2.2 The Greatest Common Divisor

Note Title 9/27/2004

Theorem 2.2 For integers a, b, c

(a) $a|0$ since $a \cdot 0 = 0$

$1|a$ since $1 \cdot a = a$

$a|a$ since $a \cdot 1 = a$

(b) $a|1 \iff a = \pm 1$

if $a=1$, Then $a \cdot 1 = 1$

if $a=-1$, Then $a \cdot (-1) = 1$

if $a|1$, Then $a \cdot c = 1$ for some C

if $|c| \neq 1$, Then $|c| > 1$. By def., $|a| \geq 1$

$\therefore |a||c| > 1$, contradicting $a \cdot c = 1$.

$\therefore |c| = 1$, $\therefore c = \pm 1$. If $c = 1$, Then

$ac = a = 1$. If $c = -1$, Then $ac = -a = 1$.

(c) if $a|b$ and $c|d$, Then $ac|bd$

$ax = b$, $cy = d$, $\therefore ac(xy) = bd$

(d) if $a|b$ and $b|c$, Then $a|c$

$ax = b$, $by = c$, $\therefore ax(y) = a(xy) = C$

(e) $a|b$ and $b|a \iff a = \pm b$

$a|b \Rightarrow ax = b$. $b|a \Rightarrow by = a$

$\therefore axy = a$, $xy = 1$. Using (b), $x = \pm 1$

if $x = 1$, Then $ax = b = a$

if $x = -1$, Then $ax = b = -a$

$\therefore a = \pm b$

if $a = b$, Then $a \cdot 1 = a = b$, so $a|b$
and $b \cdot 1 = b = a$, so $b|a$

if $a = -b$, Then $a \cdot (-1) = (-b)(-1) = b$, so $a|b$
and $b \cdot (-1) = -b = a$, so $b|a$

Problems 2.2

1. $a|b \Rightarrow \exists c$ s.t. $a \cdot c = b$

(a) $a \cdot c = (-a)(-c) = b \Rightarrow -a \mid b$

(b) $-(a \cdot c) = -b = a \cdot (-c) \Rightarrow a \mid (-b)$

(c) $-(a \cdot c) = -b = (-a) \cdot c = -b \Rightarrow (-a) \mid (-b)$

2. (a) $a|b \Rightarrow \exists x$ s.t. $ax = b$.

$\therefore axc = bc \Rightarrow a \mid bc$

(b) $a|b$, $a|c \Rightarrow \exists x, y$ s.t. $ax = b$, $ay = c$

$\therefore (ax)(ay) = bc = a^2xy \Rightarrow a^2 | bc$

(c) if $a|b$, then $\exists x$ s.t. $ax = b$

$\therefore acx = bc \Rightarrow ac|bc$

if $ac|bc$, Then $\exists x$ s.t. $acx = bc$

since $c \neq 0$, $ax = b \Rightarrow a|b$

(d) if $a|b$ and $c|d$, Then $\exists x, y$ s.t.

$ax = b$, $cy = d$.

