Staple!

Team A____

Number Theory
MAS4203

**Home-A**

Prof. JLF King
*Touch:* 2Jul2018

**Hello.** Essays violate the CHECKLIST at *Grade Peril*!
Exam is due by **4:30PM, Tuesday, 07Feb2006**.

**A1:** Show no work.

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

b) Easily, $\varphi(25) =$ ______. Consequently, $27^{2006} \equiv_{25}$ ______ $\in [0..25)$. [*Hint:* Fermat, Euler, working mod 25.]

c) Let $G := \text{Gcd}(70, 42, 30)$ and $H := \text{Gcd}(105, 70, 42, 30)$. So $G=$ ______ and $H=$ ______. Use the LBolt Alg twice to find three integers with ______ $\cdot 70 +$ ______ $\cdot 42 +$ ______ $\cdot 30 = G$. Now find four integers with ______ $\cdot 105 +$ ______ $\cdot 70 +$ ______ $\cdot 42 +$ ______ $\cdot 30 = H$.

d+) As polynomials in $\mathbb{Z}_7[x]$, let

$$B(x) := 6x^3 - x^2 + x - 2\,;$$
$$C(x) := 3x^2 + 7x - 6\,.$$

Write t.fol polys, using coeffs in [-3..3]. Compute quotient and remainder polynomials
$q(x)=$ ______ & $r(x)=$ ______,
with $B = [q \cdot C] + r$ and $\text{Deg}(r) < \text{Deg}(C)$.

e+) With $B, C$ from above, polys in $\mathbb{Z}_7[x]$: Let $D$ be $\text{Gcd}(B, C)$. Write these three polys using coeffs in [-3..3]: The monic $D(x) =$ ______.
Compute polys $S(x)=$ ______,
$T(x)=$ ______ st. $[S \cdot B] + [T \cdot C] = D$.

**A2:** Showing all the steps, compute the Jacobi symbol $\left(\frac{1003}{5775}\right) =$ ______. Now compute by a *different* method.

**A3:** Show all the interesting steps, in the repeated-squaring algorithm, to compute $k \in [0..77)$, where $7^{707} \equiv_{77} k =$ ______.

**A4:** Fix integers $N \geqslant 3$ and $B \perp N$.

i) Prove that $\varphi(N)$ is even.

ii) Let $L = L_N(B)$ be the number of $x \in [1..\lfloor \frac{N}{2} \rfloor]$ such that $x^2 \equiv_N B$. Prove that

$$*: \qquad \prod(\Phi(N)) \equiv_N [-1]^L \cdot B^{\varphi(N)/2}\,,$$

by mimicking the pairing/involution argument from class. [*Hint:* Does the $N$-even case need special treatment?]

iii) Do something extra. *E.g, with $N$ fixed, how many different values does $L_N(B)$ take on, as $B$ varies over $\Phi(N)$?* Or: *Can you find values of $N$ where $L_N(1)$ is really big?* Or: (Do something creative.)

End of Home-A

| | | |
|---|---|---|
| **A1:** | ___ ___ | 85pts |
| **A2:** | ___ ___ | 60pts |
| **A3:** | ___ ___ | 65pts |
| **A4:** | ___ ___ | 85pts |
| **Total:** | ___ ___ ___ | 295pts |

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: ______