MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM **Pure Mathematics 3370** FALL 2000

Marks

[3] 1. (a) If $a \mid b$ and $a \mid c$, prove that $a \mid bx + cy$ for all $x, y \in \mathbb{Z}$.

[3] (b) Solve the Diophantine equation $3029x + 1066y = 26533$.

[2] (c) Find the positive solutions, if any.

[5] 2. (a) Given $g = (a, m)$, prove that $ax \equiv b \pmod{m}$ has a solution if and only if $g \mid b$.

[3] (b) Find all the incongruent solutions of $85x \equiv 15 \pmod{105}$.

[2] 3. (a) State the Chinese Remainder Theorem.

[3] (b) Find the common solution modulo 90 of the pair of congruences $3x \equiv 7 \pmod{10}$ and $5x \equiv 2 \pmod{9}$.

[3] (c) Find the last two digits of the Mersenne prime $p = 2^{2203} - 1$.

[4] 4. (a) Define a *primitive root* modulo a positive integer m, and calculate the number of primitive roots modulo 2×101^4. (Note that 101 is a prime.)

[3] (b) If a has order h modulo m, prove that $h \mid \phi(m)$.

[2] 5. (a) State the Division Algorithm for Gaussian Integers.

[3] (b) For $\beta = 8 - 9i$ and $\alpha = 3 + 5i$, find a quotient satisfying the requirements of the Division Algorithm.

[4] (c) Prove that any rational prime $p \equiv 3 \pmod{4}$ is a Gaussian prime.

[5] 6. Given $n = 77, e = 17$, and the encryption function $E : M \mapsto M^e \pmod{n}$, find d so that $D : C \mapsto C^d \pmod{n}$ is the decryption function. Briefly explain how the RSA public-key cryptosystem works. That is, explain how 'Bob' can send a secret message to 'Alice' so that Alice knows it comes from Bob.

---

[45]