The Greatest Common Divisor (gcd)

IF a AND b ARE ARBITRARY INTEGERS, THEN AN INTEGER d IS SAID TO BE A COMMON DIVISOR OF a AND b IF BOTH $d|a$ AND $d|b$. NOTE THAT 1 IS A DIVISOR OF EVERY INTEGER. SO, THE SET OF THEIR POSITIVE COMMON DIVISORS IS NONEMPTY. WE NOW OBSERVE IF $a=b=0$ THE SET OF POSITIVE COMMON DIVISORS OF a AND b IS INFINITE AS EVERY INTEGER SERVES AS A COMMON DIVISOR OF a AND b. HOWEVER, WHEN AT LEAST ONE OF a AND b IS DIFFERENT FROM 0, THERE ARE ONLY A FINITE NUMBER OF POSITIVE COMMON DIVISORS. AMONG THESE NUMBERS, THERE IS A LARGEST ONE, CALLED THE GREATEST COMMON DIVISOR (gcd) OF a AND b.

DEFINITION: LET $a, b \in \mathbb{Z}$, NOT BOTH ZERO. THE GREATEST COMMON DIVISOR OF a AND b, DENOTED BY $\gcd(a,b)$ OR (a,b), IS THE POSITIVE INTEGER d SATISFYING THE FOLLOWING

(i) $d|a$ AND $d|b$

(ii) IF $c|a$ AND $c|b$ THEN $c \leq d$.

EXAMPLE: THE POSITIVE DIVISORS OF 12 ARE $1,2,3,4,6,12$ WHILE THOSE OF -18 ARE $1,2,3,6,9,18$. HENCE, THE POSITIVE COMMON DIVISORS OF 12 AND -18 ARE $1,2,3,6$. SINCE 6 IS THE LARGEST OF THESE INTEGERS WE CONCLUDE THAT $\gcd(12,-18)=6$. OBSERVE ALSO $\gcd(-18,12)=6$. IN ADDITION, $\gcd(12,18)=\gcd(-12,18)=\gcd(12,-18)=\gcd(-12,-18)=6$.

EXERCISE 1: LET $a, b \in \mathbb{Z}$, NOT BOTH ZERO AND LET $d \in \mathbb{N}$. PROVE THE FOLLOWING (i)–(iii) ARE EQUIVALENT:

(i) $d|a$, $d|b$ AND IF $c|a$ AND $c|b$ THEN $c \leq d$.

(ii) $d|a$, $d|b$ AND THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT $as + bt = d$.

(iii) $d|a$, $d|b$ AND IF $c|a$ AND $c|b$ THEN $c|d$.

WHEN (i)–(iii) HOLD, WE SAY $d = \gcd(a,b)$.

SOLUTION: WE FIRST OBSERVE IT IS ENOUGH TO SHOW THAT (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii) AND (iii) $\Rightarrow$ (i) SINCE, FOR INSTANCE, TO SHOW (ii) $\Rightarrow$ (i) WE USE (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii) LET $S = \{ au + bv : au + bv > 0,\ u, v \in \mathbb{Z} \}$. WITHOUT LOSS OF GENERALITY, WE CAN ASSUME THAT $a \neq 0$. THEN, WE OBSERVE THAT $|a| \in S$ SINCE $|a| = a \cdot u + b \cdot 0$ WHERE $u = 1$ IF $a > 0$ AND $u = -1$ IF $a < 0$. THEN, S IS NONEMPTY AND BY THE WELL-ORDERING PRINCIPLE, S HAS A SMALLEST ELEMENT d. THEN, $d \in S$ AND BY THE DEFINITION OF S, THERE EXIST INTEGERS $s, t \in \mathbb{Z}$ SUCH THAT $d = a \cdot s + b \cdot t$. WE CLAIM THAT $d = \gcd(a,b)$. TO PROVE THIS CLAIM, WE OBSERVE BY THE DIVISION ALGORITHM THEOREM, THERE EXIST $q, r \in \mathbb{Z}$ SUCH THAT $a = q \cdot d + r$ WITH $0 \leq r < d$. THEN,

$$r = a - q \cdot d = a - q(as + bt) = a \cdot (1 - q s) + b \cdot (-qt).$$

IF $r > 0$ THEN $r = a \cdot u + b \cdot v$ WITH $u := 1 - qs$, $v := -qt$. THIS SHOWS THAT $r \in S$ AND SO $d \leq r$ SINCE d IS THE

