HOMEWORK 9

DUE NOV 13

(1) Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and then we have $a = bq + r, 0 \leq r < |b|$, by division algorithm. Show that $\gcd(a, b) = \gcd(b, r)$.
(2) Show that for $a, b \in \mathbb{Z}$, with at least one of them non-zero, $\gcd(a, b) = 1$ if and only if $\gcd(a, b^n) = 1$ for any $n \in \mathbb{N}$.
(3) Let $a, b \in \mathbb{Z}$ with both non-zero and $\gcd(a, b) = 1$. Let $x, y \in \mathbb{Z}$. Show that there exists a $z \in \mathbb{Z}$ such that $z \equiv x \pmod{a}, z \equiv y \pmod{b}$. (This is called the Chinese remainder Theorem).
(4) Let $r \in \mathbb{Q}$ and assume that for an $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{Z}$, we have $r^n + a_1 r^{n-1} + a_2 r^{n-1} + \cdots + a_{n-1} r + a_n = 0$. Then show that $r \in \mathbb{Z}$.
(5) Let p be a prime and $x \in \mathbb{Z}$ where p does not divide x . Show that $x^{p(p-1)} \equiv 1 \pmod{p^2}$.