NT & ECC
MAT4930 5662

Class-A

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*. Use $\varphi()$ for the Euler phi-fnc. Essays violate the CHECKLIST at *Grade Peril*!

A4: Short answer: Show no work.

z Prof. King believes that writing in complete, coherent sentences is crucial in communicating Mathematics, improves posture, and whitens teeth. Circle one:

True! **Yes!** ***What's a sentence?***

a Euler $\varphi(34300) =$ ____.

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

b Consider the four congruences C1: $z \equiv_{21} 1$, C2: $z \equiv_{18} 7$, C3: $z \equiv_{20} -13$ and C4: $z \equiv_{15} 18$. Let z_j be the *smallest natnum* satisfying (C1) $\overset{\text{All}}{!!}$ (Cj). Then

$z_2=$ ____ ; $z_3=$ ____ ; $z_4=$ ____.

c LBolt: $\text{Gcd}(36, 90)=$ ____ $\cdot 36 +$ ____ $\cdot 90$.

So (LBolt again) $G := \text{Gcd}(36, 90, 15)=$ ____ and

____ $\cdot 36 +$ ____ $\cdot 90 +$ ____ $\cdot 15 = G$.

d Note $p := 137$ is prime. The (multiplicative) order of 18 mod 137 is ____.

[*Hint:* $p - 1$ has very few prime factors.]

e With $V := 12 + 10\boldsymbol{i}$ and $D := 3 + 4\boldsymbol{i}$, produce GIs $q=$ ____ and $r=$ ____ s.t $V = [Dq] + r$, with norm $\mathcal{N}(r) < \mathcal{N}(D)$. (Recall that $\mathcal{N}(x + y\boldsymbol{i}) = x^2 + y^2$, when $x, y \in \mathbb{Z}$.)
[*Hint:* Mult. V and D by $\overline{D}$.]

f Bitstring ""00111111100101110"001", via the Elias code, decodes to ____,

a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits ____.

Conv, Elias(84)= ____ (bitstring)

A5: Compute a Huffman code for these five symbols.

A: 4/27 ____

B: 1/27 ____

C: 14/27 ____

D: 2/27 ____

E: 6/27 ____

When coalescing, use "0" to go to the smaller-prob. word.

And MECL($\frac{4}{27}, \frac{1}{27}, \frac{14}{27}, \frac{2}{27}, \frac{6}{27}$)= ____ bits.

ii Give the example (with picture) from class of a minimum expected-length code which is **not** a Huffman code. Argue that your code is indeed of MECL, and is not Huffman.

iii State the Huffman Coding thm from class. Sketch a proof of it; just show the main ideas. (And pictures)

A6: Carefully state Hensel's lemma. (Do not prove it!)

B Let $f(x) := 2x^2 + 5x + 2$ and $z_0 := c_0 := 2$. Note $f(z_0) \equiv_5 0$. Note $f'(z_0)=$ ____ $\not\equiv_5 0$.

Use Hensel's lemma repeatedly to compute coefficients $c_k \in [\text{-}2 \,..\, 2]$ (these are the blanks, below)

$$z_3 = \overbrace{\underbrace{c_0 \cdot 5^0 + \_\_\_\_ \cdot 5^1}_{z_1} + \_\_\_\_ \cdot 5^2}^{z_2} + \_\_\_\_ \cdot 5^3$$

so that integers $z_k := \sum_{i=0}^{k} c_i 5^i$ satisfy

$$f(z_k) \quad \equiv_{5^{k+1}} \quad 0\,,$$

for $k = 1, 2, 3$. Show the update rule explicitly.

A-Home:	___ ___ ___	785pts
A4:	___ ___ ___	175pts
A5:	___ ___ ___	105pts
A6:	___ ___	85pts
Total:	___ ___ ___ ___	1150pts

Print name ____ Ord:

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

Signature: ____