Discrete Mathematics
Lecture 4 - The Integers

Nurlan Ismailov
nurlan.ismailov@astanait.edu.kz

Astana IT University

Numbers

We encountered so far sets of real numbers $\mathbb{R}$, set of rational numbers $\mathbb{Q}$, set of integers $\mathbb{Z}$ and set of natural numbers $\mathbb{N}$. What are some of the important properties of the real numbers?

They have a definite order. The binary relation $\leq$ is a partial order on these sets, reflexive, antisymmetric and transitive.

We can add two real numbers a and b and obtain their sum $a + b$, or we can multiply two real numbers a and b and obtain their product $a \cdot b$ (usually written ab, without the centered dot). These two operations satisfy a number of important properties.

Properties of $+$ and $\cdot$

Let a, b, c be real numbers. Then

- (**closure**) $a+b$ and ab are both real numbers.
- (**commutativity**) $a+b=b+a$ and $ab=ba$.
- (**associativity**) $(a+b)+c=a+(b+c)$ and $(ab)c=a(bc)$.
- (**identities**) $a+0=a$ and $a \cdot 1=a$.
- (**distributivity**) $a(b+c)=ab+ac$ and$(a+b)c=ac+bc$.
- (**additive inverse**) $a+(-a)=0$.
- (**multiplicative inverse**) $a(\frac{1}{a})=1$ if $a \neq 0$.
- $a \leq b$ implies $a+c \leq b+c$.
- $a \leq b$ and $c \geq 0$ implies $ac \leq bc$.
- $a \leq b$ and $c \leq 0$ implies $ac \geq bc$.

A third well-known operation, subtraction, is defined in terms of addition by the rule

$$a-b=a+(-b).$$

It is not unusual for a set of real numbers to have no smallest element; for example, there is no smallest element in the set $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots\}$. Similarly, there is no smallest positive number. On the other hand, this sort of thing does not occur with sets of natural numbers, according to the *Well-Ordering Principle*.

Well-Ordering Principle

Any nonempty set of natural numbers has a smallest element.

Using this principle, in forthcoming lectures we will establish Principle of Mathematical Induction which allows us to prove many interesting statements.

In the rest of this lecture, we will concentrate on the integers.

Definition (quotient, remainder)

If a and b are natural numbers and $a = qb + r$ for nonnegative integers q and r with $0 \leq r < b$, the integer q is called the *quotient* and the integer r is called the *remainder* when a is divided by b.

Example

Let $a = 19$ and $b = 7$. When 19 is divided by 7, the quotient is 2 and the remainder is 5. We have $19 = 2 \cdot 7 + 5$.

The Division Algorithm

Theorem

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$.

The Division Algorithm

Theorem

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$.

Proof. We first prove existence of integers q and r and then show that they are unique.

The Division Algorithm

Theorem

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$.

Proof. We first prove existence of integers q and r and then show that they are unique.
(*Proof of existence of integers q and r.*)
Case 1: $a = 0$.
Then $q = 0$, $r = 0$ gives a solution.

The Division Algorithm

Theorem

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$.

Proof. We first prove existence of integers q and r and then show that they are unique.
(*Proof of existence of integers q and r.*)
Case 1: $a = 0$.
Then $q = 0$, $r = 0$ gives a solution.
Case 2: $b > 0$ and $a > 0$.
Consider the sequence of nonnegative multiples of b; that is, $0 \cdot b = 0$, $1 \cdot b = b$, $2 \cdot b = 2b$, $3 \cdot b = 3b, \ldots$. The first term in this increasing sequence of numbers is 0, which is less than a since a is a natural number. On the other hand, some term is bigger than a (for example, $(2a)b > a$ because $2b > 1$), so by the Well-Ordering Principle, the set of multiples of b that exceed a has a smallest element, say $(q+1)b$. So we have $qb \leq a < (q+1)b$. Set $r = a - qb$. Since $qb \leq a$, we have $r \geq 0$. Since $(q+1)b > a$, we have $r < b$. Hence, $0 \leq r < b$, we have found q and r as required.

...proof continued

Case 3: $b > 0$ and $a < 0$.
Since $-a > 0$, we can apply **Case 2** to $-a$ and b obtaining q and r, with $0 \leq r < b$, such that $-a = qb + r$. Therefore, $a = (-q)b - r$. If $r = 0$, $a = (-q)b$, while if $r > 0$, $a = (-q-1)b + (b-r)$ with $0 < b - r < b = |b|$. In either case, we have expressed a in the desired form.

...proof continued

Case 3: $b > 0$ and $a < 0$.
Since $-a > 0$, we can apply **Case 2** to $-a$ and b obtaining q and r, with $0 \leq r < b$, such that $-a = qb + r$. Therefore, $a = (-q)b - r$. If $r = 0$, $a = (-q)b$, while if $r > 0$, $a = (-q-1)b + (b - r)$ with $0 < b - r < b = |b|$. In either case, we have expressed a in the desired form.
Case 4: $b < 0$ and $a > 0$ or $a < 0$.
Here $-b > 0$, so **Case 2** and **Case 3** tell us that there exist integers q and r, $0 \leq r < -b = |b|$, such that $a = q(-b) + r = (-q)b + r$. Again we have expressed a in the desired form.

...proof continued

Case 3: $b > 0$ and $a < 0$.
Since $-a > 0$, we can apply **Case 2** to $-a$ and b obtaining q and r, with $0 \leq r < b$, such that $-a = qb + r$. Therefore, $a = (-q)b - r$. If $r = 0$, $a = (-q)b$, while if $r > 0$, $a = (-q-1)b + (b - r)$ with $0 < b - r < b = |b|$. In either case, we have expressed a in the desired form.
Case 4: $b < 0$ and $a > 0$ or $a < 0$.
Here $-b > 0$, so **Case 2** and **Case 3** tell us that there exist integers q and r, $0 \leq r < -b = |b|$, such that $a = q(-b) + r = (-q)b + r$. Again we have expressed a in the desired form.
(*Proof of uniqueness of integers q and r.*)

...proof continued

Case 3: $b > 0$ and $a < 0$.
Since $-a > 0$, we can apply **Case 2** to $-a$ and b obtaining q and r, with $0 \leq r < b$, such that $-a = qb + r$. Therefore, $a = (-q)b - r$. If $r = 0$, $a = (-q)b$, while if $r > 0$, $a = (-q-1)b + (b - r)$ with $0 < b - r < b = |b|$. In either case, we have expressed a in the desired form.
Case 4: $b < 0$ and $a > 0$ or $a < 0$.
Here $-b > 0$, so **Case 2** and **Case 3** tell us that there exist integers q and r, $0 \leq r < -b = |b|$, such that $a = q(-b) + r = (-q)b + r$. Again we have expressed a in the desired form.
(*Proof of uniqueness of integers q and r.*)
To see that q and r are unique, assume that a can be expressed in the given form in two ways; that is, suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ with $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$. Then $(q_1 - q_2)b = r_2 - r_1$. Now $(q_1 - q_2)b$ is an integral multiple of b while $-b < r_2 - r_1 < b$. The only possibility is that this multiple is 0, and so $q_1 = q_2$, $r_1 = r_2$ as desired $\Box$

Examples

a	b	q	r

Examples

a	b	q	r
58	17	3	7

$$58 = 3 \cdot 17 + 7 \quad \text{with} \quad 0 \leq 7 < 17,$$

Examples

a	b	q	r
58	17	3	7
58	-17	-3	7

$$58 = 3 \cdot 17 + 7 \quad \text{with} \quad 0 \leq 7 < 17,$$

$$58 = (-3) \cdot (-17) + 7 \quad \text{with} \quad 0 \leq 7 < |-17|,$$

Examples

a	b	q	r
58	17	3	7
58	-17	-3	7
-58	17	-4	10

$$58 = 3 \cdot 17 + 7 \quad \text{with} \quad 0 \leq 7 < 17,$$

$$58 = (-3) \cdot (-17) + 7 \quad \text{with} \quad 0 \leq 7 < |-17|,$$

$$-58 = (-4) \cdot 17 + 10 \quad \text{with} \quad 0 \leq 10 < 17,$$

Examples

a	b	q	r
58	17	3	7
58	-17	-3	7
-58	17	-4	10
-58	-17	4	10

$$58 = 3 \cdot 17 + 7 \quad \text{with} \quad 0 \leq 7 < 17,$$

$$58 = (-3) \cdot (-17) + 7 \quad \text{with} \quad 0 \leq 7 < |-17|,$$

$$-58 = (-4) \cdot 17 + 10 \quad \text{with} \quad 0 \leq 10 < 17,$$

$$-58 = 4 \cdot (-17) + 10 \quad \text{with} \quad 0 \leq 10 < |-17|.$$

Divisibility

Definition

Given integers a and b with $b \neq 0$, we say that b is a *divisor* or a *factor* of a and a *is divisible by* b if and only if $a = qb$ for some integer q. We write $b|a$ to signify that a is divisible by b and say "b divides a". $b \nmid a$ means "b does not divide a".

