2.2 The Greatest Common Divisor

Theorem 2.2 For integers $a, b, c$

(a) $a \mid 0 \quad \text{since} \quad a \cdot 0 = 0$
   
   $1 \mid a \quad \text{since} \quad 1 \cdot a = a$
   
   $a \mid a \quad \text{since} \quad a \cdot 1 = a$

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

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

   if $a \mid 1$, then $a \cdot c = 1$ for some $c$

   if $|c| \neq 1$, then $|c| > 1$. By def., $|a| = 1$
   
   $\Rightarrow |a| \cdot |c| > 1$, contradicting $a \cdot c = 1$
   
   $\therefore |c| = 1$. If $c = 1$, then $a \cdot c = a = 1$
   
   If $c = -1$, then $a \cdot c = -a = 1$

(c) if $a \mid b$ and $c \mid d$, then $ac \mid bd$

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

(d) if $a \mid b$ and $6 \mid c$, then $a \mid c$

   $ax = b, 6y = c \quad \therefore a \cdot (y) = a \cdot (xy) = c$
(e) \( a \mid b \) and \( b \mid a \iff a = \pm b \)

\[ a \mid b \iff ax = b \quad b \mid a \iff by = a \]
\[ \therefore ax = ay = a \quad xy = 1 \]
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 \( a \mid b \)

and \( b \cdot 1 = b = a \), so \( b \mid a \)

If \( a = -b \), then \( a \cdot (-1) = (-b)(-1) = b \), so \( a \mid b \)

and \( b \cdot (-1) = -b = a \), so \( b \mid a \)

Problems 2.2

1. \( a \mid b \iff \exists c \ s.t. \ a \cdot c = b \)
   
   (a) \( a \cdot c \cdot (-a)(-c) = b \iff -a \mid b \)
   
   (b) \( -a \cdot c = -b = a \cdot (-c) \iff a \mid (-b) \)
   
   (c) \( -a \cdot c = -b = (-a) \cdot c = -b \iff (-a) \mid (-b) \)

2. (a) \( a \mid b \iff \exists x \ s.t. \ ax = b \)
   
   \[ \therefore a \cdot x = 6c \iff a \mid 6c \]

   (b) \( a \mid b \), \( a \mid c \iff \exists x, y \ s.t. \ ax = b, ay = c \)
\[ (ax)(cy) = bc = a^2xy \implies a^2 \mid bc \]

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

\[ \therefore ax = bc \implies ac \mid bc \]

if \( ac \mid bc \), then \( \exists x \) s.t. \( ax = 6c \)

Since \( c \neq 0 \), \( ax = 6 \implies a \mid 6 \)

(d) if \( a \mid b \) and \( c \mid d \), then \( \exists x, y \) s.t.

\[ ax = 5, \quad cy = d. \]

\[ \therefore (ax)(cy) = 5d \implies ac \mid 5d \]

3. Not True. Let \( a = 3 \), \( b = 2 \), \( c = 7 \)

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

4. (a) \( 8 \mid 5^{2n} + 7 \)

Proof: \( n = 1 \) : \( 5^{2n} + 7 = 32 \) and \( 8 \mid 32 \)

\[ \text{Suppose } 8 \mid 5^{2k} + 7. \implies \exists x \text{ s.t. } 8x = 5^{2k} + 7 \]

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

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

\[ = 5^2(8x) - 7(5^2 - 1) \]

\[ = 5^2(8x) - 7(24) \]
\[ = 8 \times (25) - 8(7.3) \]
\[ = 8 \sum 25x - 217 \]
\[ \therefore 8 \left[ 5 - 2(5+1) \right] \]

(3) \[ 15 \mid 2^{4n} - 1 \]

\[ n = 1; \quad 15 = 2^4 - 1 = 16 - 1 \]

Assume \( 15 \mid (2^{4k} - 1) \), \( \therefore 3 \) s.t. \( 15x = 2^{4k} - 1 \)

\[ 2^{4(k+1)} - 1 = 2^4 \cdot 2^{4k} - 1 + 2^4 - 2^4 \]
\[ = 2^4(2^{4k} - 1) + (2^4 - 1) \]
\[ = 2^4(15x) + 15 = 15(2^{4k} + 1) \]
\[ \therefore 15 \mid 2^{4(k+1)} - 1 \]

(3) \[ 5 \mid (3^{3n+1} + 2^{n+1}) \]

\[ n = 1; \quad 3^{3+1} + 2^2 = 81 + 4 = 85 \] and \( 5 \mid 85 \)

