Chinese Remainder Theorem

Systems of Modular Congruences

Raymond Feng

December 28, 2020

Outline

Definitions

Definition (Linear Congruence)

A linear congruence is of the form

$$ax + b \equiv c \pmod{m}.$$

Definitions

Definition (Linear Congruence)

A linear congruence is of the form

$$ax + b \equiv c \pmod{m}.$$

Not all congruences are solvable

For example, take

$$2x \equiv 5 \pmod{8}.$$

Definitions

Definition (Linear Congruence)

A linear congruence is of the form

$$ax + b \equiv c \pmod{m}.$$

Not all congruences are solvable

For example, take

$$2x \equiv 5 \pmod{8}.$$

Definition (Modular inverse)

The modular inverse of an integer b modulo m is an integer b^{-1} such that

$$b \cdot b^{-1} \equiv 1 \pmod{m}.$$

Building Intuition

- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{5}$?

Building Intuition

- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{5}$?
- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{6}$?

Building Intuition

- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{5}$?
- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 4 \pmod{6}$?
- Is there an integer x with $x \equiv 1 \pmod{2}$ and $x \equiv 3 \pmod{6}$?

Building Intuition

- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 4 \pmod 5$?
- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 4 \pmod 6$?
- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 6$?
- Is there an integer x with $x \equiv i \pmod 2$ and $x \equiv j \pmod 5$ for any choice of $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4\}$?

Building Intuition

- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 4 \pmod 5$?
- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 4 \pmod 6$?
- Is there an integer x with $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 6$?
- Is there an integer x with $x \equiv i \pmod 2$ and $x \equiv j \pmod 5$ for any choice of $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4\}$?
- Is there an integer x with $x \equiv i \pmod 2$ and $x \equiv j \pmod 6$ for any choice of $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4, 5\}$?

Building Intuition

When can we solve these systems?

When the modular bases are relatively prime, the different modular systems seem to be independent of each other (like mod 2 and mod 5 are independent), but when the bases share common factors (as with 2 and 6) there can be interference, since $x \equiv 3 \pmod{6}$ automatically implies $x \equiv 1 \pmod{2}$.

Building Intuition

When can we solve these systems?

When the modular bases are relatively prime, the different modular systems seem to be independent of each other (like mod 2 and mod 5 are independent), but when the bases share common factors (as with 2 and 6) there can be interference, since $x \equiv 3 \pmod{6}$ automatically implies $x \equiv 1 \pmod{2}$.

To rigorize this intuition that relatively prime bases for modular congruences are independent, we will introduce the following theorem. However, the intuition behind this theorem is more important than the statement. (It should *feel* true that relatively prime bases for moduli act independently.)

Theorem (CRT)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers, and let $M = m_1 m_2 \ldots m_n$. For any integers $y_1, \ldots, y_n$ there exists an integer x satisfying

$$x \equiv y_i \pmod m_i.$$

Furthermore, this x is unique modulo M.

Theorem (CRT)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers, and let $M = m_1 m_2 \ldots m_n$. For any integers $y_1, \ldots, y_n$ there exists an integer x satisfying

$$x \equiv y_i \pmod{m}_i.$$

Furthermore, this x is unique modulo M.

Example

Find all x with $x \equiv 1 \pmod 2, x \equiv 3 \pmod 5$.

- We see that $x \equiv 3 \pmod{10}$ always works, and by CRT these must be the only solutions. (We can easily check that all other numbers do not work.)

Using CRT

Why is CRT useful? After all, it is just an existence theorem, and doesn't give any way to solve the congruences. We will exhibit an algorithm for the case of 2 bases, the rest follow similarly.

Using CRT

Why is CRT useful? After all, it is just an existence theorem, and doesn't give any way to solve the congruences. We will exhibit an algorithm for the case of 2 bases, the rest follow similarly.

