Prove that $\gcd(2^a - 1, 2^b - 1) \mid 2^{\gcd(a,b)} - 1$

for all $a, b \in \mathbb{N}$

$\gcd(2^a - 1, 2^b - 1) \mid 2^a - 1$

$2^a \equiv 1 \mod(\gcd(2^a - 1, 2^b - 1))$

$2^{ax} \equiv 1^x \mod(\gcd(2^a - 1, 2^b - 1))$

$\gcd(2^a - 1, 2^b - 1) \mid 2^b - 1$

$2^b \equiv 1 \mod(\gcd(2^a - 1, 2^b - 1))$

$2^{by} \equiv 1^y \mod(\gcd(2^a - 1, 2^b - 1))$

$2^{ax}\, 2^{by} \equiv 1^x\, 1^y \mod(\gcd(2^a - 1, 2^b - 1))$

$2^{ax + by} \equiv 1 \mod(\gcd(2^a - 1, 2^b - 1))$

$2^{\gcd(a,b)} \equiv 1 \mod(\gcd(2^a - 1, 2^b - 1))$

$\gcd(2^a - 1, 2^b - 1) \mid 2^{\gcd(a,b)} - 1$

2 Prove that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$

0 $GCD(2^m-1, 2^n-1)$

1 Proof that $(2^m-1, 2^n-1) = 2^d-1$ where $d = (m, n)$

1 Find the GCD of $2^{60}-1$ and $2^{50}-1$

0 Algebra(Euclid method)

0 Let a and b be nonnegative integers. prove that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$

0 Show $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$ for positive integers a, b

0 Prove that $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$

163 Prove that $\gcd(a^n-1, a^m-1) = a^{\gcd(n,m)}-1$

22 x^a-1 divides x^b-1 if and only if a divides b

18 $\gcd(b^x-1, b^y-1, b^z-1, \ldots)$ $= b^{\gcd(x,y,z,\ldots)}-1$

6 Prove that if d divides n, then 2^d-1 divides 2^n-1

4 Gcd number theory proof: $(a^n-1, a^m-1) = a^{(m,n)}-1$

3 Show that $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$

3 The ideal generated by x^m-1 and x^n-1 in $\mathbb{Z}[X]$ is principal.

0 Greatest common divisor of $(2^{21}-1, 2^{27}-1)$

2 Prove $\gcd(k, l) = d \Rightarrow \gcd(2^k-1, 2^l-1)$ $= 2^d-1$

-2 number theory division of power for the case (n^r-1) divides (n^m-1) if and only if r divides m.

