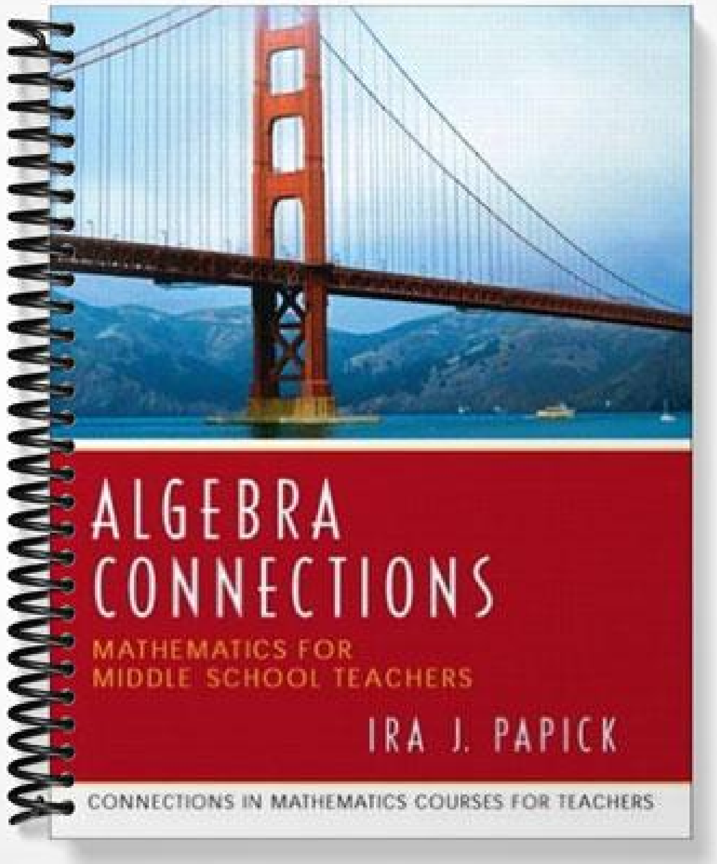
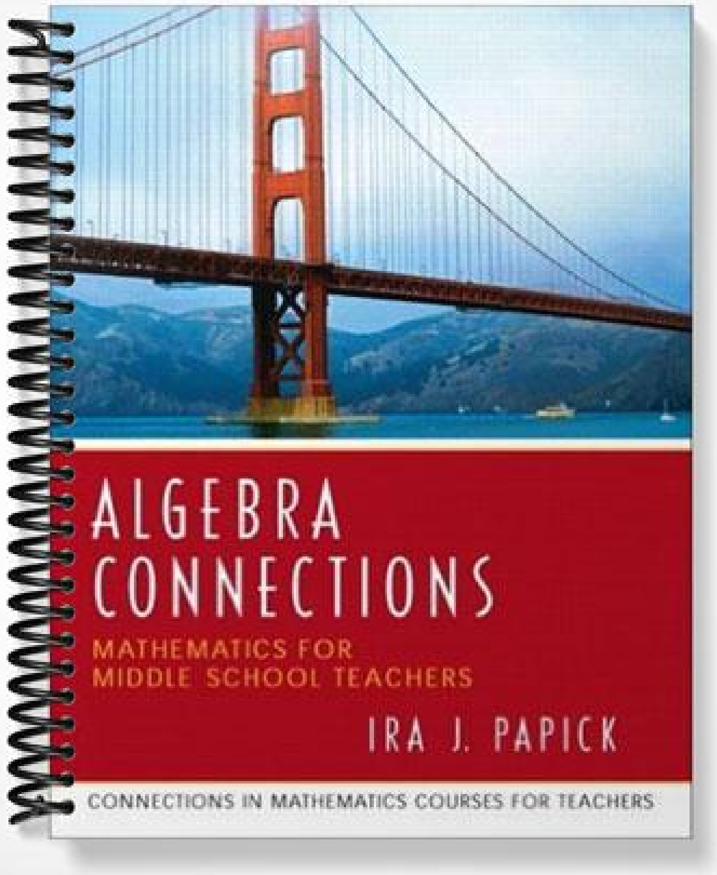
SOLUTIONS MANUAL



SOLUTIONS MANUAL



Algebra Connections

Chapter 2: Arithmetic and Algebra of the Integers

2.1: A few mathematical questions concerning the periodical cicadas

1. $1998-(13\cdot 17)=1998-221=1777$; $1998+(13\cdot 17)=1998+221=2219$. The last time they appeared was in 1777, and the next time the will appear is 2219.

