M E T U
Department of Mathematics

	Elementary Number Theory I Final Exam	

Code : *Math 365* Acad. Year : *2018-2019* Semester : *Fall* Instructor : *Tolga Karayayla* Date : *7.01.2019* Time : *17.40* Duration : *120 minutes*	Last Name : First Name : Student ID : Department : Signature : **7** Questions on **4** Pages SHOW DETAILED WORK!

1	2	3	4	5	6	7		

1. (5+10+5 pts.) Let A and B be two people who want to communicate with each other using the RSA cryptosystem. Suppose that the public key of A is (k_A, n_A) and the public key of B is (k_B, n_B).
a) If A wants to send a message to B, after converting the text of the message to an integer M by replacing the letters of the alphabet by 01, 02,..., 26 and spaces between words by 27, what does A send to B as the encrypted message? (Assume that the message is short enough so that it is not necessary to break it into smaller pieces.)

b) Let S be the encrypted message that B receives from A. How does B find M?

c) Why can't a third person C easily find M even if C gets the inforation S (encrypted message) and knows the public keys of A and B?

2. (5+10 pts.) Show that $r = 5$ is a primitive root of $p = 47$.

b) Using the information $5^{10} \equiv 12 \pmod{47}$, solve the congruence $x^6 \equiv 12 \pmod{47}$ (Express the solutions as powers of 5 modulo 47).

3. (10 pts.) Use the information that 2 is a primitive root of 11 to find a primitive root r_1 of $N_1 = 11^{17}$ and a primitive root r_2 of $N_2 = 2 \cdot 11^{17}$.

4. (15 pts.) Solve $2x^2 + 7x + 4 \equiv 0 \pmod{83}$.

5. (10 pts.) Let p be an odd prime and $gcd(p^n, a) = 1$. Show that if x_1 and x_2 are two solutions of $x^2 \equiv a \pmod{p^n}$, then either $x_1 \equiv x_2 \pmod{p^n}$ or $x_1 \equiv -x_2 \pmod{p^n}$.

6. (10+10 pts.) Find the number of solutions modulo n of

a) $x^2 \equiv 16 \pmod{n}$ where $n = 105$.

b) $x^2 \equiv 149 \pmod{n}$ where $n = 5^3 7^4 11^2$.

7. (10 pts.) Find the largest $k \in \mathbb{Z}$ such that $125^k | 61 \cdot 62 \cdots 199 \cdot 200$.