Algorithm to solve modular congruences

Suppose we want to solve

$$x \equiv y_1 \pmod{m_1}, x \equiv y_2 \pmod{m_2}$$

with $\gcd(m_1, m_2) = 1$.

- Let m_2^{-1} be an integer such that $m_2 \cdot m_2^{-1} \equiv 1 \pmod{m_1}$ and let m_1^{-1} be an integer such that $m_1 \cdot m_1^{-1} \equiv 1 \pmod{m_2}$.

Using CRT

Why is CRT useful? After all, it is just an existence theorem, and doesn't give any way to solve the congruences. We will exhibit an algorithm for the case of 2 bases, the rest follow similarly.

Algorithm to solve modular congruences

Suppose we want to solve

$$x \equiv y_1 \pmod{m_1}, x \equiv y_2 \pmod{m_2}$$

with $\gcd(m_1, m_2) = 1$.

- Let m_2^{-1} be an integer such that $m_2 \cdot m_2^{-1} \equiv 1 \pmod{m_1}$ and let m_1^{-1} be an integer such that $m_1 \cdot m_1^{-1} \equiv 1 \pmod{m_2}$.
- Begin by setting $e_1 = m_2 \cdot m_2^{-1}$ such that

$$e_1 \equiv 1 \pmod{m_1}, e_1 \equiv 0 \pmod{m_2}.$$

Similarly let $e_2 = m_1 \cdot m_1^{-1}$ such that

$$e_2 \equiv 0 \pmod{m_1}, e_2 \equiv 1 \pmod{m_2}.$$

Using CRT

Why is CRT useful? After all, it is just an existence theorem, and doesn't give any way to solve the congruences. We will exhibit an algorithm for the case of 2 bases, the rest follow similarly.

Algorithm to solve modular congruences

Suppose we want to solve

$$x \equiv y_1 \pmod{m_1}, x \equiv y_2 \pmod{m_2}$$

with $\gcd(m_1, m_2) = 1$.

- Let m_2^{-1} be an integer such that $m_2 \cdot m_2^{-1} \equiv 1 \pmod{m_1}$ and let m_1^{-1} be an integer such that $m_1 \cdot m_1^{-1} \equiv 1 \pmod{m_2}$.
- Begin by setting $e_1 = m_2 \cdot m_2^{-1}$ such that

  $$e_1 \equiv 1 \pmod{m_1}, e_1 \equiv 0 \pmod{m_2}.$$

  Similarly let $e_2 = m_1 \cdot m_1^{-1}$ such that

  $$e_2 \equiv 0 \pmod{m_1}, e_2 \equiv 1 \pmod{m_2}.$$

- Check that $x = y_1 e_1 + y_2 e_2$ fits the bill, and use CRT to find all solutions.

Example usage

Here is an example which exhibits the above algorithm, step by step.

Example usage

Here is an example which exhibits the above algorithm, step by step.

Example

- Suppose we want to solve $x \equiv 3 \pmod{5}, x \equiv 4 \pmod{7}$.

Example usage

Here is an example which exhibits the above algorithm, step by step.

Example

- Suppose we want to solve $x \equiv 3 \pmod 5, x \equiv 4 \pmod 7$.
- Then following the earlier algorithm, we set $e_1 = 7 \cdot 3 = 21$ and $e_2 = 5 \cdot 3 = 15$.

Example usage

Here is an example which exhibits the above algorithm, step by step.

Example

- Suppose we want to solve $x \equiv 3 \pmod 5, x \equiv 4 \pmod 7$.
- Then following the earlier algorithm, we set $e_1 = 7 \cdot 3 = 21$ and $e_2 = 5 \cdot 3 = 15$.
- Now note that $x = 3 \cdot 21 + 4 \cdot 15 = 123$ fits the bill.

Example usage

Here is an example which exhibits the above algorithm, step by step.

