Math 2070 Week 6

Elementary Number Theory, Euclid's Lemma, Congruences, Chinese Remainder Theorem

---

6.1 Further Results in Elementary Number Theory

Definition 6.1. The **Greatest Common Divisor** $gcd(a, b)$ of $a, b \in \mathbb{Z}$ is the largest positive integer d which divides both a and b (Notation: $d|a$ and $d|b$).

Note. If $a \neq 0$, then $gcd(a, 0) = |a|$. $gcd(0, 0)$ is undefined.

6.1.1 Euclidean Algorithm

Lemma 6.2. *If* $b = aq + r$ $(a, b, q, r \in \mathbb{Z})$*, then* $gcd(b, a) = gcd(a, r)$.

Proof of Lemma 6.2. If $d|a$ and $d|b$, then $d|r = b - aq$. Conversely, if $d|a$ and $d|r$, then $d|a$ and $d|b = qa + r$. So, the set of common divisors of a, b is the same as the set of the common divisors of a, r. If two finite sets of integers are the same, then their largest elements are clearly the same. In other words:

$$gcd(b, a) = gcd(a, r).$$

□

Suppose $|b| \geq |a|$. Let $b_0 = b$, $a_0 = a$. Write $b_0 = a_0 q_0 + r_0$, where $0 \leq r_0 < |a_0|$.

For $n > 0$, let $b_n = a_{n-1}$ and $a_n = r_{n-1}$, where r_n is the remainder of the division of b_n by a_n. That is,

$$b_n = a_n q_n + r_n, \quad 0 \leq r_n < |a_n|.$$

If $r_0 = 0$, then that means that $a|b$, and $gcd(a, b) = |a|$. Now, suppose $r_0 > 0$. Since r_n is a non-negative integer and $0 \leq r_n < r_{n-1}$, eventually, $r_n = 0$ for some $n \in \mathbb{N}$.

Claim 6.3. $gcd(b, a) = |a_n|$.

Proof of Claim 6.3. By the previous lemma,

$$\begin{aligned} gcd(b, a) &= gcd(b_0, a_0) \\ &= gcd(a_0, r_0) = gcd(b_1, a_1) \\ &= gcd(a_1, r_1) = gcd(b_2, a_2) \\ &= \dots \\ &= gcd(a_n, r_n) = gcd(a_n, 0) = |a_n| . \end{aligned}$$

□

Example 6.4. Find $gcd(285, 255)$.

$$\underbrace{285}_{b_0} = \underbrace{255}_{a_0} \underbrace{1}_{q_0} + \underbrace{30}_{r_0}$$
$$\underbrace{255}_{b_1=a_0} = \underbrace{30}_{a_1=r_0} \underbrace{8}_{q_1} + \underbrace{15}_{r_1}$$
$$\underbrace{30}_{b_2} = \underbrace{15}_{a_2} \underbrace{2}_{q_2} + \underbrace{0}_{r_2}$$

So, $gcd(285, 255) = r_1 = 15$.

Claim 6.5 (Bézout's Lemma). *Let a, b be nonzero integers. There exist $x, y \in \mathbb{Z}$ such that $gcd(a, b) = ax + by$.*

Proof of Bézout's Lemma. **Sketch of Proof:**

Approach 1. Recall the notation used in Section 6.1.1 (Euclidean Algorithm) . We saw that if $r_n = 0$, then $gcd(a, b) = r_{n-1}$.

We may prove Bézout's Lemma via mathematical induction as follows:

First, for integers $0 \leq l < \min(n - 1, 2)$, show that there exist $x_l, y_l \in \mathbb{Z}$ such that $r_l = ax_l + by_l$. This is the base step of the induction proof.

We now carry out the inductive step. Suppose $n - 1 \geq 2$. For any integer $2 \leq k \leq n - 1$, suppose $r_l = ax_l + by_l$ for some $x_l, y_l \in \mathbb{Z}$, for all $0 \leq l < k$.

Show that:

$$r_k = \underbrace{b_k}_{a_{k-1}=r_{k-2}} - q_k \underbrace{a_k}_{r_{k-1}}$$

also has the form $r_k = ax_k + by_k$ for some $x_k, y_k \in \mathbb{Z}$.

