M E T U
Department of Mathematics

	Elementary Number Theory I Midterm 1	
Code : *Math 365* Acad. Year : *2018-2019* Semester : *Fall* Instructor : *Tolga Karayayla* Date : *21.11.2018* 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. (10+5 pts.) a) Apply Euclidean Algorithm to calculate $d = gcd(9269, 2249)$ and find $x, y \in \mathbb{Z}$ such that $d = 9269x + 2249y$.

$9269 = 4 \cdot 2249 + 273$
$2249 = 273 \cdot 8 + 65$
$273 = 65 \cdot 4 + 13$ ← last non-zero remainder.
$65 = 13 \cdot 5 + 0$
By Euclidean Algorithm,
$\gcd(9269, 2249) = 13$

$13 = 273 + 65 \cdot (-4)$
$= 273 + (2249 - 8 \cdot 273) \cdot (-4)$
$= 273 \cdot 33 + 2249 \cdot (-4)$
$= (9269 - 2249 \cdot 4) \cdot 33 + 2249 \cdot (-4)$
$= 9269 \cdot 33 + 2249 \cdot (-136)$
$13 = 9269x + 2249y$
for $(x, y) = (33, -136)$

b) Find all solutions $(x, y) \in \mathbb{Z}^2$ of the Diophantine equation $9269x + 2249y = 314$.

$13 \mid 9269 \wedge 13 \mid 2249 \Rightarrow 13 \mid 9269x + 2249y$ for $x, y \in \mathbb{Z}$
But $13 \nmid 314$ $(314 = 13 \cdot 24 + 2)$
Hence there is no solution $(x, y) \in \mathbb{Z}^2$

2. (7 pts.) Suppose that n is an integer and n is not divisible by any prime $p \leq \sqrt[3]{n}$. Show that either n is a prime or n is a product of (not necessarily distinct) two primes.

Assume the given condition holds.
If n is a prime, we are done. If n is not a prime, then
$n = p_1 p_2 \cdots p_r$ (a product of r primes, $r \geq 2$) by unique factorization Thm (Fund. Thm of Arithmetic)
We want to show that $r = 2$. If $r > 2$, then $p_1 p_2 p_3 \mid n$. Thus $p_1 p_2 p_3 \leq n$
But $p_i \mid n$, and by the given condition, $p_i > \sqrt[3]{n}$ for all $i = 1, 2, \ldots, r$.
Thus $p_1 \cdot p_2 \cdot p_3 > \sqrt[3]{n} \cdot \sqrt[3]{n} \cdot \sqrt[3]{n} = n$

$p_1 p_2 p_3 > n$ contradicting $p_1 p_2 p_3 \leq n$. Hence $r = 2$ ∎

3. (20 pts.) Solve the system of congruences

$x \equiv 8 \pmod{14}$
$x \equiv 4 \pmod{39}$
$x \equiv 5 \pmod{55}$

$n_1 = 14, n_2 = 39, n_3 = 55$

$\gcd(n_i, n_j) = 1$ for $i \neq j$

Apply Chinese Remainder Thm.

$N = n_1 n_2 n_3$, $N_i = \frac{N}{n_i}$ $\Rightarrow N_1 = 39 \cdot 55$, $N_2 = 14 \cdot 55$, $N_3 = 39 \cdot 14$

