April 6, 2012

Table 1

Mod 5 ; base "2" has a pattern of +4 cricket. Base "3" has a pattern of +4 Cricket. Base "4" has a pattern of +2 Cricket.

mod 26: see crickets of 1, 12, 2, 3, 4, 6,

mod 9: using bigger numbers & replacing them w/ smaller negative numbers that are equavilant to the larger number. There is symmetry among the columns of the mods. additive inverses.

$$2^{*} + (-2) \equiv 0 \bmod 9$$
$$2 + 7 \equiv 0 \bmod 9$$

$\left\{\begin{array}{l} \text{if } n \text{ is even}, (-2)^n = (2)^n \\ \text{if } m \text{ is odd}, (-2)^m = -(2)^m \end{array}\right.$ *

Question; Explain why statements are true.

mod 6; the pattern repeats after the power of three.

mod 25; Base of 5, we would get "0" all the way down w/ all the powers.

$$\begin{array}{cc} 10^{2} & 10^{2} \\ \wedge & \wedge \\ 2\ \ 5 & 2^{2}\ \ 5^{2} \end{array}$$

Look for a # who has a factor of 5 & we know that our output will always be zero.

If we get "0's" we wont get to the "1.2.3.4.5..." pattern

* Conjecture; half way of the mod we will have the row that is 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ... pattern.

* The cricket that provide us w/ the pattern of 1, 2, 3, 4, 5, 6, 7 is a +6 cricket b/c it needs to repeat regularly.

one above the mod is when

Conjecture

For mod m identity row is the
m^{th} power. True for mod 7, 5, 11,
13 for all prime numbers.

Fermat's Little Therom

Theorem:

If p is prime, then $x = x \bmod p$

$$x^{p-1} \equiv 1 \bmod p$$

Notes

MTHT 467
April 6th, 2012

Mod 5 we did ~~power~~ until power 4 & we didn't see a pattern until we did the row of power 5

	1	2	3	4
2	1	4	4	1
3	1	3	2	4
4	1	1	1	1
5	1	2	3	4

→ If you get all the ones, the next row is 1, 2, 3, 4, 5

→ Interesting row. When do we get 1, 2, 3, 4, 5 in other charts? What about mod 6? Do we ever get there? →

Crickets: what is the cricket that jumps from 2 to the next 2 on the same colum of base 2? +4

row 3 +4 cricket

row 4 +2 cricket

Crickets on mod 26: 1, 12, 2, 3, 4, 6
What are the crickets on mod 26?

Mod 9. Negative #s.

base 8 is also a -1 & then the pattern goes -1, +1, -1, +1

base 7 is also a -2 ; 1 is -8 ; 7 is 16, 4 is -14

Rosa $2 + (-2) \equiv 0$

even #s are always the same

-2 raised to any ~~positive~~ even exponent

$(-2)^2 \equiv (2)^2$

$4 \equiv 4$

Explain HW due wednesday

On exam: Explain why these statements are true:

- $(-2)^n = (2)^n \longrightarrow$ if n is even
- $(-2)^m = (2)^m \rightarrow$ if m is odd

b/c a positive * positive = positive
negative * negative = positive
negative * positive = negative

ex. $(-2) \cdot 3 = -2 \cdot 3$

no. why? b/c of those zeros.

$3^2 = 9 \equiv 0 \mod 9$

- When is it that we are going to get the first zero?
  for 8? 2^3

- In mod 25

	5	10
^2	$5^2 = 25 \equiv 0$	$10^2 = 100 \equiv 0$
	0	$10^2 = (2\cdot5)^2 = 2^2\cdot5^2$
	0	
	0	
	0	

- mod 13 : In mod 13 when am I going to get to 1,2,3,4,5... again?
  Row 13.

- Conjecture: The #s 1,2,3,4,5... appear on the # that is half of the # of the mod. We see it on mod: 6, 10, 14,
- In mod 7, the +6 cricket is the one that gets you to the identity : 1,2,3,4,5....

- for what m is the identity on the m^{th} power? mod $\underbrace{5, 7, 11, 13, 17}_{\text{odd \#s, prime \#s.}}$, 3

- Mod 3 :

	1	2
^2	1	1
^3	1	2

for mod m, where m is prime, identity row is on the m^{th} power

Prime numbers

- Theorem: If p is prime, then X^p ⇒ $X^p \equiv X \mod p$
  (X ↑ any #; ^{p} ↑ raise it to the p power,)

- The row before: $X^{p-1} \equiv 1 \mod p$
  ex. the 6^{th} row for 7
  (6 ↑ power; 7 ↑ mod)

$$\boxed{\begin{array}{c} a \cdot c \equiv b \cdot c \mod m \\ \Uparrow \\ a \equiv b \mod m \end{array}}$$ → we need to talk about this.

Theorem: Little Fermat's Theorem :

only for prime mods

$$\boxed{\text{If } p \text{ is prime, then} \quad x^{p-1} \equiv 1 \mod p}$$

power

$$x^{p-1} \equiv 1$$

↓

any #