2. If both types of locusts appear during the same year then there are more locusts competing for the same fixed food supply. Thus evolutionary pressures have resulted in the two types appearing simultaneously on a very infrequent schedule.

2.4: Multiples and divisors

1. Property 1: $a\,|\,b \Rightarrow b=ax$ for some $x\in\mathbf{Z}$, and $b\,|\,a \Rightarrow a=by$ for some $y\in\mathbf{Z}$. Thus, $a=by=(ax)y=axy \Rightarrow xy=1 \Rightarrow$ either $x=y=-1$ or $x=y=1$, and so $a=\pm b$.
   Property 2: $a\,|\,b \Rightarrow b=ay$ for some $y\in\mathbf{Z} \Rightarrow bx=(ay)x=a(yx) \Rightarrow a\,|\,bx$.
   Property 3: $a\,|\,b$ and $a\,|\,c \Rightarrow aw=b$ and $av=c$ for some $w,v\in\mathbf{Z}$.
   Thus, $bx+cy=(aw)x+(av)y=a(wx+vy)$;
   Similarly, $bx-cy=(aw)x-(av)y=a(wx-vy)$, so $a\,|\,(bx\pm cy)$.
   Property 5: $a\,|\,b$ and $b\,|\,c \Rightarrow ax=b$ and $by=c$ for some $x,y\in\mathbf{Z}$.
   Thus, $c=by=(ax)y=a(xy) \Rightarrow a\,|\,c$.
   Property 6: $a\,|\,b$ and $c\,|\,d \Rightarrow ax=b$ and $cy=d$ for some $x,y\in\mathbf{Z}$.
   Thus, $bd=(ax)(cy)=ac(xy) \Rightarrow ac\,|\,bd$.

2. (a). False. Set $a=1$ and $b=0$. Then $c=27$ which is not divisible by 7.
   (b). True. $3\,|\,51$ and $3|801$ so Property 3 implies that $3\,|\,c$.
   (c). False. Set $a=1$ and $b=0$. Then $c=26$ which is not divisible by 8.
   (d). True. If $15\,|\,(3a-2b)$ then $3\,|\,(3a-2b)$. Thus, $3\,|\,4a(3a-2b)$ by Property 2.
   (e). True. Apply Property 4.
   (f). True. If $12\,|\,(2a+4b)$ then $2\,|\,(a+4b)$. Now apply Property 4.
   (g). False. $2\,|\,(1+3)$, but 2 does not divide 1 and 2 does not divide 3.
   (h). False. $6\,|\,(2\cdot 3)$, but 6 does not divide 2 and 6 does not divide 3.
   (i). This is true, but we cannot give a complete proof until Chapter 3.
   (j). False. If this were true 3 | 3 would imply that 9 | 3.
   (k). True. Apply Property 6.
   (l). True, but we cannot give a complete proof until Chapter 3.
   (m) True. $196^{20}=(2^2 7^2)^{20}=2^{40}7^{40}=2^{35}(2^5 7^{40})$.

3. $$(a-1)(a^{n-1}+a^{n-2}+...+a^1+1)=a(a^{n-1}+a^{n-2}+...+a^1+1)-1(a^{n-1}+a^{n-2}+...+a^1+1)$$
$$=(a^n+a^{n-1}+...+a^2+a^1)-(a^{n-1}+a^{n-2}+...+a^1+1)=$$
$$a^n+(a^{n-1}-a^{n-1})+(a^{n-2}-a^{n-2})+...+(a^1-a^1)-1=a^n-1\Rightarrow(a-1)\,|\,(a^n-1).$$

4. Let $1\le i\le s$ and suppose that $(a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_s)+1=a_ik$ for some nonzero integer k. Then $1=(a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_s)-a_ik=a_i(a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_s-k)$. This implies that $a_i=1$, a contradiction.

2.6: The Fundamental Theorem of Arithmetic

1. (a). Composite: $1{,}274=2\cdot7^2\cdot13$
   (b). Composite: $7{,}921=89^2$
   (c). Composite: $6{,}561=3^8$
   (d). Prime
   (e). Composite: $11{,}111=41\cdot271$
   (f). Prime

2. Suppose $\gcd(a,b)>1$ then by the FTA there are primes $p_1,p_2,\ldots,p_k$ so that $\gcd(a,b)=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$. Then each of the primes $p_1,p_2,\ldots,p_k$ are common factors of a and b. Suppose some prime p is a common factor of a and b. Then $1<p\le\gcd(a,b)$.

