PSet 6 Solutions

1) a) **a=1:** $1^1 \equiv 1$, so the order is $\underline{1}$.

a=2:

$2^2 = 4$ // complete detail shown in this
$2^3 = 8$ // case; subsequent cases will be
$2^4 = 16 \equiv 3 \bmod 13$ // more brief.
$2^5 \equiv 6 \bmod 13$
$2^6 \equiv 12 \bmod 13$
$2^7 \equiv 12 \cdot 2 \equiv 11 \bmod 13$
$2^8 \equiv 2 \cdot 11 \equiv 9 \bmod 13$
$2^9 \equiv 2 \cdot 9 \equiv 5 \bmod 13$
$2^{10} \equiv 2 \cdot 5 \equiv 10 \bmod 13$
$2^{11} \equiv 2 \cdot 10 \equiv 7 \bmod 13$
$2^{12} \equiv 2 \cdot 7 \equiv 1 \bmod 13$ so the order is $\underline{12}$.

a=3: $3^2 = 9$
$3^3 = 3 \cdot 9 \equiv 1 \bmod 13$ so the order is $\underline{3}$

a=4: Multiplying by 4 repeatedly and reducing mod 13 gives the following sequence:

$4,\ 16 \equiv 3,\ 12,\ 48 \equiv 9,\ 36 \equiv 10,\ 40 \equiv 1$
$\Rightarrow$ the order is $\underline{6}$.

a=5 Powers are $5,\ 25 \equiv 12,\ 60 \equiv 8,\ 40 \equiv 1$
$\Rightarrow$ order $\underline{4}$.

a=6 Powers are $6,\ 36 \equiv 10,\ 60 \equiv 8,\ \cancel{54}\, 48 \equiv 9,\ 54 \equiv 2,\ 12,$
$72 \equiv 7,\ 42 \equiv 3,\ 18 \equiv 5,\ 30 \equiv 4,\ 24 \equiv 11,\ 66 \equiv 1.$
$\Rightarrow$ order $\underline{12}$.

$\underline{a=7}$ powers $7,\ 49\equiv 10,\ 70\equiv 5,\ 35\equiv 9,\ 63\equiv 11,\ 77\equiv 12,$
$84\equiv 6,\ 42\equiv 3\ \ 21\equiv 8,\ 56\equiv 4,\ 28\equiv 2,\ 14\equiv 1$
$\Rightarrow$ <u>order 12.</u>

$\underline{a=8}$ powers $8,\ 64\equiv 12,\ 96\equiv 5.\ 40\equiv 1$
$\Rightarrow$ <u>order 4</u>

$\underline{a=9}$ powers $9,\ 81\equiv 3,\ 27\equiv 1$
$\Rightarrow$ <u>order 3.</u>

$\underline{a=10}$ powers are $10,\ 100\equiv 9,\ 90\equiv 12,\ 120\equiv 3,\ 30\equiv 4,\ 40\equiv 1$
$\Rightarrow$ <u>order 6.</u>

$\underline{a=11}$ powers are $11,\ 121\equiv 4,\ 44\equiv 5,\ 55\equiv 3,\ 33\equiv 7,\ 77\equiv 12$
$132\equiv 2,\ 22\equiv 9,\ 99\equiv 8,\ 88\equiv 10,\ 110\equiv 6,\ 66\equiv 1$
$\Rightarrow$ <u>order 12</u>

$\underline{a=12}$ powers are $12,\ 144\equiv 1$
$\Rightarrow$ <u>order 2</u>

In summary:

a	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2

<u>NOTE.</u> You can keep the figures more manageable by reducing to a number in $\{-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6\}$ instead.

eg the orbit of 11 would be the same as the orbit of -2:

$-2,\ 4,\ -8,\ 16\equiv 3,\ -6,\ 12\equiv -1,\ 2,\ -4,\ 8\equiv -5,\ 10\equiv -3,\ 6,\ -12\equiv 1.$

I will do this in the next solution.

b) To make the figures easy to manage, I will reduce all powers to a number in $\{-7,-6,\dots,6,7\}$ instead of $\{0,1,\dots,14\}$.

