NT & Crypto
MAT4930 *2H22*

Quizzes Q

Summer 2016

Number Sets. Expression $k \in \mathbb{N}$ [read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$"] means that k is a natural number; a ***natnum***. Expression $\mathbb{N} \ni k$ [read as "$\mathbb{N}$ ***owns*** k"] is a synonym for $k \in \mathbb{N}$.

$\mathbb{N}$ = natural numbers = $\{0, 1, 2, \dots\}$.

$\mathbb{Z}$ = integers = $\{\dots, -2, -1, 0, 1, \dots\}$. For the set $\{1, 2, 3, \dots\}$ of positive integers, the ***posints***, use $\mathbb{Z}_+$. Use $\mathbb{Z}_-$ for the negative integers, the ***negints***.

$\mathbb{Q}$ = rational numbers = $\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_+\}$. Use $\mathbb{Q}_+$ for the positive rationals and $\mathbb{Q}_-$ for the negative rationals.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

For $\omega \in \mathbb{C}$, let "$\omega > 5$" mean "ω *is* ***real*** *and* $\omega > 5$". [Use the same convention for $\geq, <, \leq$, and also if 5 is replaced by any real number.]

Use $\overline{\mathbb{R}} = [-\infty, +\infty] := \{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$, the ***extended reals***.

An "***interval of integers***" $[b \,..\, c)$ means the intersection $[b, c) \cap \mathbb{Z}$; ditto for open and closed intervals. So $[\mathrm{e} \,..\, 2\pi] = \{3, 4, 5, 6\} = [3 \,..\, 6] = (2 \,..\, 6]$. We allow b and c to be $\pm\infty$; so $(-\infty \,..\, -1]$ is $\mathbb{Z}_-$. And $[-\infty \,..\, -1]$, is $\{-\infty\} \cup \mathbb{Z}_-$.

Floor function: $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$. Ceiling fnc: $\lceil \pi \rceil = 4$. Absolute value: $|-6| = 6 = |6|$ and $|-5 + 2\mathbf{i}| = \sqrt{29}$.

Mathematical objects. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). trnfn: '*transformation*'. cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'. CoV: '*Change-of-Variable*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'. RoC: '*Radius of Convergence*'.

Soln: '*Solution*'. Thm: '*Theorem*'. Prop'n: '*Proposition*'. CEX: '*Counterexample*'. eqn: '*equation*'. RhS: '*RightHand side*' of an eqn or inequality. LhS: '*lefthand side*'. Sqrt **or** Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', *but* pt: '*point*' as in "a fixed-pt of a map".

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'.

The ***logarithm*** function, defined for $x>0$, is $\log(x) := \int_1^x \frac{dv}{v}$. Its inverse-fnc is $\exp()$.

For $x>0$, then, $\exp(\log(x)) = x = \mathrm{e}^{\log(x)}$. For real t, naturally, $\log(\exp(t)) = t = \log(\mathrm{e}^t)$.

PolyExp: '*Polynomial-times-exponential*', e.g, $[3 + t^2]\cdot\mathrm{e}^{4t}$. PolyExp-sum: '*Sum of polyexps*'. E.g, $f(t) := 3t\mathrm{e}^{2t} + [t^2]\cdot\mathrm{e}^t$ is a polyexp-sum.

Phrases. WLOG: '*Without loss of generality*'. IFF: '*if and only if*'. TFAE: '*The following are equivalent*'. ITOf: '*In Terms Of*'. OTForm: '*of the form*'. FTSOC: '*For the sake of contradiction*'. And ⯳ ="Contradiction".

IST: '*It Suffices To*', as in ISTShow, ISTExhibit.

Use w.r.t: '*with respect to*' and s.t: '*such that*'.

Latin: e.g: *exempli gratia*, '*for example*'. i.e: *id est*, '*that is*'. N.B: *Nota bene*, '*Note well*'. inter alia: '*among other things*'. QED: *quod erat demonstrandum*, meaning "end of proof".

Plex [2023g] quizzes so far...

Q1: Fri. 20 Jan Euler $\varphi(56) =$ ⌞. . . . . ⌟.

Mod K:=51, the reciprocal $\left\langle \frac{1}{20} \right\rangle_K =$ ⌞. . . . . ⌟ $\in [0\,..\,K)$.