Suppose \( 5 \mid (3^{3k+1} + 2^{k+1}) \)
\[ \begin{align*}
\therefore \, 3 \cdot 5^k \cdot 5^x &= 3^{3k+1} + 2^{k+1} \\
\frac{3^{(3k+1)} + 2^{k+1}}{3} &= 3^3 + 2^2 \\
&= 3^3 \cdot 3^k + 2 \cdot 2^{k+1} + 3^2 \cdot 2^{k+1} - 3 \cdot 2^{k+1} \\
&= 3^3 (3^k + 2^{k+1}) - 2^{k+1} (3^3 - 2) \\
&= 3^3 (5^k) - 2^{k+1} (2^3 - 2^5) \\
&= 5 (3^3 - 5 \cdot 2^{k+1}) \\
\therefore \text{true for } k+1 \\
\text{(d)} 21 | 4^{n+1} + 5^{2n-1} \\
n = 1 : 4^2 + 5^{-1} = 21 \\
\text{Suppose for } k \text{ } 21 | 4^{k+1} + 5^{-2k-1} \\
\therefore \, 3 \cdot 5^k \cdot 21 \cdot 5^x = 4^{k+1} + 5^{-2k-1} \\
4^{k+2} + 5^{-2(2k+1)} = 4^{k+2} + 5^{-2k+1} \\
= 4 \cdot 4^{k+1} + 5^{-2} \cdot 5^{-2k-1} + 4 \cdot 5^{-2k-1} - 4 \cdot 5^{-2k-1}
\end{align*} \]
\[ = 4 \left(4 \cdot 2^{k+1} + 5 \cdot 2^{k-1}\right) + 2 \cdot 1 \left(5 \cdot 2^{k-1}\right) \]
\[ = 4 \left(2 \cdot \frac{7^k}{3} + 2 \cdot \frac{5^k}{3}\right) \]
\[ \therefore \text{true for } k+1 \]

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

\[ \eta = 1: 2 \cdot 7 + 3 \cdot 5 - 5 = 14 + 15 - 5 = 24 \]

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

\[ \therefore 3 \times 5 \cdot 5 - 24 \times 2 = 2 \cdot 7^k + 3 \cdot 5^k - 5 \]

\[ \therefore 2 \cdot 7^{k+1} + 3 \cdot 5^{k+1} - 5 = 7 \left(2 \cdot 7^k\right) + 5 \left(3 \cdot 5^k\right) - 5 \]
\[ = 2 \left(2 \cdot 7^k\right) + 5 \left(2 \cdot 7^k\right) + 5 \left(3 \cdot 5^k\right) - 5 + 5 \cdot 5 - 5 \cdot 5 \]
\[ = 5 \left(2 \cdot 7^k + 3 \cdot 5^k - 5\right) + 2 \left(2 \cdot 7^k\right) - 5 + 5 \cdot 5 \]
\[ = 5 \left(24 \times 2\right) + 2 \left(2 \cdot 7^k\right) + 20 \quad \text{[Eq. 1]} \]

But \(24 \mid 4 \cdot 7^k + 20\)

\[ \therefore k = 1: 4 \cdot 7 + 20 = 4 \cdot 5 = 24 \cdot 2 \]
Suppose $24 \mid 4 \cdot 7^s + 20$

$\therefore \exists \gamma \text{ s.t. } 24\gamma = 4 \cdot 7^s + 20$

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

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

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

$\therefore \exists \delta \text{ s.t. } 24\delta = 4 \cdot 7^k + 20$

$\therefore [\text{Eq. 1}] = 5(24\delta) + 24\delta$

$\therefore \text{True for } k+1$

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 $3 \mid a+2$ . $\therefore a+2 = 3q_1 + 1$ or $a+2 = 3q_2 + 2$
\[3q_1 + 1: \therefore a = 3q_1 - 1, \text{ so } a + 4 = 3q_1 + 3\]
\[\therefore 3 \mid a + 4\]

\[3q_2 + 2: \therefore a = 3q_2 - 3, \text{ so } 3 \mid a\]

(C) Suppose \(3 \mid a + 4\). \[\therefore a + 4 = 3q_1 + 1 \text{ or } 3q_2 + 2\]

\[3q_1 + 1: \therefore a = 3q_1 - 3, \text{ so } 3 \mid a\]

\[3q_2 + 2: \therefore a = 3q_2 - 2, \text{ so } a + 2 = 3q_2\]

\[\therefore 3 \mid a + 2\]