$\underline{a=1}$ $\underline{\text{order } 1}$

$\underline{a=2}$ powers $2, 4, 8 \equiv -7, -14 \equiv 1$ $\Rightarrow$ $\underline{\text{order } 4}$

$a=3$ powers $3, 9 \equiv -6, -18 \equiv -3, -9 \equiv 6, 18 \equiv 3, \dots$

Note that this sequence repeats but never returns to 1.
This is because $\gcd(3,15) \neq 1$. (no order)

$\underline{a=4}$ powers $4, 16 \equiv 1$ $\Rightarrow$ $\underline{\text{order } 2}$

$a=5$: $\gcd(5,15) \neq 1$.

$a=6$: $\gcd(6,15) \neq 1$.

$\underline{a=7}$: powers $7, 49 \equiv 4, 28 \equiv -2, -14 \equiv 1$. $\Rightarrow$ $\underline{\text{order } 4}$.

$\underline{a=8}$ $(\equiv -7)$ powers $-7, 49 \equiv 4, -28 \equiv 2, -14 \equiv 1$ $\Rightarrow$ $\underline{\text{order } 4}$.

$a=9$: $\gcd(9,15) \neq 1$.

$a=10$: $\gcd(10,15) \neq 1$.

$\underline{a=11}$ $(\equiv -4)$ powers $-4, 16 \equiv 1$ $\Rightarrow$ $\underline{\text{order } 2}$.

$a=12$: $\gcd(12,15)\neq 1$.

$\underline{a=13}$ $(\equiv -2)$ powers $-2, 4, -8\equiv 7, -14\equiv 1$ $\Rightarrow$ $\underline{\text{order } 4}$

$\underline{a=14}$ $(\equiv -1)$ powers $-1, 1$ $\Rightarrow$ $\underline{\text{order } 2}$.

Summary:

a:	1	2	4	7	8	11	13	14
order:	1	4	2	4	4	2	4	2

of note: $\varphi(15)=8$, yet $a^4\equiv 1 \bmod 15$ for all a coprime with 15. This shows that $\varphi(m)$ need not be the optimal "universal exponent".

(2) $x\equiv y \bmod a$ means $a \mid (x-y)$.
$x\equiv y \bmod b$ means $b \mid (x-y)$.

Since $\gcd(a,b)=1$, this implies (by HW #3, problem 3) that $ab \mid (x-y)$. This is the same as $x\equiv y \bmod ab$, as desired.

(3) Just place each number $0,\dots,41$ in the appropriate row & column:

class mod 6 \ class mod 7	0	1	2	3	4	5	6
0	0	36	30	24	18	12	6
1	7	1	37	31	25	19	13
2	14	8	2	38	32	26	20
3	21	15	9	3	39	33	27
4	28	22	16	10	4	40	34
5	35	29	23	17	11	5	41

Note some patterns:
- to move down, add 7
- to move right, subtract 6
- to move down-right, add 1.

④ 97 is prime, so $\varphi(97) = 96$.

$$8800 = 8 \cdot 11 \cdot 10^2 = 2^3 \cdot 11 \cdot 2^2 \cdot 5^2$$
$$= 2^5 \cdot 5^2 \cdot 11 \implies \text{prime factors } 2, 5, 11.$$

So
$$\varphi(8800) = \varphi(2^5) \cdot \varphi(5^2) \cdot \varphi(11)$$
$$= (32-16) \cdot (25-5) \cdot (11-1)$$
$$= 16 \cdot 20 \cdot 10$$
$$= \underline{3200}$$

OR
$$\varphi(8800) = 8800 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} \cdot \tfrac{10}{11}$$
$$= 3200.$$

⑤ $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$

Therefore, since
$$5085 \equiv 5 \mod 40$$
it follows from Euler's theorem that

$$19^{5085} \equiv 19^5 \mod 100.$$

Now:
$$19^2 = 361 \equiv 61 \mod 100$$
$$19^3 \equiv 19 \cdot 61 \equiv 1159 \equiv 59 \mod 100$$
$$19^4 \equiv 19 \cdot 59 \equiv 1121 \equiv 21 \mod 100$$
$$19^5 \equiv 19 \cdot 21 \equiv 399 \equiv 99 \mod 100.$$

So the last two digits of 19^{5085} are "99."