Lecture 28: Prime and irreducible

Thursday, December 1, 2016 10:02 PM

Let's recall the definitions of prime and irreducible integers:

Definition. ① $n \in \mathbb{Z}^{>1}$ is called irreducible if

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

② $p \in \mathbb{Z}^{>1}$ is called prime if

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

- Recall that $n \in \mathbb{Z}^{>1}$ is irreducible if and only if the only positive divisors of n are 1 and n.

Theorem. $\forall n \in \mathbb{Z}^{>1}$, n is irreducible $\Leftrightarrow$ n is prime.

- An alternative way to formulate the above theorem is

  Suppose $n \in \mathbb{Z}^{>1}$. n has only two positive divisors if and only if the following holds $n \mid ab \Rightarrow n \mid a$ or $n \mid b$.

- ($\Rightarrow$) side of the above statement is called Euclid's lemma.

Proof of Theorem. ($\Rightarrow$) We assume n is irreducible, and we have to prove $n \mid ab \Rightarrow (n \mid a \vee n \mid b)$. It is enough to prove $(n \mid ab \wedge n \nmid a) \Rightarrow n \mid b$.

Lecture 28: Prime and irreducible

Thursday, December 1, 2016 10:28 PM

$$\left.\begin{array}{r}\gcd(a,n)\mid a\\ n\nmid a\end{array}\right\}\Rightarrow \left.\begin{array}{r}\gcd(a,n)\neq n\\ \gcd(a,n)\mid n\\ \text{the only positive}\\ \text{divisors of } n\\ \text{are } 1 \text{ and } n\end{array}\right\}\Rightarrow \gcd(a,n)=1.$$

$$\left.\begin{array}{r}n\mid ab\\ \gcd(n,a)=1\end{array}\right\}\Rightarrow n\mid b \quad \text{by Corollary 2.}$$

($\Leftarrow$) $n=ab$. Since $n\neq 0$, $a\neq 0$ and $b\neq 0$; and $n\mid ab$.

Since n is prime, $n\mid a$ or $n\mid b$.

<u>Case 1</u>. $n\mid a$.

In this case, as $a\neq 0$, we have $n\leq |a|$. So $|a||b|\leq |a|$.

Thus $|b|\leq 1$. Hence $|b|=1$, which implies $n=|a|$.

<u>Case 2</u>. $n\mid b$.

By a similar argument, as in <u>case 1</u>, we get $n=|a|$. ∎

This theorem is the key result in proving any 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 28: 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 any $x \in \mathbb{Z}$, $ax \overset{2}{\equiv} 0 \overset{2}{\not\equiv} 1$. So $ax \overset{2}{\equiv} 1$ has no solution.
- If $a \overset{2}{\equiv} 1$, then any 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 any 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 28: 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 any 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 $3k+2$.

<u>Ex.</u> 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.)

Next we will prove two lemmas that give alternative arguments for this case.

<u>Lemma</u>. For any $n \in \mathbb{Z}^+$, $a \overset{n}{\equiv} b \Rightarrow \gcd(a,n) = \gcd(b,n)$.

<u>Proof</u>. Let $d_1 = \gcd(a,n)$ and $d_2 = \gcd(b,n)$. To show $d_1 = d_2$, it is enough to show $d_1 | d_2$ and $d_2 | d_1$ (notice that $d_i \geq 1$.).

By symmetry it is enough to show $d_1 | d_2$.

$a \overset{n}{\equiv} b \Rightarrow \exists k \in \mathbb{Z},\ b = nk + a$.

$\left.\begin{array}{l} d_1 | n \\ d_1 | a \end{array}\right\} \Rightarrow d_1 | nk+a$. So $d_1 | b$ and $d_1 | n$.

$\left.\begin{array}{l} d_1 | b \\ d_1 | n \end{array}\right\} \Rightarrow d_1 | \gcd(b,n) \Rightarrow d_1 | d_2$. $\blacksquare$

In the next lecture, we will use this lemma to prove Euclid's algorithm for finding gcd of two integers.

<u>Lemma</u>. If $ax \equiv b \pmod{n}$ has a solution, then

$$\gcd(a,n) | b.$$

(We have already proved this lemma, when we discussed

Lecture 28: Linear equations in congruence arithmetic

Friday, December 2, 2016 12:26 AM

linear Diophantine equations.)

<u>Proof of lemma</u>. For some integer x, we have $ax \overset{n}{\equiv} b$.

So, by the previous lemma, $\gcd(ax, n) = \gcd(b, n)$.

Let $d = \gcd(a, n)$. Then $\left.\begin{array}{l} d \mid a \\ d \mid n \end{array}\right\} \Rightarrow \left\{\begin{array}{l} d \mid ax \\ d \mid n \end{array}\right\} \Rightarrow d \mid \gcd(ax, n)$.

Hence $d \mid \gcd(b, n)$. On the other hand $\gcd(b, n) \mid b$.

Therefore $d \mid b$, which means $\gcd(a, n) \mid b$. ■

In the next lecture we will prove the convers.