Staple!

Ord: ___ ___

NT
MAS4203 *4D70*

Indiv-Proj-D

Prof. JLF King
Frid, 19Apr2019

Due: BoC, 3PM, Thursday, 25Apr2019

slid *completely* under my office door, 402 LITTLE HALL. *Fill-in* every *blank* on this sheet. Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed. OYOP: *Your 3 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.*

D1: Number $p := 79380001$ is prime. Compute the multiplicative order $M =$ _____, of 7 in $\mathbb{Z}_p$, showing the steps in the Descent Algorithm. The algorithm does _____ repeated-squarings.

D2: Prime $q \equiv_4 1$ is such that $p := 1 + 2q$ is prime. Prove that 2 is a p-primroot. [E.g, $(q, p) = (5, 11), (29, 59), (41, 83), (53, 107), (89, 179), (113, 227), \ldots$].

[*Hint:* The number of p-primroots is $\varphi\big(\varphi(p)\big)$. State and prove lemmas about the possible mult-orders of NQRs and QRs mod-p.]

D3: 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,* $\left(\frac{2}{p}\right) = [-1]^{\frac{p^2-1}{8}}$. ◊

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

D1:	___	0pts
D2:	___ ___	00pts
D3:	___ ___ ___	000pts

Please PRINT your name and ordinal. Ta:

Ord: ____

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: ____

Folks, I've had a great time learning Number Theory with you. It's been a pleasure having a lively (and funny) class of Enthusiastic NTers. Stop by in future semesters for Math/chess/coffee/frisbee...
Cheers, Prof. K