Example

- 3 is a divisor of 18
- -7 is a divisor of 35
- $16| - 64$
- $-4 \nmid 38$.

Example

Given three consecutive integers a, $a+1$, $a+2$. Then one of them is divisible by 3.

Solution. By the division algorithm, we can write $a = 3q + r$ with $0 \leq r < 3$. Since r is an integer, we must have $r = 0, r = 1$, or $r = 2$. If $r = 0$, then $a = 3q$ is divisible by 3. If $r = 1$, then $a = 3q + 1$, so $a + 2 = 3q + 3$ is divisible by 3. If $r = 2$, then $a = 3q + 2$, so $a + 1 = 3q + 3$ is divisible by 3.

Example

Given three consecutive integers a, $a+1$, $a+2$. Then one of them is divisible by 3.
Solution. By the division algorithm, we can write $a = 3q + r$ with $0 \leq r < 3$. Since r is an integer, we must have $r = 0, r = 1$, or $r = 2$. If $r = 0$, then $a = 3q$ is divisible by 3. If $r = 1$, then $a = 3q + 1$, so $a + 2 = 3q + 3$ is divisible by 3. If $r = 2$, then $a = 3q + 2$, so $a + 1 = 3q + 3$ is divisible by 3.

This example can be generalized as follows.

Proposition

Given n consecutive integers a, $a+1$, $a+2, \ldots, a+n-1$. Then one of them is divisible by n.

We leave its proof to students.

Example

Given three consecutive integers a, $a+1$, $a+2$. Then one of them is divisible by 3.
Solution. By the division algorithm, we can write $a = 3q + r$ with $0 \leq r < 3$. Since r is an integer, we must have $r = 0, r = 1$, or $r = 2$. If $r = 0$, then $a = 3q$ is divisible by 3. If $r = 1$, then $a = 3q + 1$, so $a + 2 = 3q + 3$ is divisible by 3. If $r = 2$, then $a = 3q + 2$, so $a + 1 = 3q + 3$ is divisible by 3.

This example can be generalized as follows.

Proposition

Given n consecutive integers a, $a+1$, $a+2, \ldots, a+n-1$. Then one of them is divisible by n.

We leave its proof to students.

Proposition

The binary relation $\mathcal{R}$ on $\mathbb{N}$ defined by $(a, b) \in \mathcal{R}$ if and only if $a|b$ is a partial order.

GCD

Definition

Let a and b be integers not both of which are 0. An integer g is *the greatest common divisor GCD* of a and b if and only if g is the largest common divisor of a and b; that is, if and only if

- $g|a$ and $g|b$ and,
- if c is any integer such that $c|a$ and $c|b$, then $c \leq g$.

We write $g = GCD(a, b)$ to signify that g is the greatest common divisor of a and b.

GCD

Definition

Let a and b be integers not both of which are 0. An integer g is *the greatest common divisor GCD* of a and b if and only if g is the largest common divisor of a and b; that is, if and only if

- $g|a$ and $g|b$ and,
- if c is any integer such that $c|a$ and $c|b$, then $c \leq g$.

We write $g = GCD(a, b)$ to signify that g is the greatest common divisor of a and b.

Examples

- The greatest common divisor of 15 and 6 is 3
- $GCD(-24, 18) = 6$
- $GCD(756, 210) = 42$
- $GCD(-756, 210) = 42$
- $GCD(-756, -210) = 42$

Questions/Answers

- if a and b are integers such that $a|b$, what is $GCD(a,b) =?$

Questions/Answers

- if a and b are integers such that $a|b$, what is $GCD(a, b) =?$

  Answer: $GCD(a, b) = a$.

Questions/Answers

- if a and b are integers such that $a|b$, what is $GCD(a,b) =?$

  Answer: $GCD(a,b) = a$.

- Suppose a is a nonzero integer, what is $GCD(a,0) =?$

Questions/Answers

- if a and b are integers such that $a|b$, what is $GCD(a,b) =?$

  Answer: $GCD(a,b) = a$.

- Suppose a is a nonzero integer, what is $GCD(a,0) =?$

  Answer: $GCD(a,0) = a$.

How to find GCD(a,b)?

How to find GCD(a,b)? Answer: The Euclid algorithm

How to find GCD(a,b)? Answer: The Euclid algorithm

The seventh book of Euclid's *Elements* (300 years B.C) describes a procedure now known as *the Euclid algorithm* for finding the GCD of two integers a and b. Now we will demonstrate the Euclid algorithm.

How to find GCD(a,b)? Answer: The Euclid algorithm

The seventh book of Euclid's *Elements* (300 years B.C) describes a procedure now known as *the Euclid algorithm* for finding the GCD of two integers a and b. Now we will demonstrate the Euclid algorithm.

Lemma (Important)

If $a = qb + r$ for integers $a, b, q,$ and r, then $GCD(a, b) = GCD(b, r)$.

How to find GCD(a,b)? Answer: The Euclid algorithm

The seventh book of Euclid's *Elements* (300 years B.C) describes a procedure now known as *the Euclid algorithm* for finding the GCD of two integers a and b. Now we will demonstrate the Euclid algorithm.

Lemma (Important)

If $a = qb + r$ for integers a, b, q, and r, then $GCD(a, b) = GCD(b, r)$.

Proof. If $a = b = 0$, then $a = qb + r$ says $r = 0$. Similarly, if $b = r = 0$, then $a = 0$. In either case, the result is true since neither $GCD(a, b)$ nor $GCD(b, r)$ is defined. Thus, it remains to consider the case $g_1 = GCD(a, b)$ and $g_2 = GCD(b, r)$ are both well-defined integers. First, $g_2|b$ and $g_2|r$, so $g_2|(qb + r)$; that is $g_2|a$. Thus, g_2 is a common divisor of a and b and, since g_1 is the greatest common divisor of a and b, we have $g_2 \leq g_1$.

How to find GCD(a,b)? Answer: The Euclid algorithm

The seventh book of Euclid's *Elements* (300 years B.C) describes a procedure now known as *the Euclid algorithm* for finding the GCD of two integers a and b. Now we will demonstrate the Euclid algorithm.

Lemma (Important)

If $a = qb + r$ for integers a, b, q, and r, then $GCD(a, b) = GCD(b, r)$.

Proof. If $a = b = 0$, then $a = qb + r$ says $r = 0$. Similarly, if $b = r = 0$, then $a = 0$. In either case, the result is true since neither $GCD(a, b)$ nor $GCD(b, r)$ is defined. Thus, it remains to consider the case $g_1 = GCD(a, b)$ and $g_2 = GCD(b, r)$ are both well-defined integers. First, $g_2|b$ and $g_2|r$, so $g_2|(qb + r)$; that is $g_2|a$. Thus, g_2 is a common divisor of a and b and, since g_1 is the greatest common divisor of a and b, we have $g_2 \leq g_1$.
On the other hand, since $g_1|a$ and $g_1|b$, we know that $g_1|(a - qb)$; that is $g_1|r$. As a common divisor of b and r, it cannot exceed the GCD of these numbers. Thus, $g_1 \leq g_2$, so $g_1 = g_2$, as desired □

How to find GCD(a,b)? Answer: The Euclid algorithm

The seventh book of Euclid's *Elements* (300 years B.C) describes a procedure now known as *the Euclid algorithm* for finding the GCD of two integers a and b. Now we will demonstrate the Euclid algorithm.

Lemma (Important)

If $a = qb + r$ for integers a, b, q, and r, then $GCD(a, b) = GCD(b, r)$.

