Sheet 4

(1) Use Euclid's algorithm to calculate both $\gcd(357, 133)$, and integers r and s such that

$$r * 357 + s * 133 = \gcd(357, 133).$$

(2)(i) In the lectures it has been or will be proved that for all nonzero integers a, b, c we have $\gcd(a, b) = 1$ and $a|bc$ implies $a|c$. Deduce that for a prime p we have $p|ab$ implies $p|a$ or $p|b$.

(ii) Show that every positive integer n can be writen as $n = p_1^{k_1} \cdots p_r^{k_r}$, where the p_i are distinct primes and the k_i are ≥ 1, and that this factorisation is unique up to order. *Hint.* The existence is an easy induction argument and for the uniqueness you need part (i).

(iii) For nonzero integers a an b define $\mathrm{lcm}(a, b)$ (the *least common multiple* of a and b) as the unique positive generator of the subgroup $\mathbb{Z}a \cap \mathbb{Z}b$ of $\mathbb{Z}$. Show that for all nonzero integers m we have $a, b|m$ if and only if $\mathrm{lcm}(a, b)|m$ (*). Note that there can only be one positive integer with this property.

(iv) Let a and b be nonzero integers. Show that $\mathrm{lcm}(a, b) \gcd(a, b) = ab$.
Hint. Write $a = p_1^{k_1} \cdots p_r^{k_r}$ and $b = p_1^{l_1} \cdots p_r^{l_r}$, where the p_i are distinct primes and the k_i and l_i are integers ≥ 0. Note that we allow zero exponents in order to have the same set of primes in both factorisations. Now write $\mathrm{lcm}(a, b)$ and $\gcd(a, b)$ in the same way and deduce the result.