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

Proof: By Div. Alg., \(a = 2q \text{ or } a = 2q + 1\)

\[2q: \text{ Then } a(a+1) = 2q(2q + 1)\]
\[\therefore 2 \mid a(a+1)\]

\[2q + 1: \text{ Then } a(a+1) = (2q + 1)(2q + 2) = 2(2q + 1)(q + 1)\]
\[\therefore 2 \mid a(a+1)\]

\[3 \mid a(a+1)(a+2) \quad a = 3q, 3q + 1, \text{ or } 3q + 2\]

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

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

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

\[\text{pf: } \quad a = 3q, \ 3q + 1, \ 3q + 2\]

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

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

\[3q + 2: \quad a(2a^2 + 7) = (3q+2)[2(3q+2)^2 + 7] \]
\begin{align*}
\quad & = (3q+2) \left[ 2 \left( 9q^2 + 12q + 4 \right) + 7 \right] \\
& = (3q+2) \left( 18q^2 + 24q + 18 \right) \\
& = 3 \left( 3q+2 \right) \left( 6q^2 + 8q + 6 \right) \\
\therefore & \quad 3 \mid a \left( 2a^2 + 7 \right) \\
(C) & \quad a \text{ is odd, Then } 32 \mid (a^2 + 8)(a^2 + 7) \\
\text{Proof: } & \quad \exists \ q \text{ s.t. } a = 2q + 1 \\
\therefore & \quad (a^2 + 3)(a^2 + 7) = \left( 4q^2 + 4q + 4 \right) \left( 4q^2 + 4q + 8 \right) \\
& = 16q^4 + 16q^3 + 32q^2 \\
& \hspace{1cm} + 16q^3 + 16q^2 + 32q \\
& \hspace{1cm} + 16q^2 + 16q + 32 \\
& = 16q^4 + 32q^3 + 64q^2 + 48q + 32 \\
\text{If } & \quad q \text{ is even, Then } q = 2x, \\
\text{so } & \quad 16q^4 = 16(2x)^4 = 32 \cdot 2^3 \cdot x^4 \\
\text{and } & \quad 48q = 96x \\
\therefore & \quad \text{all terms divisible by 32}
\end{align*}
If \( q \) is odd, \( q = 2x + 1 \),

\[
\begin{align*}
16q^4 + 32q^3 + 64q^2 + 48q + 32 &= 16(2x+1)^4 + 32q^3 + 64q^2 + 48(2x+1) + 32 \\
&= 16(2x+1)^4 + 32q^3 + 64q^2 + 96x + 80 \\
&= 16\left(\binom{4}{4} 2^4 x + \binom{4}{1} 2^3 x^3 + \binom{4}{2} 2^2 x^2 + \binom{4}{3} 2x + 1\right) \\
&\quad + 32q^3 + 64q^2 + 96x + 80 \\
&= 32\left(\binom{3}{4} 2^3 x^3 + \binom{4}{2} 2^2 x^2 + \binom{4}{3} x\right) \\
&\quad + 32q^3 + 64q^2 + 96x + 96
\end{align*}
\]

So all terms divisible by 32.

7. If \( q, 6 \) are odd, then \( 16 \mid a^4 + 6^4 - 2 \)

**Proof:** Let \( a = 2r + 1 \), \( 6 = 2s + 1 \)

\[
\begin{align*}
a^4 &= (2r+1)^4 \\
&= 2^4r^4 + \binom{4}{1}2^3r^3 + \binom{4}{2}2^2r^2 + \binom{4}{3}2r + 1 \\
&= 16r^4 + 32r^3 + 24r^2 + 8r + 1 \\
\therefore a^4 + 6^4 - 2 &= 16r^4 + 32r^3 + 24r^2 + 8r + 16s^4 + 32s^3 + 24s^2 + 8s
\end{align*}
\]
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 $w$.
\[24r^2 + 8r = 24(2w + 1)^2 + 8(2w + 1)\]
\[= 96w^2 + 96w + 24 + 16w + 8\]
\[= 96w^2 + 96w + 16w + 32,\]
which is divisible by 16.

