Name: Solutions

Directions: Show all work. No credit for answers without work.

1. [**4 points**] Let $p = 41$ and note that p is prime. Use Fermat's Little Theorem and the fast power algorithm to find the inverse of 26 in $\mathbb{Z}_p$.

$(26)^{-1} = 26^{p-2} = 26^{39}$

$\cdot\, 26^2 = (-15)^2 = 225 = 61 = 20$

$\cdot\, 26^4 = 26^2 \cdot 26^2 = 20 \cdot 20 = 400 = -10 = 31$

$\cdot\, 26^8 = 26^4 \cdot 26^4 = (-10)(-10) = 100 = 18$

$\cdot\, 26^{16} = 26^8 \cdot 26^8 = 18 \cdot 18 = 324 = 119 = -4 = 37$

$\cdot\, 26^{32} = 26^{16} \cdot 26^{16} = (-4)(-4) = 16$

$39 = 32 + 4 + 2 + 1$

$(26)^{39} = (26)^{32} \cdot (26)^4 \cdot (26)^2 \cdot 26$

$= 16 \cdot (-10) \cdot (20) \cdot 26$

$= 16 \cdot 26 \cdot (-200) = 16 \cdot 26 \cdot 5$

$= 16 \cdot 130 = 16 \cdot 7 = 70 + 42 = 70 + 1$

$= 71 = -11 = \boxed{30}$

So the inverse of 26 is $\boxed{30}$. Check: $26 \cdot 30 = (26)(-11) = -260 - 26 = -55 - 26 = -14 - 26 = -40 = 1$ ✓.

2. [**2 parts, 2 points each**] Let $a = 49$ and let $m = 113$.

(a) Compute enough powers of a to determine the order of a in $\mathbb{Z}_m$. (Hint: the order of a is at most 10.)

k	1	2	3	4	5	6	7
a^k	49	28	16	106	109	30	1

So the order of a is $\boxed{7}$.

(b) Let $n = 372032$. Use part (a) to compute a^n in $\mathbb{Z}_m$.

Note: $n = \underbrace{(53147)}_{q}(7) + 3$, so

$a^n = a^{7q+3} = a^{7q} \cdot a^3 = (a^7)^q \cdot a^3 = 1^q \cdot a^3 = a^3 = \boxed{16}$

3. [**2 points**] Let $p = 79$, and note that p is prime. According to Fermat's Little Theorem, what are the possible orders of elements in $\mathbb{Z}_p$?

Since $a^{p-1} = 1$ in $\mathbb{Z}_p$ for all $a \in \mathbb{Z}_p^*$, it follows that every order divides $p-1$. Since $p-1 = 78 = 2 \cdot 39 = 2 \cdot 3 \cdot 13$, the possible orders are:

$\boxed{1, 2, 3, 13, 6, 26, 39, 78}$.