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.)

The encrypted message S from A to B is calculated as

$M^{k_B} \equiv S \pmod{n_B}$ where $0 \leq S < n_B$

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

B knows that $n_B = p \cdot q$ for large and distinct primes. (B knows p and q, indeed B determines n_B by choosing these primes p and q).
Note that if M is short enough then $M < p$, $M < q$ so $\gcd(M, n_B) = 1$
thus $\gcd(S, n_B) = 1$. k_B is such that $\gcd(k_B, \varphi(n_B)) = 1$.
B calculates multiplicative inverse j of k_B modulo $\varphi(n_B) = (p-1)\cdot(q-1)$
$j \cdot k_B \equiv 1 \pmod{\varphi(n_B)} \Rightarrow j \cdot k_B = 1 + N \cdot \varphi(n_B)$ for $N \in \mathbb{Z}$.

Then B calculates $S^j \equiv x \pmod{\varphi(n_B)}$ where $0 \leq x < n_B$

Then $S^j \equiv (M^{k_B})^j \equiv M^{j \cdot k_B} \equiv M^{1 + N \cdot \varphi(n_B)} \equiv M \cdot (M^{\varphi(n_B)})^N \equiv M \cdot 1 \equiv M \pmod{n_B}$
$\equiv 1$ by Euler's Thm.

Thus $S^j \equiv x \equiv M \pmod{n_B}$
$0 \leq x < n_B$
$0 \leq M < n_B$
$\Rightarrow \boxed{x = M}$

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?

C knows n_B but does not know the 2 primes p and q such that $n_B = p \cdot q$
so C cannot immediately calculate $\varphi(n_B) = (p-1)\cdot(q-1)$ and apply the process in part b. To factorize large n_B takes long enough time so that RSA is considered safe.

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

Let k = order of $r=5$ modulo 47. Then $k \mid \varphi(47) \Rightarrow k \mid 46 \Rightarrow k \in \{1, 2, 23, 46\}$

$r^1 \equiv 5 \pmod{47}$, $r^2 \equiv 25 \pmod{47}$ $r^4 \equiv 625 \equiv 14 \pmod{47}$

($\not\equiv 1$, so $k \neq 1$) ($\not\equiv 1$, so $k \neq 2$

$r^8 \equiv (14)^2 \equiv 196 \equiv 8 \pmod{47}$ $r^{16} \equiv 8^2 \equiv 64 \equiv 17 \pmod{47}$

$r^{23} \equiv r^{16} \cdot r^4 \cdot r^3 \equiv 17 \cdot 14 \cdot 125 \equiv 238 \cdot 125 \equiv 3 \cdot 125 \equiv 375 \equiv 46 \equiv -1 \pmod{47}$

Therefore, $k = 46 = \varphi(47)$, so $r = 5$ is a primitive root of 47. ($\not\equiv 1$, so $k \neq 23$)

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).

$x^6 \equiv 12 \pmod{47} \Leftrightarrow 5^{\operatorname{ind}_5 x^6} \equiv 5^{10} \pmod{47}$

$\Leftrightarrow 6 \operatorname{ind}_r x \equiv 10 \pmod{\varphi(47)} \pmod{46}$

$\Leftrightarrow 3y \equiv 5 \pmod{23}$ where $y = \operatorname{ind}_5 x$

$8 \cdot 3 \cdot y \equiv 8 \cdot 5 \pmod{23} \Leftrightarrow y \equiv 17 \pmod{23}$

Then $y \equiv 17 \vee y \equiv 40 \pmod{46}$

$x \equiv 5^{\operatorname{ind}_5 x} \equiv 5^y \equiv 5^{17}$ or $5^{40} \pmod{47}$

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 $N_2 = 2 \cdot 11^{17}$.

