MTH 452 HW3

Sunday, February 25, 2024 8:54 AM

p.189 #4, 5, 10, 11, 12, 13, 14, 15, 16

(GS) p.190 #27, 28

$a^{p-1} \bmod p = 1$

$a^p \bmod p = a \bmod p$

Fermat thm ↑

---

p.189

#4 remainder of 3^{47} when div by 23

Soln: $47 = 2(23)+1$

⇓

$3^{47} = 3^{2(23)+1} = (3^{23})^2 \cdot 3$

⇓ $3^{23} \bmod 23 = 3 \bmod 23$

same thing!

$3^{47} \bmod 23 = (3^{23})^2(3) \bmod 23$

$= (3)^2(3) \bmod 23$

$= 27 \bmod 23$

$= 4$

#5 $37^{49} \bmod 7$

Soln:

$49 = 7^2$ (7 copies)

$37^{49} = 37^7 \, 37^7 \, 37^7 \cdots 37^7$

$= (37^7)^7$

But $37^7 \bmod 7 = 37 \bmod 7 = 2$

So

$37^{49} \bmod 7 = (37^7)^7 \bmod 7$

$= 2^7 \bmod 7$ (apply fermat thm, a=37)

$= 2$ (apply fermat thm a=2)

Thm 20.12

$m \in \mathbb{Z}^+$; $a, b \in \mathbb{Z}_m$

$d = \gcd(a, m)$

$ax \bmod m = b$

iff

$d | b$ (& there's d solns)

#11 Solve $2x \bmod 4 = 6$

Soln: $d = \gcd(2,4) = 2$

⇓ d divides 6

d = 2 solns

x	2x mod 4	
0	0	
1	2	✓
2	0	
3	2	✓

⇒ solns are $x = 1, 3$

#12 $22x \bmod 15 = 5$

Soln: $d = \gcd(22, 15) = 1$

⇓ d divides 5

d = 1 soln

x	22x mod 15
0	0
1	7
2	14
3	6
4	13
5	5 ✓

⇒ $x = 5$

don't need to keep looking!

36 → 2, 18 → 9, 2 → 3, 3

24 → 12, 2 → 6, 2 → 3, 2

#13 $36x \bmod 24 = 15$

Soln: $d = \gcd(36, 24) = 12$

⇓ d does NOT divide 15

No soln!

Input

Table[(36 x) mod 24, {x, 0, 14}]

Result

x	(36 x) mod 24
0	0
1	12
2	0
3	12
4	0
5	12
6	0
7	12
8	0
9	12
10	0
11	12
12	0
13	12
14	0

#14 $45x \bmod 24 = 15$

$d = \gcd(45, 24) = 3$

⇓ 3 divides 15

d = 3 solns

Input

Table[(45 x) mod 24, {x, 0, 23}]

Result

outputs of 45x mod 24 → {0, 21, 18, 15, 12, 9, 6, 3, 0, 21, 18, 15, 12, 9, 6, 3, 0, 21, 18, 15, 12, 9, 6, 3}

↑ x=3 ↑ x=11 ↑ x=19

#15 $39x \bmod 9 = 125$

$d = \gcd(39, 9) = 3$

⇓ 3 does NOT divide $125 = 5^3$

NO SOLN

39 → 3, 13

125 mod 9 = 8

Input

Table[(39 x) mod 9, {x, 0, 8}]

Result

x	0	1	2	3	4	5	6	7	8
(39 x) mod 9	0	3	6	0	3	6	0	3	6

#16 $41x \bmod 9 = 125$

125 mod 9 = 8

⇓

$d = \gcd(41, 9) = 1$

⇓ 1 divides 125

d = 1 soln exists!

Input

Table[(41 x) mod 9, {x, 0, 8}]

Result

x	0	1	2	3	4	5	6	7	8
(41 x) mod 9	0	5	1	6	2	7	3	8	4

x = 7 is the soln

---

grad students

p.190 #27 Show that 1 and p−1 are the only elements of $\mathbb{Z}_p$ that are their own mult. inverse.

Soln: This is asking to show that

$x^2 - 1 \bmod p = 0$

has only 2 solns ~ $x = 1$ and $x = p-1$.

idea being $x^2 = 1 \bmod p$ is precisely "x^2 is 1" in mod p

First we show they are solns:

x=1: $1^2 - 1 \bmod p = 0 \bmod p = 0$ ✓

x=p−1: $(p-1)^2 - 1 \bmod p = (p^2 - 2p + 1) - 1 \bmod p$

$= p(p-2) \bmod p$

$= 0 \bmod p$

Since

$x^2 - 1 \bmod p = 0$

means

p divides $x^2 - 1 = (x-1)(x+1)$

means

p divides x−1 or p divides x+1

⇓ ⇓

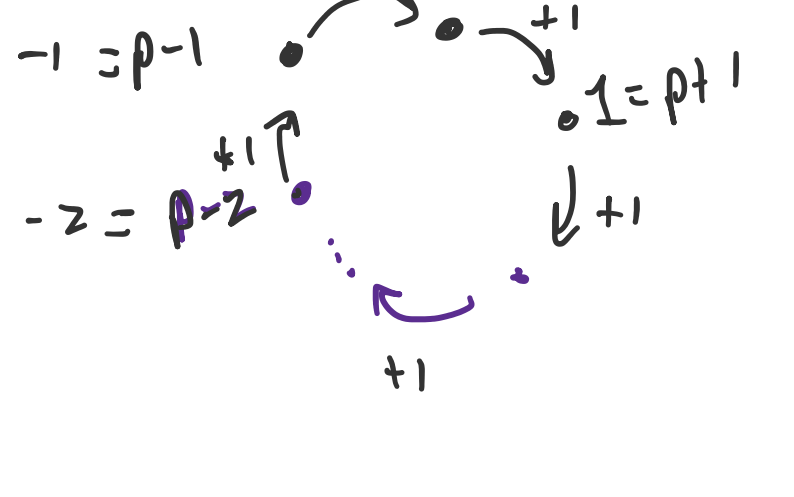
$x - 1 = pl$ for some l | $x + 1 = pl$ for some l

⇓ ⇓

$x - 1 \bmod p = 0$ | $x = -1 \bmod p$

⇓ ⇓

$x = 1 \bmod p$ | $x = p - 1$



⇓

these were the two only possibilities