Announcements: 1) Use the Zoom meeting login for this week (posted on the deadlines file). Zoom seems to work better for me (I meet with friends over Zoom), so maybe it's Google and not the internet that doesn't like me.

2) Check out the PCS account on Instagram: https://www.instagram.com/pcsofgv/ I still have a few post ideas but I need more ideas for later too. Let me know if you have some cool memes, or other stuff to post.

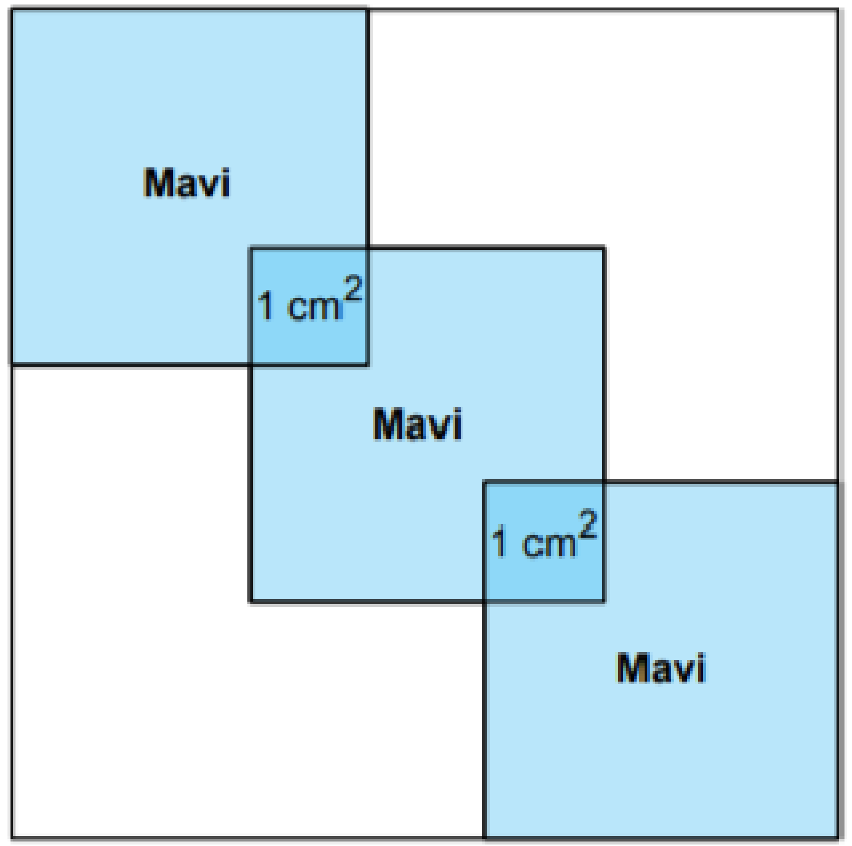
3) For fun: My nephew took a high school entrance exam two weeks ago. I'm including a problem from the test (the others aren't much easier) with the translation below.

Question: In the given picture, three blue squares are given inside a large square. If the area of the white space is 6x^2+36x+54, what is the circumference of the large square?

4) One more Q, this time a NT Q: Check out the 2nd example problem on this page about GRE prep: http://digitaleditions.walsworthprintgroup.com/publication/?m=7656&i=529803&p=24

And, I definitely don't agree with the authors about this problem being difficult to do in general. What do you think? And I think number 3 is also similarly not hard.

19. Kare şeklindeki boş bir panoya kare şeklindeki üç eş mavi karton, köşegenleri panonun köşegeni ile çakışacak şekilde aşağıdaki gibi yerleştirilmiştir.



Panoda boş bırakılan bölgelerin alanları toplamı $6x^2 + 36x + 54$ santimetrekaredir. Kartonların üst üste gelen bölgelerinin her biri, alanları 1 cm^2 olan karesel bölgelerdir.

Buna göre panonun çevresinin uzunluğunu santimetre cinsinden veren cebirsel ifade aşağıdakilerden hangisidir?

A) $12x + 40$ B) $12x + 36$ C) $12x + 32$ D) $12x + 28$

1 a,b

Use the Chinese Remainder Theorem method to solve the following systems of congruence equations:

a.
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod 7$

Since we only have 2 modulli, n/n_1 = 7 and n/n_2 = 5. s_1 is then the solution to 7*x = 3 mod 5; and s_2 is the solution to 5*x = 4 mod 7.