2 is a primitive root of 11 $\Rightarrow r' = 2$ or $r'' = 2 + 11 = 13$ is a primitive root of $11^2 = 121$

($r'^{10} \not\equiv 1 \pmod{121} \Rightarrow r'$ is a prim. root of 121)

($r''^{10} \not\equiv 1 \pmod{121} \Rightarrow r''$ is a prim. root of 121)

$2^{10} \equiv 1024 \equiv 56 \not\equiv 1 \pmod{121} \Rightarrow$ 2 is a prim. root of 11^2.

Then 2 is a prim. root of 11^k for all $k \geq 2$. Hence $\boxed{r_1 = 2}$

2 is a prim. root of $11^{17} \Rightarrow$ 2 or $2 + 11^{17}$ is a prim. root of $2 \cdot 11^{17}$.

But $\gcd(2, 2 \cdot 11^{17}) = 2 \neq 1 \Rightarrow$ 2 is not a prim. root of $2 \cdot 11^{17}$.

Therefore $2 + 11^{17}$ is a prim. root of $2 \cdot 11^{17}$.

Hence $\boxed{r_2 = 2 + 11^{17}}$

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

$8 \cdot (2x^2 + 7x + 4) \equiv 8 \cdot 0 \pmod{83}$

$16x^2 + 56x + 32 \equiv 0 \pmod{83}$

$(4x+7)^2 \equiv 49 - 32 \equiv 17 \pmod{83}$

Let $y = 4x+7$, so $y^2 \equiv 17 \pmod{83}$ — 83 is a prime, there are at most 2 solutions.

$y^2 \equiv 100 \pmod{83}$

$y \equiv 10 \pmod{83} \vee y \equiv -10 \equiv 73 \pmod{83}$

$y \equiv 4x+7 \equiv 10 \pmod{83}$

$4x \equiv 3 \pmod{83}$

$21 \cdot 4x \equiv 21 \cdot 3 \pmod{83}$

$84x \equiv x \equiv 63 \pmod{83}$

$y \equiv 4x+7 \equiv 73 \pmod{83}$

$4x \equiv 66 \pmod{83}$

$21 \cdot 4x \equiv 21 \cdot 66 \pmod{83}$

$84x \equiv x \equiv 7 \cdot 3 \cdot 66 \equiv 7 \cdot 198 \equiv 7 \cdot 32 \equiv 224 \equiv 58 \pmod{83}$

$x \equiv 63 \pmod{83} \vee x \equiv 58 \pmod{83}$

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 $x_1 \equiv -x_2 \pmod{p^n}$.

Way 1: Assume $x_1^2 \equiv a \pmod{p^n}$ and $x_2^2 \equiv a \pmod{p^n}$

Then $x_1^2 \equiv x_2^2 \equiv a \pmod{p^n} \Rightarrow x_1^2 - x_2^2 \equiv 0 \pmod{p^n}$

$\Rightarrow p^n \mid x_1^2 - x_2^2 \Rightarrow p^n \mid (x_1 - x_2)(x_1 + x_2)$

(since p is a prime, by unique factorization) $\Rightarrow p^r \mid (x_1 - x_2) \wedge p^s \mid x_1 + x_2$ where $1 \le r, s \le n$, $r + s = n$

Case 1: $p^n \mid x_1 - x_2$, then $x_1 \equiv x_2 \pmod{p^n}$

Case 2: $p^n \mid x_1 + x_2$, then $x_1 \equiv -x_2 \pmod{p^n}$

Case 3: $p^n \nmid x_1 - x_2$, $p^n \nmid x_1 + x_2$, thus $1 \le r < n$, $1 \le s < n$

$(x_1 \not\equiv x_2 \wedge x_1 \not\equiv -x_2 \pmod{p^n})$

Then $p \mid x_1 - x_2$, $p \mid x_1 + x_2$ $\Rightarrow p \mid 2x_1 \Rightarrow p \mid x_1$ (p is odd prime)

$p \mid x_1 \wedge p \mid x_1 + x_2 \Rightarrow p \mid x_2$.

