Staple!

Ord: ___ ___

NT
MAS4203 *4D70*

Class-C

Prof. JLF King
Wedn., 01Aug2018

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

C1:

a Prof. King thinks that submitting a ROBERT LONG PRIZE ESSAY [typically 2 prizes, \$500 total] is a *really good idea*, and the due date for the emailed-PDF is typically mid-March. $\boxed{\text{Circle}}$:

Yes **True** ***Résumé material!***

b With $N := 19$, then $\varphi(N)$= ______ . Thus EFT (Euler-Fermat) says that $7^{3630} \equiv_N$ ______ $\in [0\,..\,N)$.

c Carmichael fnc $\lambda(385 \cdot 29 \cdot 43) = 2^A \cdot 3^B \cdot 5^C \cdot 7^D \cdot 11^E$ where $A=$ ___ , $B=$ ___ , $C=$ ___ , $D=$ ___ , $E=$ ___ .

d Modulo 109, the multiplicative-order of 2 is ______ . [*Hint:* $\varphi(109)$ has very few prime factors.]

e Modulo $Q := 72$, poly $h(x) := x^2 + 16x - 17$ has ______ many roots. E.g, ______ $\in [0\,..\,Q)$.

f $S(98{,}000{,}000)$= ______ where, for posints k, let $S(k)$ be the number of mod-k square-roots of 1. Also, $S(162) =$ ______ .

[For $N \in \mathbb{N}$, recall $\Phi(2^{N+2}) \overset{\text{gp}}{\cong} \mathsf{C}_2 \times \mathsf{C}_{2^N}$.]

g And y= ______ is the smallest natnum with

$$y \equiv_{20} 1, \qquad y \equiv_{15} 11, \qquad y \equiv_{12} 5.$$

C2:

Polynomial $f(x) := x^2 - x - 22$ has $\mathbb{Z}_2$-root $Y_1 = 1$.

This lifts to $\mathbb{Z}_8$-root $Y_3 =$ ______ . And f has a $\mathbb{Z}_5$-root of $Z_1 = -1$, lifting to $\mathbb{Z}_{25}$-root Z_2= ______ .

Magic G_1= ______ , G_2= ______ realize ring-iso $\mathbb{Z}_8 \times \mathbb{Z}_{25} \hookrightarrow\!\!\!\!\rightarrow \mathbb{Z}_{200}$, which maps (Y_3, Z_2) to ______ , a $\mathbb{Z}_{200}$-root of f.

End of Class-C

C1: ___ ___ ___ 165pts

C2: ___ ___ 45pts

Total: ___ ___ ___ 210pts

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: ______________________________