Similarly for $24s^2 + 8s$.
\[\therefore 16 | a^4 + b^4 - 2\]

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

Proof: Let $a = 2r + 1$, $b = 2s + 1$.
\[\therefore a^2 + b^2 = 4r^2 + 4r + 1 + 4s^2 + 4s + 1\]
\[= 4(K) + 2 = 2(2K')\]
\[\therefore \text{if } c \text{ exists, it must be even.}\]
Let $c = 2w$, some unique $w$.\]
\[ \therefore c^2 = 4w^2 \]

By Div. A(q), \( a^2 + b^2 = 4q + r \), 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)

\[ \therefore a^2 + b^2 = c^2 \text{ if } a, b \text{ are odd} \]

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

Pf: A few examples show that the product of the last and first 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.

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

Suppose \( a \) is even. Then \( a = 2n \).
\[
\begin{align*}
\therefore a(\alpha+1)(\alpha+2)(\alpha+3) &= 2n(2n+1)(2n+2)(2n+3) \\
&= (4n^2+2n)(4n^2+10n+6) \\
&= 16n^4 + 40n^3 + 24n^2 \\
&\quad + 8n^3 + 20n^2 + 12n \\
&= 16n^4 + 48n^3 + 44n^2 + 12n
\end{align*}
\]

\[
\begin{align*}
\sqrt{\frac{2n(2n+3) + (2n+1)(2n+2)}{2}} &- 1 \\
&= \left(\frac{4n^2 + 6n + 1}{2}\right)^2 - 1 \\
&= (4n^2 + 6n + 1)(4n^2 + 6n + 1) - 1 \\
&= 16n^4 + 24n^3 + 4n^2 \\
&\quad + 24n^3 + 36n^2 + 6n \\
&\quad + 4n^2 + 6n + 1 - 1 \\
&= 16n^4 + 48n^3 + 44n^2 + 12n \quad \checkmark
\end{align*}
\]

If \( a \) is odd, then \( a = 2n+1 \)

\[
\begin{align*}
\therefore a(\alpha+1)(\alpha+2)(\alpha+3) &= (2n+1)(2n+2)(2n+3)(2n+4) \\
&= (4n^2+6n+2)(4n^2+14n+12) \\
&= 16n^4 + 56n^3 + 48n^2 \\
&\quad + 24n^3 + 84n^2 + 72n \\
&\quad + 8n^2 + 28n + 24
\end{align*}
\]
\[
\frac{a(a+3) + (a+1)(a+2)}{2} - 1 = \left[ \frac{(2n+1)(2n+4) + (2n+2)(2n+3)}{2} \right] - 1
\]

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

\[
= \left( 4n^2 + 10n + 5 \right)^2 - 1
\]

\[
= (4n^2 + 10n + 5)(4n^2 + 10n + 5) - 1
\]

\[
= 16n^4 + 40n^3 + 20n^2 + 40n^3 + 100n^2 + 50n + 20n^2 + 50n + 25 - 1
\]

\[
= 16n^4 + 80n^3 + 140n^2 + 100n + 24
\]

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

\textbf{Proof:} Suppose \(a\) is even. \(\therefore a = 2n\)

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

\[
= 8n^3 + (3)4n^2 + (3)2n + 1 - 8n^3
\]

\[
= 12n^2 + 6n + 1
\]
\[= 2^3 K + 1, \text{ so } (a + 1)^3 - a^3 \text{ is odd}\]

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

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

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

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

\[= (2n + 1)(6n + 6) + 1\]

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

\[= 2(K) + 1, \text{ so } (a + 1)^3 - a^3 \text{ is odd.}\]

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

**Proof:** 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) \( a \neq 0, \quad g(a, a) = |a| \)

**Proof:**

By Th. 2.2, \( a \div a \). \( \therefore |a| \) is a common divisor.

Let \( c \) be another common divisor.

\( \therefore c \div a \), and \( \therefore |c| \leq |a| \), by Th. 2.2

\( \therefore |a| \) is gcd.

(c) \( a \neq 0, \quad g(a, 1) = 1 \)

**Proof:**

By Th. 2.2, \( 1 \div a \), \( 1 \div 1 \). \( \therefore 1 \) is a common divisor

Let \( c \) be another common divisor.

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

\( \therefore |1| \) is gcd.

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

**Proof:**

Let \( x \) be the gcd of any one pair. \( x \mid x \)

Since \( x \mid y \Rightarrow x \mid (-y) \), \( x \) is a common divisor of any other pair.

Let \( c \) be another common divisor.

