Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Make a multiplication table for the unit group $\mathbb{Z}_9^*$. What is $\phi(9)$?

2. Modular exponentiation in $\mathbb{Z}_7$.

   (a) Fill in the table so that row a and column k contains a^k, where $a^k \in \mathbb{Z}_7$.

a^k	0	1	2	3	4	5	6	7	$\cdots$
0	1	0	0	0	0	0	0	0	
1									
2									
3									
4									
5									
6									

   (b) The *order* of an element $a \in \mathbb{Z}_m^*$ is the smallest positive integer k such that $a^k = 1$ in $\mathbb{Z}_m$. Find the unit group $\mathbb{Z}_7^*$, and for each $a \in \mathbb{Z}_7^*$, find the order of a.

   (c) An element $a \in \mathbb{Z}_7$ is a *primitive root* if its order equals $|\mathbb{Z}_7^*|$; that is, if the sequence $a^0, a^1, a^2, \ldots$ contains each element in $\mathbb{Z}_7^*$. Use the table to find all primitive roots in $\mathbb{Z}_7^*$. Verify that the number of primitive roots equals $\phi(6)$.

3. Use the fast power algorithm to compute $2^{300} \pmod{1000}$. Show intermediate powers of 2.

4. Common divisors divide the gcd.

   (a) Let a and b be integers and let $d = \gcd(a, b)$. Prove that if ℓ is a common divisor of a and b, then $\ell \mid \gcd(a, b)$.

   (b) Let a, b, g, and m be integers such that $g^a \equiv 1 \pmod{m}$ and $g^b \equiv 1 \pmod{m}$. Prove that $g^{\gcd(a,b)} \equiv 1 \pmod{m}$.