Staple!

Team A

NT MAS4203 *4D70* | **Home-A** | Prof. JLF King Fri, 13Jul2018

Due: BoC, Tuesday, 17July2018. *Fill-in* every *blank* on this sheet. This is the *first-page* of your write-up, with your essays securely stapled to it.

A1: *Show no work. Write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a $N := \varphi(100) =$ ____. So $\varphi(N) =$ ____. EFT says that $3^{1621} \equiv_N$ ____ $\in [0\,..\,N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are ____.

b Suppose $y \perp N$, where $N \in \mathbb{Z}_+$ You compute Bézout mults U and V st. $yU + NV = 1$. Then "*U is a mod-N square*" is: *AT AF Nei*

c With $A := 29$, $B := 20$, $U := A{\cdot}B = 580$, let **J** be $(-290\,..\,290]$. There is a ring-iso $g{:}\mathbb{Z}_A{\times}\mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G =$ ____ $\in$**J** and $H =$ ____ $\in$**J**. A mod-U root of poly $f(x) := 20{\cdot}[x+10]^3 + 29{\cdot}[x-2]$ is $($ ____ , ____ $) \overset{g}{\mapsto}$ ____ $\in$**J**.

OYOP: *Your 2 essay(s) must be* TYPED*, and Double spaced. Use the Print/Revise cycle to produce good, well thought out, essays. Start each essay on a new sheet. Do* **not** *restate the problem; just solve it.*

A2: For primes $\alpha < \beta$, their product $\mathsf{P} := \alpha\beta$ has

$$\varphi(\mathsf{P}) = 37520101020 \quad \textit{and} \quad \sigma(\mathsf{P}) = 37521045408\,.$$

Describe an efficient algorithm [not brute-search] to compute $\alpha =$ ____ $< \beta =$ ____.

With $\mathcal{E}$ and $\mathcal{D}$ denoting the number of bits in $\varphi(\mathsf{P})$ and $\sigma(\mathsf{P})$, respectively, estimate the Running-Time of this algorithm, as function of ordered-pair $(\mathcal{E}, \mathcal{D})$, or of just $\mathcal{D}$.

A3: The ***Blip-numbers*** comprise $\mathcal{B} := 1 + 3\mathbb{N}$. In terms of factorization $T = p_1^{E_1} \cdot \ldots \cdot p_K^{E_K}$ [where $p_1 < \ldots < p_K$ are $\mathbb{Z}$-primes, and each E_j is a posint]:

i Give/prove an IFF-characterization for when $T \in \mathcal{B}$.

ii Give/prove an IFF-char. of when T is Blip-*irreducible*.

iii Give/prove an IFF-char. of when T is Blip-*prime*.

iv Using theorems from our text, prove or disprove: "*There are ∞ly many Blip-primes.*"

End of Home-A

A1:	___ ___	85pts
A2:	___ ___	90pts
A3:	___ ___	90pts
Total:	___ ___ ___	265pts

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: ____