Math 116 HW2 Jun Ryu

1) Factor 46375 by hand.

$$\frac{46375}{5} = 9275 \to \frac{9275}{5} = 1855$$

$$\to \frac{1855}{5} = 371 \to \frac{371}{7} = 53$$

So, $46375 = 5^3 \cdot 7 \cdot 53$

$\Rightarrow \text{ord}_3(46375) = \boxed{0}$

$\text{ord}_5(46375) = \boxed{3}$

$\text{ord}_7(46375) = \boxed{1}$

$\text{ord}_{11}(46375) = \boxed{0}$

2) a) We have $a = p^{\text{ord}_p(a)} A$ and

$b = p^{\text{ord}_p(b)} B$, where

$A, B \in \mathbb{N}$ s.t. $p \nmid A$ and $p \nmid B$

Then, we have

$$ab = p^{\text{ord}_p(a)} A \cdot p^{\text{ord}_p(b)} B = p^{\text{ord}_p(a) + \text{ord}_p(b)} \cdot AB$$

Since $p \nmid AB$, $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$ ✓

b) WLOG, let's claim $ord_p(a) \geq ord_p(b)$

We have,

$$a+b = p^{ord_p(a)} A + p^{ord_p(b)} B$$

$$= p^{ord_p(b)} \left(p^{ord_p(a) - ord_p(b)} A + B \right)$$

From this, we know

$$p^{ord_p(b)} \mid a+b \Rightarrow ord_p(a+b) \geq ord_p(b)$$

Since we had that $ord_p(a) \geq ord_p(b)$,

$$ord_p(a+b) \geq ord_p(b) = \min\{ord_p(a), ord_p(b)\}$$

We could similarly prove $ord_p(a+b) \geq ord_p(a)$ if $ord_p(b) \geq ord_p(a)$. ✓

c) WLOG, we claim $ord_p(a) > ord_p(b)$

Using the same setup as part b), we have

$$a+b = p^{ord_p(b)} \left(p^{ord_p(a) - ord_p(b)} A + B \right)$$

Since $p \mid p^{ord_p(a) - ord_p(b)} A$, but $p \nmid B$,

$$p \nmid \left(p^{ord_p(a) - ord_p(b)} A + B \right)$$

Thus, $p^{ord_p(b)}$ is the largest power of p that divides $a+b$

$$\Rightarrow ord_p(a+b) = ord_p(b) = \min\{ord_p(a), ord_p(b)\}$$

Again, we can similarly prove $ord_p(a+b) = ord_p(a)$ by considering $ord_p(b) > ord_p(a)$. ✓

3) a) Calculate $11u + 47v = 1$

$$\begin{pmatrix} 47 = 11 \cdot 4 + 3 \\ 11 = 3 \cdot 3 + 2 \\ 3 = 2 \cdot 1 + 1 \end{pmatrix} \qquad \begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 2 &= 11 - 3 \cdot 3 \\ 3 &= 47 - 11 \cdot 4 \end{aligned}$$

$$1 = 3 - (11 - 3 \cdot 3)$$

$$\Rightarrow 1 = (47 - 11 \cdot 4) - (11 - (47 - 11 \cdot 4) \cdot 3)$$

$$\Rightarrow 1 = 47 \cdot 4 - 11 \cdot 17$$

$$(u, v) \Rightarrow (-17, 4)$$

$\Rightarrow 11^{-1} \equiv -17 \equiv \boxed{30} \pmod{47}$

b) by fast powering algorithm,

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

$$11^{-1} \equiv 11^{45} \pmod{47}$$

$$11^{2} \equiv 27 \pmod{47}$$

$$11^{4} = (11^{2})^{2} \equiv 24 \pmod{47}$$

$$11^{8} = (11^{4})^{2} \equiv 12 \pmod{47}$$

$$11^{16} = (11^{8})^{2} \equiv 3 \pmod{47}$$

$$11^{32} = (11^{16})^{2} \equiv 9 \pmod{47}$$

$$11^{45} \equiv 11^{32} \cdot 11^{8} \cdot 11^{4} \cdot 11 \equiv 9 \cdot 12 \cdot 24 \cdot 11$$

$$\equiv \boxed{30} \pmod{47}$$

4) a) i) in $\mathbb{F}_7$, $a^6 \equiv 1 \pmod 7$

if a not primitive $\Rightarrow$ $ord(a) \mid 6$ but $ord(a) \neq 6$. So, $ord(a) \mid 6/2$ or $ord(a) \mid 6/3$

If $a^2 \not\equiv 1$, $a^3 \not\equiv 1$, then a is primitive:

$$2^2 \equiv 4 \pmod 7, \quad 2^3 \equiv 1 \pmod 7$$

So, 2 is NOT primitive

ii) in $\mathbb{F}_{13}$, $a^{12} \equiv 1 \pmod{13}$

by the same logic as above,

if $a^4 \not\equiv 1$ & $a^6 \not\equiv 1$, then a is primitive

(since $12 = 2^2 \cdot 3$)

