence implies that the class $[a]$ has an inverse, namely $[s]$, because their product is $[1]$, the multiplicative identity in $\mathbb{Z}_n$.

(2) Therefore, the fact that a is relatively prime to n ensures the existence of its multiplicative inverse in $\mathbb{Z}_n$. Specifically, $[a]$ is invertible in $\mathbb{Z}_n$ and its inverse is $[s]$.

□

Exercise 1.7.14a. Suppose a is relatively prime to n.
(a.) Show that for all $b \in \mathbb{Z}$, the congruence $ax \equiv b \mod n$ has a solution.

Proof. If a is relatively prime to n, then by Bezout's Lemma, there exist integers s and t such that:

$$as + nt = 1$$

Taking this equation modulo n, we get:

$$as \equiv 1 \mod n$$

This means s is the multiplicative inverse of a modulo n. Now, to find a solution for $ax \equiv b \mod n$, we can multiply both sides of this congruence by s.

$$s(ax) \equiv s(b) \mod n$$
$$a(sx) \equiv sb \mod n$$

Given that $as \equiv 1 \mod n$, this equation becomes:

$$x \equiv sb \mod n$$

Therefore, $x = sb$ is a solution to the congruence $ax \equiv b \mod n$. Since b was an arbitrary integer from $\mathbb{Z}$, this proves that for all $b \in \mathbb{Z}$, the congruence $ax \equiv b \mod n$ has a solution. □

Exercise 1.7.14c. Suppose a is relatively prime to n.
(c.) Solve the congruence $8x \equiv 12 \mod 125$.

Proof. To solve the congruence $8x \equiv 12 \mod 125$, we first want to determine if 8 is relatively prime to 125.

125 is equal to 5^3. Since 8 and 5 are relatively prime (their greatest common divisor is 1), 8 is relatively prime to 125.

This means we can find an inverse for 8 modulo 125. This inverse, when multiplied by 8, will be congruent to 1 mod 125.

Using the Extended Euclidean Algorithm, we can find integers s and t such that $8s + 125t = 1$. (I'll spare the full details of the algorithm here for brevity.) For this congruence, the multiplicative inverse of 8 mod 125 is 47.

Given this inverse, to solve the original congruence, we multiply both sides by 47:

$$8x \equiv 12 \mod 125$$
$$47(8x) \equiv 47(12) \mod 125$$
$$x \equiv 564 \mod 125$$

Breaking 564 down mod 125, we have $564 = 4(125) + 64$. Thus:

$$x \equiv 64 \mod 125$$

So, the solution to the congruence $8x \equiv 12 \mod 125$ is $x \equiv 64 \mod 125$. □