Lecture 29: Linear equations in congruence arithmetic

Friday, December 2, 2016 9:18 AM

In the previous lecture we proved

Lemma 1. For $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, if $ax \equiv b \pmod{n}$ has a solution, then $\gcd(a,n) \mid b$.

We want to prove the converse. We start with the following special case:

Lemma 2 For $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, $ax \equiv 1 \pmod{n}$

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

Definition. We say $\underline{a'}$ is a modular inverse of $\underline{a}$ modulo n if $a'a \equiv 1 \pmod{n}$.

So we are proving that

$$a \text{ has a modular inverse mod. } n \iff \gcd(a,n) = 1.$$

Proof of Lemma 2 ($\Rightarrow$) By Lemma 1, $\gcd(a,n) \mid 1$. So $\gcd(a,n) = 1$.

($\Leftarrow$) $\gcd(a,n) = 1 \Rightarrow \exists r, s \in \mathbb{Z},\ ra + sn = 1$

$\Rightarrow 1 \overset{n}{\equiv} ra + sn \overset{n}{\equiv} ar$. So $x = r$ is a solution of $ax \equiv 1 \pmod{n}$. ∎

Lecture 29: Linear equations in congruence arithmetic

Friday, December 2, 2016 9:31 AM

Lemma 3. For $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, if $\gcd(a,n)=1$, then for any $b \in \mathbb{Z}$, $ax \equiv b \pmod{n}$ has a solution.

Proof. Since $\gcd(a,n)=1$, by Lemma 2 a has a modular inverse a' modulo n, i.e. $\exists a' \in \mathbb{Z}$ such that $a'a \overset{n}{\equiv} 1$. If x is a solution, then

$$ax \overset{n}{\equiv} b \implies a'ax \overset{n}{\equiv} a'b \implies x \overset{n}{\equiv} a'b.$$

Now let's check the converse:

$$x \overset{n}{\equiv} a'b \implies ax \overset{n}{\equiv} a(a'b) = (aa')b \overset{n}{\equiv} b.$$

■

Remark. In the above proof we showed $ax \overset{n}{\equiv} b$ has a unique solution modulo n if $\gcd(a,n)=1$.

Lemma 4. $\gcd(a,b)=d \implies \gcd\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

Proof. $\gcd(a,b)=d \implies \exists r,s \in \mathbb{Z}$, $ar+bs=d$

So $r\left(\frac{a}{d}\right)+s\left(\frac{b}{d}\right)=1$. Hence

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) \,\Big|\, r\left(\frac{a}{d}\right)+s\left(\frac{b}{d}\right)=1,$$ and so $\gcd(a/d, b/d)=1$. ■

Lecture 29: Linear equations in congruence arithmetic

Friday, December 2, 2016 9:40 AM

<u>Theorem</u> For any $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$,

$$ax \overset{n}{\equiv} b \text{ has a solution} \iff \gcd(a,n) \mid b.$$

<u>Proof.</u> ($\Longrightarrow$) It is proved in Lemma 1.

($\Longleftarrow$) $ax \overset{n}{\equiv} b$ has a solution means there are integers x and y such that $ax - b = ny$. I

Let $d = \gcd(a,n)$. By assumption we have $d \mid b$.

Dividing both sides of I by d we get

$$\left(\frac{a}{d}\right)x - \left(\frac{b}{d}\right) = \left(\frac{n}{d}\right)y,$$

which has an integer solution exactly when

$$\left(\frac{a}{d}\right)x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \quad \text{II}$$

has a solution.

By Lemma 4, $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, and so by Lemma 3 II has a solution. ■

How can we find a solution? As you can see in the proof everything boils down to writing $\gcd(a,b)$ as an integer linear combination of a and b.

- How can we compute $\gcd(a,b)$ effectively?

- You might know how to use prime factorization to find g.c.d., but at the moment there is no fast algorithm for decomposing an integer into its prime factors. If I give you pq where p and q are 15 digit primes, it takes you more than 1000 years to find p and q using the current methods.

- For computing g.c.d. of two numbers, there is a fast algorithm due to Euclid. It is based on a lemma that we proved in the previous lecture.

Recall. Lemma. $\forall\, a,b \in \mathbb{Z},\, n \in \mathbb{Z}^+$,

$$a \overset{n}{\equiv} b \Rightarrow \gcd(a,n) = \gcd(b,n).$$

Let's use this lemma to compute $\gcd(2016, 109)$.

We know $a \overset{n}{\equiv} r$ if r is the remainder of a divided by n.

We use this technique to decrease the size of relevant" numbers.

