(a) Solve the congruence

$$99x \equiv 1 \pmod{367}.$$

[5 marks]

(b) Prove that there are infinitely many primes p satisfying $p \equiv 5 \pmod 6$. [4 marks]

(c) Find four solutions of $a^2 + b^2 = 22345$ with a, $b \in \mathbf{N}$ and $a < b$. (Note that $22345 = 5 \times 41 \times 109$.) [8 marks]

(d) Either

(i) Prove that if p is prime and $p \equiv 1 \pmod 4$ then the congruence $x^2 \equiv -1 \pmod p$ has a solution. (You may use Wilson's theorem.)

or

(ii) Prove that if p is prime and $p \equiv 3 \pmod 4$ then the congruence $x^2 \equiv -1 \pmod p$ has no solution. (You may use Fermat's little theorem.)

[6 marks]

(e) Using the pigeonhole principle or otherwise, prove that if p is an odd prime and there is $c \in \mathbf{Z}$ with $c^2 \equiv -2 \pmod p$ then $p = a^2 + 2b^2$ for some a, $b \in \mathbf{Z}$. [10 marks]

RJC 28/1/2009