$\therefore (ax)(cy) = ac(xy) = bd \Rightarrow ac|bd$

3. Not true. Let $a=3$, $b=2$, $c=7$

Then $a|(b+c) \equiv 3|(2+7)$, but $3 \nmid 2$, $3 \nmid 7$

4. (a) $8 | 5^{2n} + 7$

Pf: $n=1$: $5^{2n} + 7 = 32$, and $8|32$

Suppose $8 | 5^{2k} + 7$. $\therefore \exists x$ s.t. $8x = 5^{2k} + 7$

$$5^{2(k+1)} + 7 = 5^2 \cdot 5^{2k} + 7$$

$$= 5^2(5^{2k} + 7) - 5^2 \cdot 7 + 7$$

$$= 5^2(8x) - 7(5^2 - 1)$$

$$= 5^2(8x) - 7(24)$$

$$= 8x(25) - 8(7\cdot 3)$$

$$= 8[25x - 21]$$

$\therefore 8 \mid 5^{-2(k+1)}$

(b) $15 \mid 2^{4n} - 1$

$n=1: \; 15 = 2^4 - 1 = 16 - 1$

Assume $15 \mid (2^{4k} - 1)$. $\therefore \exists x$ s.t. $15x = 2^{4k} - 1$

$$2^{4(k+1)} - 1 = 2^4 \cdot 2^{4k} - 1 + 2^4 - 2^4$$

$$= 2^4(2^{4k} - 1) + (2^4 - 1)$$

$$= 2^4(15x) + 15 = 15(x2^4 + 1)$$

$\therefore 15 \mid 2^{4(k+1)} - 1$

(c) $5 \mid (3^{3n+1} + 2^{n+1})$

$n=1: \; 3^{3+1} + 2^2 = 81 + 4 = 85$, and $5 \mid 85$

Suppose $5 \mid (3^{3k+1} + 2^{k+1})$

$\therefore \exists x$ s.t. $5x = 3^{3k+1} + 2^{k+1}$

$3^{3(k+1)+1} + 2^{k+2} = 3^{3k+4} + 2^{k+2}$

$= 3^3 \cdot 3^{3k+1} + 2 \cdot 2^{k+1} + 3^3 \cdot 2^{k+1} - 3^3 \cdot 2^{k+1}$

$= 3^3 (3^{3k+1} + 2^{k+1}) - 2^{k+1}(3^3 - 2)$

$= 3^3 (5x) - 2^{k+1}(25)$

$= 5(x 3^3 - 5 \cdot 2^{k+1})$

$\therefore$ true for $k+1$

(d) $21 \mid 4^{n+1} + 5^{2n-1}$

$n=1: \; 4^2 + 5^1 = 21$

Suppose for k $\; 21 \mid 4^{k+1} + 5^{2k-1}$

$\therefore \exists x$ s.t. $21x = 4^{k+1} + 5^{2k-1}$

$4^{k+2} + 5^{2(k+1)-1} = 4^{k+2} + 5^{2k+1}$

$= 4 \cdot 4^{k+1} + 5^2 \cdot 5^{2k-1} + 4 \cdot 5^{2k-1} - 4 \cdot 5^{2k-1}$

$$= 4\left(4^{k+1} + 5^{2k-1}\right) + 21\left(5^{2k-1}\right)$$

$$= 4\left(21x\right) + 21\left(5^{2k-1}\right)$$

$\therefore$ true for $k+1$

(e) $24 \mid 2\cdot 7^n + 3\cdot 5^n - 5$

$n=1: 2\cdot 7^1 + 3\cdot 5^1 - 5 = 14+15-5 = 24$

Suppose $24 \mid 2\cdot 7^k + 3\cdot 5^k - 5$

$\therefore \exists\, x$ s.t. $24x = 2\cdot 7^k + 3\cdot 5^k - 5$

$$\therefore 2\cdot 7^{k+1} + 3\cdot 5^{k+1} - 5 = 7\left(2\cdot 7^k\right) + 5\left(3\cdot 5^k\right) - 5$$

$$= 2\left(2\cdot 7^k\right) + 5\left(2\cdot 7^k\right) + 5\left(3\cdot 5^k\right) - 5 + 5\cdot 5 - 5\cdot 5$$

$$= 5\left(2\cdot 7^k + 3\cdot 5^k - 5\right) + 2\left(2\cdot 7^k\right) - 5 + 5\cdot 5$$

$$= 5\left(24x\right) + 2\left(2\cdot 7^k\right) + 20 \qquad [\text{Eq. } 1]$$

But $24 \mid 4\cdot 7^k + 20$

pf: $k=1: 4\cdot 7 + 20 = 48 = 24\cdot 2$

suppose $24 \mid 4 \cdot 7^s + 20$

$\therefore \exists y$ s.t. $24y = 4 \cdot 7^s + 20$

$\therefore 4 \cdot 7^{s+1} + 20 = 7(4 \cdot 7^s) + 20$

$= 7(4 \cdot 7^s + 20) + 20 - 140$

$= 7(24y) - 24 \cdot 5$

$\therefore \exists q$ s.t. $24q = 4 \cdot 7^k + 20$

$\therefore$ [Eq. 1] $= 5(24x) + 24q$

$\therefore$ True for $k+1$

5. For integer a, one of $a, a+2, a+4$ is divisible by 3.

Pf: (a) Suppose $3 \nmid a$. $\therefore a = 3q_1 + 1$ or $a = 3q_2 + 2$

$3q_1 + 1$: Then $a + 2 = 3q_1 + 3 = 3(q_1 + 1)$, so $3 \mid a+2$

$3q_2 + 2$: Then $a + 4 = 3q_2 + 6 = 3(q_2 + 2)$ so $3 \mid a+4$

(b) Suppose $3 \nmid a+2$. $\therefore a+2 = 3q_1 + 1$ or $a+2 = 3q_2 + 2$

$3q_1+1$: $\therefore a = 3q_1 - 1$, so $a+4 = 3q_1+3$
$\therefore 3 \mid a+4$
$3q_2+2$: $\therefore a = 3q_2$, so $3 \mid a$

(c) Suppose $3 \nmid a+4$. $\therefore a+4 = 3q_1+1$ or $3q_2+2$

$3q_1+1$: $\therefore a = 3q_1 - 3$, so $3 \mid a$

$3q_2+2$: $\therefore a = 3q_2 - 2$, $a+2 = 3q_2$,
so $3 \mid a+2$

6. (a). $2 \mid a(a+1)$

Pf: By Div. Alg. $a = 2q$ or $a = 2q+1$

$2q$: Then $a(a+1) = 2q(2q+1)$
$\therefore 2 \mid a(a+1)$
$2q+1$: Then $a(a+1) = (2q+1)(2q+2)$
$= 2(2q+1)(q+1)$
$\therefore 2 \mid a(a+1)$

