# Lecture 15: The gcd of two integers

Friday, September 2, 2022 10:05 PM

In the previous lecture, we mentioned the following theorem.

<u>Theorem</u>. Suppose $a,b\in\mathbb{Z}$ and at least one of them is not zero. Then there exist $r,s\in\mathbb{Z}$ such that $ar+bs=\gcd(a,b)$.

We start with the following lemma which we have essentially proved in the previous lecture.

<u>Lemma</u>. Suppose $a,b\in\mathbb{Z}$, $d\mid a$, and $d\mid b$. Then, for every $x,y\in\mathbb{Z}$,

$$d\mid ax+by.$$

In particular, $\gcd(a,b)\mid ax+by$ for every $x,y\in\mathbb{Z}$.

<u>Proof</u>. $$\left.\begin{array}{l} d\mid a \Rightarrow a\overset{d}{\equiv}0 \\ d\mid b \Rightarrow b\overset{d}{\equiv}0\end{array}\right\} \Rightarrow ax+by\overset{d}{\equiv}(0)(x)+(0)(y)\overset{d}{\equiv}0 \Rightarrow d\mid ax+by.$$

(Alternatively, $$\left.\begin{array}{l} d\mid a \Rightarrow a=dk \text{ for some } k\in\mathbb{Z} \\ d\mid b \Rightarrow b=d\ell \text{ for some } \ell\in\mathbb{Z}\end{array}\right\}\Rightarrow$$

$$ax+by=dkx+d\ell y=d(\underbrace{kx+\ell y}_{\text{in } \mathbb{Z}}) \Rightarrow d\mid ax+by.)$$

Since $\gcd(a,b)\mid a$ and $\gcd(a,b)\mid b$, $\gcd(a,b)\mid ax+by$ for every $x,y\in\mathbb{Z}$. ■

By the previous lemma, every positive integer of the form $ax+by$ is at least $\gcd(a,b)$. We will show that the smallest positive integer of the

# Lecture 15: The gcd and integer linear combination

Monday, November 28, 2016 6:33 PM

form $ax+by$ is $\gcd(a,b)$. Before we go to the proof of the previous theorem, let's recall the well-ordering principle.

If $S$ is a non-empty subset of $\mathbb{Z}^+$, then $S$ has a minimum.

Proof of Theorem. Let $S = \{ n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z},\ n = ax+by \}$.

By the assumption, either $a \neq 0$ or $b \neq 0$. Without loss of generality, we can and will assume that $a \neq 0$. Then $|a| > 0$. Notice that

$$|a| = a\ \mathrm{sgn}(a) + b\,(0) > 0 \quad \text{where } \mathrm{sgn}(a) = \begin{cases} 1 & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a < 0 \end{cases}.$$

Hence, $|a| \in S$; in particular, $S \neq \emptyset$. Hence by the well-ordering principle, $S$ has the minimum. Let $m$ be the minimum of $S$.

We want to show that $m$ is $\gcd(a,b)$. Notice that, since $m \in S$, $m = ax+by$ for some $x, y \in \mathbb{Z}$. Hence, by the previous lemma, $\gcd(a,b) \mid m$. Therefore $|\gcd(a,b)| \leq |m|$, and so $\gcd(a,b) \leq m$ as $\gcd(a,b)$ and $m$ are positive.

Next we want to show that $m \leq \gcd(a,b)$. To this end, we prove that $m$ is a common divisor of $a$ and $b$, which implies that $m \leq \gcd(a,b)$.

# Lecture 15: gcd and integer linear combination

Thursday, December 1, 2016 9:40 PM

By symmetry it is enough to show $m \mid a$. (By symmetry, we mean that by a similar argument we can get $m \mid b$.)

To prove $m \mid a$, we will prove that the remainder of $a$ divided by $m$ is $0$. Let $r$ be the remainder of $a$ divided by $m$. Hence, there exists $q \in \mathbb{Z}$, such that

$$a = mq + r \quad \text{and} \quad 0 \le r < m. \qquad (\mathrm{I})$$

Therefore $r = a - mq = a - (ax+by)q$

$$\Rightarrow \quad r = a\underbrace{(1-xq)}_{\text{in } \mathbb{Z}} - b\underbrace{(yq)}_{\text{in } \mathbb{Z}}. \qquad (\mathrm{II})$$

Suppose to the contrary that $m \nmid a$. Then $r \neq 0$. $\quad (\mathrm{III})$

By (I) and (III), $r > 0$, and so by (II), $r \in S$.

Therefore, $r$ is at least the minimum of $S$, which means $r \ge m$. This contradicts (I). Hence $m \mid a$. Similarly $m \mid b$.

