

1. (a) (5 marks) $a \mid b \iff aq = b$ for some $q \in \mathbb{N}$. Let $q = p_1^{d_1} p_2^{d_2} \cdots p_\ell^{d_\ell}$ for some $d_i \geq 0$. Then $aq = b \iff p_1^{e_1+d_1} p_2^{e_2+d_2} \cdots p_\ell^{e_\ell+d_\ell} = p_1^{f_1} p_2^{f_2} \cdots p_\ell^{f_\ell} \iff e_i + d_i = f_i$ for all $i \iff e_i \leq f_i$ for all i .
- (b) (5 marks) Let $d = p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell}$. Then by (a) above, $d \mid a$ and $d \mid b$, so that d is a common divisor of a and b . Suppose $x = p_1^{u_1} p_2^{u_2} \cdots p_\ell^{u_\ell}$ is a common divisor of a and b , where $u_i \geq 0$. Then $x \mid a$ and $x \mid b$, so that by (a) above, $u_i \leq e_i$ and $u_i \leq f_i$. It follows that $u_i \leq \min\{e_i, f_i\} = m_i$ for all i , which is equivalent to $x \mid d$. So $d = \gcd(a, b)$.
- (c) (5 marks) Similarly, let $m = p_1^{g_1} p_2^{g_2} \cdots p_\ell^{g_\ell}$. Then by (a) above, $a \mid m$ and $b \mid m$, so that m is a common multiple of a and b . Suppose $y = p_1^{v_1} p_2^{v_2} \cdots p_\ell^{v_\ell}$ is a common multiple of a and b , where $v_i \geq 0$. Then $a \mid y$ and $y \mid m$, so that by (a) above, $e_i \leq v_i$ and $f_i \leq v_i$. It follows that $\max\{e_i, f_i\} = g_i \leq v_i$ for all i , which is equivalent to $m \mid y$. So $m = \text{lcm}(a, b)$. Finally, since $\max\{e_i, f_i\} + \min\{e_i, f_i\} = e_i + f_i$, it follows that $ab = md = p_1^{g_1} p_2^{g_2} \cdots p_\ell^{g_\ell} \cdot p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell}$
2. (a) (5 marks) We first use Euclidean Algorithm to find $\gcd(2598, 604)$:

d	x	y	
2598	1	0	r_1
604	0	1	r_2
182	1	-4	$r_3 = r_1 - 4r_2$
58	-3	13	$r_4 = r_2 - 3r_3$
8	10	-43	$r_5 = r_3 - 3r_4$
2	-73	314	$r_6 = r_4 - 7r_5$
0	302	-1299	$r_7 = r_5 - 4r_6$

From this we see that $\gcd(2598, 604) = 2$, and that $2 = 2598 \cdot (-73) + 604 \cdot 314$.

- (i) Since $2 = 2598 \cdot (-73) + 604 \cdot 314$, it follows that $14 = 2598 \cdot (-511) + 604 \cdot 2198$, so that $(-511, 2198)$ is a solution and the general solution of the equation $2598x + 604y = 14$ is $x = -511 - \frac{604}{2}t = 511 - 302t$, $y = 2198 + \frac{2598}{2}t = 2198 + 1299t$ for $t \in \mathbb{Z}$.
- (ii) (5 marks) From the working above we know that $\gcd(2598, 604) = 2$, and that $2 = 2598 \cdot (-73) + 604 \cdot 314$, and $12 = 2 \cdot 6$, so $12 = 2598 \cdot (-438) + 604 \cdot 1884$. Thus the general solution of the equation $2598x + 604y = 12$ is $x = -438 - \frac{604}{2}t = -438 - 302t$, $y = 1884 + \frac{2598}{2}t = 1884 + 1299t$ for $t \in \mathbb{Z}$.
- (b) (5 marks) From the result of part (a) we know that the general solution is $x = -438 - \frac{604}{2}t = -438 - 302t$, $y = 1884 + \frac{2598}{2}t = 1884 + 1299t$ for $t \in \mathbb{Z}$. Now $10 \leq x \leq 200 \iff 10 \leq -438 - 302t \leq 200 \iff 448 \leq -302t \leq 638$, so $t = -2$. Thus the solution is $(x, y) = (166, -714)$.

3. (a) (5 marks) $3x^2 - x - 4 \equiv 0 \pmod{5} \iff \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{0}$ in \mathbb{Z}_5 . Now

$$\begin{aligned} \bar{x} = \bar{0} &\implies \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{1} \\ \bar{x} = \bar{1} &\implies \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{3} \\ \bar{x} = \bar{2} &\implies \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{1} \\ \bar{x} = \bar{3} &\implies \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{0} \\ \bar{x} = \bar{4} &\implies \bar{3}\bar{x}^2 - \bar{x} + \bar{1} = \bar{0}. \end{aligned}$$

Thus $\bar{x} = \bar{3}$ and $\bar{4}$ are the solutions in \mathbb{Z}_5 , and so $x \in \bar{3} \cup \bar{4}$ are solutions, that is, $x \in \{5k + 3, 5k + 4 : k \in \mathbb{Z}\}$.

(b) (2 marks) $35x \equiv 14 \pmod{42} \iff 35x + 42y = 14$ for some $y \in \mathbb{Z} \iff 5x + 6y = 2$ for some $y \in \mathbb{Z} \iff 5x \equiv 2 \pmod{6}$. $\iff \bar{5} \cdot_6 \bar{x} = \bar{2}$ in \mathbb{Z}_6 .

(3 marks) Now

\bar{x}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{5} \cdot_6 \bar{x}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Thus $5x \equiv 2 \pmod{6} \iff \bar{x} = \bar{4} \iff x \in \bar{4}$, that is, $x \in \{6k + 4 : k \in \mathbb{Z}\}$.