NT & Crypto
MAT4930 *2H22*

Quizzes P

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*** <u>and</u> $\omega > 5$". [Use the same convention for $\geq, <, \leq$, and also if 5 is replaced by any real number.]

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). 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*', <u>*but*</u> 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*** fnc, 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".

P1: Wed. 30 Jun With $M := 22$ and $\mathbf{J} := [0 \,..\, M)$, use *repeated-squaring* to compute $6^{1024} \equiv_M$ ______ $\in \mathbf{J}$. Since 1033 equals $2^{10} + 2^3 + 2^0$, power $6^{1033} \equiv_M$ ______ $\in \mathbf{J}$.

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

P2: Fri. 01 Feb LBolt: $\text{GCD}(70, 42) = \_\_\_\_\_\_ \cdot 70 + \_\_\_\_\_\_ \cdot 42$.

So (LBolt again) $G := \text{GCD}(70, 42, 60) = \_\_\_\_\_\_$ and $\_\_\_\_\_\_ \cdot 70 + \_\_\_\_\_\_ \cdot 42 + \_\_\_\_\_\_ \cdot 60 = G$.

P3: Wed. 06 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 $A = \_\_\_$, $B = \_\_\_$, $C = \_\_\_$, $D = \_\_\_$, $E = \_\_\_$.

P4: Fri. 08 Feb *Magic integers* G_1, G_2, G_3, each in $[0..330)$, are such that the $g{:}\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_{11} \hookrightarrow\!\!\!\!\to \mathbb{Z}_{330}$ mapping is a ring-isomorphism, where

$$g\big((z_1, z_2, z_3)\big) := \Big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 \Big\rangle_{330}.$$

Then $G_3 = \underline{\qquad\qquad} \in [0..330)$. $\begin{bmatrix}\text{Reduced product is} \\ \vec{\mathbf{R}} = (66, 55, 30).\end{bmatrix}$

P5: Mon. 11 Feb TMWFIt, 8 is a mod-125 primroot, since its mult-order $\pmod{125}$ is $100 \stackrel{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute <u>the</u> corresponding mod-250 primroot $R = \underline{\qquad\qquad} \in [0..250)$.

P6: Fri. 01 Mar For prime $p = 59$, value -2 is a p-QR. *T* *F*

[*Hint:* LST or LST+RS.]

P7: Mon. 11 Mar a Suppose $y \in \mathrm{QR}_N$, where N is oddprime. You compute Bézout mults U and V st. $yU + NV = 1$. Then "*U is a mod-N square*" is: *AT* *AF* *Nei*

b With $p := 323$, and $H := \frac{p-1}{2}$, note $66^H \equiv_p -2$. Thus p is $\underline{\qquad\qquad\qquad\qquad\qquad\qquad}$.

P8: Mon. 08 Apr De-Elias bit-string 0110100100001011000010, writing it in form

$\langle n_1 \rangle \langle n_2 \rangle \ \ldots \ \langle n_L \rangle$ $\boxed{\text{remaining bits}}$:

$\llcorner$. . . . . $\lrcorner$.

P9: Wed. 17 Apr Let $f(x) := x^2 - 4x - 2$, and $\mathbf{z}_1 := c_0 := 3$; so $f(\mathbf{z}_1) \equiv_5 0$. Note $f'(\mathbf{z}_1) =$ $\llcorner$. . . . . $\lrcorner$ $\not\equiv_5 0$. Use Hensel's lem. to compute coefficients $c_j \in [0 .. 5)$ [*put them in the blanks, below*]

$$\mathbf{z}_4 = \underbrace{\overbrace{c_0 \cdot 5^0 + \underline{\quad\quad} \cdot 5^1}^{\mathbf{z}_2} + \underline{\quad\quad} \cdot 5^2}_{\mathbf{z}_3} + \underline{\quad\quad} \cdot 5^3$$

so that *natnums* $\mathbf{z}_j := \sum_{i \in [0 .. j)} c_i 5^i$ satisfy

$$f(\mathbf{z}_j) \equiv 0 \pmod{5^j}, \quad \text{for } j = 2, 3, 4.$$

PA: $*^{\text{Mon.}}_{\text{22 Apr}}$ Let $f(x) := x^2 - x - 17$, and $\mathbf{z}_1 := c_0 := 2$; so $f(\mathbf{z}_1) \equiv_5 0$. Note $f'(\mathbf{z}_1) =$ ________ $\not\equiv_5 0$. Use Hensel's lem. to compute coefficients $c_j \in [0 .. 5)$ [*put them in the blanks, below*]

$$\mathbf{z}_4 = \underbrace{\overbrace{c_0 \cdot 5^0 + \underline{\quad\quad} \cdot 5^1}^{\mathbf{z}_2} + \underline{\quad\quad} \cdot 5^2}_{\mathbf{z}_3} + \underline{\quad\quad} \cdot 5^3$$

so that *natnums* $\mathbf{z}_j := \sum_{i \in [0 .. j)} c_i 5^i$ satisfy

$$f(\mathbf{z}_j) \equiv 0 \pmod{5^j}, \quad \text{for } j = 2, 3, 4.$$

This semester we studied Affine codes, Diffie-Hellman, El Gamal, RSA, LBolt, Chinese Remainder thm, Euler phi, Carmichael lambda, repeated squaring, Primitive roots, Legendre & Jacobi symbols, Quad reciprocity, Kraft-McMillan, expected coding-length, Huffman, Ziv-Lempel, Entropy, WLLN, Hamming codes,

among other topics. T F

Henselling to fame and fortune: Lisp:

```
% (hensel 2  :p 5  :f (cree-poly 1 -1 -17) :EndExpon 3)

  Henselling over ring <InTeGeRs>, using prime P := 5.

  Evaluate poly  F(x) := x^2 + -1x + -17
at  z1 := 2.  Happily, F(2) = -15 =P= 0,
so let's lift z1, if possible.

  Note  F'(x) = 2x + -1.
Hence   F'(z1) =P= 3  is NOT mod-P zero.  LBolt
gives
        <1/3>_P  =  2.

The update rule [Newton's Method] is:

 *:  z_{j+1}  ==  z_j  -  2*F(z_j)     [mod 5^{j+1}].

Ratio  R := [F(z_j) / 5^j]  is an integer.
Let  c_j  , modulo 5.  Thus

**:  z_{j+1}  ==  z_j  +  [c_j * 5^j]   [mod 5^{j+1}].

    Iterating:

  j:      5^j |       z_j |           F(z_j) | c_j
---+----------+-----------+------------------+----
  1:        5 |         2 |              -15 |   1
  2:       25 |         7 |               25 |   3
  3:      125 |        82 |             6625 |   4
```

Note that $F(82) = 6625 = 1000 \cdot 6 + 625$. So

$$\frac{F(82)}{125} = [8 \cdot 6] + 5 \equiv_5 [-2 \cdot 1] + 0\,.$$

Hence $c_3 \equiv -1 \cdot 2 \cdot -2 \equiv 4$.