MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM **PM 3370 – Solutions** FALL 2004

Marks

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

Solution: After just three divisions with quotients 2, 3, and 5, we have $81(16)+35(-37) = 1$ and hence the inverse of 35 is $-37 \equiv 44 \pmod{81}$.

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

Solution: It is easy to see that $(245, 567) = 7(35, 81) = 7$, so we should first divide through by 7. Hence we solve first $35x \equiv 1 \pmod{81}$. From part (a) a solution is $x = 44$. Hence all seven incongruent solutions are given by

$$x = 44, 44 + 81, 44 + 2(81), \cdots, 44 + 6(81) = 530.$$

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

Solution: From part (a) information we have

$$x = 16(803) + 35t = 12848 + 35t, y = -37(803) - 81t = -29711 - 81t \text{ for } t \in \mathbb{Z}.$$

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

Solution: We need to solve for t, $x > 0$ and $y > 0$. We have $\dfrac{-12848}{35} < t < \dfrac{-29711}{81}$ and since $\frac{-12848}{35} \approx -367.0857$ and $\frac{-29711}{81} \approx -366.802$, we have one positive solution when $t = -367$. The solution is $x = 3, y = 16$.

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

Proof: Let $a = \prod_{i=1}^{r} p_i^{\alpha_i}, b = \prod_{i=1}^{r} p_i^{\beta_i}$, and $c = \prod_{i=1}^{r} p_i^{\gamma_i}$, where the p_i are prime and the α_i, β_i, and $\gamma_i \geq 0$ for $1 \leq i \leq r$. We are given that $\beta_i \gamma_i = 0$ for all i, and we need to prove that

$$\min\{\alpha_i, \beta_i\} + \min\{\alpha_i, \gamma_i\} = \min\{\alpha_i, \beta_i + \gamma_i\}$$

for all i. We consider first the case for those i for which $\beta_i = 0$. Then the result is obvious since the left side is just $0 + \min\{\alpha_i, \gamma_i\}$ and the right side is just $\min\{\alpha_i, \beta_i + \gamma_i\} = \min\{\alpha_i, 0+\gamma_i\}$. The second case is for the remaining i, those for which $\beta_i \neq 0$. Since $\beta_i\gamma_i = 0$ for all i, then $\gamma_i = 0$. By a similar argument, since the result is symmetric in β_i and γ_i, the result follows.

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

Proof: Since $a \mid c$, the $c = ad$ for some $d \in \mathbb{Z}$. Since $(a, b) = 1$, $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Multiplying by d we have $adx + bdy = d$, and since $c = ad$ and $b \mid c$, then $b \mid (adx + bdy)$, so $b \mid d$. Hence $d = be$ for some $e \in \mathbb{Z}$. Hence $c = ad = abe$ and so $ab \mid c$.

[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 $n \geq 1$.

Proof: For $n = 6$, $5f_{n-4}+3f_{n-5} = 5f_2+3f_1 = 5+3 = 8 = f_6$ and for $n = 7$, $5f_{n-4}+3f_{n-5} = 5f_3 + 3f_2 = 10 + 3 = 13 = f_7$. Assume the result holds for $n = k$ and $n = k + 1$. Then

$$\begin{aligned} f_{k+2} &= f_k + f_{k+1} = (5f_{k-4} + 3f_{k-5}) + (5f_{k-3} + 3f_{k-4}) \\ &= 5(f_{k-4} + f_{k-3}) + 3(f_{k-5} + f_{k-4}) = 5f_{k-2} + 3f_{k-3} \end{aligned}$$

so the result holds for $n = k + 2$. Hence, by the principle of mathematical induction, the result holds for all $n > 5$.

For $n = 1$, $f_5 = 5$, so clearly $5 \mid f_5$. Assume that $5 \mid f_{5k}$, then $f_{5(k+1)} = f_{5k+5} = 5f_{5k+1}+3f_{5k}$, using the result proved above. Since $5 \mid f_{5k}$, then clearly $5 \mid f_{5k+5}$. So, by the principle of mathematical induction, the result holds for all $n \geq 1$.

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

Euler's Theorem: If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof: Let $r_1, r_2, \ldots, r_{\phi(m)}$ be the positive integers less than m which are relatively prime to m. Since $(a, m) = 1$, we claim that $ar_1, ar_2, \ldots, ar_{\phi(m)}$ are congruent, not necessarily in order of appearance, to $r_1, r_2, \ldots, r_{\phi(m)}$. For each i, we have $(ar_i, m) = 1$ since $(r_i, m) = 1$ and $(a, m) = 1$. If $ar_i \equiv ar_j \pmod{m}$ then, by the cancellation law, $r_i \equiv r_j \pmod{m}$ and hence $i = j$. That is, $ar_i \not\equiv ar_j \pmod{m}$ if $i \neq j$. Hence the set $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ contains $\phi(m)$ elements which are relatively prime to m and incongruent modulo m. Hence they are congruent to *all* of the possible remainders that are relatively prime to m. Multiplying, we obtain $\prod_{j=1}^{\phi(m)}(ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$ and hence $a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod{m}$. Now $(r_j, m) = 1$ so we can use the cancellation law to cancel the r_j and we obtain $a^{\phi(m)} \equiv 1 \pmod{m}$.