Since \( c \div a \Rightarrow c \div (aq) \) and \( c \div b \Rightarrow c \div (-b) \), \( c \div x \) by Th. 2.6. \( \therefore |c| \leq |x| \)

\( \therefore x \) is the gcd of the other pair.
12. Let \( a \) be any integer, \( \gcd(a, a+n) \mid n \)

**Proof:** Let \( d = \gcd(a, a+n) \)

\[
\exists x, y \text{ s.t. } a = dx, \ a+n = dy
\]

\[
dx + n = dy \quad \Rightarrow \quad n = d(y-x) \quad \Rightarrow \quad d \mid n
\]

And by Th. 2.2, \( d \mid 1 \iff d = \pm 1. \)

\[\therefore \gcd(a, a+1) = 1.\]

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

\[\exists m, n \text{ s.t. } a = dm \quad \text{and} \quad b = dn \]

\[\therefore c = ax + by = d(mx + ny) \quad \therefore d \mid c \]

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

\[\exists x_0, y_0 \text{ s.t. } d = ax_0 + by_0 \]

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

\[\therefore c = dp = (ax_0 + by_0)p = ax_0p + by_0p \]

\[\therefore \text{Let } x = x_0p, \ y = y_0p \]

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

\[
\frac{a}{d} x + \frac{b}{d} y = 1,
\]
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.

\[
\therefore \gcd = 1 \text{ or } 2. \text{ But a odd } \Rightarrow 3a \text{ is odd.}
\]

\[
\therefore 2 \times 3a. \therefore \gcd = 1
\]

15. \( \gcd(2a-3b, 4a-5b) \mid 6 \)

Proof: 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 \( d \).
\[
-3 \text{ n s.t. } d \mid n = (2)(2a-3b) + (1)(4a-5b) = 6
\]
\[
\therefore d \mid 6
\]

Now let \( b = -1 \). \( \therefore \gcd(2a+3, 4a+5) \mid (-1) \)
\[
\therefore \gcd = 1.
\]

16. If \( a \) is odd, \( 12 \mid a^2 + (a+2)^2 + (a+4)^2 + 1 \)

**Proof:** \( \text{Let } a = 2n+1 \)
\[
\therefore (2n+1)^2 + (2n+3)^2 + (2n+5)^2 + 1
\]
\[
= 4n^2 + 4n + 1
+ 4n^2 + 12n + 9
+ 4n^2 + 20n + 25 + 1
\]
\[
= 12n^2 + 36n + 36 = 12(n^2 + 3n + 3)
\]

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

**Proof:** \( n = 1 : 3! / 3! = 1 \)

\( k \Rightarrow k+1: \text{Suppose } (3k)! / (3!)^k = k \) is an integer
\[
\therefore \left[ 3(k+1)! / (3!)^{k+1} \right]
\]
\[
= (3k+3)! / (3!) \cdot (3!)
\]
\[
\frac{(3k+3)(3k+2)(3k+1)(3k)!}{3 \cdot 2 \cdot 1 \cdot (3!)^k} = \frac{3(k+1)(3k+2)(3k+1)}{3 \cdot 2} \cdot k
\]
\[
= \frac{(k+1)(3k+2)(3k+1)}{2} \cdot k
\]

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 \( x \).

\[ \text{entire expression is an integer.} \]

19. (a) \( G \mid a(a+1)(a+2) \)

\[ \text{Proof: } 6 = 3 \cdot 2, \text{ and } \gcd(2, 3) = 1 \text{ (Problem 12).} \]
Let \( k = a(a+1)(a+2) \)

If \( a \) is even, then \( 2 \mid a \), \( \therefore 2 \mid k \)
If \( a \) is odd, then \( 2 \mid (a+1) \), \( \therefore 2 \mid k \)

Let \( a = 3q + r \)
\[
\begin{align*}
\text{if } r = 0, \text{ then } 3 \mid a_1, \therefore 3 \mid k \\
\text{if } r = 1, \text{ then } a + 2 = 3q + 3, 3 \mid a + 2, 3 \mid k \\
\text{if } r = 2, \text{ then } a + 1 = 3q + 3, 3 \mid a + 2, 3 \mid k \\
\therefore 3 \mid k \text{ and } 2 \mid k, \text{ and by Corollary 2 on } p, 24 \mid 3 \cdot 2 \mid k \\
\therefore 6 \mid a(a+1)(a+2) \\
(6) \quad 24 \mid a(a+1)(a+2)(a+3) \\
\rho \Rightarrow n = 1 : 1 \cdot 2 \cdot 3 \cdot 4 = 24 \\
\text{K \Rightarrow k} + 1 : \text{ Suppose } 24 \mid k(k+1)(k+2)(k+3)(k+4) \\
\therefore 24 \mid k(k+1)(k+2)(k+3), \text{ some } \rho \\
\therefore (k+1)(k+2)(k+3)(k+4) = k(k+1)(k+2)(k+3) + 4(k+1)(k+2)(k+3) \\
= 24 \rho + 4(k+1)(k+2)(k+3) \\
\text{But by (a), } (k+1)(k+2)(k+3) = 6q \\
\text{for some } q. \\
\therefore (k+1)(k+2)(k+3)(k+4) = 24 \rho + 24 q \\
\therefore 24 \mid (k+1)(k+2)(k+3)(k+4)
\end{align*}
\]
(c) \[ 120 | a(a+1)(a+2)(a+3)(a+4) \]