Example

- Suppose we want to solve $x \equiv 3 \pmod{5}, x \equiv 4 \pmod{7}$.
- Then following the earlier algorithm, we set $e_1 = 7 \cdot 3 = 21$ and $e_2 = 5 \cdot 3 = 15$.
- Now note that $x = 3 \cdot 21 + 4 \cdot 15 = 123$ fits the bill.
- We can reduce this mod $5 \cdot 7 = 35$ and apply CRT to conclude that all solutions are of the form $x \equiv 123 \equiv 18 \pmod{35}$.

"Solving" congruences

Exercise 3.4

How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

Exercise 3.4

How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

- There is one solution for every 20 numbers by CRT.

Exercise 3.4

How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

- There is one solution for every 20 numbers by CRT.
- Therefore, there are a total of 5 integers between 1 and 100.

"Solving" congruences

Exercise 3.4

How many integers between 1 and 100 leave a remainder of 2 when divided by 4 and also a remainder of 4 when divided by 5?

- There is one solution for every 20 numbers by CRT.
- Therefore, there are a total of 5 integers between 1 and 100.
- Note how we avoided solving the congruence: we just needed the existence of a solution and its uniqueness, which CRT provides.

Exponentiation!

Classic

Find the last 2 digits of 3^{2004}.

Exponentiation!

Classic

Find the last 2 digits of 3^{2004}.

We know from Euler's Totient Theorem (since $\gcd(3, 100) = 1$) that $3^{40} \equiv 1 \pmod{100}$, so

$$3^{2004} \equiv \left(3^{40}\right)^{50} \cdot 3^4 \equiv 1^{50} \cdot 81 \equiv \boxed{81} \pmod{100}.$$

Exponentiation!

Classic

Find the last 2 digits of 3^{2004}.

We know from Euler's Totient Theorem (since $\gcd(3, 100) = 1$) that $3^{40} \equiv 1 \pmod{100}$, so

$$3^{2004} \equiv \left(3^{40}\right)^{50} \cdot 3^4 \equiv 1^{50} \cdot 81 \equiv \boxed{81} \pmod{100}.$$

Now what happens if the base is not coprime with 100?

Classic

Find the last 2 digits of 2^{2004}.

Classic

Find the last 2 digits of 3^{2004}.

We know from Euler's Totient Theorem (since $\gcd(3, 100) = 1$) that $3^{40} \equiv 1 \pmod{100}$, so

$$3^{2004} \equiv \left(3^{40}\right)^{50} \cdot 3^4 \equiv 1^{50} \cdot 81 \equiv \boxed{81} \pmod{100}.$$

Now what happens if the base is not coprime with 100?

Classic

Find the last 2 digits of 2^{2004}.

We use CRT to break down the problem into two parts. Note that $2^{2004} \equiv 0 \pmod 4$ and

$$2^{2004} \equiv \left(2^{20}\right)^{100} \cdot 2^4 \equiv 1^{100} \cdot 16 \equiv 16 \pmod{25}.$$

Exponentiation!

Classic

Find the last 2 digits of 3^{2004}.

We know from Euler's Totient Theorem (since $\gcd(3, 100) = 1$) that $3^{40} \equiv 1 \pmod{100}$, so

$$3^{2004} \equiv \left(3^{40}\right)^{50} \cdot 3^4 \equiv 1^{50} \cdot 81 \equiv \boxed{81} \pmod{100}.$$

Now what happens if the base is not coprime with 100?

Classic

Find the last 2 digits of 2^{2004}.

We use CRT to break down the problem into two parts. Note that $2^{2004} \equiv 0 \pmod{4}$ and

$$2^{2004} \equiv \left(2^{20}\right)^{100} \cdot 2^4 \equiv 1^{100} \cdot 16 \equiv 16 \pmod{25}.$$

Now put the two congruences back together (as $4 \cdot 25 = 100$) to find that the answer is $\boxed{16}$ $\pmod{100}$.

CRT for constructions

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Classic

Does there exist a sequence of 2020 consecutive integers such that every integer has at least 2020 factors?