$3 \mid a(a+1)(a+2)$ $\quad a = 3q, 3q+1$, or $3q+2$

$3q$: $a(a+1)(a+2) = 3q(3q+1)(3q+2)$
$\therefore 3 \mid a(a+1)(a+2$

$3q+1:\quad a(a+1)(a+2) = (3q+1)(3q+2)(3q+3)$
$= 3(3q+1)(3q+2)(q+1)$
$\therefore 3 \mid a(a+1)(a+2)$

$3q+2:\quad a(a+1)(a+2) = (3q+2)(3q+3)(3q+4)$
$= 3(3q+2)(q+1)(3q+4)$
$\therefore 3 \mid a(a+1)(a+2)$

(6) $3 \mid a(2a^2+7)$

Pf: $a = 3q,\ 3q+1,\ 3q+2$

$3q:\quad a(2a^2+7) = 3q(\quad)$. $\therefore 3 \mid a(2a^2+7)$

$3q+1:\quad a(2a^2+7) = (3q+1)[2(3q+1)^2+7]$
$= (3q+1)[2(9q^2+6q+1)+7]$
$= (3q+1)(18q^2+12q+9)$
$= 3(3q+1)(6q^2+4q+3)$
$\therefore 3 \mid a(2a^2+7)$

$3q+2:\quad a(2a^2+7) = (3q+2)[2(3q+2)^2+7]$

$$= (3q+2)\left[2(9q^2+12q+4)+7\right]$$

$$= (3q+2)\left(18q^2+24q+15\right]$$

$$= 3(3q+2)(6q^2+8q+5)$$

$$\therefore\ 3 \mid a(2a^2+7)$$

(c) a is odd, Then $32 \mid (a^2+3)(a^2+7)$

Pf: $\exists q$ s.t. $a = 2q+1$

$$\therefore (a^2+3)(a^2+7) = (4q^2+4q+4)(4q^2+4q+8)$$

$$\begin{aligned} = {} & 16q^4 + 16q^3 + 32q^2 \\ + {} & \quad\quad\ 16q^3 + 16q^2 + 32q \\ + {} & \quad\quad\quad\quad\ 16q^2 + 16q + 32 \end{aligned}$$

$$= 16q^4 + 32q^3 + 64q^2 + 48q + 32$$

If q is even, Then $q = 2x$,

so $16q^4 = 16(2x)^4 = 32 \cdot 2^3 \cdot x^4$

and $48q = 96x$

$\therefore$ all terms divisible by 32

If q is odd, $q = 2x+1$,

$$\therefore 16q^4 + 32q^3 + 64q^2 + 48q + 32$$

$$= 16(2x+1)^4 + 32q^3 + 64q^2 + 48(2x+1) + 32$$

$$= 16(2x+1)^4 + 32q^3 + 64q^2 + 96x + 80$$

$$= 16\left(2^4x^4 + \binom{4}{1}2^3x^3 + \binom{4}{2}2^2x^2 + \binom{4}{3}2x + 1\right)$$
$$+32q^3 + 64q^2 + 96x + 80$$

$$= 32\left(2^3x^4 + \binom{4}{1}2^2x^3 + \binom{4}{2}2x^2 + \binom{4}{3}x\right)$$
$$+32q^3 + 64q^2 + 96x + 96$$

So all terms divisible by 32.

7. If a, b are odd, then $16 \mid a^4 + b^4 - 2$

Pf: let $a = 2r+1$, $b = 2s+1$

$$a^4 = (2r+1)^4 = 2^4r^4 + \binom{4}{1}2^3r^3 + \binom{4}{2}2^2r^2 + \binom{4}{3}2r + 1$$

$$= 16r^4 + 32r^3 + 24r^2 + 8r + 1$$

$$\therefore a^4 + b^4 - 2 = 16r^4 + 32r^3 + 24r^2 + 8r +$$
$$16s^4 + 32s^3 + 24s^2 + 8s$$

All terms divisible by 16 except perhaps $24r^2+8r$, $24s^2+8s$

But if r is even, then $r=2w$ for some w, and $\therefore 24r^2+8r = 96w^2+16w$, which is divisible by 16.

If r is odd, then $r=2w+1$, some w.

$$\begin{aligned}\therefore 24r^2+8r &= 24(2w+1)^2+8(2w+1)\\ &= 96w^2+96w+24+16w+8\\ &= 96w^2+96w+16w+32,\end{aligned}$$

which is divisible by 16.

Similarly for $24s^2+8s$

$\therefore 16 \mid a^4+b^4-2$

8. (a) If a, b are odd, then $a^2+b^2 \neq c^2$ for some integer c.

