MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM **Pure Mathematics 3370 - Solutions** FALL 2000

Marks

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

Proof: We are given that $b = as$ and $c = at$ for some $s, t \in \mathbb{Z}$. Hence $bx + cy = asx + aty = a(sx + ty)$. Since $sx + ty \in \mathbb{Z}$ then $a \mid bx + cy$.

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

Solution: First note $13 = (3029, 1066) = 3029(-19) + 1066(54)$. The quotients in the Euclidean Algorithm are 2, 1, 5, 3, and 4. Since $13 \mid 26533$ we can solve the equivalent congruence $233x + 82y = 2041$. Observe also that $1 = 233(-19) + 82(54)$. Hence the general solution is

$$x = -19(2041) + 82t = -38779 + 82t, \;\; y = 54(2041) - 233t = 110214 - 233t, \text{ for } t \in \mathbb{Z}.$$

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

Solution: To find the positive solutions, if any, we need to solve for t the inequalities $x > 0$ and $y > 0$. Hence, $\dfrac{38779}{82} < t < \dfrac{110214}{233}$. Since $\dfrac{38779}{82} \approx 472.91$ and $\dfrac{110214}{233} \approx 473.02$, we have just one solution, $t = 473$. Hence,

$$x = -38779 + 82(473) = 7 \text{ and } y = 110214 - 233(473) = 5.$$

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

Proof: Given a solution $x = x_0$, then $ax_0 = b + mk$ for some $k \in \mathbb{Z}$, and hence $b = ax_0 - mk$. Since $g \mid a$ and $g \mid m$, then $g \mid (ax_0 - mk)$ so $g \mid b$.

Conversely, if $g \mid b$, then $ax \equiv b \pmod{m}$ has a solution if, and only if, $\dfrac{a}{g}x \equiv \dfrac{b}{g} \pmod{\dfrac{m}{g}}$ has a solution. There exist X, Y such that $1 = \dfrac{a}{g}X + \dfrac{m}{g}Y$. Then a solution to the latter equation is $x_0 = \dfrac{b}{g}X$. This is also a solution to $ax \equiv b \pmod{m}$.

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

Solution: We can solve this congruence since $5 = (85, 105)$ and $5 \mid 15$. We solve first $\frac{85}{5}x \equiv \frac{15}{5} \pmod{\frac{105}{5}}$. That is, solve $17x \equiv 3 \pmod{21}$. This can be solved in an *ad hoc* way or simply note that $1 = 17(5) + 21(-4)$ so a solution is $x = 3(5) = 15$. Hence all the solutions of the given congruence are given by:

$$x = 15, 15 + 21, 15 + 2(21), 15 + 3(21), \text{ and } 15 + 4(21) = 99.$$

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

The Chinese Remainder Theorem. *Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences $x \equiv a_j \pmod{m_j}$ for $j = 1, 2, 3, \cdots r$ has a unique solution modulo $M = m_1 m_2 \ldots m_r$.*

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

Solution: Note first that $3x \equiv 7 \pmod{10}$ is equivalent to $x \equiv 9 \pmod{10}$ and $5x \equiv 2 \pmod{9}$ is equivalent to $x \equiv 4 \pmod{9}$.

From the congruence $x \equiv 9 \pmod{10}$ we have $x = 9 + 10a$ for some $a \in \mathbb{Z}$ and from the congruence $x \equiv 4 \pmod{9}$ we have $9 + 10a \equiv 4 \pmod{9}$. Hence $a \equiv 4 \pmod{9}$, and hence $x = 9 + 10a = 9 + 10(4 + 9b) = 49 + 90b$ for some $b \in \mathbb{Z}$. Hence the common solution is $x = 49$.

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

Solution: We need first to find what p is congruent to modulo 4 and 25. Since $\phi(25) = 20$ we have $p \equiv -1 \equiv 3 \pmod{4}$ and $p \equiv 2^{20(110)+3} - 1 \equiv 2^3 - 1 \equiv 7 \pmod{25}$. Since $p = 7 + 25a$ for some $a \in \mathbb{Z}$, then $7 + 25a \equiv 3 \pmod{4}$. Hence $a \equiv 0 \pmod{4}$. Hence $p = 7 + 25a = 7 + 25(4b) = 7 + 100b$ for some $b \in \mathbb{Z}$. Hence the last two digits of p are 0 and 7.

[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.)

Solution: The number a is a primitive root modulo m if $(a, m) = 1$ and the order of a modulo m is $\phi(m)$, where ϕ is Euler's phi function. That is, $a^t \not\equiv 1 \pmod{m}$ for $1 \leq t < \phi(m)$.

The number of primitive roots modulo 2×101^4 is $\phi(\phi(2 \times 101^4) = \phi(101^3 \times 100) = 101^2 \times 100 \times \phi(100) = 101^2 \times 100 \times 40 = 40804000$.

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

Proof: We have $\phi(m) = hq + r$ where $0 \leq r < h$. Then by Euler's theorem, $1 \equiv a^{\phi(m)} \equiv a^{hq+r} \equiv (a^h)^q a^r \equiv a^r \pmod{m}$, using the fact that $a^h \equiv 1 \pmod{m}$. Since h is minimal and $r < h$ then $r = 0$ and hence $h \mid \phi(m)$.

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

(Division Algorithm). Given $\alpha, \beta \in \mathbf{G}, \alpha \neq 0$, there exist $\gamma, \delta \in \mathbf{G}$ such that $\beta = \gamma\alpha + \delta$ where $N(\delta) < N(\alpha)$.

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

Solution: We have $\dfrac{\beta}{\alpha} = \dfrac{8-9i}{3+5i} = \dfrac{(8-9i)(3-5i)}{3^2+5^2} = \dfrac{24-45-27i-40i}{34} = \dfrac{-21}{34} - \dfrac{67}{34}i \approx -0.6176 - 1.97i$. Hence choose $\gamma = -1 - 2i$ and then $\delta = \beta - \gamma\alpha = 1 + 2i$. Then $N(\delta) = 5$ and $N(\alpha) = 34$ and clearly $N(\delta) < N(\alpha)$.

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

Proof: If p is not a Gaussian prime, then $p = \alpha\beta$ for some $\alpha, \beta \in \mathbf{G}$ where neither α nor β is a unit. Taking norms we have $p^2 = N(\alpha)N(\beta)$ and hence $N(\alpha) = p$. Let $\alpha = a + bi$, then $p = N(\alpha) = a^2 + b^2$. But, modulo 4, $a^2 + b^2$ can only be 0, 1, or 2, and not 3. This contradiction proves that p 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.

Solution: Please see text for the explanation of the RSA public-key cryptosystem. You will need to compute d the inverse of e modulo $\phi(n)$. Check that $d = 53$.

---

[45]