The desired identity $gcd(a, b) = r_{n-1} = ax_{n-1} + by_{n-1}$ then follows by mathemtical induction.

Approach 2. Consider the set:

$$S = \{n \in \mathbb{Z}_{>0} | n = ax + by \text{ for some } x, y \in \mathbb{Z}\}.$$

Show that the the minimum element $d \in S$ is the greatest common divisor of a and b.

$\square$

Exercise 6.6. Find $x, y \in \mathbb{Z}$ such that:

$$gcd(285, 255) = 285x + 255y.$$

Exercise 6.7. For any nonzero a, b in the group $G = (\mathbb{Z}, +)$, we have:

$$\langle a, b \rangle = \langle gcd(a, b) \rangle.$$

Definition 6.8. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $gcd(a, b) = 1$.

Claim 6.9. *Two integers $a, b \in \mathbb{Z}$ are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Proof of Claim 6.9. If a, b are relatively prime, then by definition $gcd(a, b) = 1$. So, by Claim 6.5 (Bézout's Lemma) there exist $x, y \in \mathbb{Z}$ such that:

$$ax + by = gcd(a, b) = 1.$$

Conversely, suppose $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Then, any common divisor of a and b must also be a divisor of 1. Since 1 is only divisible by ± 1, we conclude that $gcd(a, b) = 1$. $\square$

Definition 6.10. An integer $p \geq 2$ is **prime** if its only proper divisors (i.e. divisors different from $\pm p$) are ± 1.

Lemma 6.11 (Euclid's Lemma)**.** *Let a, b be integers. If p is prime and $p|ab$, then p divides at least one of a and b.*

Proof of Euclid's Lemma. Suppose p does not divide b (Notation: $p \nmid b$), then $gcd(p, b) = 1$, which implies that $1 = px + by$ for some $x, y \in \mathbb{Z}$. Since $p|apx$ and $p|aby$, we have $p|a = a\underbrace{(px + by)}_{=1}$. $\square$

More generally,

Claim 6.12. *If a, b are relatively prime and $a|bc$, then $a|c$.*

Proof of Claim 6.12. **Exercise.** □

Claim 6.13. *If a, b are relatively prime and:*

$$a|c, \quad b|c,$$

then:

$$ab|c.$$

Proof of Claim 6.13. By assumption, there are $s, t \in \mathbb{Z}$ such that:

$$c = as = bt.$$

So, $a|as = bt$, which by Claim 6.12 implies that $a|t$, since $gcd(a, b) = 1$.

Hence, $t = au$ for some $u \in \mathbb{Z}$, and we have $c = bt = abu$. It follows that $ab|c$. □

Theorem 6.14 (The Fundamental Theorem of Arithmetic)**.** *Let a be a positive integer ≥ 2. Then,*

1. *The integer a is either a prime or a product of primes.*
2. **Unique Factorization** *The integer a may be written uniquely as*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l},$$

where $p_1, p_2, \cdots, p_l$ are distinct prime numbers, and $n_1, n_2, \ldots, n_l \in \mathbb{N}$.

Proof of The Fundamental Theorem of Arithmetic. We prove Part 1 of the theorem by contradiction.

Suppose there exist positive integers ≥ 2 which are neither primes nor products of primes.

Let m be the smallest such integer. Since m is not prime, there are positive integers $a, b \neq 1$ such that $m = ab$.

In particular, $a, b < m$. So, a and b must be either primes or products of primes, which implies that m is itself a product of primes, a contradiction.

We now prove Part 2 (**Unique Factorization**) of the theorem by induction.
The base step corresponds to the case $l = 1$.
Suppose:

$$a = p_1^{n_1} = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k},$$

where p_1 is prime, and the q_i's are distinct primes, and $n_1, m_i \in \mathbb{N}$.

Then, p_1 divides the right-hand side, so by Euclid's Lemma p_1 divides one of the q_i's.

Since the q_i's are prime, we may assume (reindexing if necessary) that $p_1 = q_1$.