\[ \text{Proof: } n = 1 : 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120 \]

\[ K = 7 K + 1 : \text{ Suppose } 120 \mid k(k+1)(k+2)(k+3)(k+4) \]

\[ \exists \rho \text{ s.t. } 120 \rho = k(k+1)(k+2)(k+3)(k+4) \]

But

\[ k(k+1)(k+2)(k+3)(k+4)(k+5) = \]

\[ k(k+1)(k+2)(k+3)(k+4) + 5(k+1)(k+2)(k+3)(k+4) \]

\[ = 120 \rho + 5 \cdot 2^4 q, \quad \text{for some } q, \text{ by (6) above} \]

\[ = 120(\rho + q) \]

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

19. (d) \[ G \mid a(a^2 + 11) \]

\[ \text{Proof: Let } a = 6q + r, \text{ where } 0 \leq r < 6 \]

Consider each case for \( r \)

\[ r = 0: a(a^2 + 11) = 6q \sqrt{(6q)^2 + 11} \]

\[ \therefore G \mid a(a^2 + 11) \]
\[ r=1: \quad a(a^2 + 11) = (6q + 1)(6q + 1)^2 + (6q + 1)11 \\
= 6q^3 + \binom{3}{1}(6q)^2 + \binom{3}{2}6q + \binom{3}{3} + (6q)11 + 11 \\
= 6 \sum \binom{3}{d} + 11 \\
= 6 \sum \binom{3}{d} + 12 = 6 \sum \binom{3}{d}^3 \]

\[ r=2: \quad a(a^2 + 11) = (6q + 2)^3 + (6q + 2)11 \\
= 6 \sum \binom{3}{d}^2 + (6q)11 + 22 \\
= 6 \sum \binom{3}{d} + 30 = 6 \sum \binom{3}{d}^3 \]

\[ r=3: \quad a(a^2 + 11) = (6q + 3)^3 + (6q + 3)11 \\
= 6 \sum \binom{3}{d}^3 + (6q + 3)^3 + 33 \\
= 6 \sum \binom{3}{d} + 27 + 33 = 6 \sum \binom{3}{d} + 60 \\
= 6 \sum \binom{3}{d}^3 \]

\[ r=4: \quad a(a^2 + 11) = (6q + 4)^3 + (6q + 4)11 \\
= 6 \sum \binom{3}{d}^4 + 4^4 \\
= 6 \sum \binom{3}{d} + 64 + 44 = 6 \sum \binom{3}{d} + 108 \]
\[ = 6 \sum_3 + 6 \cdot 18 = 6 \sum_3 \]
\[ r = 4: \ a (a^2 + 11) = (6 \mathbf{9} + \mathbf{s} \, \mathbf{5})^3 + (6 \mathbf{9} + \mathbf{s} \, \mathbf{5}) \mathbf{1} \mathbf{1} \]
\[ = 6 \sum_3 + (3) \mathbf{5 \, \mathbf{s} \, \mathbf{5}^3 + 5 \mathbf{5} \mathbf{5} \mathbf{5} \]
\[ = 6 \sum_3 + 12 \mathbf{s} \, \mathbf{5} \mathbf{5} \mathbf{5} = 6 \sum_3 + 6 \cdot 3 \mathbf{0} \]
\[ = 6 \sum_3 \]

(6) \ a \text{ is odd, then } 24 | a (a^2 - 1)

**Proof:** First, show \( a^2 \) is of form \( 8K + 1 \)

Let \( a = 4q + r, \) \( \therefore r = 1 \text{ or } 3 \) since \( a \) is odd.

