

NT-Cryptography Prof. JLF King
 MAT4930 2H22 IndividualOP-Y Fri., 15Apr2016
 MAT6932 21BH

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 TYPESET, and Double or Triple spaced. Use the Print/Revise cycle to produce good, well thought out, essays. Start each essay on a NEW sheet of paper. Do not restate the problem; just solve it.

Please 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

$$\left(\frac{z}{p}\right) \text{ or, in email, also as } (z//p).$$

By defn, $\left(\frac{z}{p}\right)$ is +1, if $z \in \text{QR}_p$; is -1, if $z \in \text{NQR}_p$; and is 0, if $z \not\equiv p$, i.e. $z \not\equiv \bullet p$.

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: 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 $(\Phi_p, \cdot, 1) \rightarrow (\{\pm 1\}, \cdot, 1)$; 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 $-1 \in \text{QR}_p$ 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, when $p \in 4\text{Pos}$.

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

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 $s^2 \equiv_p r$.

Y2: Let $\vec{1} := 1111\dots$, 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 $P(k) \leq k$. 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 $\lim_{k \rightarrow \infty} \frac{Z(k)}{k}$.

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*