NT & ECC
MAT4930 5662

Class-B

Prof. JLF King
Touch: 2Jul2018

Open brain/calculator, closed book/notes. If a question is not well-defined, then write **DNE** for *Does Not Exist*.

B3: Short answer: Show no work.

a Using dictionary 0:ε, 1: "1", 2: "0", compute EnZiv(11001010)= ____, in $\langle 7\rangle 1\langle 34\rangle 0\ldots$ notation. In bits, EnZiv(11001010) is ____.

b The Huffman code with letter-probabilities

$I{:}\frac{12}{66}$ $\mathcal{M}{:}\frac{5}{66}$ $O{:}\frac{7}{66}$ $\mathcal{R}{:}\frac{4}{66}$ $\mathcal{S}{:}\frac{32}{66}$ $\mathcal{T}{:}\frac{6}{66}$

codes these to bitstrings: I: ____ $\mathcal{M}$: ____ O: ____ $\mathcal{R}$: ____ $\mathcal{S}$: ____ $\mathcal{T}$: ____. Bitstring 1101101110011001110 decodes to ____, answering: "*What is Big Moose's name?*"

c Let $K := 162 = 2\cdot 3^4$. Cyclotomic-poly $\mathbf{C}_K$ has degree ____. Writing $\mathbf{C}_K(x)$ as $\frac{x^{2N}-1}{x^N-1}\Big/\frac{x^{2D}-1}{x^D-1}$ gives N= ____ and D= ____. In standard form, $\mathbf{C}_K(x)$ = ____.

d′ Evaluate $Id \circledast \boldsymbol{\mu}$ on the numbers $1, 2, 4, 5, 10, 20$: ____ ____ ____ ____ ____ ____.

Mystery function $f{:}\mathbb{Z}_+\to\mathbb{Z}$ satisfies $f \circledast \boldsymbol{\tau} = Id$. So $f(20)$= ____.

B4: Mod $M := 145157$, note $A^2 \equiv B^2 \equiv C^2 \equiv 83521$, where $A := 289$, $B := 144868$ and $C := 17524$. These give a non-trivial factor $F :=$ ____ of M. *Explain* how you computed F from A, B, C.

ii Explain where this idea might appear in the Miller-Rabin primality testing algorithm.

iii Give a formal, precise, description of the full Miller-Rabin alg.. There are several cases where M-R-Alg says "*Composite*". In each, explain the certificate of compositeness.

B5: Use Pollard-ρ to find a non-trivial factor of $N := 250997$, using seed $s_0 := 33287$ and map $f(x) := 1+x^2$. Make a nice table, labeled

Time	Tortoise	Hare	$s_{2k} - s_k$	Gcd(??)

—*but* ***replace*** *the "??" with the correct expression.* You found non-trivial factor $E :=$ ____.

[*Fact:* Your table has $\leqslant$4 lines.]

B-Home:	___ ___ ___	355pts
B3:	___ ___ ___	100pts
B4:	___ ___	55pts
B5:	___ ___	25pts
Total:	___ ___ ___	535pts

Print name ____ Ord: ____

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: ____