CIS 3362 11/19/25

1) Give Back Quizzes ✓

2) Quiz Feedback

Q1,2,3 - Similar last year's mode (29 or 30) ~ B

Q4 - forgot p formula adding a Point to itself (37-40) ~ A

Q5 - bonus qs (1 person got this one)

$(3^5)^6 \neq 3^5 \times 3^6$ Different

$3^5 \times 3^6 = 3^{5+6} = 3^{11}$ but

$(3^5)^6 = 3^5 \times 3^5 \times 3^5 \times 3^5 \times 3^5 \times 3^5 = 3^{5(6)} = 3^{30}$

$\lambda = \frac{3x_p^2 + a}{2y_p}$

cont do ~~$x_p - x_p$~~ ~~$y_p - y_p$~~ / $x_p - x_p$ Stuck!

$\frac{22}{2} \bmod p$

$\equiv \frac{11}{1} \bmod p$

$\equiv 11 \bmod p$

$\frac{28}{8} \bmod p$

$\equiv \frac{7}{2} \bmod p$

$\equiv 7 \times 2^{-1} \bmod p$

Q5 - who spent time on their own to look @ my code.

Meta Point

numbits

$p = 1\ 0\ 1\ 1$ [_ _ _ _ _ _ _ _ _ _ _ _ _ _ _]

$p >> numbits$

1011 = limit (11)

it's safe to set these bits to 0 through 10

all # form 1010 ____16 bits____ $< p$

potential x = 0000 ____msg____

Q: Does this # have a matching y?

$(0 << 16) + msg = 0 + msg$

$(1 << 16) + msg = 2^{16} + msg$

$(2 << 16) + msg = 2 \times 2^{16} + msg$

$(3 << 16) + msg = 3 \times 2^{16} + msg$

numbits

more generally I try

$msg + ,\ msg + 2^{NB},\ msg + 2 \times 2^{NB},\ msg + 3 \times 2^{NB}, \ldots,$

$msg + (limit - 1) \times 2^{NB}$

$$y^2 = x^3 + ax + b \mod p$$

1. Calc $c = x^3 + ax + b \mod p$
2. Is there a solution to $y^2 = c$?

Only if $p \equiv 3 \mod 4$ ($p = 79$)

If $c^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (i.e. $\not\equiv 0 \mod p$) NO SOL

If $c^{\frac{p-1}{2}} \equiv 1 \mod p$ then sol

$$y = c^{\frac{p+1}{4}} \mod p$$

Quiz 5 QS

First try $x = 0$: $0 \times 2^4 + 11 = 11$

$\frac{79-1}{2} = 39$: $11 \equiv 11$ → if 1 good, if −1 bad

$x = 11$, $c = 11^3 + 1 \cdot 11 + 1$

$= 1331 + 11 + 1$

$= 0$ $\quad y = 0$

my code doesn't accept $x = 11, y = 0$

Next do $16 + 11 = 27$, $27^3 + 27 + 1 \equiv 40 \mod 79$

Since $40^{39} \equiv 1 \mod 79$, this works.

Ans is $y = 40^{20} \equiv 44 \mod 79$

Final pt is (27, 44)