3. (a). $\tau(13^{13})=13+1=14$.
   (b). $\tau(2^5\cdot3^6\cdot17^4)=(5+1)(6+1)(4+1)=210$.
   (c). If m were greater than 0, then the left side of the equation would have an 11 in its prime factorization while the right side would not. Similarly, if n were greater than 0, then the right side of the equation would have a 23 in its prime factorization while the left side would not. This would contradict FTA, so we have $m=n=0$.
   (d). We have $21^{m_1}\cdot29^{m_2}=3^{m_1}\cdot7^{m_1}\cdot29^{m_2}$, so if m_1 is positive, then there is a 3 in the prime factorization of $21^{m_1}\cdot29^{m_2}$, but the 3 is not in the prime factorization of $7^{n_1}\cdot19^{n_2}\cdot23^{n_3}$. Thus, by FTA, $21^{m_1}\cdot29^{m_2}\ne7^{n_1}\cdot19^{n_2}\cdot23^{n_3}$. The cases for m_2, n_1, n_2, and n_3 are similar.

4. (a). True. By 2.6.2 since $5\,|\,7a$ but $5\nmid7$ it follows that $5\,|\,a$.
   (b). True. Apply 2.6.2.

(c). True. Apply 2.6.2.

(d). False. For example, $6 \mid (2 \bullet 3)$.

(e). False. Neither 3 nor 5 divides 637.

(f). True. The statement implies that $5 \mid 24a$. By 2.6.2 it follows that $5 \mid a$.

(g). True. The statement along with 2.6.2 implies that $3 \mid (a-3)$ or $3 \mid (a+3)$. Now apply Elementary Divisibility Property 4 from Section 2.4.

(h). True. First we apply Elementary Divisibility Property 4 from Section 2.4 to conclude that $8 \mid 35b$. According to 2.6.4, 2^n with $n \geq 3$ must appear in the prime decomposition of $35b$. It does not appear in the prime decomposition of 35, and so it must appear in the prime decomposition of b.

5. $n > 1$ is an m^{th} power $\Leftrightarrow n = a^m = (p_1^{m_1} p_2^{m_2} \bullet\bullet\bullet p_t^{m_t})^m = p_1^{m \cdot m_1} p_2^{m \cdot m_2} \bullet\bullet\bullet p_t^{m \cdot m_t}$, (where $p_1^{m_1} p_2^{m_2} \bullet\bullet\bullet p_t^{m_t}$ is the prime factorization of a) $\Leftrightarrow$ the prime factors of n occur in multiples of m.

6. Let n be a positive integer and suppose that $a^n \mid b^n$. Let $a = p_1^{m_1} p_2^{m_2} \bullet\bullet\bullet p_j^{m_j}$ be the prime factorization of a. Then there is a positive integer k so that $b^n = a^n k = (p_1^{m_1} p_2^{m_2} \bullet\bullet\bullet p_j^{m_j})^n k = (p_1^{nm_1} p_2^{nm_2} \bullet\bullet\bullet p_j^{nm_j})k$. Let $k = q_1^{n_1} q_2^{n_2} \bullet\bullet\bullet q_l^{n_l}$ be the prime factorization of k so that we have the equation
$b^n = (p_1^{nm_1} p_2^{nm_2} \bullet\bullet\bullet p_j^{nm_j})k = (p_1^{nm_1} p_2^{nm_2} \bullet\bullet\bullet p_j^{nm_j}) q_1^{n_1} q_2^{n_2} \bullet\bullet\bullet q_l^{n_l}$.
We now show that n_1, the exponent of q_1 is a multiple of n, and then similar reasoning applies to the other exponents. Since either $q_1 \neq p_s$ for all $1 \leq s \leq j$ or $q_1 = p_s$ for some $1 \leq s \leq j$, it follows that in the prime factorization of $a^n k$ the exponent of q_1 is either equal to n_1 or equal to $n_1 + nm_s$ for some $1 \leq s \leq j$. In either case the exponent of q_1 must be a multiple of n (Why?). It therefore follows that in either case n_1 itself is a multiple of n.

2.8: Relations and results concerning lcm and gcd

1. (a). $\text{lcm}(a, b) = 2^4 \bullet 3^2 \bullet 5^3 \bullet 7^3 \bullet 13^2$, $\gcd(a, b) = 2^1 \bullet 3^0 \bullet 5^2 \bullet 7^2 \bullet 13^0$

(b). $a = 2^4 \bullet 7 \bullet 11,\ b = 2^3 \bullet 5 \bullet 11^2 \Rightarrow \text{lcm}(a, b) = 2^4 \bullet 5 \bullet 7 \bullet 11^2$,
$\gcd(a, b) = 2^3 \bullet 5^0 \bullet 7^0 \bullet 11$

