

$$1. a = \prod_{i=1}^n p_i^{a_i}, b = \prod_{i=1}^n p_i^{b_i}, c = \prod_{i=1}^n p_i^{c_i}, a_i, b_i, c_i \geq 0.$$

$$\text{lcm}(ca, cb) = \prod_{i=1}^n p_i^{r_i}, \text{ where } r_i = \max\{a_i + c_i, b_i + c_i\} = c_i + \max\{a_i, b_i\}.$$

$$\text{So } \text{lcm}(ca, cb) = \prod_{i=1}^n p_i^{c_i} p_i^{\max\{a_i, b_i\}} = c \text{lcm}(a, b).$$

$$2. (a) d|n \Leftrightarrow d = \prod_{i=1}^r p_i^{d_i} \text{ with } 0 \leq d_i \leq e_i.$$

The number of such d is the number of possible ways of choosing the exponents d_i . For each prime p_i , there are $e_i + 1$ choices for d_i , namely $d_i = 0, 1, \dots, e_i$. So the number of possibilities is $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$.

(b) Suppose $n = ab$. Then $a = \prod p_i^{a_i}, b = \prod p_i^{b_i}$ with $0 \leq a_i, b_i$ and $a_i + b_i = e_i$. a and b are relatively prime if and only if $a_i = 0$ or e_i (which means that $b_i = e_i$ or 0 respectively) for each i . In other words for $i = 1, \dots, r$ there are two possibilities for each exponent a_i . That means there are 2^r possible values for a . Since $ab = ba$, the number of distinct factorizations in this form is $\frac{2^r}{2} = 2^{r-1}$.

$$3. (a) 65 \equiv -1 \pmod{11} \text{ so}$$

$$65^{67} \equiv (-1)^{67} \pmod{11}$$

$$\equiv -1 \pmod{11}$$

$$\equiv 10 \pmod{11}, \text{ the remainder is } 10.$$

$$(b) 13 \equiv -2 \pmod{5}$$

$$13^2 \equiv 4 \pmod{5}$$

$$\equiv -1 \pmod{5}$$

$$13^4 \equiv 1 \pmod{5}.$$

$$189 = 4 \cdot 47 + 1 \text{ so}$$

$$13^{189} \equiv (13^4)^{47} \cdot 13$$

$$\equiv 1^{47} \cdot (-2) \pmod{5}$$

$$\equiv -2 \pmod{5}$$

$$\equiv 3 \pmod{5}, \text{ the remainder is } 3.$$

$$4. (a) \quad (i) \begin{array}{c|cccccccc} \bar{x} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} \\ \hline \bar{4} \cdot_8 \bar{x} & \bar{0} & \bar{4} & \bar{0} & \bar{4} & \bar{0} & \bar{4} & \bar{0} & \bar{4} \end{array}$$

So no solutions to $\bar{6} = \bar{4} \cdot_8 \bar{x}$.

$$(ii) \begin{array}{c|cccccccccc} \bar{x} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} & \bar{8} & \bar{9} \\ \hline \bar{4} \cdot_{10} \bar{x} & \bar{0} & \bar{4} & \bar{8} & \bar{2} & \bar{6} & \bar{0} & \bar{4} & \bar{8} & \bar{2} & \bar{6} \end{array}$$

Solutions are $\bar{x} = \bar{4}, \bar{9}$.

$$(iii) \begin{array}{c|cccccccccccccc} \bar{x} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{7} & \bar{8} & \bar{9} & \bar{10} & \bar{11} & \bar{12} & \bar{13} & \bar{14} \\ \hline \bar{4} \cdot_{15} \bar{x} & \bar{0} & \bar{4} & \bar{8} & \bar{5} & \bar{1} & \bar{4} & \bar{9} & \bar{13} & \bar{2} & \bar{6} & \bar{10} & \bar{14} & \bar{3} & \bar{7} & \bar{11} \end{array}$$

Unique solution $\bar{x} = \bar{9}$. (We might have expected this since $\bar{4}$ is invertible in \mathbb{Z}_{15} because $\text{gcd}(4, 15) = 1$).

(b) $\overline{143}$ is invertible in $\mathbb{Z}_{368} \Leftrightarrow \gcd(143, 368) = 1$. We use the Euclidean algorithm to find $d = \gcd(143, 368)$ and to find u, v such that $d = 143u + 368v$.

$$\begin{array}{r}
 368 \quad 1 \quad 0 \\
 143 \quad 0 \quad 1 \\
 82 \quad 1 \quad -2 \\
 61 \quad -1 \quad 3 \\
 21 \quad 2 \quad -5 \\
 19 \quad -5 \quad 13 \\
 2 \quad 7 \quad -18 \\
 1 \quad -68 \quad 175.
 \end{array}$$

So $\gcd(143, 368) = 1$ and $1 = (368)(-68) + (143)(175)$.

Hence $\overline{143}$ is invertible and $(\overline{143})^{-1} = \overline{175}$.

5. $b(x) = a(x)(x - 2) + (5x^3 - 4x^2 + 10x - 8) = aq_1 + r_1$

$$a(x) = r_1(x)\left(\frac{1}{5}x + \frac{14}{25}\right) + \left(-\frac{19}{25}x^2 - \frac{38}{25}\right) = r_1q_2 + r_2$$

$$r_1(x) = r_2(x)\left(-\frac{125}{19}x + \frac{100}{19}\right), \text{ remainder } 0.$$

So $\gcd(a(x), b(x)) = r_2(x) = -\frac{19}{25}x^2 - \frac{38}{25}$ or to simplify, could use $-\frac{25}{19}r_2(x) = x^2 + 2$.

$$r_2 = a - r_1q_2 = a - (b - aq_1)q_2 = a(1 + q_1q_2) + b(-q_2) = au + bv.$$

$$u = 1 + q_1q_2 = \frac{1}{5}x^2 + \frac{4}{25}x - \frac{3}{25}.$$

$$v = -q_2 = -\frac{1}{5}x - \frac{14}{25}.$$

Alternatively,

$$x^2 + 2 = a(x)\left(-\frac{5}{19}x^2 - \frac{4}{19}x + \frac{3}{19}\right) + b(x)\left(\frac{5}{19}x + \frac{14}{19}\right).$$