$2^4 \equiv 3 \pmod{13}$, $2^6 \equiv 12 \pmod{13}$

2 is primitive

iii) in $\mathbb{F}_{19}$, $a^{18} \equiv 1 \pmod{19}$

if $a^6 \not\equiv 1$ & $a^9 \not\equiv 1$, then a is primitive

(since $18 = 2 \cdot 3^2$)

$2^6 \equiv 7 \pmod{19}$, $2^9 \equiv 18 \pmod{19}$

2 is primitive

iv) in $\mathbb{F}_{23}$, $a^{22} \equiv 1 \pmod{23}$

if $a^2 \not\equiv 1$ & $a^{11} \not\equiv 1$, then a is primitive

(since $22 = 2 \cdot 11$)

$2^2 \equiv 4 \pmod{23}$, $2^{11} \equiv 1 \pmod{23}$

2 is NOT primitive

b) in $\mathbb{F}_{29}$, $a^{28} \equiv 1 \pmod{29}$

if $a^4 \not\equiv 1$ & $a^{14} \not\equiv 1$, then a is primitive (since $28 = 2^2 \cdot 7$)

we test $a = 2$

$2^4 \equiv 16 \pmod{29}$, $2^{14} \equiv 28 \pmod{29}$

So 2 is primitive.

in $\mathbb{F}_{41}$, $a^{40} \equiv 1 \pmod{41}$

if $a^{20} \not\equiv 1$ & $a^8 \not\equiv 1$, then a is primitive (since $40 = 2^3 \cdot 5$)

we test $a = 6$ ($6^2 \equiv 36$, $6^4 \equiv 25$)

$$6^8 \equiv 10 \pmod{41}, \quad 6^{20} \equiv 6^8 \cdot 6^8 \cdot 6^4$$
$$\equiv 10 \cdot 10 \cdot 25$$
$$\equiv 18 \cdot 25$$
$$\equiv 40 \pmod{41}$$

So, 6 is primitive.

c) in $\mathbb{F}_{11}$, $a^{10} \equiv 1 \pmod{11}$

If $a^2 \not\equiv 1$, $a^5 \not\equiv 1$, then a is primitive (since $10 = 2 \cdot 5$)

$a=2$: $2^2 \equiv 4$, $2^5 \equiv 10$ ✓

$a=3$: $3^2 \equiv 9$, $3^5 \equiv 1$ ✗

$a=4$: $4^2 \equiv 5$, $4^5 \equiv 1$ ✗

$a=5$: $5^2 \equiv 3$, $5^5 \equiv 1$ ✗

$a=6$: $6^2 \equiv 3$, $6^5 \equiv 10$ ✓

$a=7$: $7^2 \equiv 5$, $7^5 \equiv 10$ ✓

$a=8$: $8^2 \equiv 9$, $8^5 \equiv 10$ ✓

$a=9$: $9^2 \equiv 4$, $9^5 \equiv 1$ ✗

$a=10$: $10^2 \equiv 1$, $10^5 \equiv 10$ ✗

all in (mod 11)

primitive roots are $\{2, 6, 7, 8\}$

$\phi(10) = \{1, 3, 7, 9\}$

Both have 4 elements ✓

5) a) $e_K(m) \equiv K_1 \cdot m + K_2 \pmod{p}$

$$e_K(204) \equiv 34 \cdot 204 + 71 \pmod{541}$$
$$\equiv 7007$$
$$\equiv \boxed{515} \pmod{541}$$

$$d_K(c) \equiv K_1^{-1} \cdot (c - K_2) \pmod{p}$$

Using sage,

$$\text{xgcd}(34, 541) = (1, -175, 11)$$

$$\Rightarrow 34(-175) + 541(11) = 1$$

so $34^{-1} \equiv -175 \equiv 366 \pmod{541}$

$$d_K(431) \equiv 366 \cdot (431 - 71)$$
$$\equiv \boxed{297} \pmod{541}$$

b) What Eve has:

$$324 \equiv K_1 \cdot 387 + K_2 \pmod{601} \quad (1)$$

& $$381 \equiv K_1 \cdot 491 + K_2 \pmod{601} \quad (2)$$

(2) − (1) gives us

$$57 \equiv K_1 \cdot 104 \pmod{601}$$

$K_1 \equiv 57 \cdot 104^{-1}$

Using sage, we get $104^{-1} \equiv 549 \pmod{601}$

$K_1 \equiv 57 \cdot 549 \equiv \boxed{41} \pmod{601}$

Now, plug into (1)

