Staple!

Team C_____

Number Theory MAS4203 | **Home-C** | Prof. JLF King *Touch*: 2Jul2018

Hello. Essays violate the CHECKLIST at *Grade Peril*! Exam is due no later than **10:00*AM*, Friday, 28Apr2006**, slid under LIT402. Please email me afterwards.

Use **symmetric residues** in your answers and essays. For N a posint, the symmetric residue $\langle x \rangle_N$ lies in $(-\frac{N}{2} \,..\, \frac{N}{2}]$. If you need the non-negative residue somewhere, please write it as $\langle\langle x \rangle\rangle_N$ in $[0 \,..\, N)$. Recall that "6 is p-QR" means there exists an $n \perp p$ so that $n^2 \equiv_p 6$.

QR, Quadratic Residue. QRThm, Quadratic Reciprocity Thm. LSThm, Legendre-Symbol Thm. CRThm, Chinese Remainder Thm. IG, Interesting generalization. SOTS, Sum of two squares. RONO, (square) root of negative one.

C1: Short answer: Show no work. Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

z Prof. K hopes you have a refreshing summer, read some Number Theory, and consider taking the continuation NT course in the Fall. Circle: **True Oui Yes**$^{2^{3^4}}$ **Only-a-SOT-would-say-no** *Gnaw, he prabibly dont kare.*

a $\square^2 + \square^2 = 625$ is a **coprime** SOTS-decomp.. Consequently, $\mathcal{R} =$ _____ $\in [1 \,..\, 312]$ is a 625-RONO. [*Hint:* Take a SOTS-decomp. of 5, and meld copies to get a coprime SOTS-decomp. $x^2 + y^2 = 5^4$. Look mod 625 and divide by x, then positize.]

Essay questions: Write in complete sentences and also fill-in the blanks. Each essay starts a new page.

C2: Solve LeVeque #17[P.85]. His use of brackets, e.g "$[a, b, \ldots, z]$", means $\text{Lcm}(a, b, \ldots, z)$.

C3: Use either the Gauss Lemma or QRThm (or both) to give a complete *solution* to: *Oddprime p has 5 as a p-QR* IFF $\langle p \rangle_N \in \mathcal{U}$. You need to determine the appropriate modulus $N = N_5$ and the set $\mathcal{U} = \mathcal{U}_5 \subset (-\frac{N}{2} \,..\, \frac{N}{2}]$. Can you prove that your N_5 is smallest?

With proof, compute pair $N_6, \mathcal{U}_6$ and $N_7, \mathcal{U}_7$. Are your N_6 and N_7 **minimal**? [*Recall:* We showed in class that $N_2 = 8$ and $\mathcal{U}_2 = \{\pm 1\}$.] [*Extra credit:* Do/can you see/prove an IG?]

C4: i Let $N := 39365$. Verify that $\mathcal{R}_1 := 4283$ and $\mathcal{R}_2 := 11463$ are N-RONOs. Apply our Modified↯ to $(N, \mathcal{R}_1)$ to produce posints x, y with $x^2 + y^2 = N$. Show all the steps and explain *why* you stopped where you did. The $(N, \mathcal{R}_2)$ pair produces $x =$ _____, and $y =$ _____. (Here, do not show the steps).

ii "*A* 4POS *prime* $K := 2273$ *is*" (says Yoda). Find a K-RONO $\mathcal{R} =$ _____ $\in [1 \,..\, 1136]$ by the repeated-squaring algorithm applied to the K-nonQR 3. Show all the steps.

[*Hint:* Let $H := \frac{K-1}{2}$. For the RS alg., it is convenient to write $H = D \cdot 2^J$, where D is odd and $J \in \mathbb{N}$.]

C5: Prove, for an arbitrary 4NEG prime p, that there exists integers $M \in [1 \,..\, p), x, y$ such that

$$x^2 + y^2 + 1 = Mp\,.$$

End of Home-C

C1:	___ ___	60pts
C2:	___ ___	85pts
C3:	___ ___ ___	120pts
C4:	___ ___ ___	120pts
C5:	___ ___	85pts
Total:	___ ___ ___	470pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: _____

Ord: _____

Ord: _____

Folks, this has been a terrific class for me, and I appreciate your contribution. Please stop by next semester to tell me what you are doing.

Sincerely, Jonathan King