Staple!

Team A____

NT & ECC MAT4930 5662 — **Home-A** — Prof. JLF King, *Touch*: 2Jul2018

Hello. Essays violate the CHECKLIST at *Grade Peril*! Exam is due by **8:28AM, Friday, 12Oct2007**, handed-in, in class, with all team-mates present.

Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

A1: Show no work.

a So $z=$ ______ is the smallest natnum satisfying

$$z \equiv_{34} 1, \quad z \equiv_{27} 9, \quad z \equiv_{51} 18, \quad z \equiv_{30} -3.$$

b And $y=$ ______ is the smallest natnum with

$$y \equiv_{9} 0, \quad y \equiv_{15} 12, \quad y \equiv_{25} 7, \quad y \equiv_{21} 17.$$

c Let $A := -13 + \boldsymbol{i}$, $B := 3 + 22\boldsymbol{i}$, $C := 2 + 9\boldsymbol{i}$. So $G := \text{Gcd}(A, B, C)=$ ______. (CForm; real & imag non-negative.) Use the LBolt Alg twice to find three Gaussian-integers for which G equals

______ $\cdot A +$ ______ $\cdot B +$ ______ $\cdot C = G$.

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

$$B(x) := x^4 - 2x^3 + x - 2\,;$$
$$C(x) := x^3 + 3x^2 - 3x\,.$$

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 $\text{Deg}(r) < \text{Deg}(C)$.

e With B, C from above, polys in $\mathbb{Z}_7[x]$: Let D be $\text{Gcd}(B, C)$. Write these three polys using coeffs in [-3 .. 3]: The **monic** $D(x) =$ ______.
Compute polys $S(x)=$ ______,
$T(x)=$ ______ st. $[S \cdot B] + [T \cdot C] = D$.

f Easily, $\varphi(175)=$ ______. Consequently, $17^{2007} \equiv_{175}$ ______ $\in [0 .. 175)$. [*Hint:* Fermat, Euler, working mod 175.]

g Note $p := 137$ is prime. The (multiplicative) order of 7 mod 137 is ______.
[*Hint:* $p - 1$ has very few prime factors.]

Essay questions: Type in complete sentences and __also__ fill-in the blanks. Each essay starts a new page.

A2: i Use Pollard-ρ to find a non-trivial factor of $M := 59749$, using seed $s_0 := 7$ and map $f(x) := 1+x^2$. Make a nice table, labeled

Time	Tortoise	Hare	$s_{2k} - s_k$	Gcd(??)

—*but* ***replace*** *the "??" with the correct expression.* You found non-trivial factor $E :=$ ______.
The hare Hits into the tortoise at time $H :=$ ______.

Repeat, showing the table for $s_0 := 24$. Experiment with different seeds; what is the typical running time? How is it related to the factor you find?

ii A seed s determines a ***tail***; the smallest natnum T for which there is a time $n > T$ with $f^n(s) = f^T(s)$. The smallest such n is $T+L$ where L is the ***period***. Derive (picture+reasoning) a formula for the hitting time $H(T, L)$. [*Hint:* $H(0, L) = L$.]

iii Produce a Floyd-done-twice algorithm that computes both T and L. The number, N, of f-evaluations is upper-bounded by some small constant times $T+L$ (=arclength of ρ). How small can you get $N(T, L)$? [*Hint:* $N(0, L) = 3L$.]

A3: Let M be the matrix

$$\begin{bmatrix} 10 - 10\boldsymbol{i} & -18 - 1\boldsymbol{i} & -1 - 2\boldsymbol{i} \\ -18 - 1\boldsymbol{i} & 16 + 17\boldsymbol{i} & -2 + 1\boldsymbol{i} \\ 8 - 9\boldsymbol{i} & -17 + 1\boldsymbol{i} & 0 \end{bmatrix}.$$

i Please put M in SNF, over the GIs, and compute the row and column bookkeeper matrices.

ii Give a GI-basis for the GI-nullspace of M.

iii Determine if $\mathsf{T} := \begin{bmatrix} 84+13\boldsymbol{i} \\ -64-88\boldsymbol{i} \\ 77+4\boldsymbol{i} \end{bmatrix}$ is in the GI-range of M. If so, derive a specific solution S for which $\mathsf{M} \cdot \mathsf{S} = \mathsf{T}$. What is the general solution? Is there a not-all-zero $\mathbb{Z}$-solution? (Prove your claim.)

End of Home-A

A1:	___ ___ ___	280pts
A2:	___ ___ ___	145pts
A3:	___ ___ ___	215pts
Total:	___ ___ ___	640pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: ....

Ord: ....

Ord: ....