3.1.6

Show using unique factorization into primes that we can compute the lcm as follows. Once we have factored the integers involved as a product of the pairwise distinct primes $p_i, ß = 1, \ldots, k$:

$$\text{lcm}(\prod_{i=1}^{k} p_i^{e_i}, \prod_{i=1}^{k} p_i^{f_i}) = \prod_{i=1}^{k} p_i^{h_i}, \quad \text{where} \quad h_i = \max(e_i, f_i)$$

Solution:

Both $\prod_{i=1}^{k} p_i^{e_i}$ and $\prod_{i=1}^{k} p_i^{f_i})$ divide $\prod_{i=1}^{k} p_i^{h_i}$, since for each i, $h_i \geq e_i$ and $h_i \geq f_i$. So we now assume that c is a common multiple of $\prod_{i=1}^{k} p_i^{e_i}$ and $\prod_{i=1}^{k} p_i^{f_i})$. After possibly adding terms of the form p_j^0, we can assume that $c = \prod_{i=1}^{k} p_i^{g_i}$. Since c is a multiple of $\prod_{i=1}^{k} p_i^{e_i}$ we must have $g_i \geq e_i$ for all i. Similarily $g_i \geq f_i$ for all i. Therefore, $g_i \geq h_i$ for all i and c is a multiple of $\prod_{i=1}^{k} p_i^{h_i}$. Hence $\prod_{i=1}^{k} p_i^{h_i}$ is the least common multiple.

6.2.1

Show that if we assume that the positive integers $m_1, \ldots, m_r$ satsify $\gcd(m_1, \ldots, m_r) = 1$, and $m = m_1, \ldots, m_r$, then the rings $\mathbb{Z}_m$ and $\mathbb{Z}_{m1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ are isomorphic.

Solution:

The map $f\colon Z_m \to \mathbb{Z}_{m1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ defined by

$$f(x \mod m) = (x \mod m_1, \ldots, x \mod m_r)$$

is a ring homomorphism (for the same reason as in the proof of Theorem 6.2.1). To prove the desired isomorphism, we will check that $\ker f = 0$. The result then follows from the first ring isomorphism theorem. Let $a \in \ker f$. Then

$$\begin{aligned} m_1|a, m_2|a, \cdots, m_r|a &\implies \\ lcm(m_1, \ldots, m_r)|a &\implies \\ m_1 m_2 \cdots m_r = m|a & \end{aligned}$$

where in the final transition we use exercise 3.1.7 and exercies 3.1.8. (Personally I suspect the reference to exercise 3.1.6 should have been to exercise 3.1.8) From these exercises we see that

$$\text{lcm}(m_1, \ldots, m_r) = \frac{m_1 m_2 \cdots m_r}{\gcd(m_1, m_2, \ldots, m_r)} = m_1 m_2 \cdot m_2$$

6.2.2

Draw the analogous figures for $\mathbb{Z}_{35}$.

Solution:

Draw the Cayley graphs $X(\mathbb{Z}_{35}, \{\pm 1\})$ and $X(\mathbb{Z}_{35}, \{5, 30, 7, 28\})$, where the latter graph is the same as $X(\mathbb{Z}_{35}, \{\pm 5, \pm 7\})$

2.3.11

Show that if m and n satisfy $\gcd m, n = 1$, then Euler's function satisfies $\phi(mn) = \phi(m)\phi(n)$.

Solution:

By the Chinese remainder theorem, the map $f\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ sending $x \mod mn$ to $(x \mod m, x \mod n)$ is an isomorphism. Since $\phi(k) = |\mathbb{Z}_k|$, we are done if we can show that the restriction of f, $g\colon \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \oplus \mathbb{Z}_n^*$ sending $x \mod mn$ to $(x \mod m, x \mod n)$ is an isomorphism. Since the map f preserves multiplication, it takes units to units, so g is well-defined. The map f must also take non-units to non-units, so g must be surjective. Finally, since f is injective, so is its restriction g. We conlclude that:

$$\phi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \oplus \mathbb{Z}_n^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*| = \phi(m)\phi(n)$$

2.3.12

Use the preceding exercise (and exercise 2.3.3) to prove equation (2.4) for $\phi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})$

Solution:

Equation (2.4) is:

$$\phi(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdot (p_r^{e_r} - p_r^{e_r-1})$$

The first equality follows from (2.3.11) and the second from (2.3.3)

6.3.6

a) Find all roots of $f(x) = 3x^2 + x + 4$ in $\mathbb{Z}_7$ by the process of substituting all elements of $\mathbb{Z}_7$.
b) Find all roots of the polynomial $f(x)$ in part a) using the quadratic formula for $\mathbb{Z}_7$. Do your answers agree? Should they?

