Warm up!

Let m = 3 be a modulus.

By combining set notation and congruence classes,

- Express the set of all integers, $\mathbb{Z}$.
- Express the empty set $\emptyset$.

- Let $m = 3$. Then $[0] \cup [1] \cup [2] = \mathbb{Z}$ and $[0] \cap [1] \cap [2] = \emptyset$.

Reminder!

- We never defined division for congruence classes.
  - [a / b] is not recommended!
  - [a] / [b] is not recommended!

MATH 135: Lecture 26

Dr. Nike Dattani

12 November 2021

- <u>Friday 12 November:</u>
  - Moebius quiz tonight! (covers up to middle of page 121)

- <u>Friday 12 November:</u>
  - Look at WA08 (covers up to end of pg 133) and solutions to WA07

- <u>Reading: Up to end of Chapter 8.</u>
  - Moebius quizzes seem to have covered things out of order
  - Knowing FℓT, CRT and "Splitting mod" can help you on quizzes

- **<u>Wednesday 17 November:</u>**
  - **Submit Written Assignment 8: WA8 (covers up to page 133)**

Objectives

- $\mathrm{F}\ell\mathrm{T}$
- CRT

FLT: Fermat's Last Theorem

The proposition was first stated as a theorem by Pierre de Fermat around 1637 in the margin of a copy of *Arithmetica*; Fermat added that he had a proof that was too large to fit in the margin. Although other

F ℓ T: Fermat's Little Theorem

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640 to his friend and confidan Frenicle de Bessy as the following [1]: p divides $a^{p-1} - 1$ whenever p is prime and a is coprime to p.

As usual, Fermat did not prove his assertion, only stating:

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.
>
> (And this proposition is generally true for all progressions and for all prime numbers; the proof of which I would send to you, if I were not afraid that it would be too long.)

- Euler gave the first published proof (1736)
- Leibniz gave the same proof as Euler in an unpublished paper (before 1683)

F ℓ T: Fermat’s Little Theorem

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640 to his friend and confidant Frenicle de Bessy as the following [1]: p divides $a^{p-1} - 1$ whenever p is prime and a is coprime to p.

$ax + by = c$	This is a linear Diophantine equation.
$w^3 + x^3 = y^3 + z^3$	The smallest nontrivial solution in positive integers is $12^3 + 1^3 = 9^3 + 10^3 = 1729$. It was famously given as an evident property of 1729, a taxicab number (also named Hardy–Ramanujan number) by Ramanujan to Hardy while meeting in 1917.[1] There are infinitely many nontrivial solutions.[2]
$x^n + y^n = z^n$	For $n = 2$ there are infinitely many solutions (x, y, z): the Pythagorean triples. For larger integer values of n, Fermat's Last Theorem (initially claimed in 1637 by Fermat and proved by Andrew Wiles in 1995[3]) states there are no positive integer solutions (x, y, z).

F ℓ T

$\forall\, \boldsymbol{p} \in \mathbb{P}$, if $\boldsymbol{p} \nmid \boldsymbol{a}$, then $\boldsymbol{a}^{\boldsymbol{p}\text{-}\mathbf{1}} \equiv 1 \pmod{\boldsymbol{p}}$

Be careful! ***p*** ***<u>must be prime!</u>***

$2^{4-1} \equiv\ ?\ (\text{mod } 4)$

Be careful! ***p*** ***<u>must not divide a!</u>***

$49^{7-1} \equiv\ ?\ (\text{mod } 7)$

FℓT

$\forall\, p \in \mathbb{P}$, if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

Corollaries

$\forall\, p \in \mathbb{P}$, ~~if $p \nmid a$, then~~ $a^{p} \equiv a \pmod{p}$

If $p \nmid a$, multiply both sides of FℓT by ***a*.**

If $p \mid a$, $a^{p} \equiv a \equiv 0 \pmod{p}$

F ℓ T

$\forall\, p \in \mathbb{P}$, if $p \nmid a$, then $a^{p\text{-}1} \equiv 1 \pmod{p}$

Corollaries

$\forall\, p \in \mathbb{P}$, ~~if $p \nmid a$, then~~ $a^{p} \equiv a \pmod{p}$

$\forall\, p \in \mathbb{P}$, if $[a] \neq [0]$ in $\mathbb{Z}_p$, $[a]^{-1} = [a^{p-2}]$

Skipped since WA08 and final don’t need it

Practice!

Determine all solutions to $x^{61} + 26\,x^{41} + 11\,x^{25} + 20 \equiv 30 \pmod 3$.

$x^3 \equiv x \pmod 3$, $\forall\, x \in \mathbb{Z}$ (Corollary to FℓT)

$$x^{3\cdot 20+1} + 26\,x^{3\cdot 13+2} + 11\,x^{3\cdot 8+1} + 20 \equiv 30 \pmod 3$$

$$x^{3\cdot 20}x + 26\,x^{3\cdot 13}x^2 + 11\,x^{3\cdot 8}x + 20 \equiv 30 \pmod 3$$

$$x^{20}x + 26\,x^{13}x^2 + 11\,x^8x + 20 \equiv 30 \pmod 3$$

$$x^{21} + 26\,x^{15} + 11\,x^9 + 20 \equiv 30 \pmod 3$$

$$x^7 + 26\,x^5 + 11\,x + 20 \equiv 30 \pmod 3$$

$$x + 26\,x + 11\,x + 20 \equiv 30 \pmod 3$$

$$38\,x + 20 \equiv 30 \pmod 3$$

Chinese Remainder Theorem

有物不知其数，三三数之剩二，
五五数之剩三，七七数之剩二。**问物几何?**

There’s an unknown number ***x***,
when counted in 3s we have 2 left over,
when counted in 5s we have 3 left over,
when counted in 7s we have 2 left over,
what is the number?