0 GCD of two big numbers

1 Prove that if $a^{170} \equiv 1 \pmod n$ and a^{111} $\equiv 1 \pmod n$ then $a \equiv 1 \pmod n$

MATH 135: Lecture 25

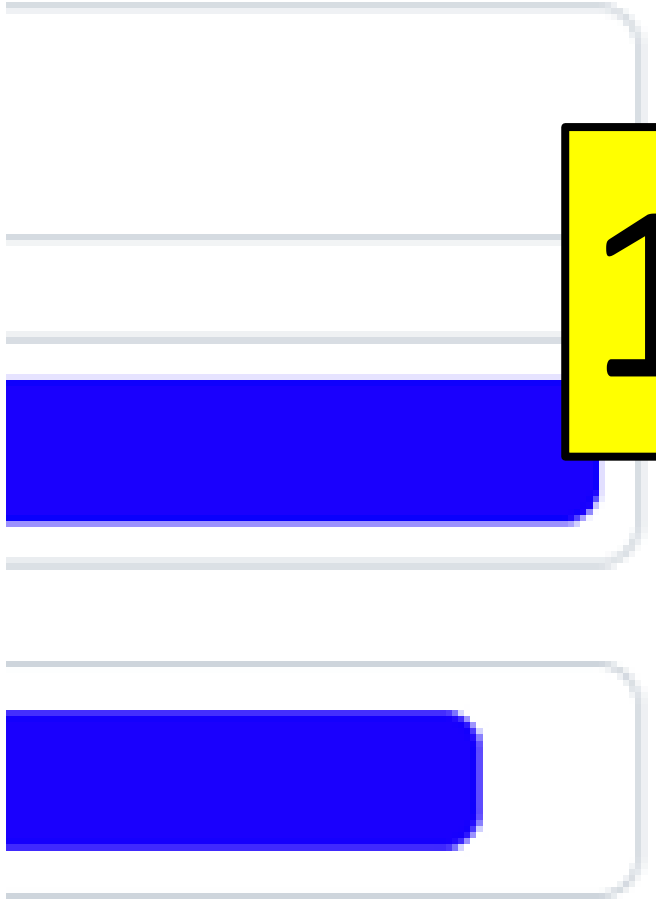
Dr. Nike Dattani

10 November 2021

I am so proud of you!

MQ 15

Nike's Section 19*



96.67 %

Anton's Section 7

60 %

100 %

95.55 %

Ali's Section 22

40 %

100 %

95.63 %

1.1% difference

*Similar for Section 16

MQ 21

19-MATH.135.007.1.LEC Apply

Statistics

Minimum: 55 %

Maximum:

Average: 90.71 %

Mode: 100 %

Median: 100 %

Standard Deviation: 12.08 %

View By: Groups Groups: 1219-MATH.135.008.1.LEC Apply

MQ21 (Mon Nov 8) Class Statistics

Number of submitted grades: 52 / 56

Minimum: 60 %

Maximum:

Average: 90.1 %

Mode: 100 %

Median: 97.5 %

Standard Deviation: 11.41 %

View By: Groups Groups: 1219-MATH.135.019.1.LEC Apply

MQ21 (Mon Nov 8) Class Statistics

Number of submitted grades: 49 / 51

Minimum: 70 %

Maximum:

