Number Theory
MAS4203 8430

Class-B

Prof. JLF King
Touch: 2Jul2018

Open brain, closed book/notes. Use $\varphi()$ for the Euler phi-fnc.

B6: Short answer: Show no work. Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

z Our continuation course will run 2[nd] period MWF in Fall 2007, and will cover *Elliptic Curve Cryptography*, among other topics. Circle one: **True! Yes! Affirmative! Oui! Da! Si!**
HUH?! You mean I don't already know everything? –What a scam!

a Consider the three congruences C1: $z \equiv_{21} 18$, C2: $z \equiv_{15} 3$, and C3: $z \equiv_{70} 53$. Let z_j be the *smallest natnum* [or *DNE*] satisfying (C1) $\overset{\text{All}}{\wedge}$ (Cj). Then

$z_2 =$ .... ; $z_3 =$ ....

b Let $N := 1024 \cdot 5$. In std. form, this cyclo-poly

$\mathbf{C}_N(x) =$ ....

c If $5^e \bullet\| [3200!]$, then $e =$ ....

d The solns to $x^{51} \equiv_{13} -5$ are:

$x =$ ....

e Modulo 35, the multiplicative-order of 3 is .... [*Hint:* $\varphi(35)$ has very few prime factors.]

Essay questions: Please write in complete sentences and *also fill-in the blanks.*

B7: i Consider a posint M. Saying that "integer R is an M-primroot" means that....

ii Thm: Our M has a primroot IFF ...

B8: Show the steps of computing $\left(\frac{9976}{76807}\right) =$ ....
Indicate each time that QR is used, and where a power-of-two is pulled out.

B9: Carefully state Gauss's Quadratic Reciprocity Theorem.

Bonus: TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is $100 \overset{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ .... $\in [0..250)$.

End of Class-B

B-Home:	___ ___ ___	395pts
B6:	___ ___ ___	145pts
B7:	___ ___	25pts
B8:	___ ___	35pts
B9:	___ ___	25pts
Bonus:	___ ___	10pts
Total:	___ ___ ___	625pts

Print name .... Ord:

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: ....