Pf: Let $a=2r+1$, $b=2s+1$

$$\begin{aligned}\therefore a^2+b^2 &= 4r^2+4r+1+4s^2+4s+1\\ &= 4(K)+2 = 2(K')\end{aligned}$$

$\therefore$ if c exists, it must be even

Let $c=2w$, some unique w.

$\therefore c^2 = 4w^2$

By Div. Alg., $a^2+b^2 = 4q+r$, where q and r are unique. From above, $a^2+b^2 = 4K+2$

if $a^2+b^2=c^2$, Then $a^2+b^2=4w^2$, which means "q" and "r" are not unique.

$\therefore a^2+b^2 \neq c^2$ if a, b are odd

(b) Let a, b, c, d be four consecutive integers. Then $a \cdot b \cdot c \cdot d = e^2-1$, for some e.

Pf: A few examples show that the product of the 1st & last terms is close to the product of the middle two terms, and That The perfect square in question is The average of the two products. An average exists because The two products are even.

$$\therefore a(a+1)(a+2)(a+3) \stackrel{?}{=} \left[\frac{a(a+3)+(a+1)(a+2)}{2}\right]^2-1$$

Suppose a is even. Then $a=2n$

$$\therefore a(a+1)(a+2)(a+3) = 2n(2n+1)(2n+2)(2n+3)$$
$$= (4n^2+2n)(4n^2+10n+6)$$
$$= 16n^4 + 40n^3 + 24n^2$$
$$+ 8n^3 + 20n^2 + 12n$$
$$= 16n^4 + 48n^3 + 44n^2 + 12n$$

$$\left[\frac{2n(2n+3) + (2n+1)(2n+2)}{2}\right]^2 - 1$$
$$= \left[\frac{4n^2+6n + 4n^2+6n+2}{2}\right]^2 - 1$$
$$= \left[\frac{8n^2+12n+2}{2}\right]^2 - 1$$
$$= (4n^2+6n+1)^2 - 1$$
$$= (4n^2+6n+1)(4n^2+6n+1) - 1$$
$$= 16n^4 + 24n^3 + 4n^2$$
$$+ 24n^3 + 36n^2 + 6n$$
$$+ 4n^2 + 6n + 1 - 1$$
$$= 16n^4 + 48n^3 + 44n^2 + 12n \quad \checkmark$$

If a is odd, Then $a = 2n+1$

$$\therefore a(a+1)(a+2)(a+3) = (2n+1)(2n+2)(2n+3)(2n+4)$$
$$= (4n^2+6n+2)(4n^2+14n+12)$$
$$= 16n^4 + 56n^3 + 48n^2$$
$$+ 24n^3 + 84n^2 + 72n$$
$$+ 8n^2 + 28n + 24$$

$$= 16n^4 + 80n^3 + 140n^2 + 100n + 24$$

$$\left[\frac{a(a+3) + (a+1)(a+2)}{2}\right]^2 - 1 =$$

$$\left[\frac{(2n+1)(2n+4) + (2n+2)(2n+3)}{2}\right]^2 - 1$$

$$= \left[\frac{4n^2 + 10n + 4 + 4n^2 + 10n + 6}{2}\right]^2 - 1$$

$$= (4n^2 + 10n + 5)^2 - 1$$

$$= (4n^2 + 10n + 5)(4n^2 + 10n + 5) - 1$$

$$\begin{aligned} = 16n^4 &+ 40n^3 + 20n^2 \\ &+ 40n^3 + 100n^2 + 50n \\ &+ \qquad\qquad 20n^2 + 50n + 25 - 1 \end{aligned}$$

$$= 16n^4 + 80n^3 + 140n^2 + 100n + 24 \checkmark$$

9. $(a+1)^3 - a^3$ is never divisible by 2

Pf: Suppose a is even. $\therefore a = 2n$

$$\therefore (a+1)^3 - a^3 = (2n+1)^3 - (2n)^3$$

$$= 8n^3 + \binom{3}{1}4n^2 + \binom{3}{2}2n + 1 - 8n^3$$

$$= 12n^2 + 6n + 1$$

$= 2(k) + 1$, so $(a+1)^3 - a^3$ is odd

Suppose a is odd. $\therefore$ $a = 2n+1$

$\therefore (a+1)^3 - a^3 = (2n+1+1)^3 - (2n+1)^3$

$= (2n+1)^3 + \binom{3}{1}(2n+1)^2 + \binom{3}{2}(2n+1) + 1 - (2n+1)^3$

$= (2n+1)\left[3(2n+1) + 3\right] + 1$

$= (2n+1)(6n+6) + 1$

$= 2\left[(2n+1)(3n+3)\right] + 1$

$= 2(k) + 1$, so $(a+1)^3 - a^3$ is odd.

