

W1: Show no work. Please write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

a Alice's RSA code has modulus is $M = 6557$, and encryption exponent $E := 749$, both public. Bob has a message that can be interpreted as a number β in $[0..M)$. Since Alice knows the secret factorization $M = p \cdot q$ into primes, $p=79$, $q=83$, she can compute the decryption exponent $d = \dots \in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle \beta^E \rangle_M = 007$. Alice decrypts it to $\langle \mu^d \rangle_M = \dots \in [0..M)$.

b The Huffman code with letter-probabilities

$I: \frac{12}{66}$ $M: \frac{5}{66}$ $O: \frac{7}{66}$ $R: \frac{4}{66}$ $S: \frac{32}{66}$ $T: \frac{6}{66}$

codes these to bitstrings: $I: \dots$ $M: \dots$
 $O: \dots$ $R: \dots$ $S: \dots$ $T: \dots$
 Bitstring 0100101110011010 decodes to
 \dots, answering: "How he leaves a room?"

c Consider the four congruences C1: $z \equiv_{18} 15$, C2: $z \equiv_8 1$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 4$. Let z_j be the smallest natnum satisfying (C1) $\wedge \dots$ (Cj). Then
 $z_2 = \dots$; $z_3 = \dots$; $z_4 = \dots$.

W2: Magic integers $G_1 = \dots$, $G_2 = \dots$,
 $G_3 = \dots$, $G_4 = \dots$, each in $[0..1260)$,
 are st. $g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_{1260}$ is a ring-iso, where

$$g((z_1, z_2, z_3, z_4)) := \langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \rangle_{1260}.$$

Now consider poly $h(x) := [x + 59][x - 1][x + 83]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 7, 4, 9, 5$, displaying the results in a nice table. (Do not show work for this step.)

Now use your ring-iso to compute all solns x to $h(x) \equiv_{1260} 0$, displaying the results in a table which shows which 4-tup each came from. There are (not counting multiplicities) $K := \dots$ many solns.

Explain your method well; then show one computation giving a root different (mod 1260) from -59, 1, -83.

In complete English sentences OYOP, please write, double-spaced, this proof. Do not restate the problem.

W3: **i** Carefully state Wilson's Thm.

ii Carefully prove Wilson's Thm. You may use for free that a degree- n polynomial over a field has at most n roots.

End of Class-W

W1: _____ 90pts

W2: _____ 90pts

W3: _____ 85pts

Total: _____ 265pts

Please PRINT your Name

.....

HONOR CODE: "I have neither requested nor received help on this exam other than from my professor."

Signature: _____