MATH 342 Problem Sheet 4: Congruences

Due Monday 25th February

1. Show that if a is an even integer then $a^2 = 0 \mod 4$ and if a is an odd integer then $a^2 = 1 \mod 8$.

2. Use question 1 to show the following.

a) If $n = 8k + 7$ ($k \in \mathbb{N}$) then n cannot be written as $a_1^2 + a_2^2 + a_3^2$ for a_1, a_2, $a_3 \in \mathbb{N}$. *Hint*: Consider each of the cases when none, one, two or all three of the a_i are odd.

b) If $b \in \mathbb{Z}$ then $b^4 = 0$ or $1 \mod 16$.

3. Let p be a prime. Show that if $k \geq 1$ then $x^2 \equiv x \mod p^k$ implies that $x \equiv 0 \mod p^k$ or $x \equiv 1 \mod p^k$.

4. Solve the following system of linear congruences.

$$\begin{cases} x \equiv 13 \mod 11 \\ 3x \equiv 12 \mod 10 \\ 2x \equiv 10 \mod 6 \end{cases}$$

5. Show that the following system of congruences has no solution.

$$\begin{cases} x \equiv 2 \mod 7 \\ 3x \equiv 4 \mod 14 \end{cases}$$

6. Write down the groups of units G_3, G_4 and G_{12}. Also, write down an explicit isomorphism between G_{12} and $G_3 \times G_4$. Write down the multiplication tables of the two groups, to check that the isomorphism does indeed preserve multiplication.

I will collect solutions at the lecture on Monday 25th February. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.