10.(a) $a \neq 0$, $\gcd(a, 0) = |a|$

Pf: From Th. 2.2 (p. 21), we know that $a|0$ and $a|a$. $\therefore$ $|a|$ is a common divisor.
Let c be another common divisor.
$\therefore$ $c|a$ and $\therefore$ $|c| \leq |a|$ by Th. 2.2
$\therefore$ $|a|$ is gcd

(b) $a \neq 0$, $g(a,a) = |a|$

Pf: By Th. 2.2, $a|a$. $\therefore$ $|a|$ is a common divisor.

Let c be another common divisor.

$\therefore$ $c|a$, and $\therefore$ $|c| \leq |a|$, by Th. 2.2

$\therefore$ $|a|$ is gcd.

(c) $a \neq 0$, $\gcd(a,1) = 1$

Pf: By Th. 2.2, $1|a$, $1|1$. $\therefore$ 1 is a common divisor.

Let c be another common divisor.

$\therefore$ $c|1$, and $\therefore$ $|c| \leq 1$ (Th. 2.2)

$\therefore$ 1 is gcd.

11. $\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$

Pf: Let x be the gcd of any one pair.

Since $x|y \Leftrightarrow x|(-y)$, then

x is a common divisor of any other pair.

Let c be another common divisor.

Since $c|a \Leftrightarrow c|(-a)$ and $c|b \Leftrightarrow c|(-b)$,

Then $c|x$ by Th. 2.6. $\therefore$ $|c| \leq |x|$,

$\therefore$ x is the gcd of the other pair.

12. $n>0$, a any integer, $\gcd(a, a+n) \mid n$

Pf: Let $d = \gcd(a, a+n)$

$\therefore \exists x, y$ s.t. $a = dx$, $a+n = dy$

$\therefore dx + n = dy$, $n = d(y-x)$, $\therefore d \mid n$

And by Th. 2.2, $d \mid 1 \Leftrightarrow d = \pm 1$.

$\therefore \gcd(a, a+1) = 1$.

13. (a). (1) Let x, y be any integers and let $d = \gcd(a, b)$

$\therefore \exists m, n$ s.t. $a = dm$ and $b = dn$

$\therefore c = ax + by = dmx + dny = d(mx + ny)$.

$\therefore d \mid c$

(2) Suppose $\gcd(a, b) \mid c$. Let $d = \gcd(a, b)$.

$\therefore \exists x_0, y_0$ s.t. $d = ax_0 + by_0$

But $d \mid c$, so that $c = dp$, for some p

$\therefore c = dp = (ax_0 + by_0)p = ax_0 p + by_0 p$

$\therefore$ Let $x = x_0 p$, $y = y_0 p$

(b) Let x, y be s.t. $ax + by = \gcd(a, b)$. Then $\gcd(x, y) = 1$

Pf: Let $d = \gcd(a, b)$. $\therefore ax + by = d$

Since $d \mid a$ and $d \mid b$, Then $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

$$\therefore \frac{a}{d}x + \frac{b}{d}y = 1,$$

and $\therefore$ x and y are relatively prime.

$\therefore \gcd(x, y) = 1$.

14. (a) Since $9(2a+1) + (-2)(9a+4) = 1$, Then by Th. 2.4 $2a+1$ and $9a+4$ are relatively prime, so $\gcd(2a+1, 9a+4) = 1$

(b) $(-7)(5a+2) + 5(7a+3) = 1$

$\therefore \gcd(5a+2, 7a+3) = 1$

(c) $\gcd(3a, 3a+2) \mid 2$ by problem 12

$\therefore \gcd = 1$ or 2. But a odd $\Rightarrow$ $3a$ is odd.

$\therefore 2 \nmid 3a$. $\therefore \gcd = 1$

15 $\gcd(2a-3b, 4a-5b) \mid b$

Pf: Let $d = \gcd(2a-3b, 4a-5b)$

For all x, y, by Corollary on p. 23, $x(2a-3b) + y(4a-5b)$ is a multiple of d.

$\therefore \exists n$ s.t. $dn = (-2)(2a-3b) + (1)(4a-5b)$
$= b$

$\therefore d | b$

Now let $b = -1$. $\therefore \gcd(2a+3, 4a+5) | (-1)$
$\therefore \gcd = 1$.

16. If a is odd, $12 | a^2 + (a+2)^2 + (a+4)^2 + 1$

Pf: Let $a = 2n+1$
$\therefore (2n+1)^2 + (2n+3)^2 + (2n+5)^2 + 1$

$$= 4n^2 + 4n + 1 + 4n^2 + 12n + 9 + 4n^2 + 20n + 25 + 1$$
$$= 12n^2 + 36n + 36 = 12(n^2 + 3n + 3)$$

17. For all $n \geq 0$, $(3n)!/(3!)^n$ is an integer

Pf: $n=1$: $3!/3! = 1$

$k \Rightarrow k+1$: Suppose $(3k)!/(3!)^k = R$ is an integer
$\therefore [3(k+1)]!/(3!)^{k+1}$

$= (3k+3)!/(3!)^k \cdot (3!)$

$$= \frac{(3k+3)(3k+2)(3k+1)\,(3k)!}{3\cdot 2\cdot 1 \quad \cdot (3!)^k}$$

$$= \frac{3(k+1)(3k+2)(3k+1)}{3\cdot 2} \cdot R$$

$$= \frac{(k+1)(3k+2)(3k+1)\cdot R}{2}$$

If k is odd, Then $k+1$ is even,
so $(k+1)/2 = x$, some integer x.
If k is even, Then $3k+2$ is even, so
$(3k+2)/2 = x$, some integer x.

