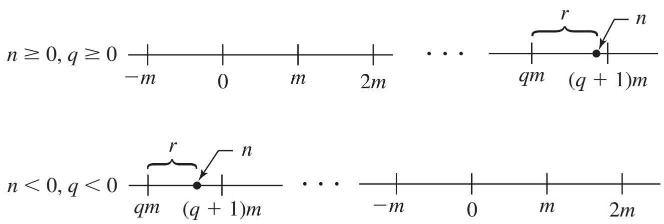
6.2 Division Algorithm for $\mathbb{Z}$ If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$

Proof We give an intuitive diagrammatic explanation, using Fig. 6.3. On the number line, mark off the multiples of m and the position of n. Now n falls either on a multiple qm of m and r can be taken as 0, or n falls between two multiples of m. If the latter is the case, let qm be the first multiple of m to the left of n. Then r is as shown in Fig. 6.3. Note that $0 \leq r < m$. Uniqueness of q and r follows since if n is not a multiple of m so that we can take $r = 0$, then there is a unique multiple qm of m to the left of n and at distance less than m from n, as illustrated in Fig. 6.3. ◆



6.3 Figure

In the notation of the division algorithm, we regard q as the **quotient** and r as the nonnegative **remainder** when n is divided by m.

6.4 Example Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solution The positive multiples of 7 are $7, 14, 21, 28, 35, 42, \cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$38 = 35 + 3 = 7(5) + 3$$

so the quotient is $q = 5$ and the remainder is $r = 3$. ▲

6.5 Example Find the quotient q and remainder r when -38 is divided by 7 according to the division algorithm.

Solution The negative multiples of 7 are $-7, -14, -21, -28, -35, -42, \cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$-38 = -42 + 4 = 7(-6) + 4$$

so the quotient is $q = -6$ and the remainder is $r = 4$. ▲

We will use the division algorithm to show that a subgroup H of a cyclic group G is also cyclic. Think for a moment what we will have to do to prove this. We will have to use the *definition* of a cyclic group since we have proved little about cyclic groups yet. That is, we will have to use the fact that G has a generating element a. We must then exhibit, in terms of this generator a, some generator $c = a^m$ for H in order to show that H is cyclic. There is really only one natural choice for the power m of a to try. Can you guess what it is before you read the proof of the theorem?

6.6 Theorem A subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group generated by a and let H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

We claim that $c = a^m$ generates H; that is,

$$H = \langle a^m \rangle = \langle c \rangle.$$

We must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some n. Find q and r such that

$$n = mq + r \qquad \text{for} \qquad 0 \leq r < m$$

in accord with the division algorithm. Then

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

so

$$a^r = (a^m)^{-q} a^n.$$

Now since $a^n \in H, a^m \in H$, and H is a group, both $(a^m)^{-q}$ and a^n are in H. Thus

$$(a^m)^{-q} a^n \in H; \qquad \text{that is,} \qquad a^r \in H.$$

Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus $n = mq$ and

$$b = a^n = (a^m)^q = c^q,$$

so b is a power of c. ◆

As noted in Examples 5.24 and 5.25, $\mathbb{Z}$ under addition is cyclic and for a positive integer n, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$ under addition, the cyclic subgroup generated by n. Theorem 6.6 shows that these cyclic subgroups are the only subgroups of $\mathbb{Z}$ under addition. We state this as a corollary.

6.7 Corollary The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$. ◆

This corollary gives us an elegant way to define the *greatest common divisor* of two positive integers r and s. Exercise 54 shows that $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of the group $\mathbb{Z}$ under addition. Thus H must be cyclic and have a generator d, which we may choose to be positive.

6.8 Definition Let r be a positive integer and s be a non-negative integer. The positive generator d of the cyclic group

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor** (abbreviated gcd) of r and s. We write $d = \gcd(r, s)$. ■

Note that $d\mathbb{Z} = H$, $r = 1r + 0s \in H$, and $s = 0r + 1s \in H$. This implies that $r, s \in d\mathbb{Z}$, which says that d is a divisor of both r and s. Since $d \in H$, we can write

$$d = nr + ms$$

for some integers n and m. We see that every integer dividing both r and s divides the right-hand side of the equation, and hence must be a divisor of d also. Thus d must