Math 2603 - Lecture 7
Section 4.1 to 4.3 Division and prime numbers

Bo Lin

September 10th, 2019

Division and divisibility

Arithmetic operations

We have been familiar with addition and multiplication among real numbers. And they have a lot of good properties.

Arithmetic operations

We have been familiar with addition and multiplication among real numbers. And they have a lot of good properties.
For integers a, b, c, we have

- (commutativity) $a + b = b + a$; $a * b = b * a$.
- (associativity) $a + (b + c) = (a + b) + c$; $a * (b * c) = (a * b) * c$.
- (distributive law) $a * (b + c) = a * b + a * c$.
- (identities) $a + 0 = a$; $a * 1 = a$.
- (additive inverse) $a + (-a) = 0$.
- (multiplicative inverse)$a * \left(\frac{1}{a}\right) = 1$ for all $a \neq 0$.

Arithmetic operations

We have been familiar with addition and multiplication among real numbers. And they have a lot of good properties.
For integers a, b, c, we have

- (commutativity) $a + b = b + a$; $a * b = b * a$.
- (associativity) $a + (b + c) = (a + b) + c$; $a * (b * c) = (a * b) * c$.
- (distributive law) $a * (b + c) = a * b + a * c$.
- (identities) $a + 0 = a$; $a * 1 = a$.
- (additive inverse) $a + (-a) = 0$.
- (multiplicative inverse)$a * \left(\frac{1}{a}\right) = 1$ for all $a \neq 0$.

Remark

In fact, there are other arithmetic operations.

Subtraction and division

Definition

For real numbers a, b*, the* **subtraction** *is defined in terms of addition that*

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

Subtraction and division

Definition

For real numbers a, b, the **subtraction** *is defined in terms of addition that*

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

Definition

For real numbers a, b with $b \neq 0$, the **division** *is defined in term of addition that*

$$a/b = c,$$

where c is the unique real number such that $c \cdot b = a$.

Subtraction and division

Definition

For real numbers a, b, the **subtraction** *is defined in terms of addition that*

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

Definition

For real numbers a, b with $b \neq 0$, the **division** *is defined in term of addition that*

$$a/b = c,$$

where c is the unique real number such that $c \cdot b = a$.

Today, we focus on the case when both a, b are integers. Note that c may not be an integer. But if $a, b \in \mathbb{Z}$, by definition $c \in \mathbb{Q}$.

Divisibility

Definition

If a and b are integers and $b \neq 0$ then a is **divisible** *by b if and only if a equals b times some integer. Instead of a is divisible by b, we can also say that*

- *a is a* **multiple** *of b;*
- *b is a* **factor** *of a;*
- *b is a* **divisor** *of a;*
- *b* **divides** *a.*

The notation $b|a$ is read b divides a. Symbolically, if a and b are integers and $b \neq 0$

$$b|a \Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } a = k \cdot b.$$

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*
(b) *Does* 4 *divide* 22*?*
(c) *Is* 28 *a multiple of* -7*?*

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$, *yes.*

Examples: checking divisibility

Example

(a) *Is* 21 *divisible by* 3*?*

(b) *Does* 4 *divide* 22*?*

(c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$*, yes.*
(b) Since $22/4 = 5.5 \notin \mathbb{Z}$*, no.*

Examples: checking divisibility

Example

- (a) *Is* 21 *divisible by* 3*?*
- (b) *Does* 4 *divide* 22*?*
- (c) *Is* 28 *a multiple of* -7*?*

Solution

(a) Since $21 = 3 \cdot 7$*, yes.*
(b) Since $22/4 = 5.5 \notin \mathbb{Z}$*, no.*
(c) Since $28 = (-7) \cdot (-4)$*, yes.*

The Well-ordering Principle

Axiom (The Well-ordering Principle)

Let S be a nonempty set of integers all of which are greater than some fixed integer C. Then S has a least element. In particular, any nonempty subset of $\mathbb{N}$ has a least element.

The Well-ordering Principle

Axiom (The Well-ordering Principle)

Let S be a nonempty set of integers all of which are greater than some fixed integer C. Then S has a least element. In particular, any nonempty subset of $\mathbb{N}$ has a least element.

