Chapter 0

1. For $n = 5, 8, 12, 20, \& 25$ find all positive integers less than n & relatively prime to n.

$n=5$: $\{1, 2, 3, 4\}$

$n = 8$: $\{1, 3, 5, 7\}$

$n = 12$: $\{1, 5, 7, 11\}$

$n = 20$: $\{1, 3, 7, 9, 11, 13, 17, 19\}$

$n = 25$: $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

2. $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2 \cdot 3^2 \cdot 7$ $(= 2 \cdot 9 \cdot 7 = 2 \cdot 63 = 126)$

$\operatorname{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$.

4. Find $s, t \in \mathbb{Z}$ s.t. $1 = 7s + 11t$ and show that they are not unique.

Let $s=8$, $t=-5$. Then $7 \cdot 8 + 11 \cdot (-5) = 56 - 55 = 1$. These are not unique since

$s = -14$, $t = 9 \Rightarrow 7 \cdot (-14) + 11 \cdot 9 = -98 + 99 = 1$.

5. Suppose $a, b, c \in \mathbb{Z}$ with $a|c$, $b|c$. If a & b are relatively prime, show that $ab|c$. Show by example that if a & b are not relatively prime, then ab need not divide c.

Proof Since a & b are relatively prime, $\exists s, t \in \mathbb{Z}$ s.t. $as + bt = 1$. Since $a|c$, $\exists q \in \mathbb{Z}$ s.t. $c = aq$. Likewise, since $b|c$ $\exists r \in \mathbb{Z}$ s.t. $c = br$. Multiplying the equation $as + bt = 1$ by c gives $acs + bct = c$. Making substitutions for c, we have $a(br)s + b(aq)t = c$. Since ab divides both terms on LHS, ab also divides c. ▨

For a counterexample when a & b are not relatively prime, let $a = 2$, $b = 4$, $c = 4$. Then $2|4$ and $4|4$ but $2 \cdot 4 = 8 \nmid 4$.

3. Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

Proof By Thm 2, we know that $\exists s, t \in \mathbb{Z}$ s.t. $as + bt = d$. Substituting for a and b, we have $da's + db't = d$. Dividing by d gives $a's + b't = 1$. Since 1 is the smallest positive integer, we must have $\gcd(a', b') = 1$ by Thm 2. ▨

10. Let $a, b \in \mathbb{Z}^+$, $d = \gcd(a, b)$, $m = \operatorname{lcm}(a, b)$. If t divides both a and b, show that $t|d$. If s is a multiple of both a and b, prove that s is a multiple of m.

Proof Assume $t|a$, $t|b$. Then $\exists q, r \in \mathbb{Z}$ s.t. $a = tq$, $b = tr$. By Thm 2, $\exists s, u \in \mathbb{Z}$ s.t. $d = as + bu$. Substituting for a and b gives $d = tqs + tru$. Since t divides both terms on the RHS, t also divides d, as desired.

Now suppose s is a multiple of a and b. [Then $\exists j, k \in \mathbb{Z}$ s.t. $s = aj$, $s = bk$.] Since m is the least common multiple of a & b, $s \geq m$. By the Division Algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $s = mq + r$ and $0 \leq r < m$. Then $r = s - mq$ is also a multiple of both a and b since $a|s$, $a|mq$, $b|s$, $b|mq$. If $0 < r < m$, this contradicts the minimality of m, so we must have $r = 0 \Rightarrow s = mq$ is a multiple of m. ▨

19. Show that $\gcd(a,bc)=1$ iff $\gcd(a,b)=1$ and $\gcd(a,c)=1$.

Proof First assume $\gcd(a,bc)=1$, and by way of contradiction suppose that either $\gcd(a,b)\neq 1$ or $\gcd(a,c)\neq 1$. Without loss of generality, take $\gcd(a,b)=d\neq 1$. Since $d>1$, by the Fundamental Thm of Arithmetic there is a prime p s.t. $p\mid d$. Then $p\mid a$ since $d\mid a$ and $p\mid bc$ since $d\mid bc$. Thus, $\gcd(a,bc)\geq p>1$ - contradiction.

Assume now that $\gcd(a,b)=\gcd(a,c)=1$. Suppose by way of contradiction that $\gcd(a,bc)=d\neq 1$. Since $d>1$, by the Fund. Thm of Arithmetic there is a prime p s.t. $p\mid d$. Since $d\mid bc$ we have $p\mid bc$. Then by Euclid's Lemma, either $p\mid b$ or $p\mid c$. If $p\mid b$, then $p\mid a$ also since $d\mid a$, so $\gcd(a,b)\geq p>1$ - contradiction. Then we must have $p\mid c$. But then still $p\mid a$ since $d\mid a$, so $\gcd(a,c)\geq p>1$ - contradiction. So in fact $\gcd(a,bc)=1$. ▨

57. Let $f: A\to B$, $g: B\to C$, $h: C\to D$ be functions. Then

(1) $h(gf)=(hg)f$

(2) If f and g are injective, then so is gf.

(3) If f and g are surjective, then so is gf.

(4) If f is injective + surjective, then there is a function $f^{-1}: B\to A$ s.t. $(f^{-1}f)(a)=a\ \forall a\in A$ and $(ff^{-1})(b)=b\ \forall b\in B$.

Proof (1) Let $a\in A$. Then $h(gf)(a)=h(gf(a))=h(g(f(a)))$ and $(hg)f(a)=(hg)(f(a))=h(g(f(a)))$, so $h(gf)(a)=(hg)f(a)\ \forall a\in A$. Thus, $h(gf)=(hg)f$.