Proof. If $a = b = 0$, then $a = qb + r$ says $r = 0$. Similarly, if $b = r = 0$, then $a = 0$. In either case, the result is true since neither $GCD(a, b)$ nor $GCD(b, r)$ is defined. Thus, it remains to consider the case $g_1 = GCD(a, b)$ and $g_2 = GCD(b, r)$ are both well-defined integers. First, $g_2|b$ and $g_2|r$, so $g_2|(qb + r)$; that is $g_2|a$. Thus, g_2 is a common divisor of a and b and, since g_1 is the greatest common divisor of a and b, we have $g_2 \leq g_1$.
On the other hand, since $g_1|a$ and $g_1|b$, we know that $g_1|(a - qb)$; that is $g_1|r$. As a common divisor of b and r, it cannot exceed the GCD of these numbers. Thus, $g_1 \leq g_2$, so $g_1 = g_2$, as desired □

The Euclid algorithm involves nothing more than a repeated application of this lemma.

Euclidean Algorithm. Let a and b natural numbers with $b < a$. To find the greatest common divisor of a and b, write

$$a = q_1 b + r_1 \text{ with } 0 \le r_1 < b,$$

$$b = q_2 r_1 + r_2 \text{ with } 0 \le r_2 < r_1,$$

$$r_1 = q_3 r_2 + r_3 \text{ with } 0 \le r_3 < r_2,$$

$$r_2 = q_4 r_3 + r_4 \text{ with } 0 \le r_4 < r_3,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$r_{k-2} = q_k r_{k-1} + r_k \text{ with } 0 \le r_k < r_{k-1},$$

Continue the process until some remainder, say $r_{k+1} = 0$. The greatest common divisor of a and b is r_k, the last nonzero remainder □

Explanations

Explanations

Question

Why must some remainder be 0?

Answer. Suppose no remainder is zero. Then $\{r_1, r_2, r_3, \ldots\}$ is a nonempty set natural numbers and hence has a smallest element r_k, by the Well-Ordering Principle. Since the next remainder is smaller than r_k, we have a contradiction. So some remainder, $r_{k+1} = 0$.

Explanations

Question

Why must some remainder be 0?

Answer. Suppose no remainder is zero. Then $\{r_1, r_2, r_3, \ldots\}$ is a nonempty set natural numbers and hence has a smallest element r_k, by the Well-Ordering Principle. Since the next remainder is smaller than r_k, we have a contradiction. So some remainder, $r_{k+1} = 0$.

Question

Why does this algorithm work?

Answer. By previous Lemma, the last nonzero remainder r_k is the GCD of a and b because

$$GCD(a, b) = GCD(b, r_1) = GCD(r_1, r_2) = GCD(r_2, r_3)$$
$$= GCD(r_3, r_4) = \cdots = GCD(r_k, r_{k+1}) = GCD(r_k, 0) = r_k.$$

Example

GCD(630,196)=?

Example

$$\text{GCD}(630,196)=?$$

Solution. We have

$$630 = 3 \cdot 196 + 42$$

Example

$$\text{GCD}(630,196)=?$$

Solution. We have

$$630 = 3 \cdot 196 + 42$$

$$196 = 4 \cdot 42 + 28$$

Example

$$\text{GCD}(630,196)=?$$

Solution. We have

$$630 = 3 \cdot 196 + 42$$

$$196 = 4 \cdot 42 + 28$$

$$42 = 1 \cdot 28 + 14$$

Example

GCD(630,196)=?

Solution. We have

$$630 = 3 \cdot 196 + 42$$

$$196 = 4 \cdot 42 + 28$$

$$42 = 1 \cdot 28 + 14$$

$$28 = 2 \cdot 14 + 0$$

Example

GCD(630,196)=?

Solution. We have

$$630 = 3 \cdot 196 + 42$$

$$196 = 4 \cdot 42 + 28$$

$$42 = 1 \cdot 28 + 14$$

$$28 = 2 \cdot 14 + 0$$

The last nonzero remainder is 14, so this is $GCD(630, 196) = 14$.

Diophantine equation $ax + by = c$

Now we study how to solve a linear equation

$$ax + by = c$$

with two unknowns x and y, where $a, b, c \in \mathbb{Z}$.
This kind of equation is called *Diophantine equation*.

A pair of integers (x_0, y_0) is said to be *a particular solution* of $ax + by = c$ if

$$ax_0 + by_0 = c.$$

Solving a Diophantine equation means find its all particular solutions if they exist.

Diophantine equation $ax + by = c$

Now we study how to solve a linear equation

$$ax + by = c$$

with two unknowns x and y, where $a, b, c \in \mathbb{Z}$.
This kind of equation is called *Diophantine equation*.

A pair of integers (x_0, y_0) is said to be *a particular solution* of $ax + by = c$ if

$$ax_0 + by_0 = c.$$

Solving a Diophantine equation means find its all particular solutions if they exist.

Theorem

The equation $ax + by = c$ has a solution in integers if and only if $GCD(a, b)|c$.
If (x_0, y_0) is any particular solution of the equation, then all solutions are given by

$$x = x_0 + \frac{b}{GCD(a,b)}t \quad \text{and} \quad y = y_0 - \frac{a}{GCD(a,b)}t,$$

where t is an arbitrary integer.

Examples

1. Find all solutions in integers of $12x + 15y = 6$.
Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution.

Examples

1. Find all solutions in integers of $12x + 15y = 6$.
Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution. By inspection, we find a particular solution $x_0 = -2$ and $y_0 = 2$.

Examples

1. Find all solutions in integers of $12x + 15y = 6$.

Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution. By inspection, we find a particular solution $x_0 = -2$ and $y_0 = 2$. Then by the Theorem we have

$$x = -2 + \frac{15}{3}t = -2 + 5t \quad \text{and} \quad y = 2 - \frac{12}{3}t = 2 - 4t \quad t \in \mathbb{Z}.$$

Examples

1. Find all solutions in integers of $12x + 15y = 6$.

Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution. By inspection, we find a particular solution $x_0 = -2$ and $y_0 = 2$. Then by the Theorem we have

$$x = -2 + \frac{15}{3}t = -2 + 5t \quad \text{and} \quad y = 2 - \frac{12}{3}t = 2 - 4t \quad t \in \mathbb{Z}.$$

Answer: $x = -2 + 5t \quad \text{and} \quad y = 2 - 4t \quad t \in \mathbb{Z}.$

Examples

1. Find all solutions in integers of $12x + 15y = 6$.

Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution. By inspection, we find a particular solution $x_0 = -2$ and $y_0 = 2$. Then by the Theorem we have

$$x = -2 + \frac{15}{3}t = -2 + 5t \quad \text{and} \quad y = 2 - \frac{12}{3}t = 2 - 4t \quad t \in \mathbb{Z}.$$

$$\textbf{Answer:} \quad x = -2 + 5t \quad \text{and} \quad y = 2 - 4t \quad t \in \mathbb{Z}.$$

By substituting integers for t we can have other particular solutions of the equation. For instance,

t	-1	0	1	$\cdots$
x	-7	2	3	$\cdots$
y	6	-2	-2	$\cdots$

Examples

1. Find all solutions in integers of $12x + 15y = 6$.
Solution. $GCD(12, 15) = 3$ and 3 divides 6 which means the equation has solution. By inspection, we find a particular solution $x_0 = -2$ and $y_0 = 2$. Then by the Theorem we have

$$x = -2 + \frac{15}{3}t = -2 + 5t \quad \text{and} \quad y = 2 - \frac{12}{3}t = 2 - 4t \quad t \in \mathbb{Z}.$$

Answer: $x = -2 + 5t$ and $y = 2 - 4t$ $t \in \mathbb{Z}$.

By substituting integers for t we can have other particular solutions of the equation. For instance,

t	-1	0	1	$\cdots$
x	-7	2	3	$\cdots$
y	6	-2	-2	$\cdots$

2. Find all integer solutions of $57x + 105y = 4$.
Solution. $GCD(57, 105) = 3$ but 3 does not divide 4. Then by the theorem the equation has not integer solution.

The theorem above can be used to determine whether $ax + by = c$ has a solution or not. Secondly, it helps to construct a general solution of $ax + by = c$, whenever we have an exact particular solution. So how to find a particular solution? To find a particular solution it is sufficient to express $GCD(a, b)$ as a linear combination of a and b.

