AC, 20^{th} October 2008

M3P14 Elementary Number Theory— Problem Sheet 1.

(1) For each pair (a, b) of integers below, find the highest common factor d of a and b, and also find integers x and y such that $ax + by = d$.

(i) $a = 30$, $b = 54$ (ii) $a = 123456789$, $b = 10$ (iii) $a = 323$, $b = 255$.

(2) Let a and b be integers, not both 0, and set $d = \text{hcf}(a, b)$. Prove that if $a = a'd$ and $b = b'd$ then a' and b' are coprime integers.

(3) For fixed integers a, b and c, with a and b not both 0, we show in this question how to find *all* integer solutions x and y to the equation

$$ax + by = c.$$

(i) If $d = \text{hcf}(a, b)$, then prove that there are integers x and y such that $ax + by = c$ if and only if d divides c.

(ii) Assume that d divides c, so there are integer solutions to the equation. Say $x = x_0$ and $y = y_0$ is one integer solution. Prove that the general integer solution is $x = x_0 + tb/d$ and $y = y_0 - ta/d$, as t runs through the integers.

(4) Find all solutions in positive integers x and y to the equation $10x - 9y = 12$.

(5) Prove, without assuming that every integer is uniquely the product of primes, that if a and b are coprime integers, and $a|c$ and $b|c$, then $ab|c$.

(6) Again in this question, don't assume that integers are uniquely the product of primes. Let a and b be positive integers, and set $d = \text{hcf}(a, b)$.

(a) Define $g = ab/d$. Show that g is an integer, and that both a and b divide g.

(b) Prove that if t is any integer such that a and b divide t, then g divides t.

(7)(i) Solve $4x \equiv 7 \bmod 9$ by brute force—that is, go through all nine choices of $x \bmod 9$ and see which ones work.

(ii) Find integers λ and μ such that $4\lambda + 9\mu = 1$ (guessing is fine; Euclid will also work). Deduce what the inverse of 4 in the group $(\mathbb{Z}/9\mathbb{Z})^\times$ is [that is, find some integer t such that $4t \equiv 1 \bmod 9$].

(iii) Now solve $4x \equiv 7 \bmod 9$ by multiplying by the inverse of 4.

(8) Find *all* solutions modulo 30 of the congruence:

$$27x \equiv 6 \bmod 30.$$