MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM | **Pure Mathematics 3370** | FALL 2004

Marks

[2] 1. (a) Find the inverse of 35 modulo 81.

[2] (b) Find all the incongruent solutions of the congruence $245x \equiv 7 \pmod{567}$.

[2] (c) Solve the Diophantine equation $81x + 35y = 803$.

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

[3] 2. Prove, using the canonical decomposition of the integers, that $(a, b)(a, c) = (a, bc)$ if $(b, c) = 1$.

[3] 3. If $a \mid c$, $b \mid c$, and $(a, b) = 1$, prove that $ab \mid c$. (Prove any results used.)

[5] 4. Let $\{f_n\}$ be the Fibonacci sequence. For $n > 5$ prove that $f_n = 5f_{n-4} + 3f_{n-5}$. Hence prove that $5 \mid f_{5n}$ for $n \geq 1$.

[4] 5. (a) State and prove Euler's Theorem.

[3] (b) Find the remainder when 17^{357} is divided by 55.

[3] 6. (a) Prove the Chinese Remainder Theorem for **two** congruences. That is, if $(m, n) = 1$ then show that the congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ have a common solution modulo mn. (You do not need to prove uniqueness.)

[2] (b) Illustrate the proof by finding the common solution modulo 238 of the pair of congruences $x \equiv -3 \pmod{14}$ and $x \equiv 13 \pmod{17}$.

[2] 7. (a) Define the *order* of an integer modulo a positive integer m.

[2] (b) If a has order h modulo m and $a^n \equiv 1 \pmod{m}$, prove that $h \mid n$.

[2] (c) Calculate $\phi(\phi(200 \times 41^3))$, where ϕ is Euler's phi function.

[3] 8. If $a^2 + b^2 = c^2$ is a primitive Pythagorean triple with b even, give **two** examples of such triples with $b = 308$.

[3] 9. (a) Factor into Gaussian primes the number $210 + 90i$.

[3] (b) State and prove the Division Algorithm for Gaussian Integers.

[4] 10. Given $n = 391 = 17 \times 23, e = 101$, 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.

---

[50]