Staple!

Team B

NT & ECC
MAT4930 5662

Home-B

Prof. JLF King
Touch: 2Jul2018

Hello. Essays violate the CHECKLIST at *Grade Peril*!
Exam is due by **4PM, Thursday, 15Nov2007**, slid under my office door, LIT402.

Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

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

B0: Show no work.

a Bits 0100101010010000111000111011011001111 *decode* in Idx-form, e.g ⟨7⟩1 ⟨3⟩1 ⟨9⟩0 . . . ⟨3⟩1 ⟨0⟩⟨4⟩, to

. .

As 15 bits, it is .

having used *Ziv* seeded with ⟨0⟩=‘’, ⟨1⟩=‘1’, and ⟨2⟩=‘0’.

Employing our fivebit-code, the 15 bits decode to symbols . . .

b Let $f(x) := x^2 - 9x + 14$, and $N := 28225 \overset{\text{note}}{=\!=} p \cdot 25$, where $p := 1129$ is prime. The *number* of solns $x \in [0\,..\,N)$ to $f(x) \equiv_N 0$ is $K =$. A number $Z \in [0\,..\,N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is .

[*Hint:* Find solns mod-p and mod-25, then use CRT.]

c Let $f(x) := 2x^3 + 7x + 5$ and $z_0 := c_0 := 2$. Note $f(z_0) \equiv_7 0$. Note $f'(z_0) =$ $\not\equiv_7 0$.

Use Hensel's lemma repeatedly to compute coefficients $c_k \in [-3\,..\,3]$ (these are the blanks, below)

$$z_3 = \overbrace{\underbrace{c_0 \cdot 7^0 + \quad \cdot 7^1}_{z_2} + \quad \cdot 7^2}^{z_1} + \quad \cdot 7^3$$

so that integers $z_k := \sum_{i=0}^{k} c_i 7^i$ satisfy

$$f(z_k) \quad \equiv_{7^{k+1}} \quad 0\,,$$

for $k = 1, 2, 3$.

d Let $N := 250$. In std. form, this cyclo-poly $\mathbf{C}_N(x) =$.

e Define the ***numeral map*** h:[1 .. 12]↻, where $h(n)$ is the number of letters in the n^{th} numeral. So $h(12)$ equals 6, since “twelve” has 6 letters.

Compute the convolution $[h \circledast \boldsymbol{\mu}](12) =$.

f The divisor-sum $\boldsymbol{\sigma}(1500) =$.

Express your answer a product $p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots$ of primes to posint powers, with $p_1 < p_2 < \ldots$.

B1: Suppose the letters A F H M N U have frequencies $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$, respectively. Construct the unique Huffman prefix-code with these frequencies; at each coalescing, use 0 for the less-probable branch and 1 for the more-probable. **Draw** the Huffman tree (large!). Label the branches and leaves with bits and letters. The name HUFFMAN encodes to

.

Examining the tree, what kind of *Being* is HUFFMAN?

Answering the question “*What're y'all?*”, message 10100010101001110100110111010*!* decodes to *!*

B2:

i Use Pollard-ρ to find a non-trivial factor of $M := 59749$, using seed $s_0 := 7$ 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 $E :=$.

The hare Hits into the tortoise at time $H :=$.

Repeat, showing the table for $s_0 := 24$. Experiment with different seeds; what is the typical running time? How is it related to the factor you find?

ii A seed s determines a ***tail***; the smallest natnum T for which there is a time $n > T$ with $f^n(s) = f^T(s)$. The smallest such n is $T+L$ where L is the ***period***. Derive (picture+reasoning) a formula for the hitting time $H(T, L)$. [*Hint:* $H(0, L) = L$.]

iii Produce a Floyd-done-twice algorithm that computes both T and L. The number, N, of f-evaluations is upper-bounded by some small constant times $T+L$ (=arclength of ρ). How small can you get $N(T, L)$? [*Hint:* $N(0, L) = 3L$.]

B3: Choose your own NT problem and solve it. Show off!

B0:	___ ___ ___	180pts
B1:	___ ___	55pts
B2:	___ ___ ___	105pts
B3:	___ ___	15pts
Total:	___ ___ ___	355pts

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: