ELEMENTARY NUMBER THEORY

HOMEWORK 4

(1) Show that $y^2 = x^3 + 7$ has no integer solutions.
  Hints: (This proof is due to V.A. Lebesgue)
  (a) Show that x is odd.
  (b) Write the equation as $y^2 + 1 = x^3 + 8$ and factor the right hand side.
  (c) Show that the quadratic factor is divisible by some prime $p \equiv 3 \bmod 4$
  (d) Look at the left hand side.

(2) Generalize the preceding exercise to an infinite family of diophantine equations $y^2 = x^3 + c$.
  This is already a research problem, although I think that the most natural generalization ($y^2 = x^3 + m^3 - n^2$) is discussed quite often in the literature (one would have to check Mordell's book on diophantine equations). I do not know whether generalizations of the form $y^2 = x^3 + m^3 - kn^2$ for integers $k \neq 1$ are known. If you can find a nontrivial result in this direction before the end of the semester, let me know!

(3) (This is a conjecture by Euler) Prove that if $p \equiv 1 \bmod 4$ is prime and $a = \frac{p-1}{4} - n - n^2$, then $(q/p) = +1$ for every $q \mid a$.

(4) (Euler) If $p \equiv 1 \bmod 4$ is prime, then $\frac{p-1}{4} - n(n+1)$ is a quadratic residue modulo p for every integer n.

The homework will be collected in class next Monday.