$p \mid x_1 \wedge x_1^2 \equiv a \pmod{p^n} \Rightarrow a = x^2 + b \cdot p^n \Rightarrow p \mid a$

$\Rightarrow \gcd(a, p^n) \neq 1$, contradiction. Case 3 does not occur.

$\gcd(2, \varphi(p^n)) = 2$

2 | ind$_r a \Rightarrow$ There are exactly 2 solutions

Way 2

p^n has a primitive root r

$x^2 \equiv a \pmod{p^n}$

$2 \text{ ind}_r x \equiv \text{ind}_r a \pmod{\varphi(p^n)}$

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

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

$105 = 3 \cdot 5 \cdot 7$ (2 solutions)

$\Leftrightarrow$ $x^2 \equiv 16 \pmod 3 \rightarrow x \equiv 14 \pmod 3$ (2 sol.)
$x^2 \equiv 16 \pmod 5 \rightarrow x \equiv 14 \pmod 5$ (2 sol.)
$x^2 \equiv 16 \pmod 7 \rightarrow x \equiv 14 \pmod 7$ (2 sol.)

3, 5, 7 are primes, each has at most 2, hence exactly 2 solutions.

Then
$x \equiv c_1 \pmod 3$
$x \equiv c_2 \pmod 5$
$x \equiv c_3 \pmod 7$

where $c_i \in \{-4, 4\}$ for each i.
For each choice of (c_1, c_2, c_3), there is a unique such x mod 105 by Chinese Remainder Thm.
Then number of solutions is number of choices for (c_1, c_2, c_3) which is $2 \cdot 2 \cdot 2 = 8$

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

Legendre's symbol.

$\Leftrightarrow$ $x^2 \equiv 149 \pmod{5^3}$ — has a sol. iff $(149/5) = 1$
$x^2 \equiv 149 \pmod{7^4}$ — has a sol iff $(149/7) = 1$
$x^2 \equiv 149 \pmod{11^2}$ — has a solution iff $(149/11) = 1$

$(149/5) = (4/5) = (2^2/5) = 1$
$(149/7) = (2/7) = 1$ (since $7 \equiv -1 \pmod 8$)
$(149/11) = (6/11) = (2/11) \cdot (3/11) = (-1) \cdot (-1)^{\frac{3-1}{2} \cdot \frac{11-1}{2}} \cdot (11/3) = (11/3)$
since $11 \equiv 3 \pmod 8$
$= (2/3) = -1$

$(149/11) = -1$, thus
$x^2 \equiv 149 \pmod{11}$ and also
$x^2 \equiv 149 \pmod{11^2}$ have no solutions. Therefore, since $3 \equiv 1 \pmod 8$, number of sol. of $x^2 \equiv 149 \pmod n$ is 0

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

$125^k = 5^{3k}$

$61 \cdot 62 \cdots 199 \cdot 200 = 200!/60!$

$\sum_{k=1}^{\infty} \left[\frac{200}{5^k}\right] = \left[\frac{200}{5}\right] + \left[\frac{200}{25}\right] + \cdots = 40 + 8 + 1 + 0 + \cdots = 49$

$\Rightarrow 200! = 5^{49} \cdot M$ where $\gcd(5, M) = 1$

$\sum_{k=1}^{\infty} \left[\frac{60}{5^k}\right] = 12 + 2 + 0 + \cdots = 14 \Rightarrow 60! = 5^{14} \cdot N$ where $\gcd(5, N) = 1$

Then $\frac{200!}{60!} = \frac{5^{49} \cdot M}{5^{14} \cdot N} = 5^{35} \cdot \frac{M}{N}$ $\left(\frac{M}{N} \in \mathbb{Z}\right)$

$125^k = 5^{3k} \mid 5^{35} \cdot \frac{M}{N} \Leftrightarrow 3k \le 35 \Rightarrow \boxed{k \le 11}$ $(k \in \mathbb{Z})$

Largest such k is 11