MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAM **Pure Mathematics 3370 - Solutions** FALL 1999

Marks

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

Proof: First, note that $ax + by = (a, b) = 1$ for some x, $y \in \mathbb{Z}$. Then $acx + bcy = c$ and since $a \mid bc$ then clearly a divides the left side. Hence $a \mid c$.

[3] (b) Solve the Diophantine equation $25x + 11y = 557$.

Solution: After four applications of the Division Algorithm, with quotients 2, 3, 1 and 2, we have $25(4) + 11(-9) = 1$. Hence the general solution of the Diophantine equation is:

$$x = 4(557) + 11t = 2228 + 11t, \text{ and } y = -9(557) - 25t = -5013 - 25t, \text{ for } t \in \mathbb{Z}.$$

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

Solution: We have to solve $x > 0$ and $y > 0$. This gives the following inequality for t, $\frac{-2228}{11} < t < \frac{-5013}{25}$. Since $\frac{-2228}{11} \approx -202.545$ and $\frac{-5013}{25} \approx -200.52$ then the integer solutions are $t = -201$ and $t = -202$. Hence $x = 17, y = 12$ and $x = 6, y = 37$.

[3] 2. (a) Prove that any composite integer n has a prime factor $\leq \sqrt{n}$.

Proof: Since n is composite $n = ab$ where without any loss of generality $1 < a \leq b < n$. Let p be a prime factor of a, then clearly p is a prime factor of n. Since $a^2 \leq ab = n$, then $a \leq \sqrt{n}$, and hence $p \leq \sqrt{n}$.

[2] (b) List 50 consecutive composite numbers.

Solution: The numbers $51! + 2, 51! + 3, 51! + 4, \cdots, 51! + 51$ are 50 consecutive integers which are all composite since $j \mid 51! + j$.

[3] (c) Give a formula to generate all the primitive Pythagorean triples and list 6 such triples.

Solution: One such formula for the primitive Pythagorean triples is $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$ where $u > v, (u, v) = 1,$ and $u \not\equiv v \pmod 2$. (Note $a^2 + b^2 = c^2$.) Six such triples are $(3, 4, 5), (5, 12, 13), (7, 24, 25), (9, 40, 41), (15, 8, 17)$ and $(21, 20, 29)$. (To impress marker the last example should be $(4961, 6480, 8161)$:-))

[3] 3. (a) Find the last two digits of 9^{99999}.

Solution: The smart way to solve this problem is to let $x = 9^{99999}$ and then $9x = 9^{100000}$. Euler's theorem for $m = 100$ say that $a^{\phi(100)} \equiv 1 \pmod{100}$. Since $\phi(100) = 40$, then $9^{40} \equiv 1 \pmod{100}$. Hence $9^{100000} = 9^{(40)(2500)} = (9^{40})^{2500} \equiv 1 \pmod{100}$. Hence we have to solve for x the congruence $9x \equiv 1 \pmod{100}$. This is easy since $9x \equiv -99 \pmod{100}$. Hence $x \equiv -11 \equiv 89 \pmod{100}$. Hence the last two digits of 9^{99999} are 8 and 9.

[3] (b) Find the common solution of the congruences $x \equiv 16 \pmod{41}$, $x \equiv 2 \pmod{7}$, and $x \equiv 2 \pmod{15}$.

Solution: Note that the second congruence is equivalent to $x \equiv 16 \pmod{7}$ and hence the first two congruences are equivalence to the one congruence $x \equiv 16 \pmod{287}$. Substituting this information into the third equation we get $x = 16 + 287a \equiv 2 \pmod{15}$ and hence $a \equiv 8 \pmod{15}$. Hence $x = 16 + 287a = 16 + 287(8 + 15b) = 2312 + 4305b$ for some $b \in \mathbb{Z}$. Hence the unique solution modulo the product of the three moduli is $x = 2312$.

[2] 4. (a) Define a *primitive root* modulo a positive integer m.

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 $1 \le t < \phi(m)$.

[2] (b) How many primitive roots are there modulo $m = 125$?

Solution: The number of primitive roots are $\phi(\phi(125)) = \phi(5^2(4)) = 5(4)(2) = 40$.

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

Proof: We have $\phi(m) = hq + r$ where $0 \le r < h$. 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 $h \mid \phi(m)$.

[3] 5. (a) **Either:** Prove that a rational prime $p \equiv 1 \pmod{4}$ is not a Gaussian prime.

Proof: We proved that the congruence $x^2 \equiv -1 \pmod{p}$ has a solution $x = a$ if p is a prime congruent to 1 modulo 4. Hence $a^2 + 1 \equiv 0 \pmod{p}$. Hence there is an integer b such that $a^2 + 1 = pb$, or $(a + i)(a - i) = pb$. If p were a Gaussian prime then since $p \mid (a + i)(a - i)$ we would have $p \mid (a + i)$ or $p \mid (a - i)$. But this is impossible since neither $\frac{a}{p} + \frac{1}{p}i$ nor $\frac{a}{p} - \frac{1}{p}i$ is a (Gaussian) integer. Therefore, p is not a prime in $\mathbf{G}$.

OR: Prove, using the Either part, that such a prime can be written as the sum of two squares of rational integers.

Proof: Since p is not a prime in $\mathbf{G}$, then there exist nonunit integers α and β such that $\alpha\beta = p$. Then going to Cheers and fetching Norm, we have $N(\alpha)N(\beta) = p^2$. Since $N(\alpha) > 1$ and $N(\beta) > 1$ we must have $N(\alpha) = p$. Let $\alpha = a + bi$, then $p = N(\alpha) = a^2 + b^2$.

[3] (b) Factor the Gaussian integer $14(23 - 15i)$.

Solution: Since $7 \equiv 3 \pmod{4}$, then 7 is a Gaussian prime. Also $2 = -i(1+i)^2$, and since 23 and 15 are odd, $1+i$ divides $23 - 15i$. Hence $14(23 - 15i) = -i(1+i)^2(7)(1+i)(4 - 19i)$. Since $N(4 - 19i) = 377 = 13 \times 29$, then one of the prime divisors of 13, namely $2 \pm 3i$ must divide $4 - 19i$. We have $4 - 19i = (2 - 3i)(5 - 2i)$, and since $N(5 - 2i) = 29$, a rational prime, then $5 - 2i$ is prime, so the required factorization of $14(23 - 15i)$ is $-i(1 + i)^2(7)(1 + i)(2 - 3i)(5 - 2i)$.

[5] 6. Prove **ONE** of the following theorems:

(a) If $(a, m) = 1$ and $m \geq 1$, prove that $a^{\phi(m)} \equiv 1 \pmod{m}$.

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 $a^{\phi(m)} \equiv 1 \pmod{m}$.

(b) If p is a prime then $(p-1)! \equiv -1 \pmod{p}$.

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

(c) 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

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

and hence we have $2^nF = 2N = (2^n - 1)S$. Therefore, $S = \dfrac{2^nF}{2^n - 1} = \dfrac{(2^n - 1)F + F}{2^n - 1}$ and hence, $S = F + \dfrac{F}{2^n - 1}$. 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.

---

[40]