Remark

This principle is equivalent to the principle of mathematical induction. In other words, either one could imply the other.

What happens when $b \nmid a$

Suppose a, b are integers such that $b \nmid a$, can we still do a/b?

What happens when $b \nmid a$

Suppose a, b are integers such that $b \nmid a$, can we still do a/b?

Example

Suppose 3 *students are devouring a large pizza together. There are* 8 *slices in total. How could they share the pizza as equal as possible without dividing each slice?*

What happens when $b \nmid a$

Suppose a, b are integers such that $b \nmid a$, can we still do a/b?

Example

Suppose 3 students are devouring a large pizza together. There are 8 slices in total. How could they share the pizza as equal as possible without dividing each slice?

Remark

First, each student would get 2 slices. There are still $8 - 3 \cdot 2 = 2$ slices remaining. Since $2 < 3$, they cannot further divide them.

What happens when $b \nmid a$

Suppose a, b are integers such that $b \nmid a$, can we still do a/b?

Example

Suppose 3 students are devouring a large pizza together. There are 8 slices in total. How could they share the pizza as equal as possible without dividing each slice?

Remark

First, each student would get 2 slices. There are still $8 - 3 \cdot 2 = 2$ slices remaining. Since $2 < 3$, they cannot further divide them.

Remark

This is exactly how division between integers works.

Quotient-remainder Theorem

Theorem (Quotient-remainder Theorem)

Given any integer a and integer $b > 0$, there exists a unique pair of integers q and r such that

$$a = qb + r$$

and $0 \leq r < b$.

Quotient-remainder Theorem

Theorem (Quotient-remainder Theorem)

Given any integer a and integer $b > 0$, there exists a unique pair of integers q and r such that

$$a = qb + r$$

and $0 \leq r < b$.

Definition

The unique q above is called the **quotient** *of the division and the unique r above is called the* **remainder** *of the division.*

Proof of Quotient-remainder Theorem

Proof.

Consider the set

$$S = \{kb \mid k \in \mathbb{Z}, kb > a\}.$$

Proof of Quotient-remainder Theorem

Proof.

Consider the set

$$S = \{kb \mid k \in \mathbb{Z}, kb > a\}.$$

Since $b > 0$, when k is big enough, kb would be greater than a, so S is nonempty.

Proof of Quotient-remainder Theorem

Proof.

Consider the set

$$S = \{kb \mid k \in \mathbb{Z}, kb > a\}.$$

Since $b > 0$, when k is big enough, kb would be greater than a, so S is nonempty. By definition, all elements in S are greater than a.

Proof of Quotient-remainder Theorem

Proof.

Consider the set

$$S = \{kb \mid k \in \mathbb{Z}, kb > a\}.$$

Since $b > 0$, when k is big enough, kb would be greater than a, so S is nonempty. By definition, all elements in S are greater than a. By the The Well-ordering Principle, S has a least element, say $(q+1)b$, where $q \in \mathbb{Z}$. Then $(q+1)b > a$.

Proof of Quotient-remainder Theorem

Proof.

Consider the set

$$S = \{kb \mid k \in \mathbb{Z}, kb > a\}.$$

Since $b > 0$, when k is big enough, kb would be greater than a, so S is nonempty. By definition, all elements in S are greater than a. By the The Well-ordering Principle, S has a least element, say $(q+1)b$, where $q \in \mathbb{Z}$. Then $(q+1)b > a$. Now we look at qb. Since $qb < (q+1)b$, $qb \notin S$. While $q \in \mathbb{Z}$, so the only violation is that $qb \leq a$. Hence

$$qb \leq a < (q+1)b.$$

Finally we let $r = a - qb$. Then $0 \leq r < (q+1)b - qb = b$. □

Division algorithm

Corollary

For any integer a *and integer* $b > 0$, *the quotient of* a/b *is* $q = \left\lfloor \frac{a}{b} \right\rfloor$ *and* $r = a - qb$.

Division algorithm

Corollary

For any integer a and integer $b > 0$, the quotient of a/b is $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - qb$.

Remark

In practice, it is essential to find the consecutive integers that $\frac{a}{b}$ is between them.

