Name: Solutions

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

1. [**2 parts, 3 points each**] Orders in $\mathbb{Z}_{13}$.

   (a) Find the order of 2 in $\mathbb{Z}_{13}$. Is 2 a primitive root?

n	0	1	2	3	4	5	6	7	8	9	10	11	12
2^n	1	2	4	8	3	6	12 (−1)	11 (−2)	9 (−4)	5 (−8)	10 (−3)	7 (−6)	1 (−12)

Since 12 is the smallest positive exponent on 2 giving 1, the order is $\boxed{12.}$

Since the order of 2 equals $|\mathbb{Z}_{13}^*|$ or $13-1$, we have that $\boxed{\text{2 is a primitive root}}$.

   (b) Find the order of 3 in $\mathbb{Z}_{13}$. Is 3 a primitive root?

n	0	1	2	3	...
3^n	1	3	9	1	

Since 3 is the smallest positive exponent on 3 giving 1, the order is $\boxed{3}$.

Since the order of 3 is less than $|\mathbb{Z}_{13}^*|$, we have that $\boxed{\text{3 is not a primitive root}}$.

2. [**4 points**] Use Fermat's Little Theorem to compute the inverse of 17 in $\mathbb{F}_{37}$..

By FLT, $1 \equiv (17)^{37-1} \equiv (17)^{36} \equiv (17)(17)^{35} \pmod{37}$. So the inverse of 17 is $(17)^{35}$.

$(17)^2 \equiv 289 \equiv 289 - \overset{37\cdot 5}{\overbrace{185}} \equiv 164 \equiv 104 - \overset{37\cdot 3}{\overbrace{111}} \equiv -7 \quad (\equiv 30)$

$(17)^4 \equiv (17)^2\cdot(17)^2 \equiv (-7)(-7) \equiv 49 \equiv 12$

$(17)^8 \equiv (17)^4\cdot(17)^4 \equiv (12)^2 \equiv 144 \equiv 144-111 \equiv 33 \equiv -4 \quad (\equiv 33)$

$(17)^{16} \equiv (17)^8\cdot(17)^8 \equiv (-4)^2 \equiv 16$

$(17)^{32} \equiv (17)^{16}\cdot(17)^{16} \equiv (16)^2 \equiv 256 \equiv 256-185 \equiv 71 \equiv 71-74 \equiv -3 \quad (\equiv 34)$

$35 = 32 + 2 + 1$

$(17)^{35} = (17)^{32}\cdot(17)^2\cdot 17 = (-3)\cdot(-7)\cdot(17) = 21\cdot 17 = 210+147 = 357$

$= 357 - 370 = -13 = \boxed{24}$.

Check: $24\cdot 17 = 240 + 168 = 408 = 408-370 = 38 = 1$ ✓.