Lecture 1 slide from a different MATH 135 instructor:

Expectations from You

- Math 135 works a bit differently from you other Math courses.
- We do not have traditional “lectures”
- Instead of introducing content, we will focus more on practicing problem solving
- You are expected to read ahead (reading assigned at the end of each lecture) and take notes at home
- In class, you are expected to listen, work through examples and exercises, and share your ideas with the rest of the class
- This may not be the easiest of courses, but if you put in the effort, this can definitely be the most fun first year Math course!

MATH 135: Lecture 24

Dr. Nike Dattani

8 November 2021

Does anybody not know how to find the general solution to an LDE?

Theorem 2 **(Linear Diophantine Equation Theorem, Part 2, (LDET 2))**

Let a, b and c be integers with a and b both not zero, and define $d = \gcd(a, b)$. If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + by = c$, then the set of all solutions is given by

$$\left\{(x, y) : x = x_0 + \tfrac{b}{d}n,\ y = y_0 - \tfrac{a}{d}n,\ n \in \mathbb{Z}\right\}.$$

Chapter 7 was only 5 pages long (2 simple theorems).

- This week we're supposed to be doing Chapter 8

Week 9	Chapter 8: Congruence and Modular Arithmetic	8.1 Congruences 8.2 Elementary Properties of Congruence 8.3 Congruence and Remainders 8.4 Linear Congruences 8.5 Non-Linear Congruences	Mobius Quizzes 21, 22, 23 **Available:** Mon Nov 8, Wed Nov 10, Fri Nov 12 **Due:** midnight WA7 **Due:** Wed Nov 10 at 5 PM EST	**MQ:** 0.4% each **WA7:** 1.11%	Assessments cover the material from Weeks 1–8

Usually I wait until Wednesday, to maximize assignment help
But end of Ch6 was just prime factorization. Ch7: not much content
I started Ch8 early because…

Week 10	Chapter 8: Congruence and Modular Arithmetic Chapter 11: Polynomials	8.6 Congruence Classes and Modular Arithmetic 8.7 Fermat's Little Theorem 8.8 The Chinese Remainder Theorem 8.9 Splitting a Modulus 11.5 Integer Polynomials and the Rational Roots Theorem	Mobius Quizzes 24, 25, 26 **Available:** Mon Nov 15, Wed Nov 17, Fri Nov 19 **Due:** midnight WA8 **Due:** Wed Nov 17 at 5 PM EST	**MQ:** 0.4% each **WA8:** 1.11%	Assessments cover the material from Weeks 1–9

The proofs will be complex: Must know EVERYTHING.

(divisibility, gcd, Diophantine, modular arithmetic, congruence classes, FLT, CRT, polynomials, etc.)

- Regrade requests:
  - If you disagree with your regrade, let me know by end of Tuesday
- Monday 8 November:
  - Mobius quiz tonight! (covers up to middle of page 121)
- **Wednesday 10 November:**
  - **Submit Written Assignment 7: WA7 (covers up to page 121)**
- Reading: 8.1-8.4 (122-133) won't take long (I've covered it already!)
- Reading: 8.5-8.9 (122-148) worth getting a head start!

What's the last digit of 7^{3333}?

Latin: *digiti* = fingers
Latin: *decem* = 10.
Binary "digit" is a bit
In quantum computing: qubit

Powers of 7:
7, 49, 343, 2401, 16807

What's the last digit of 7^{3333}?

Latin: *digiti* = fingers
Latin: *decem* = 10.
Binary "digit" is a bit
In quantum computing: qubit

Powers of 7:
7, 49, 343, 2401, 16807

$$
\begin{aligned}
7^2 &\equiv -1 && \pmod{10} \\
7^{3333} &\equiv 7^{2 \cdot 1666}\, 7^1 && \pmod{10} \\
&\equiv (-1)^{2 \cdot 1666}\, 7 && \pmod{10} \\
&\equiv 7 && \pmod{10}
\end{aligned}
$$

How do you know if a number is divisible by 3?

Proposition 8 in Chapter 8.3.

How do you know if a number is divisible by 11?

Proposition 9 in Chapter 8.3:

Check if $11 \mid A - B$,

A = sum of 1^{st}, 3^{rd}, 5^{th}, 7^{th}, etc. digits
B = sum of 2^{nd}, 4^{th}, 6^{th}, 8^{th}, etc. digits

Does $11 \mid 6455874532635$?