This gives us that s_1 = 4; and s_2 = 5. So then our solution is (n/n_1) s_1 + (n/n_2) s_2 = 7 * 4 + 5 * 5 = 28 + 25 = 53. Which we can see does equal 3 mod 5 and 4 mod 7.

And, this is modulo what number? In other words, is this the least residue solution?

b.
$x \equiv 4 \pmod 9$
$x \equiv 5 \pmod{14}$

Since we only have 2 modulli, n/n_1 = 14 and n/n_2 = 9. s_1 is then the solution to 14*x = 4 mod 9; and s_2 is the solution to 9*x = 5 mod 14.

This gives us that s_1 = 8; and s_2 = 13. So then our solution is (n/n_1) s_1 + (n/n_2) s_2 = 14 * 8 + 9 * 13 = 112 + 117 = 229. Which we can see does equal 4 mod 9 and 5 mod 14.

- Miah :)

1c

1. Use the Chinese Remainder Theorem method to solve the following systems of congruence equations:

c. $$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv -2 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

First we rewrite as: $\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned}$.

From the Chinese Remainder Theorem we recall that $x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_rM_ry_r$ such that $m_1, m_2, \ldots, m_r$ is a collection of pairwise relatively prime integers and $y_1, y_2, \ldots, y_r$ are the respective inverses. Then the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1m_2 \ldots m_r$ and the solution is:

$$x = a_1M_1y_1 + a_2M_2y_2 - \cdots + a_rM_ry_r$$

We let $M = 3 \cdot 5 \cdot 7 = 105$ and

$$\begin{aligned} M_1 &= \frac{M}{m_1} = \frac{105}{3} = 35 \\ M_2 &= \frac{M}{m_2} = \frac{105}{5} = 21 \\ M_3 &= \frac{M}{m_3} = \frac{105}{7} = 15. \end{aligned}$$

We solve for the inverse of $M_1y_1 \equiv 1 \pmod 3 \to y_1 = 2$,
then the inverse of $M_2y_2 = 1 \pmod 5 \to y_2 = 1$
and the inverse of $M_3y_3 \equiv 1 \pmod 7 \to y_3 = 1$.
Using substitution into $x = a_1M_1y_1 + a_2M_2y_2 - \cdots + a_rM_ry_r$

$$\begin{aligned} x &= (1 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (4 \cdot 15 \cdot 1) \\ &= 70 + 63 + 60 \\ &= 193. \end{aligned}$$

This means

$$x = 193 \pmod{105} = 88$$

$$x \equiv 88 \pmod{105}.$$

Cy

1d

$$x \equiv 3 \pmod 5 \qquad 7\cdot 9\, x_1 \equiv 3 \pmod 5 \qquad x_1 \equiv 1 \pmod 5$$

$$x \equiv 4 \pmod 7 \longrightarrow 5\cdot 9\, x_2 \equiv 4 \pmod 7 \longrightarrow x_2 \equiv \cancel{5}\ 6 \pmod 7$$

$$x \equiv 5 \pmod 9 \qquad 5\cdot 7\, x_3 \equiv 5 \pmod 9 \qquad x_3 \equiv 4 \pmod 9$$

5*9*x2=4 (mod 7) <--> (-2)*2*x2=4 (mod 7) <-->x2=-1 (mod 7) so x2 is a bit off.

$$S_1 = 7\cdot 9\cdot 1 \qquad S_1+S_2+S_3 = 428$$

$$S_2 = 5\cdot 9\cdot \cancel{5}\ 6 \longrightarrow \boxed{x_0 \equiv \cancel{428}^{\,473} \equiv \cancel{113}^{\,158} \pmod{315}}$$

$$S_3 = 5\cdot 7\cdot 4$$

$$315 = 5\cdot 7\cdot 9$$

-Nick

1d

$$x \equiv 3 \pmod{5}$$
$$x \equiv 4 \pmod{7}$$
$$x \equiv 5 \pmod{9}$$

Bad memory approach: Suppose you don't want to memorize the whole algorithm. What's the idea behind this approach so that we can rethink it from scratch?

I'm going to write a solution as x= ( )*9*5 + ( )*7*5 + ( )*9*7 and fill in the blanks with appropriate numbers so that x satisfies the given conditions.

