MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

FALL 2005 | **Pure Mathematics 3370** **Assignment 6** | DUE: FRIDAY OCTOBER 28, 2005

Marks

[3] 1. For translating the Bible into English, William Tindale was strangled at the stake and burned to ashes on October 6, 1536. What day of the week was this? (His last words were "Lord, open the King of England's eyes.")

"I am Patrick, a sinner, most unlearned, the least of all the faithful, and utterly despised by many. I was like a stone lying in the deep mire; and He that is mighty came and in His mercy lifted me up." This is a quote from the English translation of St. Patrick's "Confession". He died on St. Patrick's day, March 17, 461. What day of the week was this?

Also, compute the day of the week on which you were born. (If possible, check with your Mom!)

[3] 2. If $(n, 100) = 1$, we know from Euler's Theorem that $n^{\phi(100)} = n^{40} \equiv 1 \pmod{100}$. For such n prove that $n^{20} \equiv 1 \pmod{100}$. (Hint: Find congruences mod 4 and mod 25.)

[3] 3. The main lemma that Lagrange needed to prove that every positive integer is the sum of four squares is the following: Let p be an odd prime. Then there are integers a and b with $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Prove this lemma by counting the elements in the sets $A = \{a^2 \mid 0 \le a \le \frac{p-1}{2}\}$ and $B = \{-b^2 - 1 \mid 0 \le a \le \frac{p-1}{2}\}$ and using the pigeonhole principle.

[10] 4. Solve the congruences(if possible), listing all the incongruent solutions:

(a) $2004x \equiv 47 \pmod{101}$ (b) $137^{567}x \equiv 18 \pmod{47}$ (c) $561x \equiv 5852 \pmod{1562}$

[3] 5. Find x which satisfy simultaneously $7x \equiv 15 \pmod{16}$, $8x \equiv 4 \pmod{15}$, $x \equiv 8 \pmod{11}$, and $x \equiv 5 \pmod{17}$.

[3] 6. Find the last three digits in the largest known prime p. (The best method, other than Maple, is to evaluate what p is mod 8 and mod 125, and piece together using the Chinese Remainder Theorem. Remember you can only guarantee that $a^{\phi(m)} \equiv 1 \pmod{m}$, if $(a, m) = 1$.)

---

[25]