[*Hint:* $\frac{1}{2}$] So $x =$ ⌞. . . . . ⌟ $\in [0\,..\,K)$ solves $5 - 20x \equiv_K 2$.

Q2: Wed. 25 Jan With $N := 85$, then $\varphi(N) =$ ⌊.....⌋. Thus EFT (Euler-Fermat) says that $3^{645} \equiv_N$ ⌊.....⌋ $\in [0 \,..\, N)$.

Q3: Fri. 27 Jan Note that $\text{GCD}(55, 33, 15) = 1$. Find particular integers S, T, U so that $55S + 33T + 15U = 1$:

$S=$ ⌞.....⌟ , $T=$ ⌞.....⌟ , $U=$ ⌞.....⌟ .

[*Hint:* $\text{GCD}\big(\text{GCD}(55, 33), 15\big) = 1$.]

Q4: Mon. 30 Jan With $M := 22$ and $\mathbf{J} := [0\,..\,M)$, use *repeated-squaring* to compute $6^{128} \equiv_M$ ⌞.....⌟ $\in \mathbf{J}$. Since 133 equals $2^7 + 2^2 + 2^0$, power $6^{133} \equiv_M$ ⌞.....⌟ $\in \mathbf{J}$.

[*Hint:* Compute with symm. residues, and use periodicity.]

Q5: Fri. 03 Feb Carmichael fnc $\boldsymbol{\lambda}(385 \cdot 29 \cdot 43) = 2^A \cdot 3^B \cdot 5^C \cdot 7^D \cdot 11^E$
where $A=$ ⌊...⌋, $B=$ ⌊...⌋, $C=$ ⌊...⌋, $D=$ ⌊...⌋, $E=$ ⌊...⌋.

Q6: Mon. 20 Feb Over alphabet $\mathbf{G} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, our UD code has length-spectrum $\vec{\ell} = (1, 2, 2, 2, 2, 3)$. Its Kraft-sum equals $\Sigma(\vec{\ell}) = 1 - \_\_\_\_\_ = \_\_\_\_\_$.

Ordering our alphabet as $\mathtt{a} < \mathtt{b} < \mathtt{c}$, the proof from our previous class constructs the following specific prefix code with spectrum $\vec{\ell}$:

____ ____ ____ ____ ____ ____.

Home-U due, 11:30AM. Wed. 22 Feb ... slid under my office door, LIT402. *After* having successfully handed-in your Home-U, *email me* that you have done so, and include your Team-U number in the message.

Have printed-out Problem sheet, and made that the *first page* of youw write-up. Number the pages (probably by hand) 1/47 [that is the Problem sheet], 2/47 .... 47/47. Handwrite-in the blanks on the problem sheet, the requested answers.

Put name/ordinals/Team-number where requested, and sign the Honor Code.

Class-U. Wed. 22 Feb

In-class closed-book Open-Brain exam. Please bring lined-paper for computation. You may also want to bring colored pens/pencils for diagrams.

Q7: Fri. 24 Feb *Am I in class today?*

circle one *"Yes!"* *"Of course!"*

"I wouldn't miss it for the world!"

Q8: Fri. 10 Mar Congruences $z \equiv_{18} 5$, and $z \equiv_5 17$, fuse into $z \equiv_{90} T$, where $T =$ ⌞ . . . . . ⌟ $\in [0 \,..\, 90)$.

[Note: $\mathrm{LCM}(18, 5) = 90$].

Q9: Mon. 20 Mar Base-2 (distribution-)entropy of $\vec{\mathbf{v}} := \left(\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{4}\right)$ is $\mathcal{H}(\vec{\mathbf{v}}) =$ ⌞ . . . . . ⌟ .

The due-date for this year's *Robert Long Essay Competition (RLEC)* is Thurs., 30 Mar., with a PDF emailed to Prof. K. **True!** **Yes!**

QA: Fri. 24 Mar Legendre symbol $\left(\frac{47}{53}\right)$ is +1 −1 0.

QB: Fri. 14 Apr ∃*Math Festival* this **Sunday, 16Apr,** 10AM–1PM, in the *Rion Ballroom* of Reitz Union, open to all.

Circle: **True!** **Yes!** *What's* "Math"?

End of semester; looking forward to our Games Party!