Name: Solutions

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

1. **[5 points]** Use the fast power algorithm to compute $(15)^{101} \pmod{467}$. Normalize your answer to a value in $\{0, \ldots, 466\}$. All computation in $\mathbb{Z}_{467}$.

$15^2 = 225$

$15^4 = 225 \cdot 225 = 50625 = 189$

$15^8 = 189 \cdot 189 = 35721 = 229$

$15^{16} = 229 \cdot 229 = 52441 = 137$

$15^{32} = 137 \cdot 137 = 18769 = 89$

$15^{64} = 89 \cdot 89 = 7921 = 449$

$101 = 64 + 32 + 4 + 1$

$15^{101} = 15^{64} \cdot 15^{32} \cdot 15^4 \cdot 15 = 449 \cdot 89 \cdot 189 \cdot 15$

$= (39961)(189)(15) = (266)(189)(15)$

$= (50274)(15) = (305)(15) = 4575 = \boxed{372}$

2. Let p be the prime number 167.

   (a) **[1 point]** How many elements in $\mathbb{Z}_p$ have inverses?

Since 167 is prime, all but $0 \in \mathbb{Z}_p$ have gcd with p of 1, so everything in $\mathbb{Z}_p$ except 0 has an inverse. So $\boxed{166}$ elements have inverses.

   (b) **[3 points]** Let $a = 105$. Compute enough powers of a to find the order of a in $\mathbb{Z}_p$.

Note: Unfortunately there was a typo, p should have been 163. Full credit for reasonable answers with Given p:

k	1	2	3	4	5	6	7	8	9	10	...	83	...	166
$(105)^k$	105	3	148	9	110	27	163	81	155	76		166 or -1		1
		$\times 105$	$\times 105$	$\times 105$										

So the first power that gives 1 is 166, too long to compute by hand. The order is 166. (at least, without additional tools)

For studying purposes, with p = 163 the solution looks like:

Modulo 163:

k	1	2	3	4	5	6
$(105)^k$	105	104	162	58	59	1

So the order of 105 modulo 163 is 6.

   (c) **[1 point]** Use part (b) to find a^{-1} without additional computation.

The typo makes this problem impractical. Full credit for everyone.

For studying purposes, with p = 163, the soln looks like this: $1 = (105)^6 = (105)(105)^5 = (105)(59)$

So $(105)^{-1} = \boxed{59}$.