A more general version

Theorem (Quotient-remainder Theorem)

Given any integer a and integer $b \neq 0$, there exists a unique pair of integers q and r such that

$$a = qb + r$$

and $0 \leq r < |b|$.

A more general version

Theorem (Quotient-remainder Theorem)

Given any integer a and integer $b \neq 0$, there exists a unique pair of integers q and r such that

$$a = qb + r$$

and $0 \leq r < |b|$.

Corollary

For any integer a and integer $b < 0$, the quotient of a/b is $q = \left\lceil \frac{a}{b} \right\rceil$ and $r = a - qb$.

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n and d:

1. $n = 20$ *and* $d = 7$*;*
2. $n = -8$ *and* $d = 3$*;*

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n and d:

(a) $n = 20$ *and* $d = 7$;

(b) $n = -8$ *and* $d = 3$;

Solution

(a) $20 = 7 \cdot 2 + 6$ *and* $0 \leq 6 < 7$, *so* $q = 2$ *and* $r = 6$.

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n and d:

a. $n = 20$ *and* $d = 7$;
b. $n = -8$ *and* $d = 3$;

Solution

(a) $20 = 7 \cdot 2 + 6$ *and* $0 \leq 6 < 7$, *so* $q = 2$ *and* $r = 6$.
(b) $-8 = 3 \cdot (-3) + 1$ *and* $0 \leq 1 < 3$, *so* $q = -3$ *and* $r = 1$.

Integers in other bases

When we write integers, we are using the **decimal representation**, which is base 10. For example,

$$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0.$$

Integers in other bases

When we write integers, we are using the **decimal representation**, which is base 10. For example,

$$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0.$$

In fact, for any integer $b > 1$, we can write integers in base b.

Integers in other bases

When we write integers, we are using the **decimal representation**, which is base 10. For example,

$$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0.$$

In fact, for any integer $b > 1$, we can write integers in base b.

Definition

Let $b > 1$ be a fixed integer. For integer $N \geq 0$, **base b representation** *of N is the unique expression*

$$(a_{n-1}a_{n-2}\cdots a_0)_b,$$

where integers $0 \leq a_i < b$ and
$N = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1 b + a_0.$

Conversion to base b

Proposition

Let $N, b \in \mathbb{N}$ with $b > 1$. Suppose the quotient and remainder of a divided by b are q and r. If $q = (a_{n-1}a_{n-2}\cdots a_1)_b$, then $N = (a_{n-1}a_{n-2}\cdots a_1 r)_b$.

Conversion to base b

Proposition

Let $N, b \in \mathbb{N}$ with $b > 1$. Suppose the quotient and remainder of a divided by b are q and r. If $q = (a_{n-1}a_{n-2}\cdots a_1)_b$, then $N = (a_{n-1}a_{n-2}\cdots a_1 r)_b$.

Remark

In order to convert N to base b, we keep dividing by b. In each round of division, the remainder becomes the next rightmost digit, and we divide b from quotient next, until the quotient becomes zero.

Example: convert to hexadecimal representation

Remark

"Base 16*" is called* **hexadecimal representation**. *The digits* 10 *through* 15 *are denoted by the uppercase letters* A *through* F.

Example: convert to hexadecimal representation

Remark

"Base 16" is called **hexadecimal representation**. *The digits 10 through 15 are denoted by the uppercase letters A through F.*

Example

Convert $(2159)_{10}$ to hexadecimal representation.

Example: convert to hexadecimal representation

Remark

"Base 16" is called **hexadecimal representation**. *The digits 10 through 15 are denoted by the uppercase letters A through F.*

Example

Convert $(2159)_{10}$ to hexadecimal representation.

Solution

2159 *divided by* 16, *we get* $2159 = 134 \cdot 16 + 15$.

Example: convert to hexadecimal representation

Remark

"Base 16" is called **hexadecimal representation**. *The digits* 10 *through* 15 *are denoted by the uppercase letters* A *through* F.

Example

Convert $(2159)_{10}$ *to hexadecimal representation.*

Solution

2159 *divided by* 16, *we get* $2159 = 134 \cdot 16 + 15$.
134 *divided by* 16, *we get* $134 = 8 \cdot 16 + 6$.