CRT

Problem 26, Volume 3 of:

孫子 (Sun Zi) 算經 (Mathematics Manual)

In China, it's called:

孙子定理 (Sun Zi Theorem), or

中国剩余定理 (Chinese Remainder Theorem)

孫子兵法 (Art of War): 430-500 BC

孫子算經: 200-400 AD (~765 years difference!)

CRT

Sun Zi explained how to solve the problem. He noticed:

$70 \equiv 1 \pmod{3} \equiv 0 \pmod{5} \equiv 0 \pmod{7}$

$21 \equiv 1 \pmod{5} \equiv 0 \pmod{3} \equiv 0 \pmod{7}$

$15 \equiv 1 \pmod{7} \equiv 0 \pmod{3} \equiv 0 \pmod{5}$

$\therefore$ $x = 2(70) + 3(21) + 2(15) = 233$ solves the problem.

Any multiple of 105 ($3 \times 7 \times 5$) is divisible by 3, 5, and 7,

$\therefore$ $233 - 2(105) = 23$ is the smallest positive answer.

CRT

Theorem 16 **(Chinese Remainder Theorem (CRT))**

For all integers a_1 and a_2, and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences

$$n \equiv a_1 \pmod{m_1}$$
$$n \equiv a_2 \pmod{m_2}$$

have a unique solution modulo $m_1 m_2$. Thus, if $n = n_0$ is one particular solution, then the solutions are given by the set of all integers n such that

$$n \equiv n_0 \pmod{m_1 m_2}.$$

[10] 3. Solve the following system of linear congruences.

$$x \equiv 12 \pmod{20}$$
$$x \equiv 11 \pmod{39}$$

$x = 20n + 12$

$(20n + 12) \equiv 11 \pmod{39}$

$20n \equiv -1 \pmod{39}$

$20n = 39y - 1$

$1 = 39y - 20n$ [now solve the Diophantine eqn]

Theorem 17 **(Generalized Chinese Remainder Theorem (GCRT))**

For all positive integers k and $m_1, m_2, \ldots, m_k$, and integers $a_1, a_2, \ldots, a_k$, if $\gcd(m_i, m_j) = 1$ for all $i \neq j$, then the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

have a unique solution modulo $m_1 m_2 \cdots m_k$. Thus, if $n = n_0$ is one particular solution, then the solutions are given by the set of all integers n such that

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}.$$

EXERCISE

Solve the problem posed by Sun Zi that was discussed at the beginning of this section.

Solve the simultaneous congruences

$$\begin{aligned} n &\equiv 2 \pmod{3} \\ n &\equiv 3 \pmod{5} \\ n &\equiv 5 \pmod{7}. \end{aligned}$$

Splitting Modulus Theorem (SMT)

Theorem 18 **(Splitting Modulus Theorem (SMT))**

For all integers a and positive integers m_1 and m_2, if $\gcd(m_1, m_2) = 1$, then the simultaneous congruences

$$\begin{aligned} n &\equiv a \pmod{m_1} \\ n &\equiv a \pmod{m_2} \end{aligned}$$

have exactly the same solutions as the single congruence $n \equiv a \pmod{m_1 m_2}$.

"Inverse Chinese Remainder Theorem"

(Do not actually call it that on the exam)

Example 22 Find all integers x such that $x^3 + x^2 \equiv 26 \pmod{35}$.

$$x^3 + x^2 \equiv 26 \equiv 1 \pmod{5}$$
$$x^3 + x^2 \equiv 26 \equiv 5 \pmod{7}.$$

$x \pmod{5}$	0	1	2	3	4
$x^2 \pmod{5}$	0	1	4	4	1
$x^3 \pmod{5}$	0	1	3	2	4
$x^3 + x^2 \pmod{5}$	0	2	2	1	0

$x \pmod{7}$	0	1	2	3	4	5	6
$x^2 \pmod{7}$	0	1	4	2	2	4	1
$x^3 \pmod{7}$	0	1	1	6	1	6	6
$x^3 + x^2 \pmod{7}$	0	2	5	1	3	3	0

$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}.$$

$x \equiv n_0 \pmod{35}$, where n_0 is one particular solution.

Example 22 Find all integers x such that $x^3 + x^2 \equiv 26 \pmod{35}$.

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

$x \equiv n_0 \pmod{35}$, where n_0 is one particular solution.

To find a suitable value for n_0, note that $n_0 = 2, 9, 16, 23, 30$ are the choices of integers between 0 and 34 that are congruent to 2 (mod 7). Now we observe that $2 \equiv 2 \pmod{5}$, $9 \equiv 4 \pmod{5}$, $16 \equiv 1 \pmod{5}$, $23 \equiv 3 \pmod{5}$ and $30 \equiv 0 \pmod{5}$, so $n_0 = 23$ is a

$$x \equiv 23 \pmod{35}.$$

Thank you!

Extra practice:

- Is 156723 divisible by 11?
- Is $5^9 + 62^{2000} - 14$ divisible by 7?
- What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?
- What is the last digit of $5^{32}3^{10} + 9^{22}$?
- Prove that $\gcd(2^a - 1, 2^b - 1) \mid 2^{\gcd(a,b)} - 1$ for all $a, b \in \mathbb{N}$.

without actually carrying out any long division.

The following pages are intentionally left blank, for writing notes from the tablet.