MATH 3540 **Name:** _____
Final

Directions

1. Complete the following questions.

---

1. Which of the following is NOT a group?

   (a) The integers under addition.

   (b) The set $\{0, 1, 2, \ldots, 27\}$ under multiplication modulo 28.

   (c) The set $\{1, 3, 7, 9\}$ under multiplication modulo 10.

   (d) The set $\{0, 1, 2, \ldots, 27\}$ under addition modulo 28.

2. The elements of $\mathbb{Z}_{15}^*$ are $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Define $f_3(x) = [x^3 \mod 15]$. What is the result of applying f_3 to the elements of $\mathbb{Z}_{15}^*$, in the order just presented?

   (a) $\{1, 8, 4, 7, 8, 11, 13, 14\}$

   (b) $\{1, 8, 4, 13, 2, 11, 7, 14\}$

   (c) $\{1, 8, 4, 8, 4, 8, 2, 14\}$

   (d) $\{1, 8, 4, 2, 13, 11, 7, 14\}$

3. Which of the following is a generator of $\mathbb{Z}_7^*$?

   (a) 2

   (b) 3

   (c) 5

   (d) 6

4. Which of the following is the multiplicative inverse of 10 modulo 15?

   (a) There is none

   (b) 2

   (c) 5

   (d) 10

5. Let G be a cyclic group of order q and with generator g. Based only on the assumption that the discrete-logarithm problem is hard for this group, which of the following problems is hard?

   (a) Given a uniform $x \in \mathbb{Z}_q$, find y such that $g^x = y$.

   (b) Find x, y such that $g^x = y$

   (c) Given a uniform $y \in G$, find x such that $g^x = y$.

   (d) Given uniform $x \in \mathbb{Z}_q$ and uniform $y \in G$, compute $y^x \cdot g$.

6. Assume "plain RSA" encryption is used with public key $(N = 33, e = 3)$. What is the encryption of the message $m = 2$?

   (a) 8

   (b) 7

   (c) 32

   (d) 10

7. What is the order of $\mathbb{Z}^*_{1261}$?

8. How many generators does the group $\mathbb{Z}^+_{13}$ contain? Explain your solution.

9. Compute $3^{2020} \mod 35$.

10. $\mathbb{Z}_{23}^*$ is a cyclic group with generator 5. Compute $DH_5(3, 10)$.

11. Suppose G is a cyclic group of order n. Assume that for an integer m between 1 and n the order of g^m is $n/\gcd(m,n)$ where g is a generator. Show that there are exactly $\phi(n)$ generators.

12. Assume El Gamal encryption, where the group being used is $\mathbb{Z}_{47}^*$ with generator 5. (This group has order 46, which is not prime. But El Gamal encryption can be defined in any cyclic group.) Assume the public key contains $h = 10$. Say an attacker sees a ciphertext $(41, 18)$ that is the encryption of some unknown message m. What is an encryption of $[5m \bmod 47]$?

13. In class we showed the following corollary:

    Take $N > 1$ and $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \mod N$.

    This implies that if $N = pq$ where p, q are relatively prime and $ed = 1 \mod \phi(N)$ then for any $x \in \mathbb{Z}_N^*$ we have $(x^e)^d = x \mod N$. Show that this holds for all $x \in \mathbb{Z}_N$. (Hint: use the Chinese Remainder Theorem)

14. True or False: Suppose π is the textbook RSA encryption scheme with parameters (N, e, d) where N is the product of two n-bit primes, along with integers e, d satisfying $ed = 1 mod(N)$. If the message m does not lie Z_N^*, can $Enc_{pk}(m)$ be decrypted given that you know the private key? Explain your answer.