Introduction to Number Theory
2. exercise set, solutions

1. Note that $P_j(x_j) = P(x_1, ..., x_j, ..., x_k)$ is a polynomial of one variable for every $1 \le j \le k$. Thus by applying repeatedly Theorem 2.4. we have

$$\begin{aligned} P(x_1, ..., x_k) &\equiv P(y_1, x_2, ..., x_k) \\ &\equiv P(y_1, y_2, x_3, ..., x_k) \\ &\dots \\ &\equiv P(y_1, ..., y_{k-1}, x_k) \\ &\equiv P(y_1, ..., y_k) \pmod{m}, \end{aligned}$$

as desired. □

2. Addition and multiplication tables for $\mathbb{Z}_6$:

$+$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Addition and multiplication tables for $\mathbb{Z}_7$:

$+$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

(ii) Those elements which posses a square root lie on the diagonal of the multiplication table. So, in $\mathbb{Z}_6$ those are $[0], [1], [3], [4]$ and in $\mathbb{Z}_7$ those are $[0], [1], [2], [4]$. Roots are $\sqrt{[0]} = [0]$, $\sqrt{[1]} = \{\pm[1]\}$, $\sqrt{[3]} = [3]$, $\sqrt{[4]} = \{\pm[2]\}$ in $\mathbb{Z}_6$ and $\sqrt{[0]} = [0]$, $\sqrt{[1]} = \{\pm[1]\}$, $\sqrt{[2]} = \{\pm[3]\}$, $\sqrt{[4]} = \{\pm[2]\}$ in $\mathbb{Z}_7$.

3. (i) As $p, q \in \mathbb{P} \setminus \{2\}$ and $p \neq q$ it follows that $\varphi(pq) = (p-1)(q-1)$. Now Euler's theorem gives $2^{(p-1)(q-1)} = 2^{\varphi(pq)} \equiv 1 \pmod{pq}$. □

(ii) No. For example, take $p = q = 3$.

4. Let us denote $[U] = \{[u] | u \in U\}$. By definition $U = \{a_1, ..., a_m\}$ is a complete residue system (mod m) if $[U] = \mathbb{Z}_m = \{[1], ..., [m]\}$.

"⇒" Let $U = \{a_1, ..., a_m\}$ be a complete residue system (mod m). By definition $|U| = m$ so (i) holds. If $[a_i] = [a_j]$ for $i \neq j$, then the set $[U] = \mathbb{Z}_m$ has less than m elements, a contradiction. So (ii) holds. Let $a \in \mathbb{Z}$. Now $[a] \in \mathbb{Z}_m = [U]$, so there exists $u \in U$ s.t. $a \equiv u$ (mod m). Thus also (iii) holds.

"⇐" We consider different combinations of (i), (ii) and (iii).

Assume that (i) and (ii) hold. By (i) we can write $U = \{a_1, ..., a_m\}$. Let us choose an arbitrary $a \in \{1, ..., m\}$. It is enough to show that $[a] \in [U]$. Let us consider classes $\{[a], [a_1], ..., [a_m]\} \subset \mathbb{Z}_m$. There are $m+1$ such classes but $|\mathbb{Z}_m| = m$. Therefore two of the classes are equal. Condition (ii) implies $[a_i] \neq [a_j]$ for $i \neq j$ so we must have $[a] = [a_i]$ for some i. Thus $[a] \in [U]$.

Assume that (i) and (iii) hold. By (i) we can write $U = \{a_1, ..., a_m\}$. If $[a_i] = [a_j]$ for $i \neq j$, we have $|[U]| < m$. Thus there exists $[a] \in \mathbb{Z}_m$ s.t. $[a] \notin [U]$: Hence there us no element $u \in U$ s.t. $u \equiv a \pmod{m}$. This contradicts (iii). Thus (ii) holds.

Assume that (ii) and (iii) hold. Write $U = \{a_1, a_2, ...\}$. As elements of U are mutually incongruent (mod m) we have $|U| \leq m$. By (iii) we can find $u \in U$ s.t. $a \equiv u \pmod{m}$ for every $a \in \{1, ..., m\}$ so $|U| \geq m$. Therefore $|U| = m$, so (i) holds. □

5. Let $m = \prod p_k^{\alpha_k}$ and $n = \prod p_k^{\beta_k}$. The condition $n|m$ implies that $\alpha_k \geq \beta_k$ for every k. Now we use the multiplicativity of Euler's function to obtain

$$\varphi(m) = \prod \varphi\left(p_k^{\alpha_k}\right) \quad \text{and} \quad \varphi(n) = \prod \varphi\left(p_k^{\beta_k}\right).$$

The claim follows if we show that $\varphi(p_k^{\beta_k})|\varphi(p_k^{\alpha_k})$ for every k. But

$$\frac{\varphi(p_k^{\alpha_k})}{\varphi(p_k^{\beta_k})} = p_k^{\alpha_k - \beta_k}$$

is an integer as $\alpha_k \geq \beta_k$. Proof completed. □

6. (i) Observe that $k!(p-k)!\binom{p}{k} = p!$ for all $1 \leq k \leq p-1$. The right-hand side is divisible by p but the term $k!(p-k)$ is not. Thus p divides $\binom{p}{k}$. □

(ii) The Binomial theorem gives

$$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \\ &\equiv \binom{p}{0} a^p + 0 + \cdots + 0 + \binom{p}{p} b^p \\ &\equiv a^p + b^p \pmod{p}\end{aligned}$$

by using part (i). □

Let us then prove that $(a_1 + \cdots + a_\ell)^p \equiv a_1^p + \cdots + a_\ell^p \pmod{p}$ for all $a_1, ..., a_\ell$. We induct on ℓ. Case $\ell = 1$ is obvious and $\ell = 2$ is treated above. Assume this is true for some $\ell \geq 2$. Then by the case $\ell = 2$ and inductive assumption

$$\begin{aligned}(a_1 + \cdots + a_\ell)^p &\equiv (a_1 + \cdots + a_{\ell-1})^p + a_\ell^p \\ &\equiv a_1^p + \cdots + a_{\ell-1}^p + a_\ell^p \pmod{p},\end{aligned}$$

as desired. □

Choosing $a_1 = \cdots = a_\ell = 1$ we get $\ell^p \equiv \ell \pmod{p}$ which is Fermat's little theorem. □

7*. Choose an element x contained in the union of all sets and let $A_1, A_2, \ldots, A_\ell$ be the sets containing x. Since the element x is counted precisely once by the left-hand side of equation

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|,$$

we need to show that it is counted precisely once by the right-hand side. On the right-hand side, the only non-zero contributions occur when all the subsets in a particular term contain the chosen element, that is, all the subsets are selected from $A_1, A_2, \ldots, A_\ell$. The contribution is one for each of these sets (plus or minus depending on the term) and therefore is just the (signed) number of these subsets used in the term. This number is

$$\binom{\ell}{1} - \binom{\ell}{2} + \cdots + (-1)^{\ell+1}\binom{\ell}{\ell} = 1 - (1-1)^\ell = 1,$$

where we used the binomial theorem. This completes the proof. □