

NT MAS4203 4D70 **Class-A** Prof. JLF King Wedn., 18Jul2018

A4: Show no work. Write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

a Prof. King wears bifocals, and cannot read small handwriting. Circle one: **True! Yes! Who??**

b For prime $p = 59$, value -2 is a p -QR. T F
[Hint: LST or LST+RS.]

c The *Blip-numbers* comprise $\mathcal{B} := 1 + 3\mathbb{N}$. \mathcal{B} -number $595 \stackrel{\text{note}}{=} 35 \cdot 17$ is \mathcal{B} -irreducible: T F
Blip $N := 55$ is **not** \mathcal{B} -prime because Blips $J :=$ _____ and $K :=$ _____ satisfy that $N \bullet [J \cdot K]$, **yet** $N \nmid J$ and $N \nmid K$.
Also, \mathcal{B} -GCD(175, 70) = _____.

d Write $27^{2009} \equiv_7$ _____ (i.e, working mod 7) and $9^{35} \equiv_7$ _____, each as a value in $[0..7)$.
[Hint: This can be done by inspection.]

e Suppose $x, y, N \in \mathbb{Z}_+$, with $x^2 + 2y^2 = N$ and $N \perp x$.
Statement “Integer $-2 \in \text{QR}_N$ ” is: AT AF Nei
And stmt “Integer $+2 \in \text{QR}_N$ ” is: AT AF Nei

f Cubic polynomial $h(x) := [x + 5][x - 11][x + 37]$ has K many roots in \mathbb{Z}_8 , and N many roots in \mathbb{Z}_{120} , where $K =$ _____ and $N =$ _____. [Hint: CRT.]

g With $K := 105$, ring \mathbb{Z}_K has $|\text{ZD}_K| =$ _____ and $|\text{NQR}_K| =$ _____.

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

A5: EFT says: For each posint N , every integer $b \perp N$ satisfies $b^{\varphi(N)} \equiv_N 1$.

Write a careful proof of this Euler-Fermat Thm. Recall that $\Phi(N)$ is the units group of \mathbb{Z}_N , and $\varphi(N) := |\Phi(N)|$.

You may use \equiv for \equiv_N , and use $U := \Phi(N)$.

End of Class-A

A4: _____ 130pts
A5: _____ 25pts
Total: _____ 155pts

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: _____