be the largest number dividing both r and s; this accounts for the name given to d in Definition 6.8.

The fact that the greatest common divisor d of r and s can be written in the form $d = nr + ms$ for some integers n and m is called Bézout's identity. Bézout's identity is very useful in number theory, as we will see in studying cyclic groups.

6.9 Example Find the gcd of 42 and 72.

Solution The positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, and 42. The positive divisors of 72 are 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, and 72. The greatest common divisor is 6. Note that $6 = (3)(72) + (-5)(42)$. There is an algorithm for expressing the greatest common divisor d of r and s in the form $d = nr + ms$, but we will not need to make use of it here. The interested reader can find the algorithm by searching the Internet for the Euclidean algorithm and Bézout's identity. ▲

Two positive integers are **relatively prime** if their gcd is 1. For example, 12 and 25 are relatively prime. Note that they have no prime factors in common. In our discussion of subgroups of cyclic groups, we will need to know the following:

If r and s are relatively prime and if r divides sm, then r must divide m. (1)

Let's prove this. If r and s are relatively prime, then we may write

$$1 = ar + bs \qquad \text{for some} \qquad a, b \in \mathbb{Z}.$$

Multiplying by m, we obtain

$$m = arm + bsm.$$

Now r divides both arm and bsm since r divides sm. Thus r is a divisor of the right-hand side of this equation, so r must divide m.

The Structure of Cyclic Groups

We can now describe all cyclic groups, up to an isomorphism.

6.10 Theorem Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof **Case I** *For all positive integers m, $a^m \neq e$.* In this case we claim that no two distinct exponents h and k can give equal elements a^h and a^k of G. Suppose that $a^h = a^k$ and say $h > k$. Then

$$a^h a^{-k} = a^{h-k} = e,$$

contrary to our Case I assumption. Hence every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$. The map $\phi : G \to \mathbb{Z}$ given by $\phi(a^i) = i$ is thus well defined, one-to-one, and onto $\mathbb{Z}$. Also,

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j),$$

so the homomorphism property is satisfied and ϕ is an isomorphism.

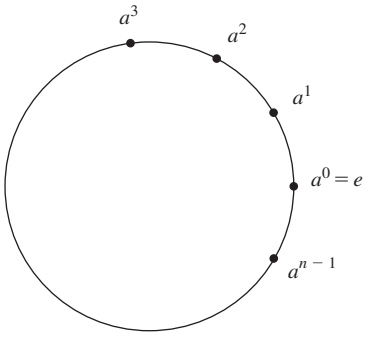
Case II *$a^m = e$ for some positive integer m.* Let n be the smallest positive integer such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. As in Case 1, if $0 \leq k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting our choice of n. Thus the elements

$$a^0 = e, a, a^2, a^3, \cdots, a^{n-1}$$

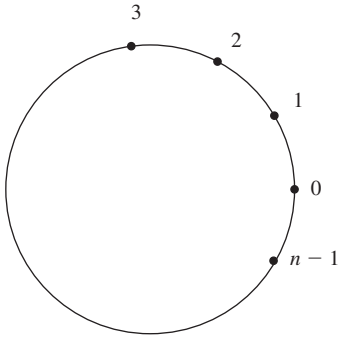
are all distinct and comprise all elements of G. The map $\psi : G \to \mathbb{Z}_n$ given by $\psi(a^i) = i$ for $i = 0, 1, 2, \cdots, n-1$ is thus well defined, one-to-one, and onto $\mathbb{Z}_n$. Because $a^n = e$, we see that $a^i a^j = a^k$ where $k = i +_n j$. Thus

$$\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j),$$

so the homomorphism property is satisfied and ψ is an isomorphism. ◆



6.11 Figure



6.12 Figure

6.13 Example Motivated by our work with U_n, it is nice to visualize the elements $e = a^0, a^1, a^2, \cdots, a^{n-1}$ of a cyclic group of order n as being distributed evenly on a circle (see Fig. 6.11). The element a^h is located h of these equal units counterclockwise along the circle, measured from the right where $e = a^0$ is located. To multiply a^h and a^k diagrammatically, we start from a^h and go k additional units around counterclockwise. To see arithmetically where we end up, find q and r such that

$$h + k = nq + r \qquad \text{for} \qquad 0 \leq r < n.$$

The nq takes us all the way around the circle q times, and we then wind up at a^r. ▲

Figure 6.12 is essentially the same as Fig. 6.11 but with the points labeled with the exponents on the generator. The operation on these exponents is *addition modulo n*.

This is simply the isomorphism between $\langle a \rangle$ and $\mathbb{Z}_n$. Of course this is the same isomorphism we saw when we defined $\mathbb{Z}_n$ from U_n, but using a instead of ζ.

As promised at the beginning of this section, we can see now that the order of an element a in a group G is simply the smallest positive number n such that $a^n = e$.

6.14 Example Let us find the order of the k-cycle, $\sigma = (a_1, a_2, a_3, \ldots, a_k)$, in the symmetric group. The order of σ is the smallest postive power of σ that is ι. Note that applying σ just maps each number to the next one in the cyclic order. So after k applications of σ, each number maps back to itself, but not before k applications of σ. Therefore, the order of a k-cycle is k. ▲