

NT MAS4203 4D70 IOP-D Prof. JLF King Tuesday, 07Aug2018

Due: BoC, 2PM, Friday, 10Aug2018

[games-party location] Fill-in every blank on this sheet. This is the first-page of your write-up, with your essays securely stapled to it.

D1: Show no work.

Let $N := 9876!$ (factorial). The base-10 numeral of N , ends in _____ many zeros?

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.

D2: Prime $q \equiv 1 \pmod{4}$ is such that $p := 1 + 2q$ is prime. Prove that 2 is a p -primroot. [E.g. $(q, p) = (5, 11), (29, 59), (41, 83), (53, 107), (89, 179), (113, 227), \dots$].

D3: An N -card deck is on the table. The positions of the cards, from table up, are $0, 1, \dots, N-1$. For $x \in \mathbb{Z}$, use $\langle x \rangle_N$ for the number in $[0..N)$ that is mod N congruent to x . [The card in position $x \in [0..N)$ has x cards below it.]

To shuffle the deck, separate it into a lower half and an upper half. With the halves side-by-side, perfectly interleave the cards. Here you have a decision: Is the new table card (the bottommost card) from the Upper-half or from the Lower-half? Call these Upper and Lower shuffles, respectively. For a lower shuffle, card 0 is a fixed-point.

When N is odd, the upper/lower decision is the same as deciding whether it is the upper or lower half which has one more card than the other. The shuffle permutation is a map $S: [0..N) \rightarrow [0..N)$. Use $S^{\circ k}$ for its k -fold composition; e.g., $S^{\circ 3} = S \circ S \circ S$.

i In the four cases, N odd/even, shuffle Upper/Lower, write [and prove] a formula for its k -fold composition. [Sugg: Derive $LS_N()$ first.]

When $N = 2H + 1$ odd:

$US_N^{\circ k}(x) =$ _____

$LS_N^{\circ k}(x) =$ _____

When $N = 2H$ even:

$US_N^{\circ k}(x) =$ _____

$LS_N^{\circ k}(x) =$ _____

ii For both N odd and even, determine a non-trivial formula for the return time UT_N and LT_N ; the smallest posint k at which time the deck has returned to its original order; i.e. $S^{\circ k} = Id$. Your formula will have the form "The smallest posint k such that [some congruence holds]". You may be able to be more explicit, using Euler-phi, or Carmichael, or Descent Alg or Wilson's or....

For an $\mathbf{m} \in [0..N)$: If

$\forall k : S^{\circ k} = Id \iff S^{\circ k}(\mathbf{m}) = \mathbf{m},$

then we call \mathbf{m} a magic card. For the four Odd/Even Upper/Lower cases, produce criteria OTForm "If fnc(x) is coprime to fnc(N), then x is magic."

iii Compute $UT_{52} =$ _____ and $LT_{52} =$ _____
 $UT_{204} =$ _____ and $LT_{204} =$ _____

iv In this same vein, do something (non-trivial) extra. Can Quad-Recipr relate shuffles in two different-sized decks? Can Hensel's lemma give info about PoP deck-sizes?

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