$324 \equiv 41 \cdot 387 + K_2 \pmod{601}$

$K_2 \equiv \boxed{83} \pmod{601}$

We use K_1 & K_2 to encrypt $m_3 = 173$

$e_K(173) \equiv 41 \cdot 173 + 83 \pmod{601}$

$\equiv \boxed{565} \pmod{601}$

6) a) i) $e_K\begin{pmatrix}2\\1\end{pmatrix} \equiv \begin{pmatrix}1 & 3\\2 & 2\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix} + \begin{pmatrix}5\\4\end{pmatrix} \pmod{7}$

$\equiv \begin{pmatrix}5\\6\end{pmatrix} + \begin{pmatrix}5\\4\end{pmatrix} \equiv \begin{pmatrix}10\\10\end{pmatrix} \equiv \boxed{\begin{pmatrix}3\\3\end{pmatrix}} \pmod{7}$

ii) $K_1^{-1} = -4\begin{pmatrix}2 & -3\\-2 & 1\end{pmatrix} \pmod{7}$

inverse of -4 is $5 \Rightarrow -4 \cdot 5 \equiv 1 \pmod{7}$

$5\begin{pmatrix}2 & -3\\-2 & 1\end{pmatrix} \equiv \begin{pmatrix}10 & -15\\-10 & 5\end{pmatrix} \equiv \boxed{\begin{pmatrix}3 & 6\\4 & 5\end{pmatrix}} \pmod{7}$

iii) $d_K\begin{pmatrix}3\\5\end{pmatrix} \equiv \begin{pmatrix}3 & 6\\ 4 & 5\end{pmatrix}\cdot\left(\begin{pmatrix}3\\5\end{pmatrix} - \begin{pmatrix}5\\4\end{pmatrix}\right) \pmod 7$

$$\equiv \begin{pmatrix}3 & 6\\ 4 & 5\end{pmatrix}\cdot\begin{pmatrix}-2\\1\end{pmatrix} \pmod 7$$

$$\equiv \begin{pmatrix}0\\-3\end{pmatrix} \equiv \boxed{\begin{pmatrix}0\\4\end{pmatrix}} \pmod 7$$

b) Let $K_1 = \begin{pmatrix}x & y\\ z & w\end{pmatrix}$, $K_2 = \begin{pmatrix}u\\v\end{pmatrix}$

Then, we have the following for m_1 & c_1:

$$\begin{pmatrix}1\\8\end{pmatrix} \equiv \begin{pmatrix}x & y\\ z & w\end{pmatrix}\begin{pmatrix}5\\4\end{pmatrix} + \begin{pmatrix}u\\v\end{pmatrix}$$

$$\equiv \begin{pmatrix}5x+4y+u\\ 5z+4w+v\end{pmatrix} \pmod{11}$$

$$\Rightarrow \begin{aligned} 5x+4y+u &\equiv 1 \\ 5z+4w+v &\equiv 8 \end{aligned} \pmod{11}$$

From m_2 & c_2:

$$\begin{aligned} 8x+10y+u &\equiv 8 \\ 8z+10w+v &\equiv 5 \end{aligned} \pmod{11}$$

From m_3 & c_3:

$$\begin{aligned} 7x+y+u &\equiv 8 \\ 7z+w+v &\equiv 7 \end{aligned} \pmod{11}$$

First, we solve for x, y, u

$$\left[\begin{array}{ccc|c} 5 & 4 & 1 & 1 \\ 8 & 10 & 1 & 8 \\ 7 & 1 & 1 & 8 \end{array}\right] \pmod{11}$$

gives us $(x, y, u) = (3, 7, 2)$

Then, solving for (z, w, v) gives us $(4, 3, 9)$

Thus, $K_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \boxed{\begin{pmatrix} 3 & 7 \\ 4 & 3 \end{pmatrix}}$, $K_2 = \begin{pmatrix} u \\ v \end{pmatrix} = \boxed{\begin{pmatrix} 2 \\ 9 \end{pmatrix}}$

7. $2^x \equiv 13 \pmod{23}$

We have that $2^7 \equiv 128 \equiv 13 \pmod{23}$

Thus, $\boxed{x = 7}$ ✓

8. We have $B = g^b \equiv 2^{871} \pmod{1373}$

$\equiv \boxed{805} \pmod{1373}$

This is what Bob sends to Alice

Their secret shared value is $A^b \pmod{p}$, Which is (using sage)

$$974^{871} \pmod{1373} \equiv \boxed{397} \pmod{1373}$$

Using sage, Alice's secret exponent:

$$B^a \equiv A^b \pmod{1373}$$

$$805^a \equiv 397 \pmod{1373}$$

```
In [11]: k.<a> = FiniteField(1373, impl='modn')
         (397*a).log(805)

Out[11]: 587
```

So, $a = \boxed{587}$

9) a) If the Diffie-Hellman problem requires for the value of g^{ab} to be found, we can simply see if the acquired value is equal to C.

b) Seeing Exercise 6.40, it seems like the decision D-H problem need not necessarily rely on its associated D-H problem, making some cases easier than it appears.