Staple!

Ord: ___ ___

NT-Cryptography
MAT4930 *2H22*
MAT6932 *21BH*

IndividualOP-Y

Prof. JLF King
Fri., 15Apr2016

This IOP is due **4:30PM, Thur., 21Apr2016**, slid *completely* under my office door, 402 LITTLE HALL. This sheet is "Page 1/N", and you've labeled the rest as "Page 2/N",..., "Page N/N".

Your 2 essay(s) must be TYPED, *and Double or Triple 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.*

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

Recall

Defn. For a prime p and integer z, the ***Legendre-symbol*** is written as $\left(\frac{z}{p}\right)$ or, in email, also as $(z\,//\,p)$.

By defn, $\left(\frac{z}{p}\right)$ is +1, if $z \in \mathrm{QR}_p$; is −1, if $z \in \mathrm{NQR}_p$; and is 0, if $z \not\perp p$, i.e $z \mid\!\bullet\, p$.

An odd integer k is **"4POS"** if $k \equiv_4 +1$; is 4**NEG** if $k \equiv_4 -1$; is 8**NEAR** if $k \equiv_8 \pm 1$ (either); is 8**FAR** 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: *For x and z integers: $\left(\frac{x}{p}\right)\cdot\left(\frac{z}{p}\right) = \left(\frac{xz}{p}\right)$. I.e, the mapping $x \mapsto \left(\frac{x}{p}\right)$ is totally-multiplicative. [I.e, $x \mapsto \left(\frac{x}{p}\right)$ is a group-hom $\left(\Phi_p, \cdot, 1\right) \to \left(\{\pm 1\}, \cdot, 1\right)$; and this part holds also for p=2.]*

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

c: *Value $-1 \in \mathrm{QR}_p$ 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, 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, $\left(\frac{2}{p}\right) = [-1]^{\frac{p^2-1}{8}}$.*

Y1: 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 ∼ for $\equiv_4$ and ≈ 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 $2 \in \mathrm{NQR}_p$ and $-1 \in \mathrm{QR}_p$. 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 $r \in \mathrm{QR}_p$. But use a different part of LST to prove that $r \in \mathrm{NQR}_p$. *Contradiction*, QED.

γ Give an example of a 2 digit prime $q :=$ [ ] with $2 \in \mathrm{NQR}_q$ and $-1 \in \mathrm{QR}_q$. Using symmetric residues, $\mathrm{QR}_q = \{$ [ ] $\}$ and $\mathrm{NQR}_q = \{$ [ ] $\}$. Finally, $[\ ]^8 \equiv_q 16$.

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

Y2: Let $\vec{1} :=$ 1111..., the half-∞ constant-1 bit-string. Using our Ziv-algorithm, with dictionary that [initially] only has the nullword, we start parsing $\vec{1}$.

Let $P(k)$ be the largest-number of bits we've parsed, having used-up at most k many bits from $\vec{1}$. I.e, we Ziv-parse, and we eventually parse a new word [which we enter into our dictionary], having read exactly $P(k)$ many bits, in total, where $P(k) \leqslant k$. As we scan for the next new word, we run past the k^{th}-bit in $\vec{1}$.

i Give an approximate formula for $N(k)$, the number of words you've parsed, having read the first $P(k)$ many bits.

ii Let $Z(k)$ be the length of the Ziv-compressed bit-string that encodes the first $P(k)$ many bits in the source-string. When k is large, give a pretty good estimate for $Z(k)$; a "closed formula", neither having a $\sum$ summation operator, nor a $\prod$ product operator.

What are approximate values for $N(500,000)$, and for $Z(500,000)$?

Compute $\lim_{k\to\infty} \frac{Z(k)}{k}$.

End of IndividualOP-Y

Y1: ___ ___ ___ 155pts

Y2: ___ ___ ___ 155pts

Total: ___ ___ ___ 310pts

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 have had a great time working with you this Semester. Stop by next semester to "Talk Math". Cheers, Prof. Sieve-brain