MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM **PM 3370 – Solutions** FALL 2005

Marks

[2] 1. (a) Find the inverse of 97 modulo 192.

Solution: After three divisions with quotients 1, 1, and 47, we have $1 = 97(-95) + 192(48)$ and hence the inverse of 97 is $-95 \equiv 97 \pmod{192}$. (That is, 97 is the inverse of 97 – cute!)

[3] (b) Find all the incongruent solutions of the congruence $485x \equiv 5 \pmod{960}$.

Solution: It is fairly easy to see that $(485, 960) = 5(97, 192)$, so we can use the information from part (a) to solve the problem. We divide the congruence by 5 and then solve. The congruence $97x \equiv 1 \pmod{192}$ has solution $x = 97$ and so *all* the solutions of $485x \equiv 5 \pmod{960}$ are given by

$$97, 97 + 192 = 289, 289 + 192 = 481, 481 + 192 = 673, 763 + 192 = 865.$$

[2] (c) Solve the Diophantine equation $192x + 97y = 5000$.

Solution: From part (a) again the general solution is

$$x = 48(5000) + 97t = 240000 + 97t, \quad y = -95(5000) - 192t = -475000 - 192t, t \in \mathbb{Z}.$$

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

Solution: We need to solve for t, $x > 0$ and $y > 0$. We have $\dfrac{-240000}{97} < t < \dfrac{-475000}{192}$ and since $\frac{-240000}{97} \approx -2474.227$ and $\frac{-475000}{192} \approx -2473.958$, we have one positive solution when $t = -2474$. The solution is $x = 22, y = 8$.

[2] (e) Find the smallest positive solution of the Diophantine equation $192x - 97y = 5000$.

Solution: From part (a), $1 = 192(48) - 97(95)$, and hence the general solution is

$$x = 48(5000) - 97t = 240000 - 97t, \quad y = 95(5000) - 192t = 475000 - 192t.$$

When $x > 0$ and $y > 0$ we get $t < \frac{240000}{97} \approx 2474.227$ and $t < \frac{475000}{192} \approx 2473.958$ and hence $t \leq 2473$. The smallest solution is given when $t = 2473$. The smallest solution is $x = 119, \ y = 184$.

[2] (f) Given $n = 221 = 17 \times 13, e = 97$, 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 in the RSA–Algorithm. (That is, $D \circ E =$ the identity function for integers mod n which are relatively prime to n.)

Solution: Since $\phi(221) = \phi(17)\phi(13) = 16 \times 12 = 192$. (Surprise, surprise ... I wonder where we saw that number before?!) Recall that d is the inverse of e modulo $\phi(n)$. In part (a) we computed the inverse of 97 to be 97 modulo 192. Hence $d = 97$. (In a serious application one would never choose n so that the secret number d would be the same as the public number e.)

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

Proof: Since $(b,c)=1$, there exist integers x and y such that $bx+cy=1$. Multiplying by a we have $abx+acy=a$. Since $c \mid ab$, c divides the left side of the last equation and hence $c \mid a$.

[3] 3. Let $\{f_n\}$ be the Fibonacci sequence. For $n \geq 1$ prove, by mathematical induction, that $f_n = \dfrac{\alpha^n - \beta^n}{\sqrt{5}}$, where α, β are the roots of $x^2 - x - 1 = 0$, α being the larger root.

Proof: Note that $\alpha = \dfrac{1+\sqrt{5}}{2}$ and $\beta = \dfrac{1-\sqrt{5}}{2}$. For $n=1$ and $n=2$,

$$\frac{\alpha^1-\beta^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = f_1, \quad \frac{\alpha^2-\beta^2}{\sqrt{5}} = \frac{(\alpha+1)-(\beta+1)}{\sqrt{5}} = 1 = f_2.$$

Assume that the formula holds for $n=k$ and $n=k+1$. Then

$$\begin{aligned} f_{k+2} = f_{k+1} + f_k &= \frac{\alpha^{k+1}-\beta^{k+1}}{\sqrt{5}} + \frac{\alpha^k - \beta^k}{\sqrt{5}} = \frac{\alpha^k(\alpha+1) - \beta^k(\beta+1)}{\sqrt{5}} \\ &= \frac{\alpha^k\alpha^2 - \beta^k\beta^2}{\sqrt{5}} = \frac{\alpha^{k+2}-\beta^{k+2}}{\sqrt{5}}. \end{aligned}$$

Hence, by the principle of mathematical induction, the result holds for all $n \geq 1$.

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

Euler's Theorem. *If $(a,m)=1$, then $a^{\phi(m)} \equiv 1$ (mod m), where ϕ is Euler's phi function.*

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

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m} \text{ and hence } a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod{m}.$$

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 11^{348} is divided by 54.