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

Solution: First note that $\phi(55) = \phi(5)\phi(11) = 4(10) = 40$. Let $x = 17^{357}$. Then the smart way to solve this problem is to note that $4913x = 17^3x = 17^{360} = (17^{40})^9 \equiv 1 \pmod{55}$, by Euler's Theorem. Since $4913 \equiv 18 \pmod{55}$, then we have to solve for x, $18x \equiv 1 \equiv -54 \pmod{55}$. Clearly the solution is $x = -3 \equiv 52 \pmod{55}$. This is the required remainder.

[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.)

Proof: To satisfy the first congruence x must be of the form $a + my$ for some $y \in \mathbb{Z}$. Hence we need to prove that $a + my \equiv b \pmod{n}$ has a solution. This is equivalent to solving $my \equiv b - a \pmod{n}$. There is a solution y since $(m, n) = 1$. (This solution can be given explicitly as $y = X(b - a)$ where $mX + nY = 1$.) Now substitute this value for y into $a + my$ and reduce modulo mn.

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

Solution: From the first congruence $x = -3 + 14y$ for some $y \in \mathbb{Z}$. Substituting in the second congruence we have $-3+14y \equiv 13 \pmod{17}$. Then $14y \equiv 16 \pmod{17}$, and hence $-3y \equiv -1 \equiv -18 \pmod{17}$. That is, $y \equiv 6 \pmod{17}$. Then $x = -3 + 14(6 + 17z) = 81 + 238z$ for some $z \in \mathbb{Z}$. Hence the common solution is $x = 81$.

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

Solution: We say that an integer a, where $(a, m) = 1$, has order h if $a^h \equiv 1 \pmod{m}$ and, if $a \neq 1$, $a^t \not\equiv 1 \pmod{m}$ for $1 \leq t < h$.

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

Proof: Let $n = hq + r$ where $0 \leq r < h$. Then $1 \equiv a^n = a^{hq+r} = (a^h)^q a^r \equiv 1^q a^r = a^r \pmod{m}$. Since h is minimal, $r = 0$, and hence $h \mid n$.

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

Solution: We have $\phi(\phi(200 \times 41^3)) = \phi(\phi(2^3 \times 5^2 \times 41^3)) = \phi(2^2 \times 20 \times 41^2 \times 40) = \phi(2^7 \times 5^2 \times 41^2) = 2^6 \times 20 \times 41 \times 40) = 2,099,200$.

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

Solution: Recall the formula for the primitive Pythagorean triples is $a = u^2-v^2, b = 2uv, c = u^2 + v^2$ where $u > v, (u, v) = 1, u \not\equiv v \pmod{2}$. Since $b = 4 \times 7 \times 11$ then for $u = 14, v = 11$, $a = 75, b = 308, c = 317$, and for $u = 22, v = 7, a = 435, b = 308, c = 533$.

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

Solution: The obvious factorization is $210+90i = 2\times3\times5\times(7+3i)$. Then $2 = -i(1+i)^2$, 3 is a Gaussian prime and 5 is not, but $5 = (1 + 2i)(1 - 2i)$, both factors being prime. Note that $7 + 3i = (1 + i)(5 - 2i)$ and since $N(5 - 2i) = 29$, then $5 - 2i$ is prime. Hence we have the factorization into primes $210 + 90i = -3i(1 + i)^3((1 + 2i)(1 - 2i)(5 - 2i)$.

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

Given $\alpha, \beta \in G,\ \alpha \neq 0$, there exist $\gamma, \delta \in G$ such that $\beta = \alpha\gamma + \delta$, where $N(\delta) < N(\alpha)$.
Proof: Note $\frac{\beta}{\alpha} = \frac{\beta\bar{\alpha}}{\alpha\bar{\alpha}} = A + Bi$ where $A, B \in G$. Choose $a, b \in \mathbb{Z}$ such that $|A - a| \leq \frac{1}{2}$ and $|B-b| \leq \frac{1}{2}$. Let $\gamma = a+bi$ and $\delta = \beta-\gamma\alpha$. We need to show that $N(\delta) < N(\alpha)$. But $N(\delta) = N(\beta - \gamma\alpha) = N\left(\alpha\left(\frac{\beta}{\alpha} - \gamma\right)\right) = N(\alpha)N\left(\frac{\beta}{\alpha} - \gamma\right) = N(\alpha)N((A - a) + (B - b)i) = N(\alpha)((A - a)^2 + (B - b)^2) \leq N(\alpha)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}N(\alpha) < N(\alpha)$ since $N(\alpha) \neq 0$.

[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.

Solution: First we compute d. Since $\phi(391) = 16 \times 22 = 352$ and since $(101, 352) = 1$, then after four steps in the Euclidean Algorithm for $\mathbb{Z}$ we have $101(-115) + 352(33) = 1$, so $d = 237 \equiv -115 \pmod{352}$. Now see text for the rest of the story.

[50]