If we reduce x mod 5, the first two pieces disappear so I'm left with last blank*9*7=3 mod 5. This simplifies to ( )*3=3 mod5, so ( )=1.

If we reduce x mod 7, the last two pieces disappear so I'm left with first blank*9*5=4 mod 7. This simplifies to ( )*3=4 mod 7, so ( )=6.

If we reduce x mod 9, the first and last pieces disappear so I'm left with middle blank*7*5=5 mod 9. This simplifies to ( )*(-1)=5 mod 7, so ( )=-5.

So the solution is x= 1*9*7 + 6*9*5 - 5*7*5=158

2

$2 \equiv -5 \quad 2x \equiv 5 \pmod 7$

$4 \equiv -2 \quad 4x \equiv 2 \pmod 6$

$x \equiv 3 \pmod 5$

Oops... going from 4x=2 (mod 6) to x=-1 (mod 6) is not quite right because I'm missing one case: x=2 (mod 6). Instead, I should convert 4x=2(mod 6) to 2x=1(mod 3) and work with that.

$$\left.\begin{array}{l} x \equiv -1 \pmod 7 \\ x \equiv -1 \pmod 6 \end{array}\right\} x \equiv -1 \pmod{42}$$

$x \equiv 3 \pmod 5$

$x = ? \cdot 42 + ? \cdot 5$

$\rightarrow \bmod 42 \quad ? \cdot 5 = -1 \Rightarrow ? = 25$

$\rightarrow \bmod 5 \quad ? \cdot 42 = 3 \Rightarrow ? = 4$

$= 4 \cdot 42 + 25 \cdot 5 = 83 \pmod{210}$

This solution is not the only solution mod 210 because of what I wrote above. It's the only solution mod 3*5*5=105 however.

3

Solve
5x==2 mod 3.
2x==4 mod 10.
4x==7 mod9

First we solve each for x mod something and get

We get
x==1 mod 3.
x==2 mod 10.
x==4 mod9

Notice that if x is 4 mod 9 it is also 1 mod 3 so we take the more restraining 4 mod 9 and solve from here

We could also say: Same as (-1)x==2 (mod 10), so x=-2=8.

We start with 9x==2 mod 10 which is the same as 72 mod 10 so x=8

Next, we have 10x==4 mod 9 which is the same as 40 mod 9 so x=4

Putting this together we get
x=9*8 + 10*4 =
112 - 90 =
22 mod 9

Cian

4

Check that $a^6 \equiv 1 \pmod 7$ for all $a \not\equiv 0$ modulo 7

$a=1$ $1 \equiv 1 \bmod 7$ ✓

$a=2$ $64 \equiv 1 \bmod 7$ ✓

$a=3$ $729 \equiv 1 \bmod 7$ ✓

$a=4$ $4096 \equiv 1 \bmod 7$ ✓

$a=5$ $15625 \equiv 1 \bmod 7$ ✓

$a=6$ $46656 \equiv 1 \bmod 7$ ✓

Michael

5

Find $\phi(15)$ and check $a^{\phi(15)} \equiv 1 \pmod{15}$ holds for $a = 2, 4, 7$

$\phi(15) = 8 \qquad a^8 \equiv 1 \bmod 15$

$a = 2 \quad 256 \equiv 1 \bmod 15$ ✓

$a = 4 \quad 65536 \equiv 1 \bmod 15$ ✓

$a = 7 \quad 5764801 \equiv 1 \bmod 15$ ✓

As we saw, a^phi(n)=1 (mod n) for every n. But if we look at the smallest power r which works for every a, i.e. a^r=1 (mod n), phi(n) does not have to be the smallest such r.

15 is actually an example. Mod 15, a^4=1 (mod 15) holds. There are quite a few such n values where phi(n) is not the smallest power which works for all different a's.

Check out the Carmichael function (the same Carmichael as in Carmichael numbers, but a slightly different concept) : https://en.wikipedia.org/wiki/Carmichael_function

Michael

I was going to write this up but decided to use my usual trick instead: GOOGLE! And I found a solution posted by a professor from my own undergrad institution (I think this professor was hired after I graduated).

http://www.fen.bilkent.edu.tr/~franz/nt/ch7.pdf

Page 2, proof of Theorem 7.1. The notation (Z/mZ)^x means all the invertible elements modulo m.

Last page