

**Exercise 10.31:** Suppose that  $\phi$  is a homomorphism from  $U(30)$  to  $U(30)$  and that  $\ker \phi = \{1, 11\}$ . If  $\phi(7) = 7$ , find all elements of  $U(30)$  that map to 7.

The elements that map onto 7 are precisely  $a \ker \phi$  where  $a \in \phi^{-1}(7)$  thus these elements are  $\{7, 17\}$ .

**Exercise 10.35:** Prove that the mapping  $\phi : Z \oplus Z \rightarrow Z$  given by  $(a, b) \rightarrow a - b$  is a homomorphism. What is the kernel of  $\phi$ ? Describe the set  $\phi^{-1}(3)$  (that is, all elements that map to 3).

Clearly  $\phi$  is well defined and thus we need only show that operation are preserved. Note that  $\phi((a, b))\phi((c, d)) = a - b + c - d = (a + c) - (b + d) = \phi(((a + c), (b + d))) = \phi((a, b) + (c, d))$ , and thus  $\phi$  is a homomorphism.

Note that  $(a, b) \in \ker \phi$  iff  $a - b = 0$  in other words where  $a = b$  thus  $\ker \phi = \{(a, a) \mid a \in \mathbb{Z}\}$ . Note that  $(3, 0) \in \phi^{-1}(3)$  thus  $\phi^{-1}(3) = (3, 0) \ker \phi = \{(a + 3, a) \mid a \in \mathbb{Z}\}$ .

**Exercise 10.40:** For each pair of positive integers  $m$  and  $n$ , we can define a homomorphism from  $Z$  to  $Z_m \oplus Z_n$  by  $x \rightarrow (x \bmod m, x \bmod n)$ . What is the kernel when  $(m, n) = (3, 4)$ ? What is the kernel when  $(m, n) = (6, 4)$ ? Generalize.

Note that  $x \in \ker \phi$  iff  $\phi(x) = (0, 0)$ . Thus  $\ker \phi = \{x \in Z \mid \phi(x) = (0, 0)\}$  or in our case  $\ker \phi = \{x \in Z \mid (m \mid x) \wedge (n \mid x)\}$  or  $\ker \phi = \{x \mid \text{lcm}(m, n) \mid x \in Z\}$ . If  $(m, n) = (3, 4)$  then  $\ker \phi = \{12x \mid x \in Z\}$ . If  $(m, n) = (6, 4)$  then  $\ker \phi = \{12x \mid x \in Z\}$ .

**Exercise 10.43:** Let  $\phi(d)$  denote the Euler phi function of  $d$  (see page 85). Show that the number of homomorphisms from  $Z_n$  to  $Z_k$  is  $\sum \phi(d)$ , where the sum runs over all common divisors  $d$  of  $n$  and  $k$ . [It follows from number theory that this sum is actually  $\text{gcd}(n, k)$ .]

First let's break up all of the homomorphisms by the size of the image. Note that the size of the image call it  $d$  must divide  $n$  since the homomorphism associated with this image divides the group  $Z_n$  into  $d$  chunks of equal size. Note that the size of the image call it  $d$  must divide  $m$  since  $\psi(Z_n)$  is a subgroup of size  $d$  in  $Z_m$ .

How many homomorphisms have a size of there image equal to  $d$ ? Well as discussed above if  $d \nmid m$  or  $d \nmid n$  then there are no homomorphisms associated with it. However if  $d \mid n$  and  $d \mid m$  then we will have homomorphisms associated with it and these homomorphisms map onto  $\langle m/d \rangle$  the only subgroup of  $Z_m$  with  $d$  elements. If we know where the generator 1 in  $Z_n$  gets mapped to in  $\langle m/d \rangle$  we know were every item gets mapped to. Noting that 1 must get mapped to a generator we know that there are exactly as many homomorphisms onto  $\langle m/d \rangle$  as  $\langle m/d \rangle$  has generators. Note that  $\langle m/d \rangle$  has  $\phi(\langle m/d \rangle) = \phi(d)$  generators.

Now simply add up the number of homomorphisms associated with any  $d$  value and we have the total number of homomorphisms. The result of this sum is exactly the sum described in the question.

**Exercise 10.48:** Suppose that  $Z_{10}$  and  $Z_{15}$  are both homomorphic images of a finite group  $G$ . What can be said about  $|G|$ ? Generalize.

We know that  $|Z_{10}| \mid |G|$  and that  $|Z_{15}| \mid |G|$  thus  $\text{lcm}(10, 15) \mid |G|$ . In general if groups  $a_1 \cdots a_n$  are homomorphic images of a finite group  $G$  then  $\text{lcm}(|a_1| \cdots |a_n|) \mid |G|$ .

**Exercise 10.59:** Suppose that  $H$  and  $K$  are distinct subgroups of  $G$  of index 2. Prove that  $H \cap K$  is a normal subgroup of  $G$  of index 4 and that  $G/(H \cap K)$  is not cyclic.

Note that  $H \not\subseteq K$  and  $K \not\subseteq H$ . Let  $a \in H \cap K^c$  and let  $b \in K \cap H^c$ . Suppose  $H$  is not normal in  $G$ . In this case there exists  $a \in G$  and  $h \in H$  such that  $aha^{-1} \notin H$ . Note that  $a \notin H$ , since  $H$  has closure. Note that  $aha^{-1} \notin H$  implies that  $aha^{-1} \in aH$  since  $H$  is index 2. Note that  $ha^{-1} \in H$  thus  $(ha^{-1})^{-1} \in H$  thus  $ah^{-1} \in H$  however  $ah^{-1} \in aH$ , a contradiction.

Note that  $H$  and  $K$  are normal subgroups of  $G$ . Note that  $H \cap K = J$  is a normal subgroup of  $G$ . Let  $a \in H$  and  $a \notin K$ , note that  $a \notin J$  and thus  $aJ$  is a separate coset from  $J$ . Let  $b \notin H$  and  $b \in K$ , note that  $b \notin J$  and since  $b \notin H = aH$ ,  $b \notin aJ$ , thus  $bJ$  is a separate coset from  $aJ$  and  $J$ . Let  $c \notin H$  and  $c \notin K$ , note that  $c \notin J$  and since  $c \notin H = aH$ ,  $c \notin aJ$ , and since  $c \notin K = bK$ ,  $c \notin bJ$ , thus  $cJ$  is a separate coset from  $bJ$ ,  $aJ$  and  $J$ . Thus  $J$  is at least of index 4.

Note that if  $d \in G$ ,  $d$  will fall in one of these 4 cosets. I will not prove all 4 cases but I will prove one case as example, Suppose  $d \notin H$  and  $d \in K$ . Thus  $d \in bH$  and  $d \in K = bH$ , so  $d \in bJ$ . Note that we now know that  $J$  is exactly of index 4.

Note that  $G/(H \cap K) = \{J, aJ, bJ, cJ\}$ . Suppose  $G/(H \cap K)$  is cyclic. Note that it must have 2 generators. Note that  $J$  is not a generator since it is identity and thus  $aJ$  or  $bJ$  will be a generator. We can break symmetry at this point between  $K$  and  $H$  and say WLoG  $aJ$  is a generator. Note that  $a^2 \in H$  (since  $a \in H$ ) and that  $a^2 \in K$  since if  $a^2 \notin K$  we would know that  $a^2 \in aJ$  and thus  $(aJ)^2 = aJ$  a impossibility, thus  $(aJ)^2 = J = e$ . We have reached a contradiction since  $aJ$  is a generator, thus we negate our supposition and conclude that  $G/(H \cap K)$  is not cyclic.