(2) Assume f,g are injective. Let $a_1,a_2\in A$ s.t. $gf(a_1)=gf(a_2)$. Then $g(f(a_1))=g(f(a_2))$ $\Rightarrow g(a_1)=g(a_2)$ since f is injective, which implies $a_1=a_2$ since g is injective. Thus, gf is injective.

(3) Assume f,g are surjective. Let $c\in C$. Since g is surjective, $\exists\, b\in B$ s.t. $g(b)=c$. Since f is surjective, $\exists\, a\in A$ s.t. $f(a)=b$. Then $c=g(f(a))=gf(a)$, so gf is surjective.

(4) Assume f is injective + surjective. Let $b\in B$; since f is surjective, $\exists\, a\in A$ s.t. $f(a)=b$. Define $f^{-1}: B\to A$ by $b\longmapsto a$. This function is well-defined: if $b_1=b_2$, then $f(a_1)=f(a_2)$ $\Rightarrow a_1=a_2$ since f is injective. Then $(f^{-1}f)(a)=f^{-1}(f(a))=f^{-1}(b)=a\ \forall a\in A$, and $(ff^{-1})(b)=f(f^{-1}(b))=f(a)=b\ \forall b\in B$. ▨

58. Let $S = \mathbb{R}$ and define $a \sim b$ if $a - b \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation on S + describe the equivalence classes.

Proof Let $a \in S$. Since $a - a = 0 \in \mathbb{Z}$, we have $a \sim a$. Suppose $a, b \in S$ with $a \sim b$. Then $a - b \in \mathbb{Z} \Rightarrow b - a = -(a-b) \in \mathbb{Z}$, so $b \sim a$. Now suppose $a, b, c \in S$ with $a \sim b$ and $b \sim c$. Then $a - b, b - c \in \mathbb{Z} \Rightarrow a - c = (a-b) + (b-c) \in \mathbb{Z}$, so $a \sim c$. Thus, $\sim$ is an equivalence relation. For $a \in S$, the equivalence class $\bar{a} = \{a + K \mid K \in \mathbb{Z}\}$. Therefore, a representative for $\bar{a}$ is $\text{frac}(a)$, the fractional part of a. ▨

(For example $2.25 \in \overline{0.25}$, $-3.128 \in \overline{0.872}$, etc.)

59. Let $S = \mathbb{Z}$ and define aRb if $ab \geq 0$. Is R an equivalence relation on S?

No; R satisfies the reflexive and symmetric properties, but not the transitive property: for example, $1R0$ and $0R(-1)$ but $1 \not R (-1)$.

60. Let $S = \mathbb{Z}$ and define $a \sim b$ if $a + b$ is even. Prove that $\sim$ is an equivalence relation, and determine the equivalence classes of S.

Proof Let $a \in S$. Since $a + a = 2a$ is even, $a \sim a$. Suppose $a, b \in S$ with $a \sim b$. Then $a + b$ is even $\Rightarrow b + a$ is even, so $b \sim a$. Now suppose $a, b, c \in S$ with $a \sim b$ and $b \sim c$. Then $a+b$, $b+c$ are even $\Rightarrow (a+b) + (b+c) = a + 2b + c$ is even $\Rightarrow a + c$ is even, so $a \sim c$. Thus, $\sim$ is an equivalence relation. ▨

We have $\bar{a} = \{a + 2K \mid K \in \mathbb{Z}\}$. Thus, $\bar{0} = \bar{2} = \bar{4} = \ldots$, and $\bar{1} = \bar{3} = \bar{5} = \ldots$ So there are two distinct equivalence classes: $\bar{0}$ and $\bar{1}$.

Chapter 1

5. In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.

A reflection turns the figure over from front to back or vice versa. Doing two reflections puts the figure on the same side it started on, and only a rotation keeps the figure on the same side.

7. In D_n, explain geometrically why a rotation followed by a rotation must be a rotation.

Doing any number of rotations does not turn the figure over to the other side, so as explained in #6, this must be a rotation.

8. In D_n, explain geometrically why a rotation and a reflection taken together in either order must be a reflection.

The rotation preserves the side (front or back) while the reflection changes the side, so no matter the order, the net result is a change of side, which must indicate a reflection.

HW 1 Solutions, Ch. 1

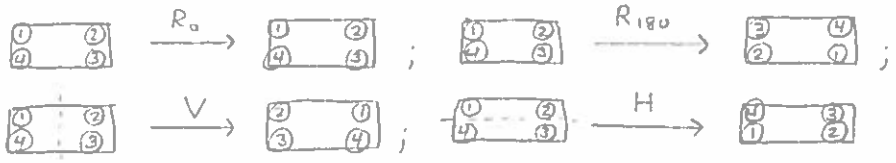
0. If r_1, r_2, r_3 are rotations in D_n and f_1, f_2, f_3 are reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

Since there are three reflections performed, the figure changes side three times. So the figure ends on a different side from where it started, and this must be a reflection.

1. Find elements $A, B, C \in D_4$ s.t. $AB = BC$ but $A \neq C$ ("cross cancellation" does not hold).

Note that $R_{90}H = D' = HR_{270}$ but $R_{90} \neq R_{270}$. (Many other possible examples.)

3. Describe the symmetries of a nonsquare rectangle + construct the corresponding Cayley table.



	R_0	R_{180}	V	H
R_0	R_0	R_{180}	V	H
R_{180}	R_{180}	R_0	H	V
V	V	H	R_0	R_{180}
H	H	V	R_{180}	R_0