**CIS 3223 Miniquiz 3**

Dr Anthony Hughes

**Name:** Parth Patel

**Temple ID (last 4 digits):** 5761

1 (8 pts) Answer the following.

(a) Find the smallest integer $b$, $1 \leq b < 34$, such that $15b \equiv 0 \pmod{35}$

$\boxed{7} = \frac{35}{\gcd(15, 35)} = \frac{35}{5}$

$\phi(11) = 11 - 1 = 10$

(b) Compute $3^{2022} \bmod 11$ $\quad 3^{2022} = 9 * 3^{2020} \xrightarrow{\text{Euler's theorem}} 9 * 3^{2020} \equiv_{11} 9 * 1 = \boxed{9}$

9

$\phi(33) = (3-1)(11-1) = 20$

(c) Compute $2^{2022} \bmod 33$ $\quad 2^{2022} = 4 * 2^{2020} \xrightarrow{\text{Euler's theorem}} 4 * 2^{2020} \equiv_{33} 4 * 1 = \boxed{4}$

4

(d) 1.13(P39)

$5^{30000} = 5^{30^{1000}} \xrightarrow{\text{Euler's theorem}} 5^{30^{1000}} \equiv_{31} = 1^{1000} = 1$

YES

$\phi(31) = 31 - 1 = 30$ $\quad 6^{123,456} = 6^6 6^{30^{4115}} \xrightarrow{\text{Euler's theorem}} 6^6 6^{30^{4115}} \equiv_{31} 6^6 \times 1$

$\equiv_{31} 5^3 = 4 * 31 + 1$

$\equiv_{31} = \boxed{1}$

Since $5^{30000} - 6^{123,456} \equiv_{31} 1 - 1 = 0$, $31 | 5^{30000} - 6^{123,456}$

2 (5 pts) Use the **modular exponentiation** algorithm to calculate $3^{13}$ **mod** 37.

30

$z = 1$ $\qquad 13 = 1101_2$

| digit | power | z |
|---|---|---|
| 1 | $3^1 \equiv_3 3$ | $3 \times 1 \equiv_3 3$ |
| 0 | $3^2 \equiv_3 9$ | $3$ |
| 1 | $3^4 \equiv_3 7$ | $3 \times 7 \equiv_3 21$ |
| 1 | $3^8 \equiv_3 12$ | $21 * 12 \equiv_3 30$ |
| | | |
| | | |

3 (2 pts) 1.10 (p39)

Given:

- (1) $a \equiv b \mod N$
- (2) $M | N$

Since $a \equiv b \mod N$, $N | b - a$. This means that $\exists c \in \mathbb{Z}$ such that $cN = b - a$

Since $M | N$, $\exists k \in \mathbb{Z}$ such that $kM = N$

Therefore $cN = ck \cdot M = b - a$

Since $ck \in \mathbb{Z}$, $M | b - a$.
Therefore $a \equiv b \mod M$

4 (3 pts) Use the **extended Euclidean algorithm** to find integers $x$ and $y$ such that $40x + 3y = \gcd(40, 3)$ (show all steps).

| $a$ | $b$ | $q$ | $r$ | $Q$ |
|---|---|---|---|---|
| 40 | 3 | 13 | 1 | $\begin{pmatrix} 0 & 1 \\ 1 & -13 \end{pmatrix}$ |
| 3 | 1 | 3 | 0 | $\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -13 \end{pmatrix} = \begin{pmatrix} 1 & -13 \\ -3 & 40 \end{pmatrix}$ |
| | | | | |
| | | | | |
| | | | | |

40 $\boxed{1}$ + 3 $\boxed{-13}$ = $\boxed{1}$

5 (2 pts) Consider an RSA key set with $N = 55$ and $e = 3$.

What value of $d$ should be used for the secret key? $\boxed{27}$

[Hint: Look at the previous question]

$$\begin{aligned} p &= 5 \\ q &= 11 \\ \implies \phi(N) &= 40 \\ e &= 3 \\ d &= -13 \end{aligned}$$

Since $d < 0$ we must consider $d \mod 40$ which is 27