Solution:

a)

$$\begin{aligned}
f(0) &= 3 \cdot 0^2 + 0 + 4 &&= 4 \\
f(1) &= 3 \cdot 1^2 + 1 + 4 &&= 1 \\
f(2) &= 3 \cdot 2^2 + 2 + 4 &&= 4 \\
f(3) &= 3 \cdot 3^2 + 3 + 4 &&= 6 \\
f(4) &= 3 \cdot 4^2 + 4 + 4 &&= 0 \\
f(5) &= 3 \cdot 5^2 + 5 + 4 &&= 0 \\
f(6) &= 3 \cdot 6^2 + 6 + 4 &&= 6
\end{aligned}$$

so there are no roots of f in $\mathbb{Z}_7$
b) Since 2 is a unit in $\mathbb{Z}_7$ we can use the quadratic formula. This gives that the roots of f are:

$$r = \frac{-1 \pm \sqrt{1 - 4 \cdot 3 \cdot 4}}{6} = \frac{-1 \pm \sqrt{2}}{6} = 1 \pm \sqrt{2} = 1 \pm 3 = \{4, 5\}$$

since $3^2 = 2$ in $\mathbb{Z}_7$.

6.3.7

Suppose that $D \in \mathbb{Z}_+$ is not a square: that is, $D \neq n^2$, for any $n \in \mathbb{Z}$. Set $\mathbb{Q}[\sqrt{D}] = \{x + y\sqrt{D} | x, y \in \mathbb{Q}\}$. Show that $\mathbb{Q}[\sqrt{D}]$ is a field.

Solution:

$\mathbb{Q}$ is clearly a ring, so it suffices to prove that every non-zero element of $\mathbb{Q}$ has a multiplicative inverse. We use the same conjugation trick you know from the complex numbers.

$$(x + y\sqrt{D})^{-1} = \frac{x - y\sqrt{D}}{x^2 - y^2 D}$$

if this fraction is defined, since

$$(x + y\sqrt{D})\frac{x - y\sqrt{D}}{x^2 - y^2 D} = \frac{x^2 - y^2 D}{x^2 - y^2 D} = 1.$$

The fraction is defined if $x^2 - y^2 D \neq 0$. If $x^2 - y^2 D = 0$, then $(\frac{x}{y})^2 = D$. But this cannot happen since $D \in \mathbb{Z}_+$ is not the square of an integer, and therefore cannot be the square of a rational number.

6.3.10

Show that, for a prime p, the multiplicative group $\mathbb{Z}_p^*$ is cyclic.

Solution:

Let r be the maximal order of an element of $\mathbb{Z}_p^*$. From the hint get that since $\mathbb{Z}_p^*$ is abelian, and if x, y are elements if $\mathbb{Z}_p^*$, there is an element of order $\operatorname{lcm} |x|, |y|$. It then follows that $x^r = 1$ for all $x \in \mathbb{Z}_p^*$. To see this, let x have maximal order r, and assume for contradiction that $y^r \neq 1$. Then $|y|$ does not divide r, so $\operatorname{lcm} |x|, |y|$ must be strictly greater than r.

The polynomial $x^r - 1$ over the field $\mathbb{Z}_p$ therefore has $p - 1$ roots, which is only possible if $r \geq p - 1$. On the other hand, we know that $r \leq |\mathbb{Z}_p^*| = p - 1$, since the order of an element always divides the order of the group. We therefore conclude that there is an element in $\mathbb{Z}_p^*$ of order $p - 1$, so $\mathbb{Z}_p^*$ is cyclic.