Please fill-in every blank on this sheet.

**V4:** Show no work. Write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

**a** Consider \( M := p \cdot q = 690227 \), where \( p < q \) are primes. Your mole in King’s organization finds out that \( F := \varphi(M) = 688560 \).

Then \( p = \ldots \) \(< q = \ldots \).

**b** Note \( p := 3001 \) is prime, and \( p - 1 = 2^3 \cdot 3^1 \cdot 5^3 \). Then the (multiplicative) order of 2758 mod 3001 is \ldots .

**c** For oddprime \( p \) and posint \( N \), there are exactly two square-roots of 1 in the \( \mathbb{Z}_p^N \) ring:

For \( M := p \cdot q \cdot r \), a product of distinct oddprimes, there are at most six square-roots of \(-1\) in \( \mathbb{Z}_M \):

**OYOP:** In grammatical English sentences, write your essay on every third line (usually), so that I can easily write between the lines.

**V5:** Abstractly describe the RSA algorithm, what is public, what private, how to compute the decryption key from the encryption key, and how to encrypt and decrypt. (Do not bother to describe Lbolt, nor Repeated-squaring, but do say where they are used.)

Alice’s RSA code has modulus is \( M = 851 \), and encryption exponent \( E := 317 \), both public. Bob has a message that can be interpreted as a number \( \beta \) in \([0 .. M)\). Since Alice knows the secret factorization \( M = p \cdot q \) into primes, \( p=37, q=23 \), she can compute the decryption exponent \( d := \ldots \in \mathbb{Z}_+ \). Bob’s encrypted message \( \mu := \langle \beta^E \rangle_M = 007 \). Alice decrypts it to \( \langle \mu^d \rangle_M = \ldots \in [0 .. M) \).

**V6:** Prove Wilson’s Thm: Fix an oddprime \( p \). Then

\[
\prod (\varphi_p) \equiv_p -1.
\]

End of Class-V

---

**V4:** 85 pts
**V5:** 40 pts
**V6:** 30 pts

Total: 155 pts

Please PRINT your name and ordinal. Ta:

Ord: ___ ___

**Honor Code:** “I have neither requested nor received help on this exam other than from my professor.”

Signature: ___ ___ ___