Introduction to Number Theory
1. exercise set, solutions

1. As $a|b_j$ for $j = 1, ..., \ell$ there exists $c_j \in \mathbb{Z}$ s.t. $b_j = ac_j$ for every j. Then $b_1 + \cdots + b_\ell = (c_1 + \cdots c_\ell)a$ meaning that $a|b_1 + \cdots + b_\ell$ as $c_1 + \cdots + c_\ell \in \mathbb{Z}$. $\square$

2. Write the prime decompositions

$$m = \prod_{k=1}^{\infty} p_k^{\alpha_k} \text{ and } n = \prod_{k=1}^{\infty} p_k^{\beta_k}.$$

We prove that

$$(m, n) = \prod_{k=1}^{\infty} p_k^{\gamma_k},$$

where $\gamma_k = \min(\alpha_k, \beta_k)$, satisfies the conditions required it to be the g.c.d of m and n. Clearly $(m, n) \geq 1$. Also $(m, n)|m$ as $\alpha_k \geq \min(\alpha_k, \beta_k) = \gamma_k$. Similarly, $\beta_k \geq \gamma_k$ gives $(m, n)|n$. Suppose then that $d'|m, n$ and write $d' = \prod_{k=1}^{\infty} p_k^{\delta_k}$. The assumption implies that $\delta_k \leq \min(\alpha_k, \beta_k) = \gamma_k$ for every k. But this means that $d'|d$. This proves the last claim. $\square$

3. Let us show that h has the required properties. Clearly $h \geq 1$. Furthermore, since $\gamma_k = \max(\alpha_k, \beta_k) \geq \alpha_k$ it follows that $p_k^{\gamma_k} \geq p_k^{\alpha_k}$ for every k. Thus $h|a$. Similarly we get $h|b$ as $\gamma_k \geq \beta_k$ for every k. Assume that $a|h'$ and $b|h'$. Let p_k be a prime which divides each of a, b, h'. Then also $p_k|h$. Let ℓ_k be an integer s.t. $p_k^{\ell_k}|h'$ but $p_k^{\ell_k+1} \nmid h'$. As $a|h'$ we have $\ell_k \geq \alpha_k$. Similarly $b|h'$ implies that $\ell_k \geq \beta_k$. Therefore $\ell_k \geq \max(\alpha_k, \beta_k)$. Doing similar analysis for each prime factor of h we deduce from the prime decomposition that $h|h'$, as required. $\square$

4. (i) We have

$$\begin{aligned}
2015 &= 2 \cdot 755 + 505 \\
755 &= 1 \cdot 505 + 250 \\
505 &= 2 \cdot 250 + 5 \\
250 &= 50 \cdot 5.
\end{aligned}$$

Therefore $(2015, 755) = 5$.

(ii) Let us first find $(276, 1578)$. By Euclid's algorithm:

$$\begin{aligned}
1578 &= 5 \cdot 276 + 198 \\
276 &= 1 \cdot 198 + 78 \\
198 &= 2 \cdot 78 + 42 \\
78 &= 1 \cdot 42 + 36 \\
42 &= 1 \cdot 36 + 6 \\
36 &= 6 \cdot 6
\end{aligned}$$

so $(276, 1578) = 6$.

Running this backwards we get $6 = 7 \cdot 1578 - 40 \cdot 276$. As $714 = 119 \cdot 6$ we get that $714 = 276 \cdot (-4760) + 1578 \cdot 833$. Now the general solution is $(x, y) = (-4760 + 263t, 833 - 46t)$, $t \in \mathbb{Z}$, by Theorem 1.12. of the lecture notes.

5. (i) Let us define

$$d = \min\{a_1x_1 + \cdots a_nx_n : x_1, ..., x_n \in \mathbb{Z}, a_1x_1 + \cdots + a_nx_n + \geq 1\}.$$

We show that this satisfies all the conditions required for the g.c.d. Write $d = a_1x'_1 + \cdots a_nx'_n$ for some integers $x'_1, ..., x'_n \in \mathbb{Z}$. Clearly $d \geq 1$. It is also obvious that if $d'|a_1, ..., a_n$ then $d'|d$. It remains to show that $d|a_1, ..., a_n$. By symmetry it is enough to show that $d|a_1$. For the sake of contradiction, suppose that $d \nmid a_1$. Then we can write $a_1 = kd + r$ for some integers k, r with $0 < r < d$. But then

$$1 \leq r = a_1 - kd = a_1(1 - kx'_1) + a_2(-kx'_2) + \cdots a_n(-kx'_n) < d$$

which contradicts the choice of d. Therefore d is indeed the greatest common divisor of $a_1, ..., a_n$. $\square$

(ii) This follows immediately from the above proof. $\square$

6. The condition $a \equiv b \pmod{m}$ means that $a = b + mk$ for some integer k. Now, $(b, m)|b, m$ so the above implies that $(b, m)|a$. Furthermore, $(b, m)|m$ giving $(b, m)|(a, m)$. Similar argument shows that $(a, m)|(b, m)$. These together yield $(a, m) = (b, m)$. $\square$

7*. As $(4k+1)(4\ell+1) = 4(4k\ell+k\ell)+1$ for every $k, \ell \in \mathbb{N}$, the set is closed under multiplication.

Let us then prove that every element of $\widetilde{\mathbb{N}}$ can be written as product of primes. Suppose otherwise. Let $n \in \widetilde{\mathbb{N}}$, $n > 1$ be the smallest element which is not a product of 'primes'. In particular, n is not a 'prime'. Thus $n = n_1n_2$ where $n_1, n_2 \in \widetilde{\mathbb{N}}$. But by assumption n_1 and n_2 can be written as products of 'primes' meaning that also n is product of 'primes'. This is a contradiction. Therefore every element of $\widetilde{\mathbb{N}}$ is a product of 'primes'. $\square$

Prime factorization is not unique as the following example shows. We have $693 = 9 \cdot 77 = 21 \cdot 33$, but $9, 21, 33$ and 77 are 'primes'.