ELEMENTARY NUMBER THEORY

HOMEWORK 2

(1) Prove the following properties of gcd's:
   (a) $\gcd(am, an) = a \gcd(m, n)$.
   (b) $\gcd(a, bc) \mid \gcd(a, b) \gcd(a, c)$.
   (c) If $d = \gcd(a, b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
   (d) If $ax + by = d$, then $\gcd(a, b) \mid d$; also show that it is not always true that $d = \gcd(a, b)$.

(2) Solve the diophantine equation $x^2 + 2y^2 = z^2$.

(3) Prove, using the Euclidean algorithm, that $\gcd(am, an) = a \gcd(m, n)$. Hint: apply the Euclidean algorithm to the pair (m, n). What can you say about the remainders when you apply the algorithm to (am, an) instead?

(4) Using the last exercise, prove that if $a \mid mn$ and $\gcd(a, m) = 1$, then $a \mid n$. Hint: we have $\gcd(an, mn) = n$; now observe that a divides both an and mn.

(5*) This problem was given to me by one of you. You may solve it if you want to: Show that 7 is the only prime $p \equiv 3 \bmod 4$ with the property that $p^2 - 3a^2 = 1$ for some a.

Hints: The equation $t^2 - mu^2 = 1$ is called the Pell equation. It has a nontrivial solution for every nonsquare $m > 0$. Let (x, y) denote the minimal solution in positive integers; then every solution (t, u) in positive integers comes from $t + u\sqrt{m} = (x + y\sqrt{m})^n$ for some $n \in \mathbb{N}$. In particular, the solutions of $p^2 - 3a^2 = 1$ come from $p_n + a_n\sqrt{3} = (2 + \sqrt{3})^n$.
   (a) Show that $p_{n+1} > p_n$.
   (b) Show that p_n is even if and only if n is odd.
   (c) Show that p_n is divisible by 7 if $n \equiv 2 \bmod 4$.
   (d) Show that $p_n \equiv 1 \bmod 4$ if $4 \mid n$.

Now prove the claim.