Example: convert to hexadecimal representation

Remark

"Base 16" is called **hexadecimal representation**. *The digits* 10 *through* 15 *are denoted by the uppercase letters* A *through* F.

Example

Convert $(2159)_{10}$ *to hexadecimal representation.*

Solution

2159 *divided by* 16, *we get* $2159 = 134 \cdot 16 + 15$.
134 *divided by* 16, *we get* $134 = 8 \cdot 16 + 6$.
8 *divided by* 16, *we get* $8 = 0 \cdot 16 + 8$. *So*

$$(2159)_{10} = (86F)_{16}.$$

Prime numbers

Definition

For $p \in \mathbb{N}$, p is called a **prime number** *if $p > 1$ and p has no positive divisors other than 1 and p. For $q > 1$, if q is not prime, then q is called a* **composite number***.*

Prime numbers

Definition

For $p \in \mathbb{N}$, p is called a **prime number** *if $p > 1$ and p has no positive divisors other than 1 and p. For $q > 1$, if q is not prime, then q is called a* **composite number***.*

Remark

Warning! 1 is neither prime nor composite.

Prime numbers

Definition

For $p \in \mathbb{N}$, p is called a **prime number** *if $p > 1$ and p has no positive divisors other than 1 and p. For $q > 1$, if q is not prime, then q is called a* **composite number**.

Remark

Warning! 1 is neither prime nor composite.

Example

The smallest prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \cdots$$

Existence of prime divisor

Proposition

For every integer $n > 1$, there exists a prime number p with $p \mid n$.

Proof.

Consider the set $\{n \in \mathbb{N} \mid n > 1, n \text{ has no prime divisor}\}$.

Existence of prime divisor

Proposition

For every integer $n > 1$, there exists a prime number p with $p \mid n$.

Proof.

Consider the set $\{n \in \mathbb{N} \mid n > 1, n \text{ has no prime divisor}\}$. If it is nonempty, by well-ordering principle it has a least element m.

Existence of prime divisor

Proposition

For every integer $n > 1$, there exists a prime number p with $p \mid n$.

Proof.

Consider the set $\{n \in \mathbb{N} \mid n > 1, n \text{ has no prime divisor}\}$. If it is nonempty, by well-ordering principle it has a least element m. Since $m \mid m$, m itself is not prime.

Existence of prime divisor

Proposition

For every integer $n > 1$, there exists a prime number p with $p \mid n$.

Proof.

Consider the set $\{n \in \mathbb{N} \mid n > 1, n$ has no prime divisor$\}$. If it is nonempty, by well-ordering principle it has a least element m. Since $m \mid m$, m itself is not prime. So there exists $1 < a < m$ such that $a \mid m$. Then a is not in the set and a has a prime divisor p.

Existence of prime divisor

Proposition

For every integer $n > 1$*, there exists a prime number* p *with* $p \mid n$*.*

Proof.

Consider the set $\{n \in \mathbb{N} \mid n > 1, n \text{ has no prime divisor}\}$. If it is nonempty, by well-ordering principle it has a least element m. Since $m \mid m$, m itself is not prime. So there exists $1 < a < m$ such that $a \mid m$. Then a is not in the set and a has a prime divisor p. Finally $p \mid a, a \mid m$ implies $p \mid m$, a contradiction. $\square$

There are infinitely many prime numbers

Theorem

There are infinitely many prime numbers.

There are infinitely many prime numbers

Theorem

There are infinitely many prime numbers.

Proof.

We prove by contradiction. Suppose there are finitely many prime numbers $p_1, p_2, \cdots, p_n$. Let N be their product plus 1. Then none of them can be a divisor of N, so N has no prime divisor, a contradiction! $\square$

There are infinitely many prime numbers

Theorem

There are infinitely many prime numbers.

Proof.

We prove by contradiction. Suppose there are finitely many prime numbers $p_1, p_2, \cdots, p_n$. Let N be their product plus 1. Then none of them can be a divisor of N, so N has no prime divisor, a contradiction! $\square$

Remark

There are numerous proofs of this fact. This elegant short proof is by Ancient Greek mathematician Euclid.