(c). $a = 2^6 \bullet 31,\ b = 2003 \Rightarrow \text{lcm}(a, b) = 2^6 \bullet 31 \bullet 2003$,
$\gcd(a, b) = 2^0 \bullet 31^0 \bullet 2003^0$

(d). $a = 7 \bullet 11 \bullet 13,\ b = 11 \bullet 9091 \Rightarrow \text{lcm}(a, b) = 7 \bullet 11 \bullet 13 \bullet 9091$,
$\gcd(a, b) = 7^0 \bullet 11 \bullet 13^0 \bullet 9091^0$

(e). $a = 2^4 \cdot 23 \cdot 47,\ b = 2^4 \cdot 1151 \Rightarrow \text{lcm}(a,\ b) = 2^4 \cdot 23 \cdot 47 \cdot 1151$,
$\gcd(a,\ b) = 2^4 \cdot 23^0 \cdot 47^0 \cdot 1151^0$

2. (a). Suppose that $\gcd(a, a+1) = d > 1$. Then there are positive integers k and j so that $a = kd$ and $a + 1 = jd$. But then $1 = (a+1) - a = (j-k)d$, which is impossible.
(b). These are consecutive integers, and so we can apply (a).
(c). Suppose that $\gcd(30a+14, 10a+4) \neq 2$. Then $\gcd(30a+14, 10a+4) = d > 2$. Then there are positive integers k and j so that $30a + 14 = kd$ and $10a + 4 = jd$. But then $2 = (30a+14) - 3(10a+4) = (k - 3j)d$, which is impossible.
(d). Suppose that $\gcd(14a+11, 4a+3) = d > 1$. Then there are positive integers k and j so that $14a + 11 = kd$ and $4a + 3 = jd$. But then $1 = 2(14a+11) - 7(4a+3) = 2kd - 7jd = (2k - 7j)d$, which is impossible.
(e). Suppose that $\gcd(12a+4, 28a+8) \neq 4$. Then $\gcd(12a+4, 28a+8) = d > 4$. So there are are positive integers k and j so that $12a + 4 = kd$ and $28a + 8 = jd$. But then $4 = 7(12a+4) - 3(28a+8) = 7kd - 3jd = (7k - 3j)d$, which is impossible.

3. (a). No. $\gcd(a, b)$ must divide $\text{lcm}(a, b)$, but here 4 does not divide 6.
(b). Yes. Let $a = 4$ and $b = 8$.
(c). $d \mid m \Rightarrow \gcd(d,\ m) = d$ and $\text{lcm}(d,\ m) = m$. Conversely, let a and b be positive integers such that $\gcd(a,\ b) = d$ and $\text{lcm}(a,\ b) = m$. Since $\gcd(a, b)$ always divides $\text{lcm}(a, b)$, we have that $d \mid m$.

4. Let $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ and $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ be the modified canonical prime factorization of a and b, respectively. Notice that $\gcd(a,b) = \text{lcm}(a,b)$ if and only if $\min\{m_j, n_j\} = \max\{m_j, n_j\}$ for each $1 \leq j \leq t$. Thus $\gcd(a,b) = \text{lcm}(a,b)$ if and only if $m_j = n_j$ for each $1 \leq j \leq t$. Thus $\gcd(a,b) = \text{lcm}(a,b)$ if and only if $a = b$.

5. (a). Let $d = \gcd(a,\ b)$, and so $a = dw$ and $b = dv$ for some integers w, v.
Thus, $1 = ax + by = (dw)x + (dv)y = d(wx + vy) \Rightarrow d \mid 1 \Rightarrow d = 1$.
(b). No. $2 = 1 \cdot 1 + 1 \cdot 1$, but $\gcd(1,\ 1) = 1 \neq 2$.

6. (a). Suppose that $d = \gcd(a,b)$. Then $d > 0$ and $d \mid a$ and $d \mid (a+b)$.
Suppose that g is a positive integer which divides a and divides $a + b$. Then $g \mid b$ also. By definition of $\gcd(a,b)$ it follows that $g \mid d$.
(b). Yes, this can be extended as the statement suggests. Follow the argument for part (a).

7. Let $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ and $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ be the modified canonical prime factorization of a and b, respectively. It follows that $a^2 = (p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t})^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_t^{2m_t}$ and $b^2 = (p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t})^2 = p_1^{2n_1} p_2^{2n_2} \cdots p_t^{2n_t}$, and so gcd($a^2$, b^2)

$= p_1^{\min\{2m_1,2n_1\}} p_2^{\min\{2m_2,2n_2\}} \cdots p_t^{\min\{2m_t,2n_t\}} = p_1^{2\cdot\min\{m_1,n_1\}} p_2^{2\cdot\min\{m_2,n_2\}} \cdots p_t^{2\cdot\min\{m_t,n_t\}} = (p_1^{\min\{m_1,n_1\}} p_2^{\min\{m_2,n_2\}} \cdots p_t^{\min\{m_t,n_t\}})^2 = (\gcd(a,\, b))^2 = d^2$.