This means $m$ is a common divisor of $a$ and $b$. Thus $m$ is at most the greatest common divisor of $a$ and $b$, which means $m \le \gcd(a,b)$. Therefore, $m = \gcd(a,b)$. Hence $\gcd(a,b) = ax+by$. ∎

# Lecture 15: Some properties of gcd

Thursday, December 1, 2016 9:52 PM

**Corollary.** Suppose $\gcd(a,b)=d$. Then $\gcd(\frac{a}{d},\frac{b}{d})=1$.

**Proof.** $\gcd(a,b)=d \Rightarrow$ there exist $r,s\in\mathbb{Z}$, $ar+bs=d$.

$$\Rightarrow \underbrace{\left(\frac{a}{d}\right)}_{\text{in } \mathbb{Z}} r + \underbrace{\left(\frac{b}{d}\right)}_{\text{in } \mathbb{Z}} s = 1$$

By a lemma, $\gcd(\frac{a}{d},\frac{b}{d}) \mid (\frac{a}{d})r+(\frac{b}{d})s$, and so $\gcd(\frac{a}{d},\frac{b}{d})\mid 1$.

Hence $\gcd(\frac{a}{d},\frac{b}{d})=1$. $\blacksquare$

**Euclid's lemma (general version)**

Suppose $a$ is a non-zero integer, $b,c\in\mathbb{Z}$. Then

$$\left.\begin{array}{l} a\mid bc \\ \gcd(a,b)=1 \end{array}\right\} \Rightarrow a\mid c.$$

**Proof.** By the previous theorem, there exist $r,s\in\mathbb{Z}$,

$ra+sb=1$. Therefore $rac+sbc=c$.

$$\left.\begin{array}{l} a\mid a \\ a\mid bc \end{array}\right\} \Rightarrow a\mid (rc)a+(s)bc=c. \qquad \blacksquare$$

Euclid was interested in this lemma in order to prove that integers can be written as a product of irreducibles in a unique way. Let's

# Lecture 15: Prime and irreducible

Thursday, December 1, 2016 10:02 PM

recall the definitions of prime and irreducible integers:

Definition. ① $p \in \mathbb{Z}$ is called irreducible if $p \neq 0$, $p \neq \pm 1$,

$\forall a, b \in \mathbb{Z}$, $p = ab \Rightarrow (|a| = 1 \text{ or } |b| = 1)$.

② $p \in \mathbb{Z}$ is called prime if $p \neq 0$, $p \neq \pm 1$,

$\forall a, b \in \mathbb{Z}$, $p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b)$.

Lemma. Suppose $p \in \mathbb{Z}$ is irreducible, and $d$ is a positive divisor of $p$. Then $d$ is either $1$ or $|p|$. In particular, for every $a \in \mathbb{Z}$, $\gcd(a, p)$ is either $1$ or $|p|$.

Proof. $d \mid p$ implies $p = dk$ for some $k \in \mathbb{Z}$. Since $p$ is irreducible, either $|d| = 1$ or $|k| = 1$. So either $d = 1$ or $d = |p|$ as $d > 0$.

For every $a \in \mathbb{Z}$, $\gcd(a, p)$ is a positive divisor of $p$, and so it is either $1$ or $|p|$. ■

Euclid's lemma (special case) $p$: irreducible $\Rightarrow$ $p$: prime.

This means, if $p$ is irreducible, then, for every $a, b \in \mathbb{Z}$,

$$p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b).$$

# Lecture 15: Prime and irreducible

Thursday, December 1, 2016 10:28 PM

Recall that $P \Rightarrow (Q \vee R) \equiv (P \wedge \neg Q) \Rightarrow R$, so we prove that

$$(p \mid ab \ \wedge \ p \nmid a) \Rightarrow p \mid b.$$

<u>Proof.</u> Since $p$ is irreducible, by the previous lemma, $\gcd(a,p)$ is either $1$ or $|p|$. Because $p \nmid a$, $\gcd(a,p) \neq |p|$. Hence $\gcd(a,p) = 1$.

$$\left.\begin{array}{l} p \mid ab \\ \gcd(p,a)=1 \end{array}\right\} \xRightarrow[\text{lemma (general version)}]{\text{Euclid's}} p \mid b. \qquad \blacksquare$$

In one of your HW assignments, you proved the converse: prime $\Rightarrow$ irred.

You will use these ideas to study Euclidean domains and PIDs in the algebra series.

This theorem is the key result in proving every integer $>1$ can be written as a product of primes in a <u>unique way</u>. You will see this either in your algebra series or in your number theory series

We say $\mathbb{Z}$ is a unique factorization domain (UFD).

# Lecture 15: Equations in congruence arithmetic

Thursday, December 1, 2016 10:48 PM

We'd like to solve congruence equations:

$\boxed{Q}$ Find all the solutions of $ax \equiv b \pmod{n}$. Does it have a solution?

<u>Ex.</u> For $n=2$ and $b=1$; there are two cases:

$a \overset{2}{\equiv} 0$ or $a \overset{2}{\equiv} 1$.

. If $a \overset{2}{\equiv} 0$, then, for every $x \in \mathbb{Z}$, $ax \overset{2}{\equiv} 0 \overset{2}{\not\equiv} 1$. So $ax \overset{2}{\equiv} 1$ has no solution.

. If $a \overset{2}{\equiv} 1$, then every odd $x$ is a solution of $x \overset{2}{\equiv} 1$.

<u>Ex.</u> For $n=3$ and $b=1$; there are three cases:

$a \overset{3}{\equiv} 0, 1,$ or $2$.

