Staple!

Team B

NT MAS4203 *4D70* | **Home-B** | Prof. JLF King Friday, 20Jul2018

Due: BoC, Tuesday, 24Jul2018. *Fill-in* every *blank* on this sheet. This is the *first-page* of your write-up, with your essays securely stapled to it.

B1: *Show no work. Write* **DNE** *in a blank if the described object does not exist or if the indicated operation cannot be performed.*

a "Integer $49 \in \mathrm{QR}_{91}$" T F and "$100 \in \mathrm{QR}_{121}$" T F.

Value $K := 857$ is prime. So "$2 \in \mathrm{QR}_K$" T F and "$-8 \in \mathrm{QR}_K$" T F.

The prime decomposition of $L := 22673$ is $7 \cdot 41 \cdot 79$. So "$2 \in \mathrm{QR}_L$" T F.

b 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

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

c As polynomials in $\Gamma := \mathbb{Z}_7[\![x]\!]$, 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]; use $\equiv$ for equality in $\mathbb{Z}_7$ and in Γ. Compute quotient and remainder polys,

$q(x) \equiv$ & $r(x) \equiv$,

with $B \equiv [q \cdot C] + r$ and $\mathrm{Deg}(r) < \mathrm{Deg}(C)$.

Let $D := \mathrm{GCD}(B, C)$. **Monic** $D(x) \equiv$.

Compute polys $S(x) \equiv$,

$T(x) \equiv$ st. $[S \cdot B] + [T \cdot C] \equiv D$.

[Alt Bézout pair: $S(x) \equiv -x^2 + 1$ and $T(x) \equiv x^3 + 2x^2 + 3x$.]

d A poly $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ of form $f(x) := \sum_{k=0}^{3} C_k x^k$ satisfies $[\forall z \in \mathbb{Z}_3 : f(z) \equiv z^2]$, yet $C_1 \not\equiv 0$. With each $C_j \in \{0, 1, 2\}$, $C_0 \equiv$, $C_1 \equiv$, $C_2 \equiv$, $C_3 \equiv$.

OYOP: *Your 2 essay(s) must be* TYPED, *and Double spaced. Use the Print/Revise cycle to produce good, well thought out, essays. Start each essay on a new sheet. Do* **not** *restate the problem; just solve it.*

B2: The building block of a cryptosystem uses *N-Serial* numbers, for large values of N. (Defns are below.)

i Prove: *For each positive integer N, there exists an N-Serial number.*

ii Produce (with proof, 'natch) a 5-Serial number $V =$. (A little extra credit: Can you prove that your V is the *smallest* 5-Serial number?)

Defns. An integer **S** is ***Cubish*** if it is divisible by some member of $\{8, 27, 64, 125, 216, \ldots, k^3, \ldots\}$; otherwise **S** is ***Flat***. (E.g $0, 162, 375$ are Cubish, and $1, 12, 90, 36$ are Flat.)

For N,**S** posints, our **S** is "***N*-Serial**" if *each* member of $\{\mathbf{S} + j\}_{j=0}^{N-1}$ is Cubish. [E.g, **S**=80 is 2-Serial, since $8 \nmid 80$ and $27 \nmid 81$, but 80 is not 3-Serial, as no cube divides 82. Another example: 375 is 2-Serial but not 3-Serial.]

B3: Below, p is an odd prime, $\langle\cdot\rangle$ means $\langle\cdot\rangle_p$, $H := \frac{p-1}{2}$, and target $\mathbf{A} \perp p$.

For large p, we quickly determine if $\mathbf{A} \in \mathrm{QR}_p$; simply compute $\langle \mathbf{A}^H \rangle$ by repeated-squaring and ask $\langle \mathbf{A}^H \rangle \overset{?}{=} 1$. But it may be time-consuming to actually *find* a square-root of **A**. Here are three special cases where it is quick.

[Relevant are LST(a,b,c,d) and Wilson's thm. And...?]

α LST tells us that $p \equiv_4 1$ implies $-1 \in \mathrm{QR}_p$. Prove that $H!$ (i.e, H factorial) is a mod-p sqroot of -1.

β Now suppose $p \equiv_4 -1$ and $\mathbf{A} \in \mathrm{QR}_p$. Prove that $\mathbf{A}^{\frac{p+1}{4}}$ is a mod-p sqroot of **A**.

γ Finally, consider $p \equiv_8 5$ and $\mathbf{A} \in \mathrm{QR}_p$. Prove that either

$$R := \mathbf{A}^{\frac{p+3}{8}} \quad \text{or} \quad S := 2\mathbf{A} \cdot [4\mathbf{A}]^{\frac{p-5}{8}}$$

is a mod-p sqroot of **A**.

B1:	___ ___ ___	115pts
B2:	___ ___	95pts
B3:	___ ___ ___	115pts
Total:	___ ___ ___	325pts

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: