NT-Cryptography
MAT4930 2H22  Home-V Prof. JLF King
MAT0932 21BH

Due: BoC, Monday, 15Feb2016, with all team-members present. Fill-in every blank on this sheet. This sheet is the first-page of your write-up, with your essays securely stapled to it.

V1: Show no work. Write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

V2: Magic integers \( G_1 = \), \( G_2 = \), \( G_3 = \), \( G_4 = \), each in \([0..1260]\), are st. \( g: \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{1260} \to \mathbb{Z}_{1260} \) is a ring-iso, where

\[
g((z_1,z_2,z_3,z_4)) = \left( z_1G_1 + z_2G_2 + z_3G_3 + z_4G_4 \right)_{1260}
\]

Now consider poly \( h(x) := \lfloor x + 59\rfloor \lfloor x - 1\rfloor \lfloor x + 83\rfloor \). Find all solutions to congruences \( h(x) \equiv 0 \pmod{M} \), for \( M = 7, 4, 9, 5 \), displaying the results in a nice table. (Do not show work for this step.)

Now use your ring-iso to compute all solns \( x \) to \( h(x) \equiv 0 \pmod{M} \) displaying the results in a table which shows which 4tup each came from. There are (not counting multiplicities) \( K = \) many solns.

Explain your method well; then show one computation giving a root different \((\bmod 1260)\) from \(-59, 1, -83\).

V3: The building block of a cryptosystem uses \( N\)-Repeating numbers, for large values of \( N \). (Defns are below.)

Prove: For each positive integer \( N \), that there exists an \( N\)-Repeating number.

Produce (with proof, `natch) a 5-Repeating number \( V = \) . (A little extra credit: Can you prove that your \( V \) is the smallest 5-Repeating number?)

Defns. An integer \( S \) is Twinned if it is divisible by some member of \( \{4, 9, 16, 25, 36, \ldots\} \); otherwise \( S \) is Lonely. (E.g, \( 0, -8, 600 \) are Twinned, and \( 1, 130, -77 \) are Lonely.)

For \( N,S \) posints, our \( S \) is "\( N\)-Repeating" if each member of \( \{S + j\}_{j=1}^{N-1} \) is Twinned. E.g. \( S=8 \) is 2-Repeating but not 3-Repeating. Ditto \( S=27 \).

---

End of Home-V

V1: _____ _____ 110pts
V2: _____ _____ 85pts
V3: _____ _____ 115pts

Not typed/double-spaced: _____ _____ -45pts

Total: _____ _____ 310pts

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: 

Team: _____