- As above $a \overset{3}{\equiv} 0$ has no solution, and every integer of the form $3k+1$ is a solution of $x \overset{3}{\equiv} 1$.
- How about $a \overset{3}{\equiv} 2$? In rational numbers we write:

$$2x = 1 \Rightarrow \left(\tfrac{1}{2}\right) 2x = \tfrac{1}{2} \Rightarrow x = \tfrac{1}{2}.$$

But here we are looking for <u>integers</u> $x$ such that $2x \overset{3}{\equiv} 1$.

# Lecture 15: Equations in congruence arithmetic

Friday, December 2, 2016 12:03 AM

As in the rational case we look for an "inverse" of 2 mod 3.

Modulo 3 every number is congruent to 0, 1, or 2. So we can look for an inverse among these numbers:

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Table of multiplication mod 3.

So 2 is an inverse of 2 mod 3. Hence

$$2x \overset{3}{\equiv} 1 \implies (2)(2x) \overset{3}{\equiv} (2)(1)$$

$$\implies x \overset{3}{\equiv} 2.$$

So $x$ is a solution if and only if $x$ is of the form $3k+2$.

Ex. For $n=4$, $b=1$; there are four cases: $a \overset{4}{\equiv} 0, 1, 2, 3$.

As before we can handle the cases of $a \overset{4}{\equiv} 0$ and $1$.

Does $2x \overset{4}{\equiv} 1$ have a solution? (Since $2x-1$ is odd, $4 \nmid 2x-1$; and so it does NOT have a solution.)

# Lecture 15: Equations in Congruences

Friday, December 2, 2016 12:17 AM

**Theorem.** Suppose $n \in \mathbb{Z}^{\geq 1}$ and $a \in \mathbb{Z}$. Then

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $\gcd(a,n)=1$.

**Proof.** ($\Rightarrow$) Suppose, for some $x \in \mathbb{Z}$, $ax \overset{n}{\equiv} 1$. Then $n \mid ax-1$, which means there exists $y \in \mathbb{Z}$ such that $ny = ax-1$. Hence, $ax - ny = 1$. Because $\gcd(a,n) \mid ax - ny$, we obtain that $\gcd(a,n) \mid 1$, and so $\gcd(a,n) = 1$.

($\Leftarrow$) $\gcd(a,n)=1$ implies there exist $r, s \in \mathbb{Z}$ such that

$$ar + ns = 1.$$

Then $n \mid ar-1$, and so $x = r$ is a solution of $ax \overset{n}{\equiv} 1$. ∎

**Proposition.** If $\gcd(a,n)=1$, then $ax \overset{n}{\equiv} 1$ has a unique solution modulo $n$.

**Proof.** We have already proved the existence of a solution. Now suppose $x_1$ and $x_2$ are solutions of $ax \overset{n}{\equiv} 1$. We have to show $x_1 \overset{n}{\equiv} x_2$.

$ax_1 \overset{n}{\equiv} 1$ and $ax_2 \overset{n}{\equiv} 1$ imply $ax_1 \overset{n}{\equiv} ax_2$. Hence $a(x_1 - x_2) \overset{n}{\equiv} 0$.

# Lecture 15: Equations in congruences

Friday, December 2, 2016 12:26 AM

$$\left.\begin{array}{l} n \mid a(x_1-x_2) \\ \gcd(a,n)=1 \end{array}\right\} \xRightarrow[\text{lemma (general version)}]{\text{Euclid's}} \quad n \mid x_1-x_2 \Rightarrow x_1 \overset{n}{\equiv} x_2 .$$

<u>Def.</u> We say $a' \in \mathbb{Z}$ is called a <u>multiplicative inverse of a modulo n</u> if $aa' \overset{n}{\equiv} 1$.

Similar to solving a linear equation over $\mathbb{Q}$ where inverse of a helps us solve $ax=b$, a multiplicative inverse of a modulo n helps us solve $ax \overset{n}{\equiv} b$.

<u>Theorem.</u> Suppose $\gcd(a,n)=1$, and $b \in \mathbb{Z}$. Then $ax \overset{n}{\equiv} b$ has a solution, and its solution is unique modulo n.

<u>Proof.</u> Since $\gcd(a,n)=1$, a has a multiplicative inverse $a'$ modulo n. This means $aa' \overset{n}{\equiv} 1$. Hence $a(a'b) \overset{n}{\equiv} b$, and so $x = a'b$ is a solution of $ax \overset{n}{\equiv} b$. Next we prove the uniqueness of the solution modulo n. Suppose $x_1$ and $x_2$ are two solutions. Hence $ax_1 \overset{n}{\equiv} b$ and $ax_2 \overset{n}{\equiv} b$. Therefore, $ax_1 \overset{n}{\equiv} ax_2$. Thus $a(x_1-x_2) \overset{n}{\equiv} 0$.


$$\left.\begin{array}{l} n \mid a(x_1-x_2) \\ \gcd(a,n)=1 \end{array}\right\} \xRightarrow[\text{lemma (general version)}]{\text{Euclid's}} \quad n \mid x_1-x_2 \Rightarrow x_1 \overset{n}{\equiv} x_2 .$$