Suppose $k > 1$. If $n_1 > m_1$, then $p_1^{n_1 - m_1} = q_2^{m_2} \cdots q_k^{m_k}$, which implies that $p_1 = q_1$ is one of $q_2, \ldots, q_k$, a contradiction, since the q_i's are distinct.

If $n_1 \leq m_1$, then $1 = p_1^{m_1 - n_1} q_2^{m_2} \cdots q_k^{m_k}$, which is impossible. We conclude that $k = 1$, and $p_1 = q_1$, $n_1 = m_1$.

Now we establish the inductive step: Suppose unique factorization is true for all positive integers a' which may be written as $a' = p_1^{n_1} p_2^{n_2} \cdots p_{l'}^{n_{l'}}$, for any $l' < l$. We want to show that it is also true for any integer a which may be written as $a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$.

In other words, suppose

$$a = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l} = q_1^{m_1} \cdots q_k^{m_k},$$

where p_i, q_i are prime and $n_i, m_i \in \mathbb{N}$. We want to show that $k = l$, and $p_i = q_i$, $n_i = m_i$, for $i = 1, 2, \ldots, l$.

If $k < l$, then by the inductive hypothesis applied to $l' = k < l$, we have $k = l$, a contradiction. So, we may assume that $k \geq l$.

By Euclid's Lemma, p_l divides, and hence must be equal to, one of the q_i's.

Reindexing if necessary, we may assume that $p_l = q_k$. Cancelling p_l and q_k from both sides of the equation, it is also clear that $n_l = m_k$. Hence, we have:

$$p_1^{n_1} p_2^{n_2} \cdots p_{l-1}^{n_{l-1}} = q_1^{m_1} \cdots q_{k-1}^{m_{k-1}}.$$

Since $l - 1 < l$, we may now apply the inductive hypothesis to the integer which is equal to the left-hand side of the above equation, and conclude that $l - 1 = k - 1$, $p_i = q_i$, $n_i = m_i$, for $1 \leq i \leq l - 1$.

Since we already know that $p_l^{n_l}$ matches $q_k^{m_k}$, we have $l = k$, and $p_i = q_i$, $n_i = m_i$, for $1 \leq i \leq l$. This establishes the inductive step, and completes the proof. $\square$

6.1.2 WeBWorK

1. **WeBWorK**

2. **WeBWorK**

3. **WeBWorK**

6.2 Modular Arithmetic

Definition 6.15. Let m be a positive integer, then $a, b \in \mathbb{Z}$ are said to be:

congruent modulo m

$$a \equiv b \mod m,$$

if $m|(a-b)$.

Claim 6.16. *The congruence relation $\equiv$ is an* **equivalence relation** . *In other words, it is:*

- **Reflexive***:*

  $a \equiv a \mod m$*;*

- **Symmetric***:*

  $a \equiv b \mod m$ *implies that* $b \equiv a \mod m$*;*

- **Transitive***:*

  $a \equiv b \mod m$*,* $b \equiv c \mod m$*, imply that* $a \equiv c \mod m$*.*

Proof of Claim 6.16.

- **Reflexivity** Since $m|0 = (a-a)$, we have $a \equiv a \mod m$.

- **Symmetry** If $a \equiv b \mod m$, then by definition m divides $a-b$. But if m divides $a-b$, it must also divide $-(a-b) = b-a$, which implies that $b \equiv a \mod m$.

- **Transitivity** If $m|(a-b)$ and $m|(b-c)$, then $m|((a-b)+(b-c)) = (a-c)$, which implies that $a \equiv c \mod m$.

□

Note. $a \equiv 0 \mod m$ if and only if $m|a$.

Claim 6.17.

1. *If* $a = qm + r$*, then* $a \equiv r \mod m$*.*
2. *If* $0 \leq r < r' < m$*, then* $r \not\equiv r' \mod m$*.*

Proof of Claim 6.17. **Exercise.** □

Corollary 6.18. *Given integer $m \geq 2$, every $a \in \mathbb{Z}$ is congruent modulo m to exactly one of* $\{0, 1, 2, \ldots, m-1\}$.

Proof of Corollary 6.18. By Part 1 of the claim, a is congruent mod m to the remainder r of the division of a by m.

