

1) Give Back Quizzes ✓

2) Quiz Feedback

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

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

Q5 - bonus qs (1 person sat this one)

$$(3^5)^6 \neq 3^5 \times 3^6 \quad \text{Different}$$

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

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

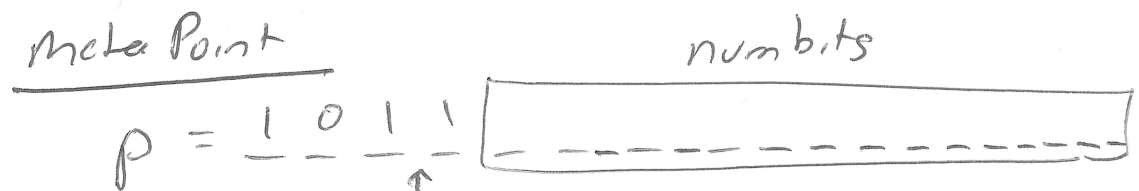
$$\lambda = \frac{3 \times p^2 + a}{2y_p}$$

can't do ~~$\frac{y_p - y_p}{x_p - x_p}$~~
stuck!

$$\begin{aligned} & \frac{22}{2} \pmod{p} \\ & \equiv \frac{11}{1} \pmod{p} \\ & \equiv 11 \pmod{p} \end{aligned}$$

$$\begin{aligned} & \frac{28}{8} \pmod{p} \\ & \equiv \frac{7}{2} \pmod{p} \\ & \equiv 7 \times 2^{-1} \pmod{p} \end{aligned}$$

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



$p \gg \text{num bits}$

1011 = limit (11)

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

all # form 1010 16 bits $< p$

pot $x = 0000$ msg
 ential

Q: Does this # have a matching y?

$$\underline{(0 < 16)} + \text{msg} = 0 + \text{msg}$$

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

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

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

more generally I try

num bits

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

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

$$y^2 = x^3 + ax + b \pmod{p}$$

1. Calc $c = x^3 + ax + b \pmod{p}$

2. Is there a solution to $y^2 = c$?

Only if $p \equiv 3 \pmod{4}$
 $p = 79$

if $c^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ NO SOL
 $\not\equiv 0 \pmod{p}$

if $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then sol
 $y = c^{\frac{p+1}{4}} \pmod{p}$

Q25 Q5

~~First try $x = 0 \times 2^4 + 11 = 11$
 $11^{\frac{79-1}{2}} = 11$ if 1 good
if -1 bad~~

$x = 11, c = 11^3 + 1 \cdot 11 + 1$
 $= 1331 + 11 + 1$
 $= 0$

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

Find pt is

(27, 44)

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

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

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