Average: 92.65 %

Mode: 100 %

Med

Standard Deviat n: 9.21 %

View By: Groups Groups: 1219-MATH.135.022.1.LEC Apply

MQ21 (Mon Nov 8) Class Statistics

Number of submitted grades: 56 / 63

Minimum: 70 %

Maximum: 100 %

Average: 93.13 %

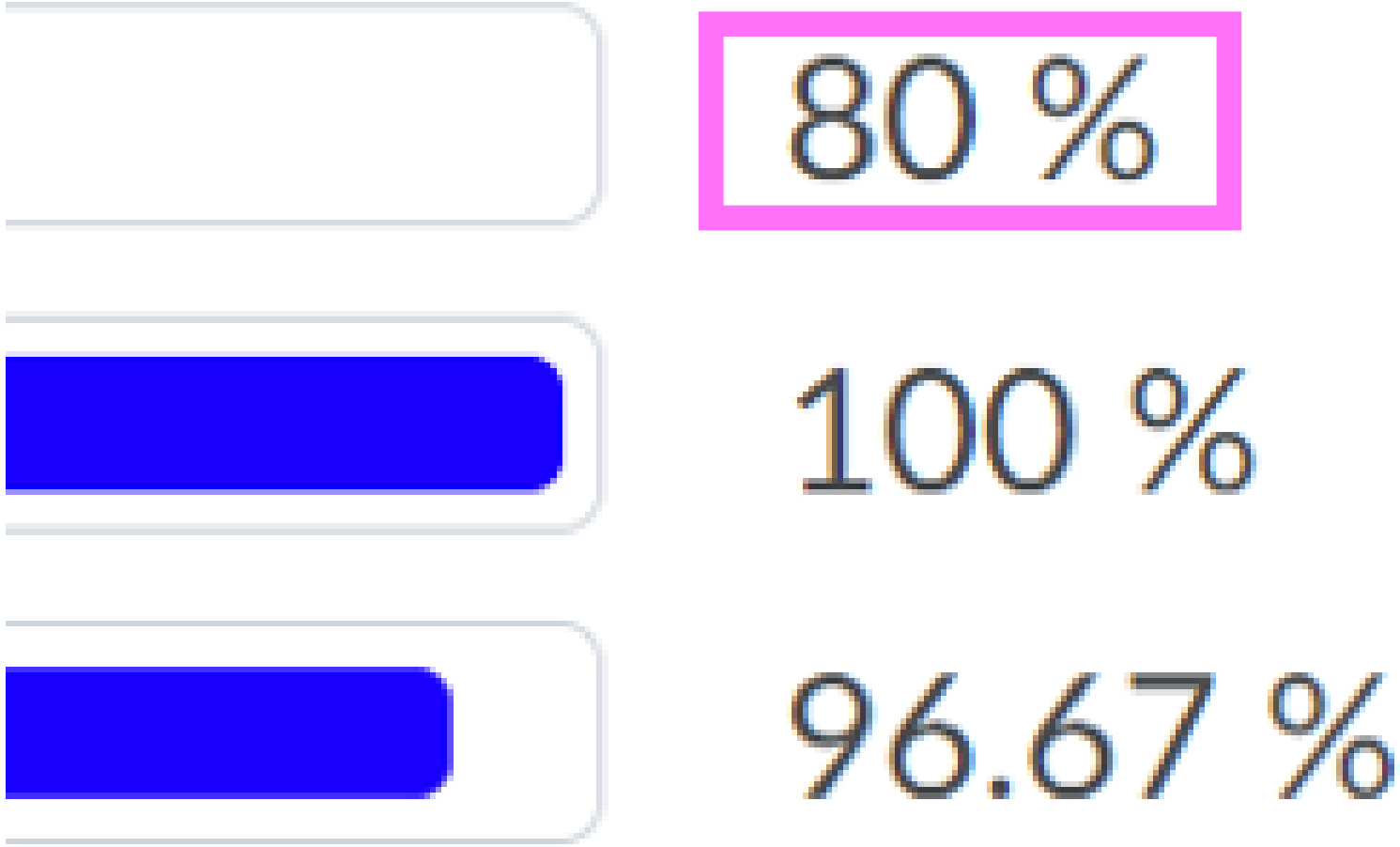
Mode: 100 %

Median: 100 %

Standard Deviation: 9.66 %

Term	Course and Title
1A Fall	CS 137 Programming Principles
	ECE 105 Classical Mechanics
	MATH 115 Linear Algebra for Engineering
	MATH 117 Calculus 1 for Engineering
	MATH 135 Algebra for Honours Mathematics
	SE 101 Introduction to Methods of Software Engineering

MQ 15



Nike's Section 19*

80 %

100 %

96.67 %

*Similar for Section 16

Anton's Section 7

60 %

100 %

94.83 %

Emma's Section 8

75 %

100 %

95.55 %

Ali's Section 22

40 %

100 %

95.63 %

This is the best MATH 135 class!

You are all awesome!

- Wednesday 10 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!

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)

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

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

I'd like to do more examples but:
There's not much sense in doing more examples until you've learned all this

Why practice proving things without these theorems,
if on the exam you'll be allowed to use them?

The faster we get there,
the sooner we can start doing practice exams more seriously / realistically.

If I went through 8.1 to 8.5 too fast:

Tell me what you need me to go through more slowly, and ***I will do it***.

- Read the course notes to fill in the gaps
- Ask on Piazza.
- Ask at office hours
- Go to online tutorial centre
- If you really think you'll learn what's in the course notes better if "lectured",
  Look at lecture notes of other instructors on LEARN
  → no assignment tips, no previous exam problems, but content covered

But be careful: Lectures don't tend to be as "refined" as the course notes.
One mistake could be very costly.