By definition, the remainder r lies in $\{0, 1, 2, \ldots, m-1\}$. If $a \equiv r' \mod m$, for some $r' \in \{0, 1, 2, \ldots, m-1\}$, then by transitivity, we have $r' \equiv r \mod m$.

By Part 2 of the claim, we have $r = r'$. □

Theorem 6.19. *Congruence is compatible with addition and multiplication in the following sense:*

- **Addition** *If* $a \equiv a' \mod m$*, and* $b \equiv b' \mod m$*, then* $a + b \equiv a' + b' \mod m$*.*
- **Multiplication** *If* $a \equiv a' \mod m$ *and* $b \equiv b' \mod m$*, then* $ab \equiv a'b' \mod m$*.*

Proof of Theorem 6.19.

- **Addition** If $m|(a - a')$ and $m|(b - b')$, then:

$$m|(a - a') + (b - b') = (a + b) - (a' + b').$$

So, $a + b \equiv a' + b' \mod m$.

- **Multiplication** If $m|(a - a')$ and $m|(b - b')$, then:

$$m|(a - a')b + a'(b - b') = (ab - a'b').$$

So, $ab \equiv a'b' \mod m$.

□

Example 6.20. For $a \in \mathbb{Z}$, $a^2 \equiv 0, 1$, or $4 \mod 8$.

Proof of Example 6.20. By Corollary 6.18 , any $a \in \mathbb{Z}$ is congruent modulo 8 to exactly one element in $\{0, 1, 2, \ldots, 7\}$. So, by Theorem 6.19 , a^2 is congruent modulo 8 to one of:

$$\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2\} = \{0, 1, 4, 9, 16, 25, 36, 49\}.$$

The numbers above a congruent modulo 8 to 0, 1, or 4. The claim follows. □

Theorem 6.21. *If* a *and* m *are relatively prime, then there exists* $x \in \mathbb{Z}$ *such that* $ax \equiv 1 \mod m$*.*

Proof of Theorem 6.21. Since a and m are relatively prime, by Claim 6.5 (Bézout's Lemma) there exist $x, y \in \mathbb{Z}$ such that:

$$ax + my = 1.$$

This implies that m divides $my = 1 - ax$. So, by definition, we have $ax \equiv 1 \mod m$. □

Theorem 6.22 (Chinese Remainder Theorem)**.** *If m_1 and m_2 are relatively prime, then the system of congruence relations:*

$$x \equiv r_1 \mod m_1$$
$$x \equiv r_2 \mod m_2$$

has a solution $x_0 \in \mathbb{Z}$. Moreover, any two solutions are congruent modulo $m_1 m_2$, and any integer which is congruent to x_0 modulo $m_1 m_2$ is also a solution.

Remark. In other words, the system of two congruence relations is equivalent to a single congruence relation:

$$x \equiv r \mod m_1 m_2$$

for some $r \in \mathbb{Z}$.

Applying this process repeatedly, a system of congruence relations of the form:

$$\begin{aligned} x \equiv & \quad r_1 \mod m_1 \\ x \equiv & \quad r_2 \mod m_2 \\ & \quad \vdots \\ x \equiv & \quad r_l \mod m_l \end{aligned}$$

where the m_i's are pairwise coprime, is equivalent to a single relation of the form:

$$x \equiv r \mod m_1 m_2 \cdots m_l$$

for some $r \in \mathbb{Z}$.

Proof of Chinese Remainder Theorem. Since m_1 and m_2 are relatively prime, by Theorem 6.21 there exists $n \in \mathbb{Z}$ such that $m_1 n \equiv 1 \mod m_2$. Let $x = m_1 n(r_2 - r_1) + r_1$.

Since:

$$m_1 n(r_2 - r_1) \equiv 0 \mod m_1,$$

we have:

$$x \equiv r_1 \mod m_1.$$

Moreover, since $m_1 n \equiv 1 \mod m_2$, we have:

$$x = m_1 n(r_2 - r_1) + r_1 \equiv r_2 - r_1 + r_1 \equiv r_2 \mod m_2.$$

This shows that the system of congruence relations has at least one solution.