$N_1 x_1 \equiv 1 \pmod{14}$

$39 \cdot 55\, x_1 \equiv 1 \pmod{14}$

$11 \cdot (-1)\, x_1 \equiv 1 \pmod{14}$

$-11 x_1 \equiv 1 \pmod{14}$

$3 x_1 \equiv 1 \pmod{14}$

$5 \cdot 3 x_1 \equiv 5 \cdot 1 \pmod{14}$

$x_1 \equiv 5 \pmod{14}$

$N_2 x_2 \equiv 1 \pmod{39}$

$14 \cdot 55\, x_2 \equiv 1 \pmod{39}$

$14 \cdot 16 x_2 \equiv 1 \pmod{39}$

$224 x_2 \equiv 1 \pmod{39}$

$29 x_2 \equiv 1 \pmod{39}$

$39 = 29 \cdot 1 + 10$

$29 = 10 \cdot 2 + 9$

$10 = 9 \cdot 1 + 1 \Rightarrow 1 = 10 - 9$

$9 = 1 \cdot 9 + 0$

$= 10 - (29 - 2 \cdot 10)$

$= 3 \cdot 10 - 29$

$= 3 \cdot (39 - 29) - 29$

$1 = 3 \cdot 39 - 4 \cdot 29$

$\Rightarrow 29 \cdot (-4) \equiv 1 \pmod{39}$

Hence $x_2 \equiv -4 \equiv 35 \pmod{39}$

$x_2 \equiv 35 \pmod{39}$

$N_3 x_3 \equiv 1 \pmod{55}$

$39 \cdot 14\, x_3 \equiv 1 \pmod{55}$

$546 x_3 \equiv 1 \pmod{55}$

$-4 x_3 \equiv 1 \pmod{55}$

$-14 \cdot (-4) x_3 \equiv -14 \pmod{55}$

$56 x_3 \equiv 41 \pmod{55}$

$x_3 \equiv 41 \pmod{55}$

By Chinese Remainder Thm,

Solution is $x \equiv \bar{x} \pmod{14 \cdot 39 \cdot 55}$

where $\bar{x} = N_1 x_1 \cdot 8 + N_2 x_2 \cdot 4 + N_3 x_3 \cdot 5$

$\bar{x} = 39 \cdot 55 \cdot 5 \cdot 8 + 14 \cdot 55 \cdot 35 \cdot 4 + 14 \cdot 39 \cdot 41 \cdot 5$

4. (15 pts.) Find all solutions modulo 642 of the congruence $198x \equiv 156 \pmod{642}$

$198x \equiv 156 \pmod{642}$

$6 \cdot 33x \equiv 6 \cdot 26 \pmod{6 \cdot 107}$

$\Leftrightarrow 33x \equiv 26 \pmod{107}$

$107 = 33 \cdot 3 + 8$

$33 = 8 \cdot 4 + 1$

$1 = 33 - 8 \cdot 4$

$= 33 - (107 - 33 \cdot 3) \cdot 4$

$= 33 \cdot 13 - 4 \cdot 107$

$1 \equiv 33 \cdot 13 \pmod{107}$

$33x \equiv 26 \pmod{107}$

$13 \cdot 33x \equiv 13 \cdot 26 \pmod{107}$

$x \equiv 169 \cdot 2 \pmod{107}$

$x \equiv 124 \equiv 17 \pmod{107}$

$\gcd(198, 642) = 6 \cdot \gcd(33, 107) = 6 \cdot 1 = 6$

modulo 642, there are 6 solutions of the form $x_0 + i \cdot \frac{642}{6} = x_0 + i \cdot 107$ where $i = 0, 1, \ldots, 5$ and x_0 is a particular solution.

All solutions modulo 642 are

$\{17, 17+107, 17+214, 17+321, 17+428, 17+535\}$

$= \{17, 124, 231, 338, 445, 552\}$

5. (15 pts.) Solve the system of congruences

$x \equiv 75 \pmod{216}$

$x \equiv 139 \pmod{400}$

$x \equiv 164 \pmod{405}$

$216 = 8 \cdot 27$, $\gcd(8, 27) = 1$

(1) $x \equiv 75 \pmod{216} \Leftrightarrow x \equiv 75 \pmod{8}$ and $x \equiv 75 \pmod{27}$ $\Leftrightarrow$ $x \equiv 3 \pmod{8}$, $x \equiv 21 \pmod{27}$

$400 = 16 \cdot 25$, $\gcd(16, 25) = 1$

(2) $x \equiv 139 \pmod{400} \Leftrightarrow \begin{cases} x \equiv 139 \pmod{16} \\ x \equiv 139 \pmod{25} \end{cases} \Leftrightarrow$ $x \equiv 11 \pmod{16}$, $x \equiv 14 \pmod{25}$

$405 = 5 \cdot 81$, $\gcd(5, 81) = 1$

(3) $x \equiv 164 \pmod{405} \Leftrightarrow \begin{cases} x \equiv 164 \bmod 5 \\ x \equiv 164 \pmod{81} \end{cases} \Leftrightarrow$ $x \equiv 4 \pmod{5}$, $x \equiv 2 \pmod{81}$

For the solution of the system, all 6 congruences in 3 boxes must hold.

But $x \equiv 2 \pmod{81} \Rightarrow x = 81k + 2 \Rightarrow x \equiv 2 \pmod{27}$

contradicting $x \equiv 21 \pmod{27}$

Therefore, there is no solution.

