Famous Theorems in Number Theory

Meeting #9

Justin Hua

McRoberts Math Circle

April 23, 2021

Outline

AMC 2018 12A # 7

Problem

For how many (not necessarily positive) integer values of n is the value of $4000 \cdot \left(\frac{2}{5}\right)^n$ *an integer?*

Chinese Remainder Theorem

Theorem (CRT)

Let m and n be integers such that $\gcd(m, n) = 1$. Then there is a bijection between residues modulo mn and pairs of residues modulo m and n.

For example, let us take $m, n = 3, 2$, we have the following table.

x modulo 6	x modulo 3	x modulo 2
0	0	0
1	1	1
2	2	0
3	0	1
4	1	0
5	2	1

Using CRT

Problem

Say $x \equiv 0 (\mod 5)$ *and* $x \equiv 2 (\mod 7)$*. What is x modulo 35?*

We can do guess and check in a smart way.

- $x \equiv 0 (\mod 5)$ means that x is divisible by 5.

Using CRT

Problem

Say $x \equiv 0(\mod 5)$ *and* $x \equiv 2(\mod 7)$. *What is x modulo 35?*

We can do guess and check in a smart way.

- $x \equiv 0(\mod 5)$ means that x is divisible by 5.
- So, let's just check all multiples of 5 until we find a number that is congruent to 2 modulo 7

Using CRT

Problem

Say $x \equiv 0 (\mod 5)$ *and* $x \equiv 2 (\mod 7)$. *What is x modulo 35?*

We can do guess and check in a smart way.

- $x \equiv 0 (\mod 5)$ means that x is divisible by 5.
- So, let's just check all multiples of 5 until we find a number that is congruent to 2 modulo 7
- Conclude that the answer is 30.

Using CRT

Problem

Say $x \equiv 0(\mod 5)$ *and* $x \equiv 2(\mod 7)$. *What is x modulo 35?*

We can do guess and check in a smart way.

- $x \equiv 0(\mod 5)$ means that x is divisible by 5.
- So, let's just check all multiples of 5 until we find a number that is congruent to 2 modulo 7
- Conclude that the answer is 30.
- Convince yourself that it is the only answer modulo 35.

Using CRT

Problem

Say $x \equiv 0(\mod 5)$ *and* $x \equiv 2(\mod 7)$. *What is x modulo 35?*

We can do guess and check in a smart way.

- $x \equiv 0(\mod 5)$ means that x is divisible by 5.
- So, let's just check all multiples of 5 until we find a number that is congruent to 2 modulo 7
- Conclude that the answer is 30.
- Convince yourself that it is the only answer modulo 35.
- This should be true by the bijectivity.

Using CRT

Problem

Say $x \equiv 2(\mod 5)$ *and* $x \equiv 3(\mod 7)$. *What is x modulo 35?*

- $x \equiv 2(\mod 5)$ means that x is of the form $5k + 2$ for some $k \in \mathbb{Z}$

Using CRT

Problem

Say $x \equiv 2(\mod 5)$ *and* $x \equiv 3(\mod 7)$. *What is x modulo 35?*

- $x \equiv 2(\mod 5)$ means that x is of the form $5k + 2$ for some $k \in \mathbb{Z}$
- So, let's just check all numbers of the form $5k + 2$ until we find a number that is congruent to 3 modulo 7

Using CRT

Problem

Say $x \equiv 2(\mod 5)$ *and* $x \equiv 3(\mod 7)$. *What is x modulo 35?*

- $x \equiv 2(\mod 5)$ means that x is of the form $5k + 2$ for some $k \in \mathbb{Z}$
- So, let's just check all numbers of the form $5k + 2$ until we find a number that is congruent to 3 modulo 7
- The numbers of the form $5k + 2$ are: $\{2,7,12,17,22,27,32\}$

Using CRT

Problem

Say $x \equiv 2(\mod 5)$ and $x \equiv 3(\mod 7)$. What is x modulo 35?

- $x \equiv 2(\mod 5)$ means that x is of the form $5k+2$ for some $k \in \mathbb{Z}$
- So, let's just check all numbers of the form $5k+2$ until we find a number that is congruent to 3 modulo 7
- The numbers of the form $5k+2$ are: $\{2,7,12,17,22,27,32\}$
- The only answer is 17.

Using CRT

Problem

Say $x \equiv 2(\mod 5)$ *and* $x \equiv 3(\mod 7)$. *What is x modulo 35?*

- $x \equiv 2(\mod 5)$ means that x is of the form $5k + 2$ for some $k \in \mathbb{Z}$
- So, let's just check all numbers of the form $5k + 2$ until we find a number that is congruent to 3 modulo 7
- The numbers of the form $5k + 2$ are: $\{2,7,12,17,22,27,32\}$
- The only answer is 17.
- This is the only answer modulo 35 and should be true by the bijectivity.

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\dots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\dots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\dots4344$ be the 79-digit number obtained that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\ldots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.
- Another useful fact: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\ldots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.
- Another useful fact: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$
- Conclude that $N \equiv 4 \pmod 5$ and $N \equiv 0 \pmod 9$

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\ldots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.
- Another useful fact: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$
- Conclude that $N \equiv 4 \pmod 5$ and $N \equiv 0 \pmod 9$
- Use CRT to say that there exists a such that $N \equiv a \pmod{45}$

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\ldots4344$ *be the 79-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.
- Another useful fact: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$
- Conclude that $N \equiv 4 \pmod 5$ and $N \equiv 0 \pmod 9$
- Use CRT to say that there exists a such that $N \equiv a \pmod{45}$
- Find a.