CRT for constructions

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Classic

Does there exist a sequence of 2020 consecutive integers such that every integer has at least 2020 factors?

- We will solve the problem for each number having 16 factors, the generalization will be obvious.

CRT for constructions

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Classic

Does there exist a sequence of 2020 consecutive integers such that every integer has at least 2020 factors?

- We will solve the problem for each number having 16 factors, the generalization will be obvious.
- Take distinct primes $p_1, \ldots, p_{8080}$.

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Classic

Does there exist a sequence of 2020 consecutive integers such that every integer has at least 2020 factors?

- We will solve the problem for each number having 16 factors, the generalization will be obvious.
- Take distinct primes $p_1, \ldots, p_{8080}$.
- By CRT, there is an integer x satisfying

$$x \equiv -i \pmod{p_{4i-3}p_{4i-2}p_{4i-1}p_{4i}}.$$

for all $1 \leq i \leq 2020$.

Since CRT at its core is an intuitive statement about the independence of modular congruences in relatively prime bases, it makes sense that it is most useful for proving the existence of certain numbers, rather than explicitly giving an exact value.

Classic

Does there exist a sequence of 2020 consecutive integers such that every integer has at least 2020 factors?

- We will solve the problem for each number having 16 factors, the generalization will be obvious.
- Take distinct primes $p_1, \ldots, p_{8080}$.
- By CRT, there is an integer x satisfying

$$x \equiv -i \pmod{p_{4i-3}p_{4i-2}p_{4i-1}p_{4i}}.$$

  for all $1 \leq i \leq 2020$.
- Now, $p_{4i-3}p_{4i-2}p_{4i-1}p_{4i} \mid x + i$ for all $1 \leq i \leq 2020$, so each $x + i$ has at least 16 factors! To get at least 2020 factors, just increase the number of primes used.

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.
- The algorithm for solving congruences: first find the e_i which are congruent to 1 modulo a base and 0 to everything else, and then make a linear combination of those e_i's to solve.

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.
- The algorithm for solving congruences: first find the e_i which are congruent to 1 modulo a base and 0 to everything else, and then make a linear combination of those e_i's to solve.
- CRT can be used for its statement of 1 solution for every $M = m_1 \cdots m_n$ consecutive integers; this can be used to avoid solving a congruence explicitly.

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.
- The algorithm for solving congruences: first find the e_i which are congruent to 1 modulo a base and 0 to everything else, and then make a linear combination of those e_i's to solve.
- CRT can be used for its statement of 1 solution for every $M = m_1 \cdots m_n$ consecutive integers; this can be used to avoid solving a congruence explicitly.
- CRT can also be used to break down exponentiation problems so that Euler's Totient Theorem may be used.

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.
- The algorithm for solving congruences: first find the e_i which are congruent to 1 modulo a base and 0 to everything else, and then make a linear combination of those e_i's to solve.
- CRT can be used for its statement of 1 solution for every $M = m_1 \cdots m_n$ consecutive integers; this can be used to avoid solving a congruence explicitly.
- CRT can also be used to break down exponentiation problems so that Euler's Totient Theorem may be used.
- Finally, CRT is routinely used for constructions in olympiad number theory; this is where a deep understanding of the intuition is very important!

Summary

- The intuition behind CRT is much more important than the statement itself; make sure you gain a deep understanding of what all that notation actually means.
- The algorithm for solving congruences: first find the e_i which are congruent to 1 modulo a base and 0 to everything else, and then make a linear combination of those e_i's to solve.
- CRT can be used for its statement of 1 solution for every $M = m_1 \cdots m_n$ consecutive integers; this can be used to avoid solving a congruence explicitly.
- CRT can also be used to break down exponentiation problems so that Euler's Totient Theorem may be used.
- Finally, CRT is routinely used for constructions in olympiad number theory; this is where a deep understanding of the intuition is very important!

Thanks for coming to Primeri Bootcamp, and I hope you enjoyed the lecture! Please let me know if you have any questions.