$\therefore$ entire expression is an integer.

18. (a). $6 \mid a(a+1)(a+2)$

Pf: $6 = 3\cdot 2$, and $\gcd(2,3) = 1$ (Problem 12).

Let $R = a(a+1)(a+2)$

If a is even, Then $2 \mid a$, $\therefore 2 \mid R$
If a is odd, Then $2 \mid (a+1)$, $\therefore 2 \mid R$

Let $a = 3q + r$

if $r=0$, then $3|a$, $\therefore 3|k$
if $r=1$, then $a+2 = 3q+3$, $3|a+2$, $3|k$
if $r=2$, then $a+1 = 3q+3$, $3|a+2$, $3|k$

$\therefore 3|k$ and $2|k$, and by Corollary 2 on p. 24, $3\cdot 2|k$
$\therefore 6 \mid a(a+1)(a+2)$

(b) $24 \mid a(a+1)(a+2)(a+3)$

Pf: $n=1$: $1\cdot 2\cdot 3\cdot 4 = 24$

$k \Rightarrow k+1$: Suppose $24 \mid k(k+1)(k+2)(k+3)$
$\therefore 24p = k(k+1)(k+2)(k+3)$, some p

$\therefore (k+1)(k+2)(k+3)(k+4) =$
$k(k+1)(k+2)(k+3) + 4(k+1)(k+2)(k+3)$
$= 24p + 4(k+1)(k+2)(k+3)$

But by (a), $(k+1)(k+2)(k+3) = 6q$ for some q.

$\therefore (k+1)(k+2)(k+3)(k+4) = 24p + 24q$

$\therefore 24 \mid (k+1)(k+2)(k+3)(k+4)$

(c) $120 \mid a(a+1)(a+2)(a+3)(a+4)$

Pf: $n=1$: $1\cdot 2\cdot 3\cdot 4\cdot 5 = 120$

$k \Rightarrow k+1$: Suppose $120 \mid k(k+1)(k+2)(k+3)(k+4)$

$\therefore \exists p$ s.t. $120p = k(k+1)(k+2)(k+3)(k+4$

But $(k+1)(k+2)(k+3)(k+4)(k+5) =$

$k(k+1)(k+2)(k+3)(k+4) + 5(k+1)(k+2)(k+3)(k+4)$

$= 120p + 5\cdot 24q$, for some q by (b) above.

$= 120(p+q)$

$\therefore 120 \mid (k+1)(k+2)(k+3)(k+4)(k+5)$

19. (a) $6 \mid a(a^2+11)$

Pf: Let $a = 6q + r$, where $0 \leq r < 6$
Consider each case for r

$r=0$: $a(a^2+11) = 6q[(6q)^2+11]$. $\therefore 6 \mid a(a^2+11)$

$r=1: \; a(a^2+11) = (6q+1)(6q+1)^2 + (6q+1)11$

$= 6^3q^3 + \binom{3}{1}(6q)^2 + \binom{3}{2}6q + \binom{3}{0} \; + 6q)11 + 11$

$= 6[\quad] + \binom{3}{0} + 11$

$= 6[\quad] + 12 = 6\{\quad\}$

$r=2: \; a(a^2+11) = (6q+2)^3 + (6q+2)\cdot 11$

$= 6[\quad] + \binom{3}{0}2^3 + (6q)(11) + 22$

$= 6[\quad] + 30 = 6[\quad]$

$r=3: \; a(a^2+11) = (6q+3)^3 + (6q+3)11$

$= 6[\quad] + \binom{3}{0}\cdot 3^3 + 33$

$= 6[\quad] + 27 + 33 = 6[\;] + 60$

$= 6[\;]$

$r=4: \; a(a^2+11) = (6q+4)^3 + (6q+4)11$

$= 6[\;] + \binom{3}{0}4^3 + 44$

$= 6[\;] + 64 + 44 = 6[\;] + 108$

$= 6[\ ] + 6\cdot 18 = 6[\ ]$

$r=4$: $a(a^2+11) = (6q+5)^3 + (6q+5)11$

$= 6[\ ] + \binom{3}{0}5^3 + 55$

$= 6[\ ] + 125 + 55 = 6[\ ] + 6\cdot 30$

$= 6[\ ]$

(b) a is odd, Then $24 \mid a(a^2-1)$

Pf: First, show a^2 is of form $8K+1$

Let $a = 4q + r$. $\therefore r = 1$ or 3 since a is odd.