CRT Destroys AMC Problem

Problem (AMC 2017 12B # 19)

Let $N = 123456789101112\dots4344$ *be the* 79*-digit number obtained that is formed by writing the integers from* 1 *to* 44 *in order, one after the other. What is the remainder when* N *is divided by* 45*?*

- Think about how you can use CRT
- Take modulo 9 and modulo 5.
- Useful fact: The remainder when you divide an integer x by 9 is the sum of the digits of x.
- Another useful fact: $1 + 2 + \dots + n = \frac{n(n+1)}{2}$
- Conclude that $N \equiv 4 \pmod{5}$ and $N \equiv 0 \pmod{9}$
- Use CRT to say that there exists a such that $N \equiv a \pmod{45}$
- Find a.
- $a = 9$

FLT

Theorem

For a prime p and $a \in$ such that $\gcd(a, p) = 1$*:*

$$a^{p-1} \equiv 1 \ mod \ p$$

Proof of FLT

Multiplication by a exhibits a bijection.

Consider the set $\{1, 2, ..., (p-1)\}$ modulo p. We claim that multiplying each element in the set by a and taking modulo p will give back the same set. For the sake of contradiction, suppose not. Then there must be 2 different numbers, i and j, which are congruent to each other after multiplication by a :

$$ai \equiv aj (\text{ mod p })$$

where $i, j < n$. However, we can rewrite this as:

$$ai - aj \equiv 0(\text{ mod p }) \implies a(i-j) \equiv 0(\text{ mod p })$$

$\implies i - j \equiv 0(\text{ mod p }) \implies i \equiv j(\text{ mod n }) \implies i = j$

This contradicts the fact that we chose 2 difference numbers i, j. $\square$

Continued Proof of FLT

Product of the sets .

Since the 2 sets are the same modulo n, if we take all the elements in each set and multiply them all together, the two resulting numbers from each set will be congruent to each other:

$$1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

$$\implies a^{p-1}(p-1)! \equiv (p-1)! (\text{ mod p }) \implies a^{p-1} \equiv 1 (\text{ mod p }) \qquad \square$$

Problem

What is the remainder when 3^{13} is divided by 13?

- Try using what we just learned. Phrase the problem using modular arithmetic.

Problem

What is the remainder when 3^{13} is divided by 13?

- Try using what we just learned. Phrase the problem using modular arithmetic.
- Notice that Fermat's Little theorem doesn't work right away

Problem

What is the remainder when 3^{13} is divided by 13?

- Try using what we just learned. Phrase the problem using modular arithmetic.
- Notice that Fermat's Little theorem doesn't work right away
- Multiply both sides by a to get $a^p \equiv a$ mod p

Problem

What is the remainder when 3^{13} is divided by 13?

- Try using what we just learned. Phrase the problem using modular arithmetic.
- Notice that Fermat's Little theorem doesn't work right away
- Multiply both sides by a to get $a^p \equiv a$ mod p
- Conclude that the final answer is 3

Euler Phi Function

Definition (Euler Phi)

The **Euler Phi** function is denoted by ϕ. $\phi(n)$ counts the number of positive integers less than n that are relatively prime to n.

Example ($\phi(6)$)

We want to count the number of positive integers less than 6 that are relatively prime to 6.Try by yourself.

Theorem (Finding $\phi(n)$)

Suppose n has prime factors $p_1, p_2, \dots, p_k$.
Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

Euler's theorem

Theorem (Euler's Theorem)

For $a, n \in$ such that $\gcd(a, n) = 1$: $a^{\phi(n)} \equiv 1 (\mod n)$

Fermat's Little Theorem actually follows from Euler's theorem since we can choose n to be equal a prime p. Notice that $\phi(p) = p - 1$ because all positive integers less than it are relatively prime to it, by definition.

Modular Arithmetic on Large Powers

Problem

Find the remainder when 3^{32} *is divided by* 7

- Can you use Fermat's Little Theorem?

Modular Arithmetic on Large Powers

Problem

Find the remainder when 3^{32} is divided by 7

- Can you use Fermat's Little Theorem?
- FLT gives that $3^6 \equiv 1 \pmod{7}$

Modular Arithmetic on Large Powers

Problem

Find the remainder when 3^{32} is divided by 7

- Can you use Fermat's Little Theorem?
- FLT gives that $3^6 \equiv 1 (\mod 7)$
- Use the power rule to find that $3^{30} \equiv 1 (\mod 7)$

Modular Arithmetic on Large Powers

Problem

Find the remainder when 3^{32} is divided by 7

- Can you use Fermat's Little Theorem?
- FLT gives that $3^6 \equiv 1 (\mod 7)$
- Use the power rule to find that $3^{30} \equiv 1 (\mod 7)$
- $3^{32} \equiv 3^{30} \cdot 3^2 \equiv 1 \cdot 3^2 \equiv 9 \equiv 2 (\mod 7)$

Modular Arithmetic on Large Powers

Problem

Find the remainder when 3^{32} is divided by 7

- Can you use Fermat's Little Theorem?
- FLT gives that $3^6 \equiv 1 (\mod 7)$
- Use the power rule to find that $3^{30} \equiv 1 (\mod 7)$
- $3^{32} \equiv 3^{30} \cdot 3^2 \equiv 1 \cdot 3^2 \equiv 9 \equiv 2 (\mod 7)$
- The answer is 2.

Resources

Art of Problem Solving-artofproblemsolving.com

1. Problems
2. Alcumus Game
3. Problem Solving Books
4. Classes