AUSTRALIAN CATHOLIC UNIVERSITY

Castle Hill

Semester VI

MT207: Number Theory and Statistics

LECTURER: W N Franzsen

October 1992

TIME ALLOWED: 2 hours, including 10 minutes reading time.

INSTRUCTIONS TO STUDENTS

(*There are 9 questions on 2 pages, plus two pages with all the theorems. You may attempt any and all questions. I expect the correct answer to 7 questions to gain a good mark.*

The marks available for each question is indicated at the end of each one.

Calculators are not permitted

When referring to any of the theorems only use the theorem number. That is say something along the lines of 'Now by 1.8 *we can . . .'.*

Do not remove the exam paper from the exam room.

1. Write down the prime factorisation of these integers:

(a) 30030 (b) 1628

(c) 2145 (d) 10101

(20)

2. (a) What do I mean when I say "n divides m"?

(b) If $a + b = c$, $n|a$ and $n|c$, show why $n|b$.

(20)

3. (a) How did I define the greatest common divisor of two integers?

(b) Find $\gcd(376, 1016)$ and $\gcd(5432, 1234)$.

(30)

4. (a) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, convince me that $ac \equiv bd \pmod{m}$.

(b) Can we find b so that $5b \equiv 1 \pmod{92}$? If so, what is one possible value for b.

(20)

5. What is the last digit in 7^{99}?

(10)

6. (a) Write down 5 numbers that divide

$$1357911$$

(b) Are either of the following claims true? Give reasons.

(*i*) If $b|(a^2+1)$ then $b|(a^4+1)$.

(*ii*) If $b|(a^2-1)$ then $b|(a^4-1)$.

(20)

7. Find *a* solution to each of the following diophantine equations.

(a) $15x + 35y = 10$ (b) $21x + 12y = 23$

(c) $5x + 7y = 93$

(20)

8. Find *all* the solutions to

$$4x + 14y = 86.$$

Also find one with both x and y positive.

(20)

9. (a) If m is odd, show that $\{2, 4, 6, \ldots, 2m\}$ is a complete residue system modulo m.

(b) If $m > 2$, why is $\{1^2, 2^2, \ldots, m^2\}$ *not* a complete residue system modulo m.

(c) If m is odd let

$$\{a_1, a_2, \ldots, a_m\}$$

be any complete system of residues modulo m. Prove that

$$a_1 + a_2 + \cdots + a_m \equiv 0 \pmod{m}.$$

(40)