8. (a). This follows from Problem 7. One could also argue directly as follows: Let $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ and $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ be the modified canonical prime factorization of a and b, respectively. Since $\gcd(a,b) = 1$ it follows that for each $1 \le j \le t$, $\min\{m_j, n_j\} = 0$. Now,
$a^2 = (p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t})^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_t^{2m_t}$ and
$b^2 = (p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t})^2 = p_1^{2n_1} p_2^{2n_2} \cdots p_t^{2n_t}$, and so gcd($a^2$, b^2)
$= p_1^{\min\{2m_1,2n_1\}} p_2^{\min\{2m_2,2n_2\}} \cdots p_t^{\min\{2m_t,2n_t\}} = p_1^{2\cdot\min\{m_1,n_1\}} p_2^{2\cdot\min\{m_2,n_2\}} \cdots p_t^{2\cdot\min\{m_t,n_t\}} =$
$p_1^0 p_2^0 \cdots p_t^0 = 1$.

(b). Suppose that $\gcd(a+b, ab) = d > 1$. Since $a^2 = a(a+b) - ab$ it follows that $d \mid a^2$. Similarly, $d \mid b^2$. Thus $\gcd(a^2, b^2) \ne 1$. By (a) it follows that $\gcd(a,b) \ne 1$.

(c). Suppose that $\gcd(a, bc) = d > 1$. Then there is a prime p which divides both a and bc. But then $p \mid b$ or $p \mid c$.

(d). Suppose that $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ and $p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}$ are the modified canonical prime factorization of *a,* and *b*, respectively. Since $\gcd(a,b) = 1$ it follows that for each $1 \le j \le t$ either $m_j = 0$ or $n_j = 0$. Now since ab is a perfect square it follows that each $1 \le j \le t$ $m_j + n_j = \max\{m_j, n_j\}$ is even. Thus for each $1 \le j \le t$ m_j is even and for each $1 \le j \le t$ n_j is even. Hence both a and b are perfect squares.

(e). Suppose that $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$, $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ and $p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}$ are the modified canonical prime factorization of *a, b* and *c*, respectively. Since $\gcd(a,b) = 1$ it follows that for each $1 \le j \le t$ either $m_j = 0$ or $n_j = 0$. Thus for each $1 \le j \le t$ $m_j + n_j = \max\{m_j, n_j\}$. Now since $a \mid c$ and $b \mid c$ it follows that for each $1 \le j \le t$ $\max\{m_j, n_j\} \le s_j$. Thus
$ab = p_1^{\max\{m_1,n_1\}} p_2^{\max\{m_2,n_2\}} \cdots p_t^{\max\{m_t,n_t\}}$ divides *c*.

9. Let $d_1 = \gcd(c, a)$ and $d_2 = \gcd(c, b)$, and so $d_1 x = a$, $d_1 y = c$, $d_2 w = c$, and $d_2 v = b$ for some integers x, y, w, and v. $c \mid a + b \Rightarrow cm = a + b = d_1 x + b$ for some integer $m \Rightarrow d_1 ym = d_1 x + b \Rightarrow d_1(ym - x) = b \Rightarrow d_1 \mid b$.
Similarly, $c \mid a + b \Rightarrow cn = a + b = a + d_2 v$ for some integer n
$\Rightarrow d_2 yn = a + d_2 v \Rightarrow d_2(yn - v) = a \Rightarrow d_2 \mid a$. Thus, d_1 and d_2 are common divisors of a and b, and so d_1 and d_2 both divide $\gcd(a, b) = 1$. Therefore, $d_1 = d_2 = 1$.

10. The argument using prime factorization is an exact copy of the first argument which justifies 2.8.3 except that "max" is everywhere replaced with "min." The alternate argument proceeds as follows. Let $y = \gcd(ca, cb)$. Let x and z be integers such that $ca = xy$ and $cb = zy$. Let $d = \gcd(a, b)$. Then $cd \mid ca$ and $cd \mid cb$, so that $cd \mid y$. Let us say that $y = mcd$. Then $ca = x(mcd) = c(xmd)$ and $cb = z(mcd) = c(zmd)$. This implies that $a = xmd$ and $b = zmd$. But then $md \mid a$ and $md \mid b$. Since d is the greatest common divisor of a and b, it follows that $m = 1$.