Number Theory 2 MAT4930 5662 **Home-Y** Prof. JLF King *Touch*: 29Jun2022

Hello. *This Gentle Exam is due* **2PM, Friday, 08Dec2006**, *slid under LIT402 door.*

Essays. *Write in complete sentences and* *also* *fill-in the blanks. Each (typed!) essay starts a new page.* Essays violate the CHECKLIST at *Grade Peril*! ☐

Y0: Show no work.

α Consider Carmichael's lambda fnc: Given posints J,K,L, write $\boldsymbol{\lambda}(3^J \cdot 5^K \cdot 7^L)$ as product of prime-powers: ______.

β For posint N, let $\widehat{N}$ be the **sum** of the N many N^{th}-RoU (roots of unity). So $\widehat{1}$= ______ and $\widehat{N_{\geq 2}}$ = ______.

Use $\mathcal{S}(N)$ for the sum of the $\varphi(N)$ many *primitive* N^{th}-RoU. Is $\mathcal{S}()$ *is multiplicative*? *T* *F*

Using familiar fncs from this semester, and **no** summation, write $\mathcal{S}(N)$= ______.

γ An explicit ring-iso $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \hookrightarrow \mathbb{Z}_{210}$ is the mapping: (w, x, y, z) goes-to

$$\langle 105Aw + 70Bx + 42Cy + 30Dz \rangle_{210}, \quad \text{where}$$

A= ______ $\in[0..1]$, B= ______ $\in[-1..1]$, C= ______ $\in[-2..2]$, D= ______ $\in[-3..3]$.

In $\mathbb{Z}_{210}$ list all $\sqrt{1}$: ± 1, $\pm$ ______, $\pm$ ______, $\pm$ ______. List all of *these* that have sqroots: ______.

δ Let $\boldsymbol{\alpha}$ be a root of $\mathbb{Q}$-irreducible polynomial $h(x) := x^3 - x^2 + 1$. So $\frac{1}{\boldsymbol{\alpha}+1} = A + B\boldsymbol{\alpha} + C\boldsymbol{\alpha}^2$, where rationals A= ______, B= ______, C= ______.

ε L= ______ is the smallest posint with $\boldsymbol{\mu}(L) + \boldsymbol{\mu}(L+1) + \boldsymbol{\mu}(L+2) = 3$. [*Hint:* If $\exists p^2 \bullet\!| \; k$ then $\boldsymbol{\mu}(k) = 0$.]

Y1: Below, N is a posint.

a Find, with proof, all N such that $\varphi(N)$ is prime.

b Suppose N composite and $N \notin \{4, 9\}$. Prove that $\boxed{\varphi(N) \leq N - 4}$.

c With p prime, let $N := 1 + 2p$. (See **10.5**P251.)
Prove: $[p \bullet\!| \; \varphi(N)]$ IFF N is prime.
Prove that N is prime IFF

$$*: \qquad 2^{N-1} \equiv_N 1.$$

When N prime, what, ITOf p, is $F := \text{Ord}_{\Phi(N)}(2)$?
Why doesn't $(*)$ give a polytime test for primality of N? Give an example of an $N = 1 + 2D$, with D odd, fulfilling $(*)$ yet N is composite. Here, what relation do you notice between F and D?
Are there ∞ly many such N?

d Generalize (c) somehow. E.g, generalize $(*)$ to: $\exists k \in [2..N)$ (with k satisfying some condition) such that $k^{N-1} \equiv_N 1$.
Alternatively, can you gen. how N is related to p?

Y2: Use "ntp-" to mean "non-trivial proper". Below, $\equiv$ means $\equiv_N$ for an $N \in \mathbb{Z}_+$. And b, c, x, y are integers.

i Suppose $N \bullet\!| \; [b \cdot c]$ yet $N \nmid b$ and $N \nmid c$. Prove that $d := \text{GCD}(b, N)$ is a ntp-factor of N.

ii (If some number has **three** mod-N sqroots, then we know that N is **not** prime, since $\mathbb{Z}_{\text{prime}}$ is a field.) Suppose $x^2 \equiv y^2$, but $x \not\equiv y$ and $x \not\equiv -y$. Produce a ntp-factor of N.

iii Rewrite the Miller-Rabin algorithm (P.249) so, if it discovers (mod-N) a $\sqrt{1}$ which is **not** ± 1, then it outputs a ntp-factor of N. The discovery can happen in either of the "`return false`" clauses.

Y3: Create/find an interesting NT problem strongly connected to the NT we did this (or last) semeseter. Here are some suggestions: **7.25 & 7.26**P177. **10.14**P266. **10.6**P252.

Y0:	___ ___ ___	150pts
Y1:	___ ___ ___	130pts
Y2:	___ ___ ___	130pts
Y3:	___ ___	95pts
Total:	___ ___ ___	505pts

NAME: ______

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

Signature: ______