The theorem above can be used to determine whether $ax + by = c$ has a solution or not. Secondly, it helps to construct a general solution of $ax + by = c$, whenever we have an exact particular solution. So how to find a particular solution? To find a particular solution it is sufficient to express $GCD(a, b)$ as a linear combination of a and b.

Example

Find all integer solutions of $9x + 13y = 1$.
Solution.

$$13 = 1 \cdot 9 + 4$$

$$9 = 2 \cdot 4 + 1$$

Hence, $GCD(13, 9) = 1$. In order to express 1 by 9 and 13, we need to pay our attention to the remainders which are 1 and 4.

$$1 = 9 - 2 \cdot 4 = 9 - 2 \cdot (13 - 1 \cdot 9) = 3 \cdot 9 - 2 \cdot 13.$$

So we have $1 = 3 \cdot 9 - 2 \cdot 13$. Now we can easily find out that $x_0 = 3$ and $y_0 = -2$ is a particular solution. We further construct a general solution and we have $x = 3 + 13t, \quad y = -2 - 9t$ for any $t \in \mathbb{Z}$.

The primes

Definition (prime, composite)

A natural number $p \geq 2$ is called *prime* if and only if the only natural numbers that divide p are 1 and p. A natural number $n > 1$ that is not prime is called *composite*. Thus, $n > 1$ is composite if $n = ab$, where a and b are natural numbers with $1 < a, b < n$.

Example

The primes less than 100 are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$

$$43,\ 47,\ 53,\ 59, 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

The primes

Definition (prime, composite)

A natural number $p \geq 2$ is called *prime* if and only if the only natural numbers that divide p are 1 and p. A natural number $n > 1$ that is not prime is called *composite*. Thus, $n > 1$ is composite if $n = ab$, where a and b are natural numbers with $1 < a, b < n$.

Example

The primes less than 100 are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,$$

$$43,\ 47,\ 53,\ 59, 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

One of the great challenges of mathematics and an active area of research today is that of finding efficient algorithms for checking whether large integers are primes. According to Wikipedia, the largest known prime number (as of January 2021) is $2^{282589933} - 1$, a number which has 24862048 digits. It was found by Patrick Laroche.

How many primes are there?

Theorem (Euclid's theorem)

There are infinitely many primes.

How many primes are there?

Theorem (Euclid's theorem)

There are infinitely many primes.

Proof. If the theorem is not true, there is just a finite number of primes $p_1, p_2, \ldots, p_t$. Let $n = (p_1 p_2 \cdots p_t) + 1$. Then n is divisible by some prime and hence by some p_i. Since $p_1 p_2 \cdots p_t$ is also divisible by p_i, the number $n - (p_1 p_2 \cdots p_t)$ must also be divisible by p_i. Thus, 1 is divisible by p_i, a contradiction □

How many primes are there?

Theorem (Euclid's theorem)

There are infinitely many primes.

Proof. If the theorem is not true, there is just a finite number of primes $p_1, p_2, \ldots, p_t$. Let $n = (p_1 p_2 \cdots p_t) + 1$. Then n is divisible by some prime and hence by some p_i. Since $p_1 p_2 \cdots p_t$ is also divisible by p_i, the number $n - (p_1 p_2 \cdots p_t)$ must also be divisible by p_i. Thus, 1 is divisible by p_i, a contradiction □

Question

What about the number of natural numbers that are not prime?

How many primes are there?

Theorem (Euclid's theorem)

There are infinitely many primes.

Proof. If the theorem is not true, there is just a finite number of primes $p_1, p_2, \dots, p_t$. Let $n = (p_1 p_2 \cdots p_t) + 1$. Then n is divisible by some prime and hence by some p_i. Since $p_1 p_2 \cdots p_t$ is also divisible by p_i, the number $n - (p_1 p_2 \cdots p_t)$ must also be divisible by p_i. Thus, 1 is divisible by p_i, a contradiction □

Question

What about the number of natural numbers that are not prime?

Answer. They are infinite too. For instance, numbers of the form $7n$, $n \in \mathbb{N}$, $n > 1$, are not prime, and there are infinitely many of these.

Lemma

If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

Lemma

If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

Proof. Since n is not prime, n can be factored $n = ab$ with $1 < a \leq b < n$. Then $a \leq \sqrt{n}$ since otherwise, $ab > \sqrt{n}\sqrt{n} = n$, a contradiction. As a natural number greater than 1, it follows that a is divisible by some prime p. Since $p|a$ and $a|n$, $p|n$ by transitivity. Also, since $a \leq \sqrt{n}$ and $p|a$, we must have $p \leq \sqrt{n}$. Thus, p is the desired prime factor of n $\square$

Lemma

If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

Proof. Since n is not prime, n can be factored $n = ab$ with $1 < a \leq b < n$. Then $a \leq \sqrt{n}$ since otherwise, $ab > \sqrt{n}\sqrt{n} = n$, a contradiction. As a natural number greater than 1, it follows that a is divisible by some prime p. Since $p|a$ and $a|n$, $p|n$ by transitivity. Also, since $a \leq \sqrt{n}$ and $p|a$, we must have $p \leq \sqrt{n}$. Thus, p is the desired prime factor of n □

To verify that n is not prime, it is enough just to test the prime numbers less than n when searching for a divisor of n. The lemma decreases considerably the amount of testing that must be done when checking for divisors of an integer.

Lemma

If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

Proof. Since n is not prime, n can be factored $n = ab$ with $1 < a \leq b < n$. Then $a \leq \sqrt{n}$ since otherwise, $ab > \sqrt{n}\sqrt{n} = n$, a contradiction. As a natural number greater than 1, it follows that a is divisible by some prime p. Since $p|a$ and $a|n$, $p|n$ by transitivity. Also, since $a \leq \sqrt{n}$ and $p|a$, we must have $p \leq \sqrt{n}$. Thus, p is the desired prime factor of n □

To verify that n is not prime, it is enough just to test the prime numbers less than n when searching for a divisor of n. The lemma decreases considerably the amount of testing that must be done when checking for divisors of an integer.
For example, to verify that 97 is prime, we need only check the prime numbers less than or equal to $\sqrt{97}$. Since none of $2, 3, 5, 7$ is a divisor of 97, we are assured that 97 is a prime number. As we see that Lemma reduces dramatically the work of testing.

The Fundamental Theorem of Arithmetic

Every integer $n \geq 2$ can be written in the form

$$n = p_1 p_2 \cdots p_r$$

for a unique set of primes $\{p_1, p_2, \dots, p_r\}$; equivalently, every integer $n \geq 2$ can be written

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_t^{\alpha_t} \quad \textit{(the prime decomposition of } n\textit{)}.$$

as the product of powers of distinct prime numbers $q_1, q_2, \dots, q_t$. These primes and the exponents $\alpha_1, \alpha_2, \dots, \alpha_t$ are unique.

Example

$120 = 2^3 \cdot 3 \cdot 5$

Again: How many primes are there?

Let $\pi(x)$ be a function that calculates the number of primes less than or equal to x, for any real number x. For example, $\pi(10) = 4$ since there are four prime numbers: $2, 3, 5$ and 7 less than or equal to 10. We have earlier noted that there are 25 primes $p \leq 100$; thus, $\pi(100) = 25$.

Theorem (Jaques Hadamard and Charler-Jean de la Vallée-Pousin (1896))

Let $\pi(x)$ denote the number of primes $p \leq n$. Then

$$lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1; \quad \text{equivalently,} \quad \pi(x) \sim \frac{x}{ln(x)}.$$

The second statement of the theorem reads “$\pi(x)$ is asymptotic to $\frac{x}{ln(x)}$”. Setting $x = 100$, we have $\frac{100}{ln(100)} \approx 21.715$.
Note that

$$\frac{\pi(100)}{100/ln(100)} \approx \frac{25}{21.715} \approx 1.151.$$

The symbol $\approx$ means “approximately”. Setting $x = 1000000$, the theorem says that the number of primes under 1 million is roughly $\frac{1000000}{ln(1000000)} \approx 72382$. In fact, there are 78498 such primes. Note that

$$\frac{\pi(1000000)}{1000000/\ln(1000000)} \approx \frac{78498}{72382} \approx 1.084.$$

As x gets larger, the fraction $\frac{\pi(x)}{x/ln(x)}$ gets closer and closer to 1.

