Math 3110 Lecture 7

February 8, 2023

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d.

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

Corollary

Let a and b be integers which are not both 0, and let $d = \gcd(a, b)$.

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

Corollary

Let a and b be integers which are not both 0, and let $d = \gcd(a, b)$. Then $S = \{ax + by : x, y \in \mathbb{Z}\}$ is precisely the set of all integer multiples of d.

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

Corollary

Let a and b be integers which are not both 0, and let $d = \gcd(a, b)$. Then $S = \{ax + by : x, y \in \mathbb{Z}\}$ is precisely the set of all integer multiples of d.

Also recall the following result from last lecture:

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

Corollary

Let a and b be integers which are not both 0, and let $d = \gcd(a, b)$. Then $S = \{ax + by : x, y \in \mathbb{Z}\}$ is precisely the set of all integer multiples of d.

Also recall the following result from last lecture:

Corollary

Let a and b be integers.

GCD Applications

Before beginning, recall that for integers a and b which are not both 0, $\gcd(a, b) = d \in S = \{ax + by : x, y \in \mathbb{Z}\}$ and that, furthermore, every member of S is a multiple of d. Let us record this result now.

Corollary

Let a and b be integers which are not both 0, and let $d = \gcd(a, b)$. Then $S = \{ax + by : x, y \in \mathbb{Z}\}$ is precisely the set of all integer multiples of d.

Also recall the following result from last lecture:

Corollary

Let a and b be integers. Then a and b are relatively prime (that is, $\gcd(a, b) = 1$) if and only if $ax + by = 1$ for some integers x and y.

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every ‘fraction’ (formally, rational number) can be expressed in so-called ‘reduced form’.

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$
3. $\frac{8}{4} = \frac{2}{1}$

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$
3. $\frac{8}{4} = \frac{2}{1}$

Note that the reduced fractions all have the property that the GCD of the numerator and denominator is 1.

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$
3. $\frac{8}{4} = \frac{2}{1}$

Note that the reduced fractions all have the property that the GCD of the numerator and denominator is 1. This is *precisely* what it *means* for a fraction to be reduced.

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$
3. $\frac{8}{4} = \frac{2}{1}$

Note that the reduced fractions all have the property that the GCD of the numerator and denominator is 1. This is *precisely* what it *means* for a fraction to be reduced. We can now prove that every rational number can be expressed in reduced form.

GCD Applications

You may recall from elementary school (or middle or high school) the following fact: every 'fraction' (formally, rational number) can be expressed in so-called 'reduced form'.

Example

1. $\frac{4}{12} = \frac{1}{3}$
2. $\frac{-40}{36} = \frac{-10}{9}$
3. $\frac{8}{4} = \frac{2}{1}$

Note that the reduced fractions all have the property that the GCD of the numerator and denominator is 1. This is *precisely* what it *means* for a fraction to be reduced. We can now prove that every rational number can be expressed in reduced form.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

Let $a, b \in \mathbb{Z}$, where a and b are not both 0, and let $d = \gcd(a, b)$.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

Let $a, b \in \mathbb{Z}$, where a and b are not both 0, and let $d = \gcd(a, b)$. Then from our above work, there exist integers x and y such that $d = ax + by$.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

Let $a, b \in \mathbb{Z}$, where a and b are not both 0, and let $d = \gcd(a, b)$. Then from our above work, there exist integers x and y such that $d = ax + by$. Now divide through by d to get $1 = \frac{a}{d}x + \frac{b}{d}y$.

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

Let $a, b \in \mathbb{Z}$, where a and b are not both 0, and let $d = \gcd(a, b)$. Then from our above work, there exist integers x and y such that $d = ax + by$. Now divide through by d to get $1 = \frac{a}{d}x + \frac{b}{d}y$. From the second corollary above, this shows that $\frac{a}{d}$and $\frac{b}{d}$ are relatively prime. $\square$

GCD Applications

Proposition

Let a and b be integers which are not both zero, and let $d = \gcd(a, b)$.Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof.

Let $a, b \in \mathbb{Z}$, where a and b are not both 0, and let $d = \gcd(a, b)$. Then from our above work, there exist integers x and y such that $d = ax + by$. Now divide through by d to get $1 = \frac{a}{d}x + \frac{b}{d}y$. From the second corollary above, this shows that $\frac{a}{d}$and $\frac{b}{d}$ are relatively prime. $\square$

Corollary

Every rational number may be represented in reduced form.

Corollary

Every rational number may be represented in reduced form.

Proof.

Consider an arbitrary rational number $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$.

Corollary

Every rational number may be represented in reduced form.

Proof.

Consider an arbitrary rational number $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Now let $d = \gcd(a, b)$.

Corollary

Every rational number may be represented in reduced form.

Proof.

Consider an arbitrary rational number $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Now let $d = \gcd(a, b)$. Note that $\frac{a}{b} = \frac{\frac{a}{d}}{\frac{b}{d}}$, and the numerator and denominator of this last fraction are relatively prime by the previous proposition. $\square$

Corollary

Every rational number may be represented in reduced form.

Proof.