Solution: Since $\phi(54) = \phi(2 \cdot 3^3) = 18$, then, by Euler's Theorem, $11^{18} \equiv 1 \pmod{54}$. Hence $11^{348} = 11^{18(19)+6} = (11^{18})^{19} 11^6 \equiv 11^6 = 1771561 \equiv 37 \pmod{54}$. Hence the required remainder is 37.

[3] 5. (a) Find x which satisfy simultaneously $x \equiv -3 \pmod{12}$ $x \equiv 1 \pmod 5$ and $x \equiv 14 \pmod{17}$.

Solution: From the first congruence $x = -3 + 12a$ for some $a \in \mathbb{Z}$. From the second congruence, $-3 + 12a \equiv 1 \pmod 5$. Hence $2a \equiv 4 \pmod 5$; that is $a \equiv 2 \pmod 5$, so $x = -3 + 12a = -3 + 12(2 + 5b)$ for some $b \in \mathbb{Z}$. Hence $x = 21 + 60b \equiv 14 \pmod{17}$, and so $4 + 9b \equiv 14 \pmod{17}$. So $9b \equiv 10 \equiv 27 \pmod{17}$. Hence $b \equiv 3 \pmod{17}$. Hence $x = 21 + 60b = 21 + 60(3 + 17c) = 201 + 1020c$ for some $c \in \mathbb{Z}$. The required x is 201.

[2] (b) Use the Chinese Remainder Theorem to find the last two digits of the number 2^{1000}.

Solution: Let $x = 2^{1000}$. We need to find x modulo 100. Clearly $x \equiv 0 \pmod 4$ and since $\phi(25) = 20$, $2^{20} \equiv 1 \pmod{25}$, by Euler's Theorem. Hence $x = (2^{20})^{50} \equiv 1 \pmod{25}$. Therefore $x = 4a \equiv 1 \equiv -24 \pmod{25}$ so $a \equiv -6 \equiv 19 \pmod{25}$. Hence $x = 4a = 4(19 + 25b) = 76 + 100b$, so the last two digits of 2^{1000} are 7 and 6.

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

Solution: Let $(a, m) = 1$. We say that a has *order* h if h is the smallest positive integer such that $a^h \equiv 1 \pmod m$.

[3] (b) If a has order h modulo m and b is the inverse of a modulo m, prove that b also has order h. (Note $ab \equiv 1 \pmod m$.)

Proof: Note first that $b^h \equiv a^h b^h = (ab)^h \equiv 1 \pmod m$. If $b^l \equiv 1 \pmod m$ for $l < h$, then $a^l \equiv a^l b^l = (ab)^l \equiv 1 \pmod m$ which contradicts the minimality of h, Hence $b^l \not\equiv 1 \pmod m$ for $l < h$, and so b has order h.

[2] (c) Calculate $\phi(\phi(100 \times 19^3))$, where ϕ is Euler's phi function.

Solution: $\phi(\phi(100 \times 19^3)) = \phi(\phi(2^2 \cdot 5^2 \cdot 19^3)) = \phi(2 \cdot 5 \cdot 4 \cdot 19^2 \cdot 18) = \phi(2^4 \cdot 3^2 \cdot 5 \cdot 19^2) = 2^3 \cdot 3 \cdot 2 \cdot 4 \cdot 19 \cdot 18 = 65664$.

[3] 7. Find all the primitive Pythagorean triples a, b, c with $a^2 + b^2 = c^2$ where one of a, b, c is equal to 140.

Solution: One of a or b must be even, say b is even. Then $a = u^2 - v^2, b = 2uv = 140$, and $c = u^2 + v^2$, where $u > v, u \not\equiv v \pmod 2$ and $(u, v) = 1$. Since $uv = 70$, we have just four cases: $u = 70, v = 1$; $u = 35, v = 2$; $u = 14, v = 5$; and $u = 10, v = 7$. Then the triples (a, b, c) are (4969, 140, 4971), (1221, 140, 1229), (171, 140, 221), and (51, 140, 149).

[3] 8. (a) Factor into Gaussian primes the number $27300(1 + 3i)$.

Solution: We have the obvious factorization $27300(1+3i) = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13(1+3i)$. The rational primes 3 and 7 are Gaussian primes. Since 1 and 3 are odd, $(1 + i) \mid (1 + 3i)$. We have $1 + 3i = (1 + i)(2 + i)$, $4 = -(1 + i)^4$, $5 = (2 + i)(2 - i)$ and $13 = (3 + i)(3 - i)$. Hence the prime factorization of $27300(1 + 3i)$ is:

$$-(1+i)^4 \cdot 3(2+i)^2(2-i)^2 \cdot 7(3+i)(3-i)(1+i)(2+i) = -3 \cdot 7(1+i)^5(2+i)^3(2-i)^2(3+i)(3-i).$$

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

(Division Algorithm): Given $\alpha \neq 0$ and $\beta \in G$, the set of Gaussian integers, there exist $\gamma,\ \delta \in G$ such that $\beta = \gamma\alpha + \delta$, where $N(\alpha) < N(\beta)$, N being the norm mapping from G to $\mathbb{N} \cup \{0\}$.