Some “interesting” open problems

Some "interesting" open problems

Integers, p and $p+2$ that are both prime are called *twin primes*. For example 3 and 5, 5 and 7, 11 and 13, 41 and 43 are twin primes. Unlike prime numbers, it is not known whether there are infinitely many twin primes.

The Twin Prime Conjecture

There are infinitely many twin primes.

Some “interesting” open problems

Integers, p and $p+2$ that are both prime are called *twin primes*. For example 3 and 5, 5 and 7, 11 and 13, 41 and 43 are twin primes. Unlike prime numbers, it is not known whether there are infinitely many twin primes.

The Twin Prime Conjecture

There are infinitely many twin primes.

The Goldbach Conjecture

Every even integer greater than 2 is the sum of two primes.

Observe that $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $28 = 17 + 11$ and $96 = 43 + 53$.

Questions for Self-Study

Let n be a positive integer.

- How many zeroes does 100! end in?
  If $\omega(n)$ denotes the number of zeros that number $n!$ ends in, then what is the formula for $\omega(n)$?
- Find the prime decomposition of 20!
  In general, how to find the prime decomposition of n factorial?
- How many digits in 100! ?
  How to find the number of digits in $n!$?
- Find the number of divisors of 5112.
  If $\tau(n)$ denotes the number of divisors of n, then what is the formula for $\tau(n)$?
- Find the sum of divisors of 5112.
  If $\sigma(n)$ denotes the sum of divisors of n, then what is the formula for $\sigma(n)$?

$a \equiv b$

Definition

Let $n > 1$ be a fixed natural number. Given integers a and b, we say that *a is congruent to b modulo n (or a is congruent to b mod n for short)* and we write $a \equiv b (mod\, n)$, if and only if $n \mid (a - b)$. The number n is called *the modulus* of the congruence.

$a \equiv b$

Definition

Let $n > 1$ be a fixed natural number. Given integers a and b, we say that *a is congruent to b modulo n (or a is congruent to b mod n for short)* and we write $a \equiv b (mod\, n)$, if and only if $n \,|\, (a - b)$. The number n is called *the modulus* of the congruence.

Examples

- $3 \equiv 17\,(mod\,7)$ because $3 - 17 = -14$ is divisible by 7
- $-2 \equiv 13\,(mod\,3)$ because $-2 - 13 = -15$ is divisible by 3
- $60 \equiv 10\,(mod\,25)$
- $-4 \equiv -49\,(mod\,9)$

Trip to Equivalence Relation

Theorem

Congruence relation on set of integer numbers $\mathbb{Z}$ is an equivalence relation.

Trip to Equivalence Relation

Theorem

Congruence relation on set of integer numbers $\mathbb{Z}$ is an equivalence relation.

Proof.
reflexive: since $a - a = 0$ is divisible by n, we have $a \equiv a\,(mod\,n)$.
symmetric: if $a \equiv b\,(mod\,n)$, then $b \equiv a\,(mod\,n)$, because if $n|(a - b)$, then $n|(b - a)$.
transitive: if $a \equiv b\,(mod\,n)$ and $b \equiv c\,(mod\,n)$, then $a \equiv c\,(mod\,n)$, because if $n|(a - b)$ and $n|(b - c)$, then since $a - c = (a - b) + (b - c)$, $n|(a - c)$ □

Trip to Equivalence Relation

Theorem

Congruence relation on set of integer numbers $\mathbb{Z}$ is an equivalence relation.

Proof.
reflexive: since $a - a = 0$ is divisible by n, we have $a \equiv a \,(mod\, n)$.
symmetric: if $a \equiv b \,(mod\, n)$, then $b \equiv a \,(mod\, n)$, because if $n|(a-b)$, then $n|(b-a)$.
transitive: if $a \equiv b \,(mod\, n)$ and $b \equiv c \,(mod\, n)$, then $a \equiv c \,(mod\, n)$, because if $n|(a-b)$ and $n|(b-c)$, then since $a - c = (a-b) + (b-c)$, $n|(a-c)$ □

The equivalence classes of congruence $mod\, n$ are called *congruence classes*, precisely, the *congruence class $mod\, n$* of an integer a is the set of all integers to which a is congruent $mod\, n$. It is denoted $\overline{a}$. Thus

$$\overline{a} = \{b \in \mathbb{Z} \,|\, a \equiv b \,(mod\, n)\}.$$

Examples

1. Let $n = 5$. There holds $-8 \equiv 17\,(mod\,5)$. Thus, by the definition $-8 \in \overline{17}$. Notice also that $17 \in \overline{-8}$. In fact, by basic theorem on equivalence relation from Lecture 2 we can have $\overline{-8} = \overline{17}$.

Examples

1. Let $n = 5$. There holds $-8 \equiv 17\,(mod\,5)$. Thus, by the definition $-8 \in \overline{17}$. Notice also that $17 \in \overline{-8}$. In fact, by basic theorem on equivalence relation from Lecture 2 we can have $\overline{-8} = \overline{17}$.

2. Let us find all congruence classes of integers $mod\,5$.

$$\begin{gathered}\overline{0} = \{b \in \mathbb{Z} \,|\, b \equiv 0\,(mod\,5)\} = \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-0)\} \\ = \{b \in \mathbb{Z} \,|\, b = 5k \text{ for some integer } k\} = 5\mathbb{Z},\end{gathered}$$

$$\begin{gathered}\overline{1} = \{b \in \mathbb{Z} \,|\, b \equiv 1\,(mod\,5)\} = \\ \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-1)\} = \{b \in \mathbb{Z} \,|\, b - 1 = 5k \text{ for some integer } k\} = \\ \{b \in \mathbb{Z} \,|\, b = 5k + 1 \text{ for some integer } k\} = 5\mathbb{Z} + 1.\end{gathered}$$

Examples

1. Let $n = 5$. There holds $-8 \equiv 17\,(mod\,5)$. Thus, by the definition $-8 \in \overline{17}$. Notice also that $17 \in \overline{-8}$. In fact, by basic theorem on equivalence relation from Lecture 2 we can have $\overline{-8} = \overline{17}$.

2. Let us find all congruence classes of integers $mod\,5$.

$$\begin{gathered}\overline{0} = \{b \in \mathbb{Z} \,|\, b \equiv 0\,(mod\,5)\} = \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-0)\} \\ = \{b \in \mathbb{Z} \,|\, b = 5k \text{ for some integer } k\} = 5\mathbb{Z},\end{gathered}$$

$$\begin{gathered}\overline{1} = \{b \in \mathbb{Z} \,|\, b \equiv 1\,(mod\,5)\} = \\ \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-1)\} = \{b \in \mathbb{Z} \,|\, b-1 = 5k \text{ for some integer } k\} = \\ \{b \in \mathbb{Z} \,|\, b = 5k+1 \text{ for some integer } k\} = 5\mathbb{Z}+1.\end{gathered}$$

Continuing, we find that

$$\overline{2} = \{b \in \mathbb{Z} \,|\, b = 5k+2 \text{ for some integer } k\} = 5\mathbb{Z}+2,$$

$$\overline{3} = \{b \in \mathbb{Z} \,|\, b = 5k+3 \text{ for some integer } k\} = 5\mathbb{Z}+3,$$

$$\overline{4} = \{b \in \mathbb{Z} \,|\, b = 5k+4 \text{ for some integer } k\} = 5\mathbb{Z}+4.$$

Examples

1. Let $n = 5$. There holds $-8 \equiv 17\,(mod\,5)$. Thus, by the definition $-8 \in \overline{17}$. Notice also that $17 \in \overline{-8}$. In fact, by basic theorem on equivalence relation from Lecture 2 we can have $\overline{-8} = \overline{17}$.