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

or \( a^2 = 16q^2 + 24q + 9 = 8K' + 1 \)

So, \( a (a^2 - 1) = 8K, \) for some \( K. \)

\[ \therefore 8 | a (a^2 - 1) \]

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

\[ 3 | (a-1)(a)(a+1) \equiv 3 | a (a^2 - 1) \]
since \( \gcd(3, 8) = 1 \) \( \Rightarrow \) \( 24 \mid a^2 - 1 \)

by Corollary 2 on p. 24

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

\[ \text{Proof: By (b) above, } a^2 \text{ is of form } 8k+1 \]
and \( b \) 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) \( 2 \times a, 3 \times a \Rightarrow 24 \mid (a^2 + 23) \)

\[ \text{Proof: Let } a = 12q + r, 0 \leq 0 < 12 \]
\[ r \text{ can only be } 1, 3, 5, 7, 9, 11 \text{ since } 2 \mid 4, \]
and since \( 3 \mid 9, \) \( r \neq 3 \text{ or } 9 \).

\[ \therefore r \text{ can only be } 1, 5, 7, \text{ or } 11. \]

\[ \therefore a^2 + 23 = (12q + r)^2 + 23 \]
\[ = 144q^2 + 24qr + r^2 + 23 \]
\[ = 24(6)q^2 + 24(qr + r^2 + 23) \]
\[ = 24 \left( \sum \right) + r^2 + 23 \]

\[ r = 1 : \quad r^2 + 23 = 24 \]

\[ r = 5 : \quad r^2 + 23 = 48 = 24(2) \]

\[ r = 7 : \quad r^2 + 23 = 72 = 24(3) \]

\[ r = 11 : \quad r^2 + 23 = 144 = 24(6) \]

\[ \therefore a^2 + 23 = 24 \left( \sum \right) + r^2 + 23 = 24 \left( \sum \right) + 24k, \text{ some } k \]

\[ \therefore 24 \left| (a^2 + 23) \right. \]

(c) \[ 360 \left| a^2(a^2-1)(a^2-4) \right. \]

\[ \therefore \quad a^2(a^2-1)(a^2-4) = a^2 (a+1)(a-1) (a+2)(a-2) \]

\[ = (a-2)(a-1)(4)(a+1)(a+2)(a) \]

\[ 360 = 5 \cdot 9 \cdot 8, \text{ and } 5, 9, 8 \text{ are } \text{ relatively prime.} \]

\[ \text{By } \#18, \quad (a-2)(a-1)(4)(a+1)(a+2) \text{ is} \]
divisible by \(24\) and \(120\). \(\therefore\) it is divisible by \(8\) and \(5\).

Also, \((a-2)(a-1)(a)\) and \(a(4a+1)(4a+2)\) are both divisible by \(6\) and so are both divisible by \(3\), and \(\therefore\) the entire product is divisible by \(9\).

\[-\] Entire product divisible by \(360\) by Corollary 2, p. 24

20. \(\text{gcd}(a, b) = 1, \text{gcd}(a, c) = 1\). Then \(\text{gcd}(a, bc) = 1\)

\(\text{Pf.}\): \(l = ax + by = au + cv\) for some \(x, y, u, v\)

\[
\therefore 1 = (ax + by)(au + cv) = a^2xy + abyu + a^2xu + bcxy
\]

\[
= a(xy + byu + axu) + bcxy
\]

\[
= aK_1 + 6cK_2
\]

\(\therefore\) \(a, bc\) relatively prime.

(b) \(\text{gcd}(a, b) = 1, c | a\). Then \(\text{gcd}(b, c) = 1\)

\(\text{Pf.}\): \(\exists x, y \text{ s.t. } ax + by = 1\), and \(\exists \ a \text{ n s.t. } cn = a\)

\[
\therefore c(nx + by) = 1 \Rightarrow \text{gcd}(c, b) = 1\]
(2) \( \gcd(a, b) = 1 \), then \( \gcd(ac, b) = \gcd(c, b) \)

**Proof:** 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

\[
    d(nc) = c
\]

\[
    \Rightarrow d \mid ca
\]

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

Since \( K \mid b \), then \( \exists n \) s.t. \( Kn = b \)

\[
    \Rightarrow d = cx + kny
\]

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

\[
    \Rightarrow apc + bqc = c
\]

\[
    \Rightarrow d = (apc + bqc)x + kny
\]

\[
    = apcx + knqc + kny
\]