Lecture 18 Congruences
PDF document

Lecture 19 Congruence Equations
PDF document

Lecture 20 Congruence Classes
PDF document

Lecture 21 Fermat's Little Theorem
PDF document

Lecture 22 Chinese Remainder Theorem
PDF document

Lecture 23 Cryptography
PDF document

Lecture 24 Complex Numbers
PDF document

Lecture 25 Polar Form
PDF document

Check this out:

$$6 \equiv 6 \pmod{11}$$

Check this out:

$$-5 \equiv 6 \equiv 6 \pmod{11}$$

Check this out:

$$17 \equiv -5 \equiv 6 \equiv 6 \pmod{11}$$

Check this out:

$$28 \equiv 17 \equiv -5 \equiv 6 \equiv 6 \pmod{11}$$

Check this out:

$$-16 \equiv 28 \equiv 17 \equiv -5 \equiv 6 \equiv 6 \pmod{11}$$

$$[6] = \{\ldots,-16,-5,6,17,28,\ldots\}$$

Definition 8.6.1

congruence class

The **congruence class** modulo m of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

Example 12

For $m = 4$, the four congruence classes are given by

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 4\} &&= \{\ldots, -8, -4, 0, 4, 8, \ldots\} &&= \{4k : k \in \mathbb{Z}\},\\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 4\} &&= \{\ldots, -7, -3, 1, 5, 9, \ldots\} &&= \{4k+1 : k \in \mathbb{Z}\},\\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 4\} &&= \{\ldots, -6, -2, 2, 6, 10, \ldots\} &&= \{4k+2 : k \in \mathbb{Z}\},\\
[3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod 4\} &&= \{\ldots, -5, -1, 3, 7, 11, \ldots\} &&= \{4k+3 : k \in \mathbb{Z}\}.
\end{aligned}$$

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$			
$[2]$	$[2]$			
$[3]$	$[3]$			

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	
$[2]$	$[2]$	$[3]$		
$[3]$	$[3]$			

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	
$[3]$	$[3]$	$[0]$		

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$				
$[1]$				
$[2]$				
$[3]$				

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$			
$[2]$	$[0]$			
$[3]$	$[0]$			

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$		
$[3]$	$[0]$	$[3]$		

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	
$[3]$	$[0]$	$[3]$		

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	

Definition 8.6.2

$\mathbb{Z}_m$, addition and multiplication in $\mathbb{Z}_m$, modular arithmetic

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\},$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing what is known as **modular arithmetic**.

$\mathbb{Z}_4$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

$$[a] + [0] = [0] + [a] = [a],$$

$$[a][0] = [0][a] = [0],$$

$$[a] + [-a] = [-a] + [a] = [0],$$

$$[a][1] = [1][a] = [a].$$

[0] = Additive Identity

[-a] = Additive Inverse

[1] = Multiplicative Identity

For any $[a] \in \mathbb{Z}_m$, if there exists $[b] \in \mathbb{Z}_m$ such that

$$[a][b] = [b][a] = [1], \tag{8.3}$$

then we say that $[b]$ is the *multiplicative inverse* of $[a]$, and in this situation we use the notation $[b] = [a]^{-1}$.

Solve for [x] in $\mathbb{Z}_{11}$:

$$[8][x] = [4]$$

$$11y + 8x = 4$$

Definition 8.6.1

congruence class

The **congruence class** modulo m of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}.$$

When does [a] have a multiplicative inverse in $\mathbb{Z}_m$?

Answer: Iff gcd(a,m) = 1

When is the multiplicative inverse in $\mathbb{Z}_m$ unique?

Answer: Always!

as + mt = 1.

$s = s_0 + \frac{mn}{\gcd(a,m)}$

[s] = { all s }

Corollary 13 **(Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$))**

For all prime numbers p and non-zero elements $[a]$ in $\mathbb{Z}_p$, the multiplicative inverse $[a]^{-1}$ exists and is unique.

Example 14 If possible, find the multiplicative inverse of $[5]$ in $\mathbb{Z}_{10}$.