Euclidean algorithm

Greatest Common Divisor

Definition

For $a, b \in \mathbb{Z}$ *not both zero, the* **greatest common divisor** *of* a, b*, denoted* $\gcd(a, b)$*, is the large common divisor* g *of* a *and* b*.*

Greatest Common Divisor

Definition

For $a, b \in \mathbb{Z}$ not both zero, the **greatest common divisor** *of a, b, denoted $\gcd(a, b)$, is the large common divisor g of a and b.*

Remark

Since 1 divides every integer, a and b always have at least one common divisor. And each common divisor is at most $\max(|a|, |b|)$, so $\gcd(a, b)$ is well-defined.

Least Common Multiple

Definition

For nonzero $a, b \in \mathbb{Z}$, the **least common multiple** *of a, b, denoted $\operatorname{lcm}(a, b)$, is the smallest positive common multiple l of a and b.*

Remark

Since $|ab|$ is always one common multiple, $\operatorname{lcm}(a, b)$ is well-defined by the well-ordering principle.

Relatively prime

Definition

Integers a *and* b *are called* **relatively prime** *(or* **coprime***) if* $\gcd(a,b)=1$*. In other words,* a *and* b *don't have any common divisor greater than* 1 *and they don't have a common prime divisor.*

Relatively prime

Definition

Integers a *and* b *are called* **relatively prime** *(or* **coprime***) if* $\gcd(a, b) = 1$. *In other words,* a *and* b *don't have any common divisor greater than* 1 *and they don't have a common prime divisor.*

Example

1 *and any integer are relatively prime.* n *and* $n + 1$ *are always relatively prime.*

Examples: find $\gcd$ and lcm

Example

Find

(a) $\gcd(15, 6)$;
(b) $\operatorname{lcm}(4, 14)$.

Examples: find $\gcd$ and lcm

Example

Find

(a) $\gcd(15, 6)$;

(b) $\operatorname{lcm}(4, 14)$.

Solution

(a) $15 = 5 \cdot 3, 6 = 2 \cdot 3$, *and they don't have a bigger common divisor. So* $\gcd(15, 6) = 3$.

Examples: find $\gcd$ and lcm

Example

Find

(a) $\gcd(15, 6)$;

(b) $\operatorname{lcm}(4, 14)$.

Solution

(a) $15 = 5 \cdot 3, 6 = 2 \cdot 3$, *and they don't have a bigger common divisor. So* $\gcd(15, 6) = 3$.
(b) 14 *itself is not a multiple of* 4. *The next multiple of* 14 *is* $2 \cdot 14 = 28 = 7 \cdot 4$, *which is a multiple of* 4. *So* $\operatorname{lcm}(4, 14) = 28$.

Examples: find $\gcd$ and lcm

Example

Find

(a) $\gcd(15, 6)$;

(b) $\operatorname{lcm}(4, 14)$.

Solution

(a) $15 = 5 \cdot 3, 6 = 2 \cdot 3$, *and they don't have a bigger common divisor. So* $\gcd(15, 6) = 3$.
(b) 14 *itself is not a multiple of* 4. *The next multiple of* 14 *is* $2 \cdot 14 = 28 = 7 \cdot 4$, *which is a multiple of* 4. *So* $\operatorname{lcm}(4, 14) = 28$.

Remark

We need a systematic method to compute $\gcd$ *and* lcm.

Euclidean algorithm

Proposition

For integers a, b, q, r, *if* $a = qb + r$, *then* $\gcd(a, b) = \gcd(b, r)$.

Euclidean algorithm

Proposition

For integers a, b, q, r*, if* $a = qb + r$*, then* $\gcd(a, b) = \gcd(b, r)$.

Remark

Note that $r < b$*, so we reduce the pair of integers in each division. Eventually we will end up with a remainder* $r = 0$*, and then* $\gcd(b, r) = b$*. This method is called the* **Euclidean Algorithm**.

Example: apply Euclidean algorithm

Example

Find $\gcd(630, 196)$.

Example: apply Euclidean algorithm

Example

Find $\gcd(630, 196)$.

Solution

First, $630 = 3 \cdot 196 + 42$. *It suffices to find* $\gcd(196, 42)$.

Example: apply Euclidean algorithm

Example

Find $\gcd(630, 196)$.

