

1) Given $\alpha \in \mathbb{Z}_p^*$ is a primitive element. Using the theorem given in question find the smallest primitive element module 97.

$$2^{48} \pmod{97} = 1$$

$$3^{48} \pmod{97} = 1$$

$$4^{48} \pmod{97} = 1$$

$$5^{58} \pmod{97} = 96 \quad \text{and} \quad 5^{32} \pmod{97} = 35$$

\Rightarrow Therefore the smallest primitive root module 97 is 5.

2)

a) Denote $d = \gcd(p-1, q-1)$, $p-1 = p'd$ & $q-1 = q'd$
Then,

$\lambda(n) = p'q'd = (p-1)q' = p'(q-1)$ we have
that $ab \equiv 1 \pmod{\lambda(n)}$, so

$$ab = k\lambda(n) + 1 = k(p-1)q' + 1 \quad \text{for some positive integer } k.$$

$$\text{Then, } x^{ab} \equiv x^{k(p-1)q'+1} \pmod{p} \equiv x \pmod{p}$$

$$\text{Similarly, } x^{ab} \equiv x^{k(q-1)p'+1} \pmod{q} \equiv x \pmod{q}$$

Since $x^{ab} \equiv x \pmod{P}$ and $x^{ab} \equiv x \pmod{q}$, it follows immediately that $x^{ab} \equiv x \pmod{n}$.

$$b) d = 6, \lambda(n) = 468 \quad \varphi(n) = 2868$$

$$b^{-1} \pmod{\lambda(n)} = 67 \quad b^{-1} \pmod{\varphi(n)} = 2467$$

$$③ 28702 = (2)^1 (113)^1 (127)^1$$

we find that,

$$\log_5 8563 \equiv 1 \pmod{2},$$

$$\log_5 8563 \equiv 67 \pmod{113}$$

$$\log_5 8563 \equiv 99 \pmod{127}$$

Using the Chinese remainder theorem, $\log_5 8563 \equiv 3903$

$$\Rightarrow 31152 = (2)^4 (11)^1 (3)^1 (59)^1$$

$$\log_{10} 12611 \equiv 14 \pmod{16}, \log_{10} 12611 \equiv 2 \pmod{3}$$

$$\log_{10} 12611 \equiv 8 \pmod{11}, \log_{10} 12611 \equiv 51 \pmod{59}$$

Using the Chinese remainder theorem, $\log_{10} 12611 \equiv 17102$

4]

a) Points on the elliptic curve $y^2 = x^3 + x + 28$
 over \mathbb{Z}_{11} are made make a table of x ,
 $x^3 + x + 28 \pmod{\mathbb{Z}_{11}}$, quadratic residues of y pts.

By doing this, we get 72 no. of pts.

b) If E were cyclic, there would be pts having
 order 72, but there are no such pts.

c) The maximum order of a point is 36. ($4, 5$)
 is one point having order 36.

[E is isomorphic to $\mathbb{Z}_{36} \times \mathbb{Z}_2$.]

5]

$$\begin{aligned} \text{First, we compute, } k &= (x_1 - x_2)(\delta_1 - \delta_2) \pmod{P-1} \\ &= -22425 \times (10915)^{-1} \pmod{31866} \\ &= 1165 \end{aligned}$$

To determine a , we will solve the congruence

$$ya \equiv x_1 - k\delta_1 \pmod{P-1} \text{ for } a.$$

$$\begin{aligned} \text{This congruence simplifies to } 23972a &\equiv 23764 \pmod{31866} \\ & \quad (\text{mod } 31866) \end{aligned}$$

We have that $\gcd(23972, 31846) = 2$ &

$2 \mid 23972$, So the congruence is equivalent to

$$\begin{aligned} 11986a &\equiv 11852 \times 11986^{-1} \pmod{15923} \\ &\equiv 7459 \pmod{15923} \end{aligned}$$

$$\begin{aligned} \text{Therefore, } a &= 7459 \text{ or } a = 7459 + (P-1)/2 \\ &= 23382 \end{aligned}$$

By computing $x^{7459} \pmod{P} = 25703 = B$

& $x^{23382} \pmod{P} = 6144 \neq B$, we see that $\boxed{x = 7459}$

c)

a) Signature $(20679, 11082)$ on the msg $x = 20543$

$$\begin{aligned} 5^{20543} \pmod{31847} &= 20688 \\ &= 26379^{20679} 20679^{11082} \pmod{31847} \end{aligned}$$

b) by solving an instance of discrete logarithm

$$a = \log_5 26379 = 7973$$

c) To determine k , we will solve the congruence

$$k\delta \equiv x - ax \pmod{P-1}$$

for k . This congruence simplifies to

$$11082k \equiv 13618 \pmod{31846}$$

$$\text{g.c.d}(11082, 31846) = 2 \quad \text{and} \quad 2 \mid 13618,$$

So the congruence is equivalent to

$$5541k \equiv 6809 \pmod{15923}$$

This congruence has the solution,

$$k \equiv 6809 \times 5541^{-1} \pmod{15923} \equiv 3464 \pmod{15923}$$

$$\text{Therefore, } k = 3464 \text{ or } k = 7459 + (P-1)/2 = 19387$$

By computing $x^{3464} \pmod{P} \equiv 11168 \neq \gamma$ &
 $x^{19387} \pmod{P} \equiv 20679 = \gamma$, we can see that

$$\boxed{k = 19387}$$