But \( K \mid ac \Rightarrow \exists r \) s.t. \( Kr = ac \)
\[ d = krx + knqcx + kny \]
\[ = K(rx + nqcx + ny) \]
\[ \therefore K \mid d \]

\[ \because \text{By Theorem 2.6, } \gcd(c, b) = \gcd(ac, b) \]

\( \therefore \gcd(a, b) = 1, c \mid a + b \rightarrow \gcd(a, c) = \gcd(b, c) = 1 \)

\( \therefore \gcd(a, b) = 1 \Rightarrow \exists x, y \text{ s.t. } ax + by = 1 \)

\[ c \mid a + b \Rightarrow \exists n \text{ s.t. } cn = a + b \]

\[ \therefore cn - b = a \]

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

\[ cnx - bx + by = 1 \]

\[ \therefore \gcd(c, b) = 1 \]

\( \therefore \gcd(c, b) = 1 \Rightarrow \gcd(c, b) = 1 \)

\[ \therefore \gcd(a, c) = 1 \]
(c) \( \gcd(a, b) = 1, \ d \mid ac, \ d \mid bc \), Then \( d \mid c \)

**Proof:** \( \exists x, y \) s.t. \( ax + by = 1 \) \( \therefore ax + by = c \)

But \( ac = dn \) and \( bc = dm \) for some \( n, m \)

\( \therefore \) \( d(nx + my) = c \)

\( \therefore d \mid c \)

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

**Proof:** From (c) above, let \( c = a \)

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

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

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

Now apply (c) again to get

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

\( \therefore \gcd(a^2, b^2) = 1 \)
21. (a) \( \frac{d}{n} \Rightarrow \frac{2^d - 1}{2^n - 1} \)

**Proof:** From Problems 1,1, #3,

\[ a^{n-1} = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1) \]

\[ \Rightarrow 2^n - 1 = 2^{n-1} + 2^{n-2} + \ldots + 2 + 1 \text{ (n terms)} \]

\[ 2^d - 1 = 2^{d-1} + 2^{d-2} + \ldots + 2 + 1 \text{ (d terms)} \]

Since \( \frac{d}{n} \Rightarrow \exists x \text{ s.t. } dx = n \)

\[ \Rightarrow 2^n - 1 = 2^{dx} - 1 = (2^d)^x - 1 \]

\[ = (2^d - 1)(2^d(x-1) + 2^d(x-2) + \ldots + 2 + 1) \]

\[ \Rightarrow 2^d - 1 \bigg| 2^n - 1 \]

Could also look at this explicitly

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

\[ = \left( \frac{d \text{ terms}}{d \text{ terms}} \right) + \left( \frac{d \text{ terms}}{d \text{ terms}} \right) + \ldots + \left( \frac{d \text{ terms}}{d \text{ terms}} \right) \]
\[ d^3(x-1) + d^2(x-2) + \ldots + d + 1 \]

(6) \(31 = 2^5 - 1\). Since \(5 \mid 35\), \(2^5 - 1 \mid 2^{35} - 1\)

\(127 = 2^7 - 1\), and \(7 \mid 35\). \(\therefore 2^7 - 1 \mid 2^{35} - 1\)

22. What values of \(n\) does \(t_n \mid t_1 + t_2 + \ldots + t_n\)

From Problems 1.3, \#3,

\[ t_1 + t_2 + \ldots + t_n = \frac{n(n+1)(n+2)}{6} \]

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

\[ \therefore \frac{n(n+1)(n+2)}{6} = \frac{n+2}{3} = \frac{n^2}{2} \]

\[ \because t_n \text{ divides } t_1 + \ldots + t_n \text{ when } \frac{n+2}{3} \text{ is an integer, or } n = (1, 4, 7, 10, \ldots) \]

23. If \(a \mid bc\), show \(a \mid \gcd(a, c) \cdot \gcd(a, c)\)
Proof: Let \( d_1 = \gcd(a, b) \), \( d_2 = \gcd(a, c) \)

\[
\begin{align*}
&= 3x, y, u, v \text{ s.t. } d_1 = ax + by \\
&\quad \quad d_2 = au + cv \\
&\text{and } \exists \eta \text{ s.t. } \eta n = 6c \\
\Rightarrow &\quad d_1 d_2 = (ax + by)(au + cv) \\
\quad &\quad = a^2 xu + acxv + abuy + bcyv \\
\quad &\quad = a(axu + cxy + byv) + anyv \\
\quad &\quad = a(axu + cxy + byv + nyv) \\
\therefore &\quad a \mid d_1 d_2
\end{align*}
\]