Staple!

Team: V

NT-Cryptography MAT4930 *0329* **Home-V** Prof. JLF King Monday, 20Mar2023

Due: Monday, 27Mar.

Class-V will take place on Wednesday, 29Mar.

Fill-in every *blank* on this sheet. Write **DNE** if the object does not exist or the operation cannot be performed. NB: **DNE** $\neq \{\} \neq 0$.

This sheet is the *first-page* of your write-up.

V1: Your goal is to prove:

†: The Sixteen Thm. *For each oddprime p, the congruence $x^8 \equiv_p 16$ admits a solution.*

In your WU, you may use $\sim$ for $\equiv_4$ and $\approx$ for $\equiv_8$, if you wish. But use $\equiv_p$ or $\equiv$ for congr-mod-p.

α FTSOC, suppose you have a p with *no* solution to $x^8 \equiv_p 16$. Prove that $2 \in \text{NQR}_p$ and $-1 \in \text{QR}_p$. Use LSThm to compute $\langle p\rangle_8$ as a non-negative residue.

β Let r be a p-sqroot of -1. Use LST to prove that $r \in \text{QR}_p$. But use a different part of LST to prove that $r \in \text{NQR}_p$. *Contradiction*, QED.

γ Give an example of a 2 digit prime $q :=$ ____ with $2 \in \text{NQR}_q$ and $-1 \in \text{QR}_q$. Using symmetric residues, $\text{QR}_q = \{$ ____ $\}$ and

$\text{NQR}_q = \{$ ____ $\}$. Finally, $[$ ____ $]^8 \equiv_q 16$.

Give an example of a 3 digit prime $p :=$ ____ with $2 \in \text{NQR}_p$, and values $r :=$ ____ and $s :=$ ____ satisfying $r^2 \equiv_p -1$ and $s^2 \equiv_p r$.

Defn. An odd integer k is "**4Pos**" if $k \equiv_4 +1$; is **4Neg** if $k \equiv_4 -1$; is **8Near** if $k \equiv_8 \pm 1$ (either); is **8Far** if $k \equiv_8 \pm 3$. □

1: Legendre-symbol Thm. *Fix an odd prime p and $H := \frac{p-1}{2}$. Use $\langle\cdot\rangle_p$ for symmetric residue, selecting from $[-H \,..\, H]$. For each integer z:*

a: *The (symmetric) residue $\langle z^H\rangle_p$ equals $\left(\frac{z}{p}\right)$.* *Euler criterion.*

b: *For x, z integers: $\left(\frac{x}{p}\right) \cdot \left(\frac{z}{p}\right) = \left(\frac{xz}{p}\right)$. I.e, mapping $x \mapsto \left(\frac{x}{p}\right)$ is totally-multiplicative.* [*I.e, $x \mapsto \left(\frac{x}{p}\right)$ is a semigroup-hom $(\mathbb{Z}_p, \cdot, 1) \to (\{\pm 1, 0\}, \cdot, 1)$, hence is a group-hom $(\Phi_p, \cdot, 1) \to (\{\pm 1\}, \cdot, 1)$. This holds also for p=2.*]

c: *Value $-1 \in \text{QR}_p$ IFF p is 4Pos, i.e, $\left(\frac{-1}{p}\right) = [-1]^{\frac{p-1}{2}}$.*

Courtesy Wilson's Thm, *value $r := [H!]$ is a mod-p sqroot of -1. i.e, is a p-RONO,*[♡1] *when $p \in$ 4Pos.*

d: *The number 2 is a p-QR IFF p is 8Near, that is, $p \equiv_8 \pm 1$. I.e, $\left(\frac{2}{p}\right) = [-1]^{\frac{p^2-1}{8}}$.* ◊

V2: Below, p is oddprime, $\langle\cdot\rangle$ means $\langle\cdot\rangle_p$, $H := \frac{p-1}{2}$, and target $\mathbf{A} \perp p$.

For large p, we quickly determine if $\mathbf{A} \in \text{QR}_p$; simply compute $\langle \mathbf{A}^H\rangle$ by repeated-squaring and ask $\langle \mathbf{A}^H\rangle \stackrel{?}{=} 1$. But it may be time-consuming to actually *find* a square-root of $\mathbf{A}$. 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 $-1 \in \text{QR}_p$. Prove that $H!$ (i.e, H factorial) is a mod-p sqroot of -1.

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

γ Finally, consider $p \equiv_8 5$ and $\mathbf{A} \in \text{QR}_p$. 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 $\mathbf{A}$.

[♡1] RONO is "(square-)Root Of Negative-One".

V3: Define $T := 2331717$ and $B := 10953506281$.

a Compute Jacobi-symbol $\left(\frac{T}{B}\right)$ using non-negative residues, showing where the sign changed due to *QuadRecip* or *powers-of-two*.

Redo the computation using symmetric-residues, showing sign changes due to: *QuadRecip* or *powers-of-two* or *negative top number*.

b Use Pollard ρ to factor B, using map $x \mapsto \langle x^2 + 1 \rangle_B$ and various seeds. Do you find a factor before time 1000?

c Determine whether T is a mod-B quadratic-residue. If it is, can you find a square-root?

z Implement the Elias-δ-code. Encode $N := 513$, briefly describing the steps.

For all of the above, include your computer code, reasonably typeset (in a large font) and *carefully commented*.

V1:	___ ___ ___	155pts
V2:	___ ___ ___	105pts
V3:	___ ___	90pts
Total:	___ ___ ___	350pts

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:
....