2. Let us find all congruence classes of integers $mod\,5$.

$$\begin{gathered}\overline{0} = \{b \in \mathbb{Z} \,|\, b \equiv 0\,(mod\,5)\} = \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-0)\} \\ = \{b \in \mathbb{Z} \,|\, b = 5k \;\text{ for some integer }\; k\} = 5\mathbb{Z},\end{gathered}$$

$$\begin{gathered}\overline{1} = \{b \in \mathbb{Z} \,|\, b \equiv 1\,(mod\,5)\} = \\ \{b \in \mathbb{Z} \,|\, 5 \,|\, (b-1)\} = \{b \in \mathbb{Z} \,|\, b - 1 = 5k \;\text{ for some integer }\; k\} = \\ \{b \in \mathbb{Z} \,|\, b = 5k+1 \;\text{ for some integer }\; k\} = 5\mathbb{Z}+1.\end{gathered}$$

Continuing, we find that

$$\overline{2} = \{b \in \mathbb{Z} \,|\, b = 5k+2 \;\text{ for some integer }\; k\} = 5\mathbb{Z}+2,$$

$$\overline{3} = \{b \in \mathbb{Z} \,|\, b = 5k+3 \;\text{ for some integer }\; k\} = 5\mathbb{Z}+3,$$

$$\overline{4} = \{b \in \mathbb{Z} \,|\, b = 5k+4 \;\text{ for some integer }\; k\} = 5\mathbb{Z}+4.$$

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}.$$

Proposition

Let a, b and n be integers with $n > 1$. Then the following statements are equivalent.

- $n \,|\, (a - b)$
- $a \equiv b \,(mod\, n)$
- $a \in \overline{b}$
- $b \in \overline{a}$
- $\overline{a} = \overline{b}$

Proposition

Let a, b and n be integers with $n > 1$. Then the following statements are equivalent.

- $n \mid (a - b)$
- $a \equiv b \, (mod \, n)$
- $a \in \overline{b}$
- $b \in \overline{a}$
- $\overline{a} = \overline{b}$

We emphasize perhaps the most important one which is

$$a \equiv b \, (mod \, n) \text{ if and only if } \overline{a} = \overline{b}.$$

Proposition

Let a, b and n be integers with $n > 1$. Then the following statements are equivalent.

- $n \mid (a - b)$
- $a \equiv b \, (mod \, n)$
- $a \in \overline{b}$
- $b \in \overline{a}$
- $\overline{a} = \overline{b}$

We emphasize perhaps the most important one which is

$$a \equiv b \, (mod \, n) \text{ if and only if } \overline{a} = \overline{b}.$$

The next proposition generalizes the special case $n = 5$, which we have already investigated.

Proposition

Let $n \in \mathbb{Z}$. Then there are n congruence classes of integers $mod \, n$ corresponding to each of the n possible remainders

$$\overline{k} = n\mathbb{Z} + k \text{ with } 0 \leq k \leq n - 1.$$

Example

$$3638 \equiv ?\,(mod\,18)$$

Example

$$3638 \equiv ?\,(mod\,18)$$

Solution. The preceding Proposition says that 3638 is congruent modulo 18 to one of the 18 integers $0, 1, 2, \ldots, 17$. Let we denote it by x.

$$3638 \equiv x\,(mod\,18) \Leftrightarrow 3638 \in \overline{x} \Leftrightarrow 3638 \in 18\mathbb{Z} + x$$

$$\Leftrightarrow 3638 = 18k + x \text{ with } 0 \leq x \leq 17.$$

Then x is just a remainder when we divide 3638 by 18.
By Division Algorithm one can easily write that

$$3638 = 18 \cdot 202 + 2$$

Hence, $x = 2$ and $3638 \equiv 2\,(mod\,18)$.

Proposition

If $n > 1$ is a natural number and a is an integer, then $a\,(mod\,n)$ is the remainder r , $0 \leq r < n$, obtained when a is divided by n.

Proposition

If $n > 1$ is a natural number and a is an integer, then $a\,(mod\,n)$ is the remainder r , $0 \leq r < n$, obtained when a is divided by n.

Examples

- $-17\,(mod\,5) = 3$ since $-17 = 5 \cdot (-4) + 3$ by division algorithm.
- $28\,(mod\,6) = 4$ since $28 = 6 \cdot 4 + 4$ by division algorithm.
- $-30\,(mod\,9) = 6$ since $-30 = 9 \cdot (-4) + 6$ by division algorithm.

Proposition

If $a \equiv x \, (mod \, n)$ and $b \equiv y \, (mod \, n)$, then

a. $a + b \equiv x + y \, (mod \, n)$

b. $ab \equiv xy \, (mod \, n)$

Proposition

If $a \equiv x \,(mod\, n)$ and $b \equiv y \,(mod\, n)$, then

a. $a + b \equiv x + y \,(mod\, n)$

b. $ab \equiv xy \,(mod\, n)$

Proof of a. We have to check that $(a + b) - (x + y)$ is divisible by n. This difference is $(a - x) + (b - y)$, which is the sum of two numbers each divisible by n, so the difference itself is divisible by n.

Proposition

If $a \equiv x \, (mod \, n)$ and $b \equiv y \, (mod \, n)$, then

a. $a + b \equiv x + y \, (mod \, n)$

b. $ab \equiv xy \, (mod \, n)$

Proof of a. We have to check that $(a + b) - (x + y)$ is divisible by n. This difference is $(a - x) + (b - y)$, which is the sum of two numbers each divisible by n, so the difference itself is divisible by n.

Proof of b. Since $ab - xy = a(b - y) + (a - x)y$, $ab - xy$ is divisible by n □

Example

$$1017 + 2876 \equiv ?\,(mod\,7)$$

Example

$$1017 + 2876 \equiv ?\,(mod\,7)$$

Solution. This can be accomplished in two ways. We could evaluate

$$1017 + 2876 = 3893 \equiv 1\,(mod\,7),$$

but, equally, we could reduce the integers 1017 and 2876 modulo 7 first like this

$$1017 \equiv 2\,(mod\,7)$$

$$2876 \equiv 6\,(mod\,7)$$

$$1017 + 2876 \equiv 2 + 6 = 8 \equiv 1\,(mod\,7).$$

Example

$$1017 + 2876 \equiv ?\,(mod\,7)$$

Solution. This can be accomplished in two ways. We could evaluate

$$1017 + 2876 = 3893 \equiv 1\,(mod\,7),$$

but, equally, we could reduce the integers 1017 and 2876 modulo 7 first like this

$$1017 \equiv 2\,(mod\,7)$$

$$2876 \equiv 6\,(mod\,7)$$

$$1017 + 2876 \equiv 2 + 6 = 8 \equiv 1\,(mod\,7).$$

The second approach is particularly useful when forming products since it keeps the numbers involved small. Observe:

$$(1017)(2876) \equiv (2)(6) = (12) \equiv 5\,(mod\,7).$$

Example

What is the remainder when $(1017)^{12}$ is divided by 7?
In other words,

$$(1017)^{12} \equiv ?\,(mod\,7)$$

Example

What is the remainder when $(1017)^{12}$ is divided by 7?
In other words,

$$(1017)^{12} \equiv ?\,(mod\,7)$$

Solution. Since $1017 \equiv 2\,(mod\,7)$ and by the second part of the previous proposition we have

$$(1017)^{12} \equiv (2)^{12} = (2^3)^4 \equiv 1^4 = 1\,(mod\,7).$$

Hence

$$(1017)^{12} \equiv\ 1\,(mod\,7).$$

In other words, the remainder when $(1017)^{12}$ is divided by 7 is 1.

Fermat's Little Theorem

Proposition

If $ac \equiv bc\,(mod\,n)$ and $GCD(c, n) = 1$, then $a \equiv b\,(mod\,n)$.

We leave its proof to the self-study.

Fermat's Little Theorem

Proposition

If $ac \equiv bc \, (mod \, n)$ and $GCD(c, n) = 1$, then $a \equiv b \, (mod \, n)$.

We leave its proof to the self-study.

Fermat's Little Theorem

If p is prime and $GCD(p, c) = 1$, then $c^{p-1} \equiv 1 \, (mod \, p)$.

Fermat's Little Theorem

Proposition

If $ac \equiv bc \, (mod\, n)$ and $GCD(c, n) = 1$, then $a \equiv b \, (mod\, n)$.

We leave its proof to the self-study.

Fermat's Little Theorem

If p is prime and $GCD(p, c) = 1$, then $c^{p-1} \equiv 1 \, (mod\, p)$.

Proof. We have $GCD(c, p) = 1$. Thus, by the Proposition, no two of the integers $c, 2c, \ldots, (p-1)c$ are congruent $mod\, p$. The same proposition also shows that none of the elements $c, 2c, \ldots, (p-1)c$ is $0 \, (mod\, p)$. Thus, modulo p, the $p-1$ integers $c, 2c, \ldots, (p-1)c$ are precisely $1, 2, \ldots, p-1$, in some order. Thus

$$c \cdot 2c \cdot 3c \cdots (p-1) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \, (mod\, p).$$

Letting $x = 1 \cdot 2 \cdot 3 \cdots (p-1)$, this equation reads

$$xc^{p-1} \equiv x \, (mod\, p)$$

and, since $GCD(p, x) = 1$, we can cancel x and obtain $c^{p-1} \equiv 1$, as required □

Examples

Fermat's Little Theorem shows the following congruences

- $9^{10} \equiv 1 \, (mod \, 11)$
- $4^{13330} \equiv 1 \, (mod \, 13331)$, since 13331 is prime (Really?).

Do you know what Fermat's best known theorem is?

Do you know what Fermat's best known theorem is?

Fermat's Last Theorem

Fermat's Last Theorem

For any integer $n > 2$, the equation

$$a^n + b^n = c^n$$

has no nonzero integer solutions a, b, c.

The proposition was first conjectured by Pierre de Fermat (a French lawyer) in around 1637. It was solved by Andrew Wiles of Princeton University in 1994.

Questions for Self-Study

- Is $2222^{5555} + 5555^{2222}$ divisible by 7?
- Nonzero integers are called *relatively prime* if and only if their greatest common divisor is 1. For instance, 15 and 28 are relatively prime because $GCD(15, 28) = 1$.
  How many positive integer are there less than 1000 that are relatively prime to 1000?
  Let $\phi(n)$ denotes the number of positive integers less than n that are relatively prime to n. What can you say about $\phi(n)$?
- Find the last two digits in the decimal representations of 9^{9^9} and 7^{8^9}.

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b \, (mod \, n).$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x = ?$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x =?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x = ?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x =?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,5),$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x =?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,5),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 1\,(mod\,5),$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x = ?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,5),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 1\,(mod\,5),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 4\,(mod\,5),$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x = ?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,5),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 1\,(mod\,5),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 4\,(mod\,5),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 2\,(mod\,5).$$

Linear Congruence

Now we study linear equations in congruence relations which are in the form

$$ax \equiv b\,(mod\,n).$$

Example 1.

$$3x \equiv 1\,(mod\,5) \qquad x = ?$$

It is easy to understand that $x \in \{0, 1, 2, 3, 4\}$ (Why?).

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,5),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,5),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 1\,(mod\,5),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 4\,(mod\,5),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 2\,(mod\,5).$$

Thus, the only solution to the congruence is $x = 2$.

Example 2.

$$3x \equiv 1\,(mod\,6) \qquad x =?$$

Then $x \in \{0, 1, 2, 3, 4, 5\}$.

Example 2.

$$3x \equiv 1\,(mod\,6) \qquad x = ?$$

Then $x \in \{0, 1, 2, 3, 4, 5\}$.

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,6),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,6),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 0\,(mod\,6),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 3\,(mod\,6),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 0\,(mod\,6).$$

$$\text{If } x = 5, \text{ then } 3x = 15 \equiv 3\,(mod\,6).$$

Example 2.

$$3x \equiv 1\,(mod\,6) \qquad x = ?$$

Then $x \in \{0, 1, 2, 3, 4, 5\}$.

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,6),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,6),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 0\,(mod\,6),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 3\,(mod\,6),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 0\,(mod\,6).$$

$$\text{If } x = 5, \text{ then } 3x = 15 \equiv 3\,(mod\,6).$$

Thus, there is no solution to this congruence because the values of $3x\,(mod\,6)$ are just 0 and 3.

Example 2.

$$3x \equiv 1\,(mod\,6) \qquad x =?$$

Then $x \in \{0, 1, 2, 3, 4, 5\}$.

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,6),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,6),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 0\,(mod\,6),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 3\,(mod\,6),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 0\,(mod\,6).$$

$$\text{If } x = 5, \text{ then } 3x = 15 \equiv 3\,(mod\,6).$$

Thus, there is no solution to this congruence because the values of $3x\,(mod\,6)$ are just 0 and 3.

Example 3.

$$3x \equiv 3\,(mod\,6) \qquad x =?$$

Example 2.

$$3x \equiv 1\,(mod\,6) \qquad x = ?$$

Then $x \in \{0, 1, 2, 3, 4, 5\}$.

$$\text{If } x = 0, \text{ then } 3x = 0 \equiv 0\,(mod\,6),$$

$$\text{If } x = 1, \text{ then } 3x = 3 \equiv 3\,(mod\,6),$$

$$\text{If } x = 2, \text{ then } 3x = 6 \equiv 0\,(mod\,6),$$

$$\text{If } x = 3, \text{ then } 3x = 9 \equiv 3\,(mod\,6),$$

$$\text{If } x = 4, \text{ then } 3x = 12 \equiv 0\,(mod\,6).$$

$$\text{If } x = 5, \text{ then } 3x = 15 \equiv 3\,(mod\,6).$$

Thus, there is no solution to this congruence because the values of $3x\,(mod\,6)$ are just 0 and 3.

Example 3.

$$3x \equiv 3\,(mod\,6) \qquad x = ?$$

The calculations in **Example 2** show that $3x \equiv 3\,(mod\,6)$ has solutions $x = 1, x = 3$ and $x = 5$.

A general method

How to solve $ax \equiv b\,(mod\,n)$ when a, b, n are sufficiently large?
A general method is to convert the linear congruence to a Diophantine equation and then solve it. That's all!

$$ax \equiv b\,(mod\,n) \Leftrightarrow n|(ax - b) \Leftrightarrow ax - b = ny \text{ for some } y \in \mathbb{Z}.$$

Hence

$$ax \equiv b\,(mod\,n) \Leftrightarrow ax - ny = b \text{ for some } y \in \mathbb{Z}.$$

A general method

How to solve $ax \equiv b \,(mod\, n)$ when a, b, n are sufficiently large?
A general method is to convert the linear congruence to a Diophantine equation and then solve it. That's all!

$$ax \equiv b \,(mod\, n) \Leftrightarrow n|(ax - b) \Leftrightarrow ax - b = ny \text{ for some } y \in \mathbb{Z}.$$

Hence

$$ax \equiv b \,(mod\, n) \Leftrightarrow ax - ny = b \text{ for some } y \in \mathbb{Z}.$$

Example. $11x \equiv 28 \,(mod\, 1943)$.

A general method

How to solve $ax \equiv b \, (mod \, n)$ when a, b, n are sufficiently large?
A general method is to convert the linear congruence to a Diophantine equation and then solve it. That's all!

$$ax \equiv b \, (mod \, n) \Leftrightarrow n | (ax - b) \Leftrightarrow ax - b = ny \text{ for some } y \in \mathbb{Z}.$$

Hence

$$ax \equiv b \, (mod \, n) \Leftrightarrow ax - ny = b \text{ for some } y \in \mathbb{Z}.$$

Example. $11x \equiv 28 \, (mod \, 1943)$. From it we derive a Diophantine equation $11x - 1943y = 28$.

A general method

How to solve $ax \equiv b\,(mod\,n)$ when a, b, n are sufficiently large?
A general method is to convert the linear congruence to a Diophantine equation and then solve it. That's all!

$$ax \equiv b\,(mod\,n) \Leftrightarrow n|(ax-b) \Leftrightarrow ax-b=ny \text{ for some } y \in \mathbb{Z}.$$

Hence

$$ax \equiv b\,(mod\,n) \Leftrightarrow ax-ny=b \text{ for some } y \in \mathbb{Z}.$$

Example. $11x \equiv 28\,(mod\,1943)$. From it we derive a Diophantine equation $11x - 1943y = 28$.