Lecture 29: Euclid's algorithm

Friday, December 2, 2016 3:54 PM

$2016 = 109 \times 18 + 54 \implies 2016 \overset{109}{\equiv} 54$

$\implies \gcd(2016, 109) = \gcd(109, 54)$.

$109 = 54 \times 2 + 1 \implies 109 \overset{54}{\equiv} 1$

$\implies \gcd(109, 54) = \gcd(54, 1)$

$54 = 1 \times 54 + 0 \implies 54 \overset{1}{\equiv} 0$

$\implies \gcd(54, 1) = \gcd(1, 0) = 1$.

Euclid's algorithm

In general, for $a \geq b > 0$, let $x_0 = a$, $x_1 = b$; and consider the following sequence of integers:

- $x_0 = x_1 \cdot q_1 + r_1$ where q_1 and r_1 are the quotient and the remainder of x_0 divided by x_1.
- If $r_1 = 0$, then answer is x_1; If not, let $x_2 = r_1$.
- $x_1 = x_2 \cdot q_2 + r_2$ where q_2 and r_2 are the quotient and the remainder of x_1 divided by x_2.
- If $r_2 = 0$, then answer is x_2; If not, let $x_3 = r_2$.

we continue like this till we end up getting the answer.

Notice that $x_{i-1} \overset{x_i}{\equiv} x_{i+1}$ and so $\gcd(x_{i-1}, x_i) = \gcd(x_i, x_{i+1})$

Lecture 29: Euclid's algorithm

Friday, December 2, 2016 4:10 PM

So $\gcd(a,b) = \gcd(x_0, x_1) = \gcd(x_1, x_2) = \gcd(x_2, x_3) = \cdots$

$$= \gcd(x_{n_0}, x_{n_0+1}) = x_{n_0}.$$

This is why Eulid's algorithm gives us the $\gcd(a,b)$.

We also notice that

$$x_0 \geq x_1 > x_2 > \cdots > x_i > x_{i+1} > \cdots \geq 0.$$

as x_{i+1} is the remainder of x_{i-1} divided by x_i. So at some point, we do reach to 0.

How can we find $r, s \in \mathbb{Z}$ such that $\gcd(a,b) = ar + bs$?

We can use the Euclid's algorithm and go backward:

- Find integers r and s such that $2016\, r + 109\, s = 1$.

- Solution. $2016 = 109 \times 18 + 54$ (a)

$109 = 54 \times 2 + 1$ (b)

So $1 = 109 - 54 \times 2$ because of (a)

$= 109 - (2016 - 109 \times 18) \times 2$ because of (b)

$= 2016 \times (-2) + 109 \times (1 + 18 \times 2)$

regroup as a linear combination of the previous pair. Have the larger number first.

$= 2016 \times (-2) + 109 \times 37.$

Lecture 29: Euclid's algorithm (extra example)

Friday, December 2, 2016 4:24 PM

. Find $x, y \in \mathbb{Z}$ such that

$$221x + 799y = \gcd(221, 799).$$

<u>Solution</u>.

$$\begin{aligned}
799 &= 221 \times 3 + 136 \quad &(1)\\
221 &= 136 \times 1 + 85 \quad &(2)\\
136 &= 85 \times 1 + 51 \quad &(3)\\
85 &= 51 \times 1 + 34 \quad &(4)\\
51 &= 34 \times 1 + 17 \quad &(5)\\
34 &= 17 \times 2 + 0
\end{aligned}$$

So $\gcd(221, 799) = 17$.

$$17 \overset{\text{from } (5)}{=} 51 - 34 \times 1$$

Regroup as a linear combination of previous pair; larger number first

$$\overset{\text{from } (4)}{=} 51 - (85 - 51 \times 1) \times 1 = 85 \times (-1) + 51 \times (1+1)$$

$$= 85 \times (-1) + 51 \times (2)$$

$$\overset{\text{from } (3)}{=} 85 \times (-1) + (136 - 85 \times 1) \times 2$$

$$= 136 \times (2) + 85 \times (-1-2) = 136 \times (2) + 85 \times (-3)$$

$$\overset{\text{from } (2)}{=} 136 \times (2) + (221 - 136 \times 1) \times (-3)$$

$$= 221 \times (-3) + 136 \times (2 + (-1) \times (-3)) = 221 \times (-3) + 136 \times (5)$$

$$\overset{\text{from } (1)}{=} 221 \times (-3) + (799 - 221 \times 3) \times (5)$$

$$= 799 \times (5) + 221 \times (-3 - 3 \times 5) = 799 \times (5) + 221 \times (-18).$$

So $799 \times (5) + 221 \times (-18) = \gcd(799, 221)$.