Staple!

Team B____

Number Theory MAS4203 8430 — **Home-B** — Prof. JLF King *Touch:* 2Jul2018

Hello. Essays violate the CHECKLIST at *Grade Peril*! Exam is due by **3PM, Thursday, 8 March**, slid **completely under** my office door, Little Hall 402.

Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.

B1: Short answer: Show no work.

__ __ a Consider the four congruences C1: $z \equiv_{33} 6$, C2: $z \equiv_{15} 12$, C3: $z \equiv_{35} 2$ and C4: $z \equiv_{25} 2$. Let z_j be the *smallest natnum* satisfying (C1) $\stackrel{\text{All}}{\therefore}$ (Cj). Then

$z_2 =$ ________; $z_3 =$ ________; $z_4 =$ ________.

__ __ b Three Jacobi symbols: Two blanks are immed.: $\left(\frac{4203}{2006}\right) =$ ____. $\left(\frac{27113}{4913}\right) =$ ____. $\left(\frac{120}{27113}\right) =$ ____.

__ __ c Let $N := 1024 \cdot 9$. In std. form, this cyclo-poly

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

__ __ d Poly $Q(x) := x^4 - 12x^3 - 8x^2 - 19x + 437$ factors completely mod 13 as:

$\left\langle Q(x) \right\rangle_{13} =$ ____________________.

__ __ e If $7^e \bullet\!\| [2007!]$, then $e =$ ____________.

__ __ f Note $p := 137$ is prime. The (multiplicative) order of 2 mod 137 is _______.

[*Hint:* $p-1$ has very few prime factors.]

[*Hint:* $p-1$ has very few prime factors. See problem B2.]

Essay questions: Type in complete sentences and also fill-in the blanks. Each essay starts a new page.

B2: #9 P.134 of Strayer.

B3: *Magic integers* $G_1 =$ ______, $G_2 =$ ______, $G_3 =$ ______, $G_4 =$ ______, each in $[0 .. 1260)$, are st. $g : \mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \to \mathbb{Z}_{1260}$ is a ring-iso, where

$$g\big((z_1, z_2, z_3, z_4)\big) := \Big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 + z_4 G_4 \Big\rangle_{1260}.$$

Now consider poly $h(x) := [x+59][x-1][x+83]$. Find all solutions to congruences $h(x) \equiv_M 0$, 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 $h(x) \equiv_{1260} 0$, 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* (mod 1260) from $-59, 1, -83$.

B4: The number $p := 1217$ is prime, and 5 is a p-nonQR. Use the **repeated squaring** method to compute a p-RoNO = ____________ $\in [0 .. \frac{p}{2})$.

Describe a probabilistic algorithm to compute a RoNO mod a 4POS prime. [*Hint:* Shoup is a resource.]

B5: Pick a NT "proof" problem and solve it elegantly.

End of Home-B

B1:	__ __ __	180pts
B2:	__ __	65pts
B3:	__ __	65pts
B4:	__ __	65pts
B5:	__ __	20pts
Total:	__ __ __	395pts

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: __ __