If x' is another solution to the system, then:

$$
\begin{aligned}
x - x' &\equiv r_1 - r_1 &\equiv 0 \mod m_1, \\
x - x' &\equiv r_2 - r_2 &\equiv 0 \mod m_2.
\end{aligned}
$$

So, $m_1|(x-x')$ and $m_2|(x-x')$. Since, m_1, m_2 are relatively prime, by a previous result we conclude that $m_1m_2|(x-x')$. In other words, $x \equiv x' \mod m_1m_2$.

Conversely, for any integer k, it is clear $x' = x + m_1m_2k$ is also a solution provided that x is a solution.

Hence, the solution set to the system of congruence relations may be described by:

$$x \equiv x_0 \mod m_1m_2,$$

where x_0 is any particular solution to the system. □

Note. The proof of the Chinese Remainder Theorem as written above is complete. However, it is worthwhile to explain how we come up with the solution $x = m_1n(r_2 - r_1) + r_1$ in the first place.

Heuristically, the solution may be arrived at as follows: For any $q \in \mathbb{Z}$, $x = m_1q + r_1$ is a solution to the first congruence relation. We want to find q such that $m_1q + r_1$ is also a solution to the second congruence relation, that is:

$$m_1q + r_1 \equiv r_2 \mod m_2$$

or, equivalently,

$$m_1q \equiv r_2 - r_1 \mod m_2. \tag{$*$}$$

Noting that there exists an $n \in \mathbb{Z}$ such that $m_1n \equiv 1 \mod m_2$, the congruence relation $(*)$ is equivalent to:

$$q \equiv n(r_2 - r_1) \mod m_2.$$

Hence, $x = m_1q + r_1$ is a solution to the system of congruence relations if and only if q is of the form $m_2l + n(r_2 - r_1)$, where $l \in \mathbb{Z}$. In particular, $l = 0$ gives $q = n(r_2 - r_1)$. Hence, $x = m_1n(r_2 - r_1) + r_1$ is a solution.

Example 6.23. Solve the following system of congruence relations:

$$x \equiv 3 \mod 34 \tag{6.1}$$
$$x \equiv -1 \mod 27 \tag{6.2}$$

The relation (6.1) holds if and only if:

$$x = 34s + 3$$

for some $s \in \mathbb{Z}$.

For any such x, the relation (6.2) holds if and only if:

$$34s + 3 \equiv -1 \mod 27,$$

or equivalently:

$$34s \equiv -4 \mod 27. \tag{6.3}$$

Since $gcd(34, 27) = 1$, by Theorem 6.21 there exists $a \in \mathbb{Z}$ such that $a \cdot 34 \equiv 1 \mod 27$. To find a, we perform the Euclidean Algorithm on 34 and 27:

$$\begin{aligned} 34 &= 27 \cdot 1 + 7 \\ 27 &= 7 \cdot 3 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6 + 0 \end{aligned}$$

Working backwards from the last equation, we see that:

$$1 = 34(4) + 27(-5)$$

Hence:

$$27 | (1 - 34 \cdot 4)$$

That is, $34 \cdot 4 \equiv 1 \mod 27$. So, we may take $a = 4$.

Multiplying both sides of (6.3) by $a = 4$, we see that (6.3) holds if and only if:

$$s \equiv -16 \mod 27,$$

which is equivalent to:

$$s \equiv 11 \mod 27.$$

Since the relation above holds if and only if $s = 27t + 11$ for some $t \in \mathbb{Z}$, we conclude that $x \in \mathbb{Z}$ is a solution to our system of congruence relations if and only if:

$$x = 34s + 3 = 34(27t + 11) + 3 = (34)(27)t + 377$$

for some $t \in \mathbb{Z}$. More concisely, the solution set to the system of congruence relations is represented by the single relation:

$$x \equiv 377 \mod 34 \cdot 27$$

Exercise 6.24. 1. **WeBWorK**

2. **WeBWorK**

3. **WeBWorK**

4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**
10. **WeBWorK**
11. **WeBWorK**
12. **WeBWorK**
13. **WeBWorK**
14. **WeBWorK**