[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]

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

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

x = 20n + 12

$$3x \equiv 5 \pmod{76}$$

$$3x + 76y = 5$$

$$3x \equiv 5 \pmod{6}$$

Solution: Since $\gcd(3, 6) = 3$ and $3 \nmid 5$, there is no solution to $3x \equiv 5 \pmod{6}$

$$4x \equiv 6 \pmod{10}$$

Small modulus! Skip the EEA:

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$4x \pmod{10}$	0	4	8	2	6	0	4	8	2	6

$$x^2 + x \equiv 2 \pmod 8$$

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1
$x^2 + x \pmod 8$	0	2	6	4	4	6	2	0

so one particular solution is given by $x = -125$. But $-125 \equiv -125 + 2(76) \equiv 27 \pmod{76}$, and hence the set of solutions to the linear congruence is given by all integers x such that

$$x \equiv 27 \pmod{76}.$$

Example 10 If possible, solve the linear congruence

$$4x \equiv 6 \pmod{10}.$$

Solution: Since $\gcd(4, 10) = 2$ and $2 \mid 6$, there is a solution, by the Linear Congruence Theorem. Moreover, since $\frac{m}{d} = \frac{10}{2} = 5$, the set of all solutions is given by the set of all integers x such that $x \equiv x_0$ or $x_0 + 5 \pmod{10}$, where x_0 is some particular solution to the congruence. Of course, we could solve the corresponding linear Diophantine equation to obtain a particular solution, but since 10 is a small modulus, we can also simply check all possibilities modulo 10 to find a particular solution:

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$4x \pmod{10}$	0	4	8	2	6	0	4	8	2	6

8.5 Non-Linear Congruences

By applying the Euclidean Algorithm or Extended Euclidean Algorithm, we have an efficient way to solve linear congruences, but we have no equivalent way to solve congruences involving higher powers of the variable. However, for higher powers, we can solve a congruence relation modulo m by checking all m values, which works quite well when m is

Example 11 Solve the congruence relation $x^2 + x \equiv 2 \pmod{8}$.

Solution: We use a table to check the 8 possible values of x.

$x \pmod{8}$	0	1	2	3	4	5	6	7
$x^2 \pmod{8}$	0	1	4	1	0	1	4	1
$x^2 + x \pmod{8}$	0	2	6	4	4	6	2	0

Hence, the solution is given by all integers x such that $x \equiv 1$ or $6 \pmod{8}$.

8.6 Congruence Classes and Modular Arithmetic

In previous sections, we have seen that the solutions to a congruence relation can be expressed in terms of sets consisting of all integers congruent to a given integer modulo m.

Proposition 8 For all non-negative integers a, a is divisible by 3 if and only if the sum of the digits in the decimal representation of a is divisible by 3.

Proof: Suppose that a has the decimal representation $d_k d_{k-1} \cdots d_1 d_0$, where $0 \leq d_i \leq 9$ for $i = 0, 1, \ldots, k$, $k \geq 0$. Then we have the equation

$$a = d_k 10^k + d_k \ _1 10^{k-1} + \cdots + d_1 10 + d_0$$

that relates a and its digits $d_k, d_{k-1}, \ldots, d_1, d_0$. Now observe that $10 \equiv 1 \pmod 3$. From the above equation for a, using propositions Congruence Add and Multiply, and Congruence Power, we get

$$\begin{aligned} a &\equiv d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0 \pmod 3 \\ &\equiv d_k (1)^k + d_{k-1} (1)^{k-1} + \cdots + d_1 (1) + d_0 \pmod 3 \\ &\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 3. \end{aligned}$$

Now let $S = d_k + d_{k-1} + \cdots + d_1 + d_0$ represent the sum of the digits in the decimal representation of a. Using this notation, what we have proved above is that $a \equiv S \pmod 3$.

But an integer is divisible by 3 if and only if the remainder when it is divided by 3 is 0. Hence from the proposition Congruent To Remainder, an integer is divisible by 3 if and only if it is congruent to 0 modulo 3. Since $a \equiv S \pmod 3$, then $a \equiv 0 \pmod 3$ if and only

Example 6 The sum of the digits of 6455874532635 is

$$6 + 4 + 5 + 5 + 8 + 7 + 4 + 5 + 3 + 2 + 6 + 3 + 5 = 63,$$

which is divisible by 3. This implies that the integer 6455874532635 is also divisible by 3.