6. (7+7 pts.) a) Find $0 \leq x \leq 18$ such that $6^{229} \equiv x \pmod{19}$.

Since 19 is a prime, by Fermat's Little Thm, $6^{18} \equiv 1 \pmod{19}$

$229 = 18 \cdot 12 + 13$

$6^{229} \equiv 6^{18 \cdot 12 + 13} \equiv (6^{18})^{12} \cdot 6^{13} \equiv 1^{12} \cdot 6^{13} \equiv 6^{13} \pmod{19}$

$6^2 \equiv 36 \equiv 17 \equiv -2 \pmod{19}$

$6^4 \equiv (-2)^2 \equiv 4 \pmod{19}$

$6^8 \equiv 4^2 \equiv 16 \equiv -3 \pmod{19}$

Then

$6^{229} \equiv 6^{13} \equiv 6^8 \cdot 6^4 \cdot 6 \equiv -3 \cdot 4 \cdot 6 \pmod{19}$

$\equiv -72 \pmod{19}$

$\equiv 4 \pmod{19}$

b) Let $n = 2p$ where $p \geq 3$ is a prime. Show that $a^{n-1} \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$.

$\forall a \in \mathbb{Z}$, $a \equiv 0 \pmod 2 \vee a \equiv 1 \pmod 2$.

$a \equiv 0 \pmod 2 \Rightarrow a^{n-1} \equiv 0^{n-1} \equiv 0 \equiv a \pmod 2$

$a \equiv 1 \pmod 2 \Rightarrow a^{n-1} \equiv 1^{n-1} \equiv 1 \equiv a \pmod 2$

Thus $a^{n-1} \equiv a \pmod 2$ for all $a \in \mathbb{Z}$

$2 \mid a^{n-1} - a$

$\forall a \in \mathbb{Z}$, $p \mid a \vee p \nmid a$

$p \mid a \Rightarrow a \equiv 0 \pmod p \Rightarrow a^{n-1} \equiv 0^{n-1} \equiv 0 \equiv a \pmod p$

$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$ (by Fermat) $\Rightarrow (a^{p-1})^2 \equiv 1^2 \pmod p$

$a^{2p-2} \equiv 1 \pmod p$

$a^{2p-1} \equiv a \pmod p \Rightarrow a^{n-1} \equiv a \pmod p$

Hence $a^{n-1} \equiv a \pmod p$, $p \mid a^{n-1} - a$ for all $a \in \mathbb{Z}$

$(2 \mid a^{n-1} - a \wedge p \mid a^{n-1} - a \wedge \gcd(2,p) = 1) \Rightarrow n = 2p \mid a^{n-1} - a$

$a^{n-1} \equiv a \pmod n$ for all $a \in \mathbb{Z}$.

7. (7+7 pts.) a) Show that if $gcd(a, b) = 1$, $c|a$ and $d|b$, then $gcd(c, d) = 1$.

$\gcd(a,b) = 1 \Leftrightarrow ax + by = 1$ for some $x, y \in \mathbb{Z}$.

$c \mid a \wedge d \mid b \Rightarrow a = cr, b = ds$ for some $r, s \in \mathbb{Z}$

$ax + by = 1$

$crx + dsy = 1$

$c(rx) + d(sy) = 1 \wedge rx, sy \in \mathbb{Z} \Rightarrow \gcd(c,d) = 1$

b) If $gcd(a, b) = p$ where p is a prime, then show that $gcd(a^3, b^4)$ is either p^3 or p^4.

$\gcd(a,b) = p \Rightarrow a = p^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ and $b = p^{\beta} t_1^{\beta_1} t_2^{\beta_2} \cdots t_s^{\beta_s}$

where $p, q_1, q_2, \ldots, q_r, t_1, t_2, \ldots, t_s$ are distinct primes

AND $\alpha = 1 \vee \beta = 1$ (and $\alpha \geq 1, \beta \geq 1$)

Then $a^3 = p^{3\alpha} q_1^{3\alpha_1} \cdots p_r^{3\alpha_r}$, $b^4 = p^{4\beta} t_1^{4\beta_1} \cdots t_s^{4\beta_s}$

The only common prime factor of a^3 and b^4 is p, and

$\gcd(a^3, b^4) = p^{\min(3\alpha, 4\beta)} = \begin{cases} p^3 & \text{if } \alpha = 1 \\ p^4 & \text{if } \beta = 1 \end{cases}$