Consider an arbitrary rational number $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Now let $d = \gcd(a, b)$. Note that $\frac{a}{b} = \frac{\frac{a}{d}}{\frac{b}{d}}$, and the numerator and denominator of this last fraction are relatively prime by the previous proposition. □

Before presenting our next result, we pause to give an example.

Corollary

Every rational number may be represented in reduced form.

Proof.

Consider an arbitrary rational number $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Now let $d = \gcd(a, b)$. Note that $\frac{a}{b} = \frac{\frac{a}{d}}{\frac{b}{d}}$, and the numerator and denominator of this last fraction are relatively prime by the previous proposition. $\square$

Before presenting our next result, we pause to give an example.

Example

Note that $4|16$ and $8|16$, but $4 \cdot 8 \nmid 16$. But also note that $4|36$ and $3|36$, and also $4 \cdot 3|36$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

Proof.

Let a, b, and c be as stated above.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

Proof.

Let a, b, and c be as stated above. Since $\gcd(a, b) = 1$, there are integers x and y for which $ax + by = 1$. Since $a|c$ and $b|c$, there are integers u and v such that $au = c$ and $bv = c$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

Proof.

Let a, b, and c be as stated above. Since $\gcd(a, b) = 1$, there are integers x and y for which $ax + by = 1$. Since $a|c$ and $b|c$, there are integers u and v such that $au = c$ and $bv = c$. Multiply through $ax + by = 1$ by c to get $acx + bcy = c$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

Proof.

Let a, b, and c be as stated above. Since $\gcd(a, b) = 1$, there are integers x and y for which $ax + by = 1$. Since $a|c$ and $b|c$, there are integers u and v such that $au = c$ and $bv = c$. Multiply through $ax + by = 1$ by c to get $acx + bcy = c$. Now replace the first c in the previous equation with bv and the second c with au to get $abvx + bauy = c$, that is, $ab(vx + uy) = c$.

GCD Applications

Proposition

Let a and b be integers such that $a|c$, $b|c$, and $\gcd(a, b) = 1$.Then $ab|c$.

Proof.

Let a, b, and c be as stated above. Since $\gcd(a, b) = 1$, there are integers x and y for which $ax + by = 1$. Since $a|c$ and $b|c$, there are integers u and v such that $au = c$ and $bv = c$. Multiply through $ax + by = 1$ by c to get $acx + bcy = c$. Now replace the first c in the previous equation with bv and the second c with au to get $abvx + bauy = c$, that is, $ab(vx + uy) = c$. This proves it. □

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$. Since $a|bc$, there is an integer z such that $az = bc$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$. Since $a|bc$, there is an integer z such that $az = bc$. Replace the bc above with az to get $axc + azy = c$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$. Since $a|bc$, there is an integer z such that $az = bc$. Replace the bc above with az to get $axc + azy = c$. Now factor out the a to get $a(xc + zy) = c$.

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$. Since $a|bc$, there is an integer z such that $az = bc$. Replace the bc above with az to get $axc + azy = c$. Now factor out the a to get $a(xc + zy) = c$. This shows that $a|c$, as desired. $\square$

GCD Applications

Proposition (Euclid's Lemma)

Let a and b be integers which are relatively prime. If $a|bc$ for some integer c, then $a|c$.

Proof.

Let a and b be relatively prime integers, and let c be an integer for which $a|bc$. We will show that $a|c$. Since a and b are relatively prime, there are integers x and y such that $ax + by = 1$. Multiply through by c to get $axc + bcy = c$. Since $a|bc$, there is an integer z such that $az = bc$. Replace the bc above with az to get $axc + azy = c$. Now factor out the a to get $a(xc + zy) = c$. This shows that $a|c$, as desired. $\square$

Example

Let a and b be integers such that $\gcd(a, b) = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Now, $cz = a + b$ for some integer z.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Now, $cz = a + b$ for some integer z. So $b = cz - a$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Now, $cz = a + b$ for some integer z. So $b = cz - a$. Sub this in for b in the equation $ax + by = 1$ to get $ax + (cz - a)b = 1$, that is, $ax - ab + czb = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Now, $cz = a + b$ for some integer z. So $b = cz - a$. Sub this in for b in the equation $ax + by = 1$ to get $ax + (cz - a)b = 1$, that is, $ax - ab + czb = 1$. We can write this as $a(x - b) + c(zb) = 1$.

Example

Let a and b be integers such that $\gcd(a, b) = 1$. If $c \in \mathbb{Z}$ and $c|a + b$, prove that $\gcd(a, c) = 1$.

Proof.

Let $a, b, c \in \mathbb{Z}$ satisfy the above hypotheses. Since $c|a + b$, $c \neq 0$, and so $\gcd(a, c)$ exists; call it d. We must show that $d = 1$. As $\gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Now, $cz = a + b$ for some integer z. So $b = cz - a$. Sub this in for b in the equation $ax + by = 1$ to get $ax + (cz - a)b = 1$, that is, $ax - ab + czb = 1$. We can write this as $a(x - b) + c(zb) = 1$. It now follows that $\gcd(a, c) = 1$. □

GCD Applications

Example

Prove that for every positive integer n, $8|(5^{2n}+7)$.

Example

Prove that the product of 4 consecutive integers is one less than a perfect square.