NT-Cryptography
MAT4930 *7554*

Quizzes C

C1: Mon. 27 Jan

a LBolt gives $G := \mathrm{GCD}(23, 413) =$ ____ . And $23S + 413T = G$, where $S=$ ____ & $T=$ ____ are integers.

b Euler $\varphi(121000) =$ ____ .
Express your answer as a product ${p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \ldots$ of *primes* to posint powers, with $p_1 < p_2 < \ldots$.

C3: *Magic integers* $G_1=$ ____ , $G_2=$ ____ , $G_3=$ ____ , each in $(-165 \,..\, 165]$, are st. mapping $g\colon \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \to \mathbb{Z}_{330}$ is a ring-isomorphism, where

$$g\big((z_1, z_2, z_3)\big) \;:=\; \Big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 \Big\rangle_{330}.$$

Verify for your map: $g\big((1,1,1)\big) = 1$ and $[5 \cdot 11] \bullet\!\mid G_1$ and analogously for G_2 and G_3.

C5: Bitstring "0101001010010001010100001", via the Elias code, decodes to ____ , a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits ____ .