Proof. Note $\frac{\beta}{\alpha} = \frac{\beta\bar{\alpha}}{\alpha\bar{\alpha}} = A + Bi$ where $A, B \in \mathbb{Q}$. 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 $N(\alpha) \neq 0$.

[3] 9. Do **ONE** part only:

(a) State and prove Wilson's Theorem.

Wilson's Theorem. *If p is a prime then $(p - 1)! \equiv -1$ (mod p).*

Proof. If $p = 2$ or $p = 3$, the congruence is easily verified. Suppose that $p \geq 5$. For each $j, 1 \leq j \leq p - 1$, we have $(j, p) = 1$ and hence there exists a (unique) inverse i modulo p with

$$ji \equiv 1 \pmod{p}.$$

The integer i can be chosen so that $1 \leq i \leq p - 1$. Since p is prime, $j = i$ if and only if $j = 1$ or $j = p - 1$. For if $j = i$, the congruence $j^2 \equiv 1 \pmod{p}$ is equivalent to $(j - 1)(j + 1) \equiv 0 \pmod{p}$. Therefore, either $j - 1 \equiv 0 \pmod{p}$, in which case $j = 1$, or $j + 1 \equiv 0 \pmod{p}$, in which case $j = p - 1$. If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \ldots, p - 2$ into pairs j, i where $j \neq i$, such that $ji \equiv 1 \pmod{p}$. When these $\frac{p-3}{2}$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdot 4 \ldots (p - 2) \equiv (p - 2)! \equiv 1 \pmod{p}.$$

Multiplying by $p - 1$ we obtain the congruence

$$(p - 1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

(b) Euclid defined perfect numbers and discovered a formula for even perfect numbers. Euler, 2000 years later, proved that this formula gave *all* the even perfect numbers. State clearly one of these results and prove it.

Theorem 1: If $2^n - 1$ is prime, then $N = 2^{n-1}(2^n - 1)$ is perfect.

Proof: Since $2^n - 1$ is prime, the divisors of N, including $N = 2^{n-1}(2^n - 1)$, are

$$1, 2, 2^2, \ldots, 2^{n-1}, (2^n - 1), 2(2^n - 1), 2^2(2^n - 1), \ldots, 2^{n-1}(2^n - 1).$$

Adding, and using the formula $1 + x + x^2 + \cdots + x^{n-1} = \dfrac{x^n - 1}{x - 1}$, with $x = 2$, we have

$$\begin{aligned} \text{sum} &= 1 + 2 + 2^2 + \ldots + 2^{n-1} + (2^n - 1)(1 + 2 + 2^2 + \ldots + 2^{n-1}) \\ &= (2^n - 1) + (2^n - 1)(2^n - 1) = (2^n - 1)(1 + (2^n - 1)) = 2N. \end{aligned}$$

Hence, the sum of all the divisors of N is $2N$ so N is perfect.

Theorem 2: Every even perfect number is of the form $N = 2^{n-1}(2^n - 1)$ with $2^n - 1$ a prime.

Proof: Let $N = 2^{n-1}F$ where $n > 1$ and F is odd. Let $1 = f_1, f_2, \ldots, f_m = F$ be the factors of F and let $S = f_1 + f_2 + \ldots + f_m$. Given that N is perfect, we have

$$\begin{aligned}
2N = \text{sum of factors of } N &= f_1 + f_2 + \ldots + f_m \\
&+ 2f_1 + 2f_2 + \ldots + 2f_m \\
&+ 2^2 f + 2^2 f_2 + \ldots + 2^2 f_m \\
&\quad\vdots \\
&+ 2^{n-1}f_1 + 2^{n-1}f_2 + \ldots + 2^{n-1}f_m \\
&= (2^n - 1)f_1 + (2^n - 1)f_2 + \ldots + (2^n - 1)f_m \\
&= (2^n - 1)S
\end{aligned}$$

and hence we have

$$2^n F = 2N = (2^n - 1)S.$$

Therefore,

$$S = \frac{2^n F}{2^n - 1} = \frac{(2^n - 1)F + F}{2^n - 1}$$

and hence,

$$S = F + \frac{F}{2^n - 1}.$$

Since S and F are integers, $2^n - 1$ must divide F evenly and hence $F/(2^n - 1)$ is an integer and a factor of F. But S is the sum of the factors of F, two of which are clearly 1 and F. Hence, $F/(2^n - 1) = 1$ and hence $F = 2^n - 1$. Since the only positive factors of F are 1 and F, F must be prime, that is, $2^n - 1$ is prime.