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: Carefully state Fermat's Little Thm.
Carefully state the Euler-Fermat Thm.
Carefully state the Legendre-symbol Thm.
Carefully state the Quadratic-reciprocity Thm.
Carefully state the Jacobi-symbol Thm.
Carefully state the Primitive-root Thm.
Carefully state Hensel's Lemma.
Carefully state the Huffman-coding Thm.
Describe the *Elias code* from natnums into bitstrings.

A5: Short answer: Show no work.

a Consider the four congruences C1: $z \equiv_8 1$, C2: $z \equiv_{18} 15$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 3$. Let z_j be the *smallest natnum* satisfying (C1) $\overset{\text{All}}{\therefore}$ (Cj). Then

$z_2 =$ ______ ; $z_3 =$ ______ ; $z_4 =$ ______ .

b Euler $\varphi(77000) =$ ______ .

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

c $N := \varphi(100) =$ ______ . So $\varphi(N) =$ ______ .

EFT says that $3^{3221} \equiv_N$ ______ $\in [0..N)$. Hence (by EFT) last two digits of $7^{[3^{3221}]}$ are ____ .

d LBolt: $\text{Gcd}(72, 45) =$ ______ $\cdot 72 +$ ______ $\cdot 45$.

So (LBolt again) $G := \text{Gcd}(72, 45, 105) =$ ______ and

______ $\cdot 72 +$ ______ $\cdot 45 +$ ______ $\cdot 105 = G$.

e *Magic integers* $G_1 =$ ______ , $G_2 =$ ______ , $G_3 =$ ______ , each in $(-165..165]$, are st. mapping $g: \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \to \mathbb{Z}_{330}$ is a ring-isomorphism, where

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

Verify for your map: $g\big((1,1,1)\big) = 1$ and $[5 \cdot 11] \bullet| G_1$ and analogously for G_2 and G_3.

f As polynomials in $\mathbb{Z}_7[x]$, let

$$B(x) := x^4 + 2x^3 + 3x^2;$$
$$C(x) := x^3 + 3x^2 + 5x + 3.$$

Write t.fol polys, using coeffs in $[-3..3]$. Compute quotient and remainder polynomials,
$q(x) =$ ______ & $r(x) =$ ______ ,
with $B = [q \cdot C] + r$ and $\text{Deg}(r) < \text{Deg}(C)$.

g Note $p := 113$ is prime. The (multiplicative) order of 2 mod 113 is ______ .

[*Hint:* $113 - 1$ equals $2^4 \cdot 7$.]

h TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is $100 \overset{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ ______ $\in [0..250)$.

i With $V := 28 + 21i$ and $D := 5 + 3i$, 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 $\overline{D}$.]

j Bitstring "0001000101111111101101001", via the Elias code, decodes to ______ , a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits ______ .

Conv, Elias(91)= ______ (bitstring)

A6: Please state Wilson's Thm. Now give a careful detailed proof. [Bonus for Legendre-Symbol Theorem]

A7: Let $f(x) := x^2 - 4x - 2$ and $z_0 := c_0 := 1$. Note $f(z_0) \equiv_5 0$. Note $f'(z_0) =$ ______ $\not\equiv_5 0$.

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

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

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

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

for $k = 1, 2, 3$.