$\therefore a^2 = 16q^2 + 8q + 1 = 8K + 1$

or $a^2 = 16q^2 + 24q + 9 = 8K' + 1$

So, $a(a^2-1) = a8K$, for some K.

$\therefore 8 \mid a(a^2-1)$

By #18 above, $6 \mid (a-1)(a)(a+1)$, so

$3 \mid (a-1)(a)(a+1) \equiv 3 \mid a(a^2-1)$

since $\gcd(3,8)=1$, $\therefore 24 \mid a(a^2-1)$
by Corollary 2 on p. 24

(c) a, b odd $\Rightarrow 8 \mid (a^2-b^2)$

Pf: By (b) above, a^2 is of form $8k+1$
and b^2 is of form $8k'+1$

$$\therefore a^2-b^2 = 8k+1-(8k'+1)$$
$$= 8(k+k'), \text{ some } k, k'$$
$$\therefore 8 \mid (a^2-b^2)$$

(d) $2 \nmid a,\ 3 \nmid a \Rightarrow 24 \mid (a^2+23)$

Pf: Let $a = 12q + r$, $0 \le 0 < 12$
r can only be $1, 3, 5, 7, 9, 11$ since $2 \nmid a$,
and since $3 \nmid a$, $r \ne 3$ or 9.
$\therefore r$ can only be $1, 5, 7,$ or 11.

$$\therefore a^2+23 = (12q+r)^2 + 23$$
$$= 144q^2 + 24qr + r^2 + 23$$
$$= 24(6)q^2 + 24qr + r^2 + 23$$

$$= 24[\ \ ] + r^2 + 23$$

$r = 1: \ r^2 + 23 = 24$

$r = 5: \ r^2 + 23 = 48 = 24(2)$

$r = 7: \ r^2 + 23 = 72 = 24(3)$

$r = 11: \ r^2 + 23 = 144 = 24(6)$

$\therefore a^2 + 23 = 24[\ \ ] + r^2 + 23$
$\qquad = 24[\ \ ] + 24k$, some k

$\therefore 24 \mid (a^2 + 23)$

(c) $360 \mid a^2(a^2-1)(a^2-4)$

Pf: $a^2(a^2-1)(a^2-4) = a^2(a+1)(a-1)(a+2)(a-2)$

$= (a-2)(a-1)(a)(a+1)(a+2)(a)$

$360 = 5 \cdot 9 \cdot 8$, and $5, 9, 8$ are relatively prime.

By #18, $(a-2)(a-1)(a)(a+1)(a+2)$ is

divisible by 24 and 120. $\therefore$ it is divisible by 8 and 5.

Also, $(a-2)(a-1)(a)$ and $a(a+1)(a+2)$ are both divisible by 6 and so are both divisible by 3, and $\therefore$ the entire product is divisible by 9.

$\therefore$ Entire product divisible by 360 by Corollary 2, p. 24

20. (a) $\gcd(a,b)=1$, $\gcd(a,c)=1$, Then $\gcd(a,bc)=1$

Pf: $1 = ax+by = au+cv$ for some x,y,u,v

$$\therefore 1 = (ax+by)(au+cv) = a^2xy + abyu + a^2xu + bcyv$$
$$= a(axy + byu + axu) + bcyv$$
$$= aK_1 + bcK_2$$

$\therefore$ a, bc relatively prime.

(b) $\gcd(a,b)=1$, $c|a$, Then $\gcd(b,c)=1$

Pf: $\exists\, x,y$ s.t. $ax+by=1$, and $\exists\, n$ s.t. $cn=a$

$$\therefore \ cnx + by = 1 \Rightarrow \gcd(c,b)=1$$

(c) $\gcd(a,b)=1$, then $\gcd(ac,b)=\gcd(c,b)$

Pf: Let $d=\gcd(c,b)$. Need to show

(1) $d \mid ac$ ($d \mid b$ by def.)