The sum of the digits of 5748562331869 is

$$5 + 7 + 4 + 8 + 5 + 6 + 2 + 3 + 3 + 1 + 8 + 6 + 9 = 67,$$

which is not divisible by 3. This implies that the integer 5748562331869 is also not divisible

We continue with a similar rule for divisibility by 11.

Proposition 9 For all non-negative integers a, a is divisible by 11 if and only if $S_e - S_o$ is divisible by 11, where

- S_e is the sum of the digits of even powers (of 10) in the decimal representation of a,
- S_o is the sum of the digits of odd powers (of 10) in the decimal representation of a.

Then, using propositions Congruence Add and Multiply, and Congruence Power, we get

$$\begin{aligned}
2^{22}3^{33}5^{55} &\equiv 2^{2+20}3^{1+32}5^{1+54} \pmod{11} \\
&\equiv 2^2(2^5)^4(3)(3^2)^{16}(5)(5^2)^{27} \pmod{11} \\
&\equiv 2^2(-1)^4(3)(-2)^{16}(5)3^{27} \pmod{11} \\
&\equiv (5)2^{18}3^{28} \pmod{11} \\
&\equiv (5)2^3(2^5)^3(3^2)^{14} \pmod{11} \\
&\equiv (5)2^3(-1)^3(-2)^{14} \pmod{11} \\
&\equiv (-5)2^{17} \pmod{11} \\
&\equiv (-5)2^2(2^5)^3 \pmod{11} \\
&\equiv (-20)(-1)^3 \pmod{11} \\
&\equiv 20 \pmod{11} \\
&\equiv 9 \pmod{11}.
\end{aligned}$$

Since $0 \leq 9 < 11$, we conclude from the proposition Congruent To Remainder that the remainder when $2^{22}3^{33}5^{55}$ is divided by 11 is equal to 9.

Example 5 What is the last decimal digit of 7^{3333}?

Solution: The last decimal digit of any non-negative integer a is precisely equal to the remainder when a is divided by 10. Therefore, we will work modulo 10, and first observe that $7^2 \equiv 49 \equiv -1 \pmod{10}$. Then, using propositions Congruence Add and Multiply, and Congruence Power, we get

$$7^{3333} \equiv 7^{1+3332} \equiv 7(7^2)^{1666} \equiv 7(-1)^{1666} \equiv 7 \pmod{10}.$$

Since $0 \leq 7 < 10$, we conclude from the proposition Congruent To Remainder that the remainder when 7^{3333} is divided by 10 is 7, and hence that the last decimal digit is 7.

Proposition 7 **(Congruent To Remainder (CTR))**

For all integers a and b with $0 \leq b < m$, $a \equiv b \pmod{m}$ if and only if a has remainder b when divided by m.

We now give some examples to demonstrate how our propositions on congruence can be applied to determine remainders in an elegant and surprisingly powerful way.

Example 3 Determine the remainder when 3^{47} is divided by 7.

Solution: Observe that $3^3 \equiv 27 \equiv -1 \pmod{7}$, so from the propositions Congruence Add and Multiply, and Congruence Power, we obtain

$$\begin{aligned} 3^{47} &\equiv 3^{2+45} \pmod{7} \\ &\equiv 3^2 3^{45} \pmod{7} \\ &\equiv 9(3^3)^{15} \pmod{7} \\ &\equiv 2(-1)^{15} \pmod{7} \\ &\equiv 2(-1) \pmod{7} \\ &\equiv -2 \pmod{7} \\ &\equiv 5 \pmod{7}. \end{aligned}$$

Since $0 \leq 5 < 7$, we conclude from the proposition Congruent To Remainder that the remainder when 3^{47} is divided by 7 is equal to 5.

Example 4 What is the remainder when $2^{22}3^{33}5^{55}$ is divided by 11?

Solution: Observe that (for reasons that will become clear in the computations that follow)

$$2^5 \equiv 32 \equiv -1 \pmod{11}, \qquad 3^2 \equiv 9 \equiv -2 \pmod{11}, \qquad \text{and} \qquad 5^2 \equiv 25 \equiv 3 \pmod{11}.$$

Thank you!