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

A general method

How to solve $ax \equiv b \,(mod\, n)$ when a, b, n are sufficiently large?
A general method is to convert the linear congruence to a Diophantine equation and then solve it. That's all!

$$ax \equiv b \,(mod\, n) \Leftrightarrow n|(ax - b) \Leftrightarrow ax - b = ny \text{ for some } y \in \mathbb{Z}.$$

Hence

$$ax \equiv b \,(mod\, n) \Leftrightarrow ax - ny = b \text{ for some } y \in \mathbb{Z}.$$

Example. $11x \equiv 28 \,(mod\, 1943)$. From it we derive a Diophantine equation $11x - 1943y = 28$.

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

Thus, $GCD(11, -1943) = 1$ and the equation has integer solutions, but we are interested in only x such that $0 \leq x < 1943$.

Using the following calculations we express the GCD by 11 and -1943

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

Using the following calculations we express the GCD by 11 and -1943

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

We have $1 = 4 - 3 = 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 = (-1943 - 11 \cdot (-177)) \cdot 3 - 11$

$$= (-1943) \cdot 3 + 11 \cdot 531 - 11 = (-1943) \cdot 3 + 11 \cdot 530$$

It follows $1 = (-1943) \cdot 3 + 11 \cdot 530.$

Using the following calculations we express the GCD by 11 and -1943

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

We have $1 = 4 - 3 = 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 = (-1943 - 11 \cdot (-177)) \cdot 3 - 11$

$$= (-1943) \cdot 3 + 11 \cdot 531 - 11 = (-1943) \cdot 3 + 11 \cdot 530$$

It follows $1 = (-1943) \cdot 3 + 11 \cdot 530$. In order to get a particular solution we need to multiply both sides by 28 and have

$$28 = (-1943) \cdot (3 \cdot 28) + 11 \cdot (530 \cdot 28).$$

We obtain $x_0 = 530 \cdot 28$ and $y_0 = 3 \cdot 28$.

Using the following calculations we express the GCD by 11 and -1943

$$-1943 = 11 \cdot (-177) + 4,$$

$$11 = 4 \cdot 2 + 3,$$

$$4 = 3 \cdot 1 + 1,$$

$$3 = 1 \cdot 3 + 0.$$

We have $1 = 4 - 3 = 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 = (-1943 - 11 \cdot (-177)) \cdot 3 - 11$

$$= (-1943) \cdot 3 + 11 \cdot 531 - 11 = (-1943) \cdot 3 + 11 \cdot 530$$

It follows $1 = (-1943) \cdot 3 + 11 \cdot 530$. In order to get a particular solution we need to multiply both sides by 28 and have

$$28 = (-1943) \cdot (3 \cdot 28) + 11 \cdot (530 \cdot 28).$$

We obtain $x_0 = 530 \cdot 28$ and $y_0 = 3 \cdot 28$.
Then $x = 530 \cdot 28 = 14840 = 1943 \cdot 7 + 1239 \equiv 1239\,(mod\,1943)$.
The answer is $x \equiv 1239\,(mod\,1943)$.

The Chinese Remainder Theorem

Let us consider a following question. Suppose we have some apples and we would like to distribute them among children. When we distribute them equally among 3 children, then we have left 2 apples, if among 5 children, then left 3 apples, if among 7 children, then left 2 apples. How many number of apples do we have?

The Chinese Remainder Theorem

Let us consider a following question. Suppose we have some apples and we would like to distribute them among children. When we distribute them equally among 3 children, then we have left 2 apples, if among 5 children, then left 3 apples, if among 7 children, then left 2 apples. How many number of apples do we have?

In fact, this question can be rephrased in terms of congruences as follows. Let x be the number of apples.
Then these distributions are equivalent to

$$x \equiv 2\,(mod\,3), \quad x \equiv 3\,(mod\,5), \text{ and } x \equiv 2\,(mod\,7).$$

The Chinese Remainder Theorem

Let us consider a following question. Suppose we have some apples and we would like to distribute them among children. When we distribute them equally among 3 children, then we have left 2 apples, if among 5 children, then left 3 apples, if among 7 children, then left 2 apples. How many number of apples do we have?

In fact, this question can be rephrased in terms of congruences as follows. Let x be the number of apples.
Then these distributions are equivalent to

$$x \equiv 2\,(mod\,3), \quad x \equiv 3\,(mod\,5), \text{ and } x \equiv 2\,(mod\,7).$$

Then we have to find x satisfying the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

There is a well-known theorem so called *Chinese Remainder Theorem* which allows to solve a system of congruences.

The Chinese Remainder Theorem

Let

$$\begin{cases} x \equiv a_1 \, (mod \, n_1) \\ x \equiv a_2 \, (mod \, n_2) \\ \dots\dots\dots\dots\dots\dots \\ x \equiv a_r \, (mod \, n_r) \end{cases}$$

such that $GCD(n_i, n_j) = 1$ for all $i \neq j$. Then

$$x = \frac{N}{n_1}a_1b_1 + \frac{N}{n_2}a_2b_2 + \ldots + \frac{N}{n_r}a_rb_r \, (mod \, N)$$

where $\frac{N}{n_i}b_i \equiv 1 \, (mod \, n_i)$ for all $1 \leq i \leq r$ and $N = n_1n_2 \cdots n_r$.

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2 \,(mod\, 3) \\ x \equiv 3 \,(mod\, 5) \\ x \equiv 2 \,(mod\, 7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

$$35b_1 \equiv 1 \,(mod\, 3) \Leftrightarrow 2b_1 \equiv 1 \,(mod\, 3) \Leftrightarrow b_1 \equiv 2 \,(mod\, 3),$$

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

$$35b_1 \equiv 1\,(mod\,3) \Leftrightarrow 2b_1 \equiv 1\,(mod\,3) \Leftrightarrow b_1 \equiv 2\,(mod\,3),$$

$$21b_2 \equiv 1\,(mod\,5) \Leftrightarrow b_2 \equiv 1\,(mod\,5),$$

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2 \, (mod \, 3) \\ x \equiv 3 \, (mod \, 5) \\ x \equiv 2 \, (mod \, 7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

$$35b_1 \equiv 1 \, (mod \, 3) \Leftrightarrow 2b_1 \equiv 1 \, (mod \, 3) \Leftrightarrow b_1 \equiv 2 \, (mod \, 3),$$

$$21b_2 \equiv 1 \, (mod \, 5) \Leftrightarrow b_2 \equiv 1 \, (mod \, 5),$$

$$15b_3 \equiv 1 \, (mod \, 7) \Leftrightarrow b_3 \equiv 1 \, (mod \, 7).$$

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

$$35b_1 \equiv 1\,(mod\,3) \Leftrightarrow 2b_1 \equiv 1\,(mod\,3) \Leftrightarrow b_1 \equiv 2\,(mod\,3),$$

$$21b_2 \equiv 1\,(mod\,5) \Leftrightarrow b_2 \equiv 1\,(mod\,5),$$

$$15b_3 \equiv 1\,(mod\,7) \Leftrightarrow b_3 \equiv 1\,(mod\,7).$$

$$x = \frac{105}{3} \cdot 2 \cdot 2 + \frac{105}{5} \cdot 3 \cdot 1 + \frac{105}{7} \cdot 2 \cdot 1 = 233 \equiv 23\,(mod\,105).$$

How many apples?

By the Chinese Remainder Theorem we solve the system of congruences

$$\begin{cases} x \equiv 2\,(mod\,3) \\ x \equiv 3\,(mod\,5) \\ x \equiv 2\,(mod\,7) \end{cases}$$

Solution. We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, and $N = 3 \cdot 5 \cdot 7 = 105$. Now find b_1, b_2 and b_3.

$$35b_1 \equiv 1\,(mod\,3) \Leftrightarrow 2b_1 \equiv 1\,(mod\,3) \Leftrightarrow b_1 \equiv 2\,(mod\,3),$$

$$21b_2 \equiv 1\,(mod\,5) \Leftrightarrow b_2 \equiv 1\,(mod\,5),$$

$$15b_3 \equiv 1\,(mod\,7) \Leftrightarrow b_3 \equiv 1\,(mod\,7).$$

$$x = \tfrac{105}{3} \cdot 2 \cdot 2 + \tfrac{105}{5} \cdot 3 \cdot 1 + \tfrac{105}{7} \cdot 2 \cdot 1 = 233 \equiv 23\,(mod\,105).$$

Then $x = 23$. Hence, we have $23 + 105t$ apples, where t is any nonnegative integer.

The End of Lecture 4