Solution

First, $630 = 3 \cdot 196 + 42$. *It suffices to find* $\gcd(196, 42)$.
Second, $196 = 4 \cdot 42 + 28$. *It suffices to find* $\gcd(42, 28)$.

Example: apply Euclidean algorithm

Example

Find $\gcd(630, 196)$.

Solution

First, $630 = 3 \cdot 196 + 42$. *It suffices to find* $\gcd(196, 42)$.
Second, $196 = 4 \cdot 42 + 28$. *It suffices to find* $\gcd(42, 28)$.
Third, $42 = 1 \cdot 28 + 14$. *It suffices to find* $\gcd(28, 14)$.

Example: apply Euclidean algorithm

Example

Find $\gcd(630, 196)$.

Solution

First, $630 = 3 \cdot 196 + 42$. *It suffices to find* $\gcd(196, 42)$.
Second, $196 = 4 \cdot 42 + 28$. *It suffices to find* $\gcd(42, 28)$.
Third, $42 = 1 \cdot 28 + 14$. *It suffices to find* $\gcd(28, 14)$.
Finally, $28 = 2 \cdot 14 + 0$. *Hence* $\gcd(630, 196) = 14$.

Bezout's Theorem

Theorem (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$ *and* $g = \gcd(a, b)$*. Then there exist integers* m, n *such that* $g = ma + nb$*.*

Bezout's Theorem

Theorem (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$ *and* $g = \gcd(a, b)$. *Then there exist integers* m, n *such that* $g = ma + nb$.

Remark

Euclidean Algorithm can explicitly find m *and* n.

Bezout's Theorem

Theorem (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$ *and* $g = \gcd(a, b)$. *Then there exist integers* m, n *such that* $g = ma + nb$.

Remark

Euclidean Algorithm can explicitly find m *and* n.

Example (Example revisited)

$630 = 3 \cdot 196 + 42$ *implies* $42 = 1 \cdot 630 + (-3) \cdot 196$.

Bezout's Theorem

Theorem (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$ *and* $g = \gcd(a, b)$. *Then there exist integers* m, n *such that* $g = ma + nb$.

Remark

Euclidean Algorithm can explicitly find m *and* n.

Example (Example revisited)

$630 = 3 \cdot 196 + 42$ *implies* $42 = 1 \cdot 630 + (-3) \cdot 196$.
$196 = 4 \cdot 42 + 28$ *implies*
$28 = 1 \cdot 196 - 4 \cdot (1 \cdot 630 + (-3) \cdot 196) = (-4) \cdot 630 + 13 \cdot 196.$

Bezout's Theorem

Theorem (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$ *and* $g = \gcd(a, b)$*. Then there exist integers* m, n *such that* $g = ma + nb$*.*

Remark

Euclidean Algorithm can explicitly find m *and* n*.*

Example (Example revisited)

$630 = 3 \cdot 196 + 42$ *implies* $42 = 1 \cdot 630 + (-3) \cdot 196.$
$196 = 4 \cdot 42 + 28$ *implies*
$28 = 1 \cdot 196 - 4 \cdot (1 \cdot 630 + (-3) \cdot 196) = (-4) \cdot 630 + 13 \cdot 196.$
$42 = 1 \cdot 28 + 14$ *implies*
$14 = (1 \cdot 630 + (-3) \cdot 196) - 1 \cdot ((-4) \cdot 630 + 13 \cdot 196) =$
$5 \cdot 630 + (-16) \cdot 196.$ *So* $m = 5, n = -16.$

Relation between $\gcd$ and lcm

Proposition

For nonzero $a, b \in \mathbb{Z}$, *we have* $\gcd(a,b)\operatorname{lcm}(a,b) = |ab|$.

Relation between gcd and lcm

Proposition

For nonzero $a, b \in \mathbb{Z}$*, we have* $\gcd(a,b)\,\mathrm{lcm}(a,b) = |ab|$.

Remark

So in order to compute $\mathrm{lcm}(a,b)$*, we can use Euclidean Algorithm to compute* $\gcd(a,b)$ *first.*

HW Assignment #4 - today's sections

Section 4.1 Exercise 4, 7, 8, 11(a).
Section 4.2 Exercise 7, 11, 12(a)(d), 27.