(2) if $k \mid ac$ and $k \mid b$, then $k \mid d$

(1): Since $d \mid c$, $\exists\, n$ s.t. $dn = c$, so

$d(na) = ca$, $\Rightarrow d \mid ca$

(2) $\exists\, x, y$ s.t. $d = cx + by$

since $k \mid b$, then $\exists\, n$ s.t. $kn = b$

$\therefore d = cx + kny$

Since $g(a,b)=1$, $\exists\, p, q$ s.t. $ap + bq = 1$

$\therefore apc + bqc = c$

$\therefore d = (apc + bqc)x + kny$

$= acpx + knqcx + kny$

But $k \mid ac \Rightarrow \exists\, r$ s.t. $kr = ac$

$\therefore d = krpx + knqcx + kny$

$= k(rpx + nqcx + ny)$

$\therefore k \mid d$

$\therefore$ By Theorem 2.6, $\gcd(c,b) = \gcd(ac,b)$

(d) $\gcd(a,b)=1,\ c \mid a+b \Rightarrow \gcd(a,c) = \gcd(b,c) = 1$

Pf: $g(a,b) = 1 \Rightarrow \exists\, x,y$ s.t. $ax+by=1$

$c \mid a+b \Rightarrow \exists\, n$ s.t. $cn = a+b$

$\therefore cn - b = a$

$\therefore (cn-b)x + by = 1$

$cnx - bx + by = 1,$

so, $cnx + b(y-x) = 1 \Rightarrow \gcd(c,b) = 1$

Similarly, $cn - a = b$, so

$ax + (cn-a)y = 1$

$ax + cny - ay = 1,$

so, $a(x-y) + cny = 1 \Rightarrow \gcd(a,c) = 1$

(e) $\gcd(a,b)=1$, $d \mid ac$, $d \mid bc$, Then $d \mid c$

Pf: $\exists\, x,y$ s.t. $ax+by=1$. $\therefore\ acx+bcy=c$

But $ac=dn$ and $bc=dm$ for some n,m

$\therefore\ dnx+dmy=c$, $d(nx+my)=c$

$\therefore\ d \mid c$

(f) $\gcd(a,b)=1$, Then $\gcd(a^2,b^2)=1$

Pf: From (c) above, let $c=a$.

$\therefore\ \gcd(a,b)=1 \Rightarrow \gcd(a^2,b)=\gcd(a,b)=1$

Also, $\gcd(a,b)=\gcd(b,a)=\gcd(b^2,a)$
$=\gcd(b,a)=1$

So, $\gcd(a^2,b)=\gcd(a,b^2)=1$

Now apply (c) again to get

$\gcd(a\cdot a,b^2)=\gcd(a,b^2)=1$

$\therefore\ \gcd(a^2,b^2)=1$

21. (a). $d \mid n \Rightarrow 2^d - 1 \mid 2^n - 1$

Pf: From Problems 1.1, #3,

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + a + 1)$$

$$\therefore 2^n - 1 = 2^{n-1} + 2^{n-2} + \dots + 2 + 1 \text{ (n terms)}$$

$$2^d - 1 = 2^{d-1} + 2^{d-2} + \dots + 2 + 1 \text{ (d terms)}$$

Since $d \mid n$, $\exists x$ s.t. $dx = n$

$$\therefore 2^n - 1 = 2^{dx} - 1 = (2^d)^x - 1$$

$$= (2^d - 1)(2^{d(x-1)} + 2^{d(x-2)} + \dots + 2^d + 1)$$

$$\therefore 2^d - 1 \mid 2^n - 1$$

Could also look at This explicitly

$$\frac{2^n - 1}{2^d - 1} = \frac{n \text{ terms}}{d \text{ terms}} = \frac{dx \text{ terms}}{d \text{ terms}}$$

$$= \frac{\overset{d \text{ terms}}{(\quad)} + \overset{d \text{ terms}}{(\quad)} + \dots + \overset{d \text{ terms}}{(\quad)}}{(d \text{ terms})}$$

$$= 2^{d(x-1)} + 2^{d(x-2)} + \dots + 2^{d} + 1$$

(b) $31 = 2^5 - 1$. Since $5 | 35$, $2^5 - 1 | 2^{35} - 1$

$127 = 2^7 - 1$, and $7 | 35$. $\therefore 2^7 - 1 | 2^{35} - 1$

22. What values of n does $t_n | t_1 + t_2 + \dots + t_n$

From Problems 1.3, #3,

$$t_1 + t_2 + \dots + t_n = \frac{n(n+1)(n+2)}{6}$$

and from Problems 1.3, #1(a), $t_n = \frac{n(n+1)}{2}$

$$\therefore \frac{\frac{n(n+1)(n+2)}{6}}{\frac{n(n+1)}{2}} = \frac{n+2}{3}$$

$\therefore t_n$ divides $t_1 + \dots + t_n$ when $\frac{n+2}{3}$ is an integer, or $n = 1, 4, 7, 10 \dots$

23. If $a | bc$, show $a | \gcd(a,c) \gcd(a,c)$

Pf: Let $d_1 = \gcd(a,b)$, $d_2 = \gcd(a,c)$

$\therefore \exists x, y, u, v$ s.t. $d_1 = ax + by$

$d_2 = au + cv$

and $\exists n$ s.t. $an = bc$

$\therefore d_1 d_2 = (ax + by)(au + cv)$

$= a^2xu + acxv + abuy + bcyv$

$= a(axu + cxv + buy) + anyv$

$= a(axu + cxv + buy + nyv)$

$\therefore a \mid d_1 d_2$