Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets for scratch work. ***Show all your work; there will be no credit for answers without a justification.***

Total Marks 100: four questions, each worth 25.

1. Consider $G = \mathbb{F}_7^*$.

   (a) Find the generator (i.e., primitive element) for G.

   (b) Find a subgroup H of G such that $1 < |H| < |G|$, and list all the cosets of H.

   SOLUTION: (a) $G = \langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 2, 6, 4, 5, 1\}$. For (b) consider the subgroup $H = \langle 2 \rangle = \{2^1, 2^2, 2^3\} = \{2, 4, 1\}$. Here are the two distinct cosets of H: $1 \cdot H = \{2, 4, 1\}$ and $3 \cdot H = \{6, 5, 3\}$.

2. Suppose that $m \equiv 1 \pmod{b}$. What is the inverse of $b \pmod{m}$?

SOLUTION: Let $x := \frac{(m-1)^2}{b} \pmod{m}$; we know that $\frac{(m-1)^2}{b}$ is an integer since $m \equiv 1 \pmod{b}$, and so $b|(m-1)$, and so $b|(m-1)^2$. This x is our inverse; indeed:

$$bx \equiv_m b\left(\frac{(m-1)^2}{b}\right) \equiv_m (m-1)^2 \equiv_m m^2 - 2m + 1 \equiv_m 0 + 0 + 1 \equiv_m 1$$

3. Prove **Fermat's Little Theorem**: If p is prime, and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

   SOLUTION: If $\gcd(a, p) = 1$ then p does not divide a. So we can show that $\{1a, 2a, 3a, \ldots, (p-1)a\}$ are all distinct numbers $\pmod{p}$. (If $ia \equiv ja \pmod{p}$, then $p|(i-j)a$, so $p|(i-j)$, so $i = j$.)

   Therefore, $\{1a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, \ldots, (p-1)\}$.

   So $a^{p-1} \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} ai \equiv \prod_{i=1}^{p-1} i \pmod{p}$.

   But each $\{1, 2, 3, \ldots, (p-1)\}$ has an inverse $\pmod{p}$. So does their product.

4. Describe the ElGamal public key cryptosystem.

SOLUTION: §2.4, pg. 81, in the textbook:

Public Parameter Creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key Creation	
Chooses private key $1 \leq a \leq p-1$. Computes $A = g^a \pmod{p}$. Publishes the public key A.	
Encryption	
	Chooses plaintext m. Chooses random ephemeral key k. Uses Alice's public key A to compute $c_1 = g^k \pmod{p}$. and $c_2 = mA^k \pmod{p}$. Sends ciphtertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	