MAS3008 NUMBER THEORY EXERCISE SHEET 1

This sheet does **not** count towards assessment (but subsequent sheets **will**). However, if you hand in your answers, they will get marked. Please put your work in the Coursework Box on Level 8 of the Laver Building by Friday 25th October.

1. For each pair a, b find $d = \gcd(a, b)$ and find integers x, y such that $d = ax + by$:

(i) $a = 34$, $b = 20$;

(ii) $a = 55$, $b = 34$;

(iii) $a = 1105$, $b = 208$.

2. Let $a > b > 1$, and let r_i denote the remainder in the ith division when applying the Euclidean Algorithm to compute $\gcd(a, b)$, with $r_0 = b$, $r_{-1} = a$. (Thus, for $i \geq 1$, in the ith division we divide r_{i-2} by r_{i-1}). Show that

$$r_{i+2} < \frac{1}{2} r_i$$

(provided that at least $i+2$ divisions are needed), and hence deduce that the number of divisions required to compute $\gcd(a, b)$ is less than $1 + 2\log_2 b$. [*Hint:* Consider separately the cases $r_{i+1} \leq \frac{1}{2} r_i$ and $r_{i+1} > \frac{1}{2} r_i$.]

3. Let a, b, $n \in \mathbb{Z}$ with $\gcd(a, n) = \gcd(b, n) = 1$. Prove that $\gcd(ab, n) = 1$.

4. Let a, $b \in \mathbb{N}$ and let $d = \gcd(a, b)$. Set $l = ab/d$. Show that l is *least common multiple* (lcm) of a and b in the sense that the following two properties hold:

(i) $a \mid l$ and $b \mid l$; (ii) if $a \mid m$ and $b \mid m$ then $l \mid m$.

(You might find Euler's Lemma useful.)
Show also that l is the unique positive integer with these properties.

5. Find the prime factorisations of the following numbers:
(i) 60 (ii) 105; (iii) 65536.
For each of these numbers n, write down $v_p(n)$ for *all* primes p. (Recall that $v_p(n)$ means the integer e such that $p^e \mid n$ but $p^{e+1} \nmid n$.)

6. Let $n \geq 1$. Show that there exist n consecutive composite numbers.
[Hint: Consider $(n+1)! + k$ for $2 \leq k \leq n+1$.]

7. Show that if $n > 3$ then

(i) n, $n+2$ and $n+4$ cannot all be prime;

(ii) n, $2n+1$ and $4n+1$ cannot all be prime.

8. Let m, n, $d \in \mathbb{N}$.

(i) Show that $v_p(mn) = v_p(m) + v_p(n)$ for all primes p. Show also that $d \mid m \Leftrightarrow v_p(d) \leq v_p(m)$ for all primes p.

(ii) Deduce that

$$d \mid m \text{ and } d \mid n \Leftrightarrow v_p(d) \leq \min(v_p(m), v_p(n)) \text{ for all primes } p,$$

and hence that

$$\gcd(m,n) = \prod_{p \in \mathbb{P}} p^{\min(v_p(m), v_p(n))}.$$

(iii) Find an expression for $\operatorname{lcm}(m,n)$ (see Question 4) similar to the expression for $\gcd(m,n)$ in (ii).

9. (This question illustrates that uniqueness of prime factorisations does require proof).

Let $H = \{1, 5, 9, 13, \ldots\}$ be the set of all natural numbers of the form $4m+1$.

(i) Show that H is closed under multiplication, that is, if $h \in H$ and $k \in H$ then $hk \in H$.

Now call $h \in H$ an *H-prime* if $h > 1$ but h cannot be written as a product of two smaller elements of H. Thus 9 is an H-prime but $45 = 5 \times 9$ isn't.

(ii) Show that if $h \in H$ and $h > 1$ then h can be written as a product of H-primes. By considering the example $h = 441$, show that this factorisation into H-primes is not always unique (up to order of the factors).

(iii) Explain why the argument used to show uniqueness in the proof of the Fundamental Theorem of Arithmetic doesn't work for H-primes.

Nigel Byott
October 2002