Number Theory
MAS 4203

InClass-Y

Prof. JLF King
Touch: 3Aug2016

Y**1:**	___ ___	90pts
Y**2:**	___ ___ ___	100pts
Y**3:**	___ ___ ___	110pts
Y**4:**	___ ___	90pts
Total:	___ ___ ___	390pts

Please PRINT your name and ordinal. Ta:

Ord: ....

Note. All variables range over the integers, unless otherwise specified.

Y**1:** FITBlank: Show no work (no partial credit).

a) Find integers s and t so $187s + 437t = 1$.
$s =$ .... and $t =$ ....

b) Find the integer x, with $0 \leqslant x < 437$, solving the congruence $30 + 187x \equiv 1$, mod 437.
$x =$ ....

c) Find integers α, β, γ so that $42\alpha + 35\beta + 30\gamma = 1$.
$(\alpha, \beta, \gamma) = ($ .... , ... , ... $)$.

Note. For the following problem please carefully write up your solution on separate sheets of paper. Show all work –there *is* partial credit.

Y**2:** The number $p := 1217$ is prime. Use the "repeated squaring, mod p" technique to compute the Legendre symbols $\left(\frac{5}{p}\right)$ and $\left(\frac{19}{p}\right)$, showing me the steps. Which of $\{5, 19\}$ has a mod-1217 square-root?

Y**3:**

i) Show all steps, except the $\lightning$ tables, to compute a magic tuple $\mathbf{G}$ so that $g: \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7 \to \mathbb{Z}_{210}$ is a ring-isomorphism, where

$$g((z_1, z_2, z_3)) := \left\langle z_1 G_1 + z_2 G_2 + z_3 G_3 \right\rangle_{210}.$$

ii) Consider poly $h(x) := [x-2][x-32][x-8]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 5, 6, 7$, 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 $\boxed{h(x) \equiv_{210} 0}$, displaying the results in a table which shows *which* 3tup each came from. There are (not counting multiplicities) $K :=$ .... many solns.

Explain your method well; then show **one** computation giving a root *different* (mod 210) from $2, 32, 8$.

Y**4:** Fix an odd prime p.

i) Give a simple proof that, mod p, the number 1 has only ± 1 as square roots.

ii) Use the foregoing to prove *Wilson's theorem*, which states that $[p-1]! \equiv_p -1$.

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

Signature: .... Filename:

Classwork/NumberThy/NT2000g/y-cl.NT2000g.latex
As of: *Wednesday 03Aug2016.* Typeset: *3Aug2016 at 17:44.*