Corollary 13 **(Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$))**

For all prime numbers p and non-zero elements $[a]$ in $\mathbb{Z}_p$, the multiplicative inverse $[a]^{-1}$ exists and is unique.

Example 14 If possible, find the multiplicative inverse of $[5]$ in $\mathbb{Z}_{10}$.

Solution: Observe that $\gcd(5, 10) = 5 \neq 1$. Hence, by the corollary Inverses in $\mathbb{Z}_m$, $[5]$ has no multiplicative inverse in $\mathbb{Z}_{10}$.

Example 15 If possible, find the multiplicative inverse of $[5]$ in $\mathbb{Z}_{42}$.

Example 15 If possible, find the multiplicative inverse of $[5]$ in $\mathbb{Z}_{42}$.

Solution: Observe that $\gcd(5, 42) = 1$. Hence, by the corollary Inverses in $\mathbb{Z}_m$, $[5]$ has a unique multiplicative inverse in $\mathbb{Z}_{42}$. To find the inverse, we consider the corresponding linear Diophantine equation $5x + 42y = 1$. Applying the Extended Euclidean Algorithm we obtain the table

y	x	r	q
1	0	42	0
0	1	5	0
1	-8	2	8
-2	17	1	2
5	-42	0	2

From the second last row we obtain $42(-2) + 5(17) = 1$, or to match up with the order of the original equation, $5(17) + 42(-2) = 1$. We conclude that $[5]^{-1} = [17]$ in $\mathbb{Z}_{42}$.

Example 16 Solve the following system of equations in $\mathbb{Z}_{11}$,

$$[2][x] + [7][y] = [4], \tag{8.4}$$
$$[3][x] + [2][y] = [9]. \tag{8.5}$$

Solution: This is a system of two linear equations in $\mathbb{Z}_{11}$ for the two unknowns $[x]$ and $[y]$. Our method of solution will be similar to the method we use to solve two linear equations in the reals for two unknowns. First, subtract [2] times equation (8.5) from [3] times equation (8.4) to obtain $[17][y] = [-6]$, and note that $[17] = [6]$, so we have the equation

$$[6][y] = [-6].$$

Now 11 is prime, and $[6] \neq [0]$, so by the corollary Inverses in $\mathbb{Z}_p$, the element [6] has a multiplicative inverse in $\mathbb{Z}_{11}$. Multiplying on both sides of the above equation by $[6]^{-1}$, we obtain

$$[6]^{-1}[6][y] = [6]^{-1}[-6],$$

and using the fact that

$$[6]^{-1}[6][y] = [1][y] = [y],$$

and

$$[6]^{-1}[-6] = [6]^{-1}[6][-1] = [1][-1] = [-1] = [10]$$

in $\mathbb{Z}_{11}$, we get $[y] = [10]$. Substituting $[y] = [10]$ into equation (8.4) gives

$$[2][x] = [4] - [7][10] = [-66] = [0].$$

But [2] has a multiplicative inverse in $\mathbb{Z}_{11}$, and multiplying on both sides of the equation $[2][x] = [0]$ by $[2]^{-1}$, we obtain $[x] = [0]$. Hence we obtain $[x] = [0], [y] = [10]$.

Checking to make sure that this is not an extraneous solution, we substitute these values for $[x]$ and $[y]$ into equations (8.4) and (8.5), to obtain

$$[2][x] + [7][y] = [2][0] + [7][10] = [70] = [4],$$

$$[3][x] + [2][y] = [3][0] + [2][10] = [20] = [9],$$

which confirms that $[x] = [0], [y] = [10]$ is indeed a solution, and hence the only solution.

8.7 Fermat's Little Theorem

In this section we consider Fermat's Little Theorem, a useful result for powers of an integer

Homework:

Read 8.6 (134-138): Thoroughly (I'm serious!)

- You don't need 8.1-8.5 (catch up on it later!)
- Most exercises were already done today!

Friday:
We'll do Fermat's Little Theorem ***and*** CRT

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.

Thank you!