SMALLEST ELEMENT OF S, CONTRADICTING THAT $r < d$. WE THUS HAVE THAT $r = 0$. SO, $a = q \cdot d$, $q \in \mathbb{Z}$ AND $d \mid a$. SIMILARLY, BY THE DIVISION ALGORITHM THEOREM, THERE EXIST $q', r' \in \mathbb{Z}$ SUCH THAT $b = q' \cdot d + r'$ WITH $0 \leq r' < d$. THEN,

$$r' = b - q'd = b - q'(as+bt) = a \cdot (-q's) + b \cdot (1 - q't)$$

IF $r' > 0$ THEN $r' \in S$ CONTRADICTING THE CHOICE OF d. THEN $r' = 0$ WHICH IMPLIES THAT $d \mid b$. HENCE, d IS A COMMON DIVISOR OF a AND b. LET c BE A POSITIVE COMMON DIVISOR OF a AND b. THEN $c \mid a$ AND $c \mid b$ WHICH IMPLIES THAT $c \mid a.s$, $c \mid b.t$ AND SO $c \mid as+bt = d$. THEN, $c \mid d$ AND SINCE $c, d > 0$, $c \leq d$. THIS SHOWS THAT $d = \gcd(a,b)$.

(ii) $\Rightarrow$ (iii) BY ASSUMPTION WE KNOW $d \mid a$ AND $d \mid b$. LET $c \in \mathbb{Z}$ SUCH THAT $c \mid a$ AND $c \mid b$. RECALL THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT $as + bt = d$ BY HYPOTHESIS. THIS SHOWS THAT $c \mid as$, $c \mid bt$ AND SO $c \mid as + bt = d$.

(iii) $\Rightarrow$ (i) BY ASSUMPTION WE KNOW $d \mid a$ AND $d \mid b$. SUPPOSE NOW THAT $c \mid a$ AND $c \mid b$. THEN, BY HYPOTHESIS, $c \mid d$. THIS IMPLIES THAT $|c| \leq |d| = d$. IF $c > 0$ THEN $c \leq d$ AND WE ARE DONE. OTHERWISE, IF $c < 0$, $c < -c = |c| \leq d$ AND THE RESULT FOLLOWS.

REMARK: LET $a,b\in\mathbb{N}$. THEN $a=b$ IFF $a|b$ AND $b|a$.

TO PROVE THIS, WE FIRST OBSERVE, IF $a=b$ WE CLEARLY HAVE $a|b$ AND $b|a$ SINCE $a|a$ FOR EVERY $a\in\mathbb{Z}$.

CONVERSELY, IF $a|b$ AND $b|a$ THEN $|a|\leq|b|$ AND $|b|\leq|a|$. THIS SHOWS $|a|=|b|$. SINCE $a,b>0$ WE THEREFORE HAVE THE INTEGERS $a=b$.

THIS REMARK IS VERY USEFUL TO PROVE TWO GIVEN NATURAL NUMBERS ARE EQUAL!

EXERCISE 2: LET $a,b\in\mathbb{Z}$ NOT BOTH ZERO. PROVE THE FOLLOWING HOLD:

(i) $(a,b)=(b,a)$.

(ii) $(a,b)=(-a,b)=(a,-b)=(-a,-b)=(|a|,|b|)$.

(iii) $(a,1)=1$.

(iv) $(a,0)=|a|$ IF $a\neq 0$.

(v) IF $b\neq 0$ AND $b|a$ THEN $(a,b)=|b|$.

SOLUTION:

(i) LET $d=(a,b)$ AND $d^*=(b,a)$. NOTE THAT $d|a$ AND $d|b$. THEN $d|b$ AND $d|a$ AND SO $d|d^*$. SIMILARLY, SINCE $d^*|b$ AND $d^*|a$ WE HAVE $d^*|a$ AND $d^*|b$ WHICH IMPLIES $d^*|d$. AS $d^*|d$ AND $d|d^*$, BY THE REMARK, WE HAVE $d=d^*$.

(ii) WE WILL PROVE THAT $(a,b)=(-a,b)$. THE REST OF THE

EXERCISE IS SIMILAR AND THEREFORE LEFT TO THE READER. LET $d=(a,b)$ AND $d^*=(-a,b)$. NOTE THAT $d|a$ AND $d|b$. THEN, WE HAVE $d|(-1)\cdot a=-a$ AND $d|b$. THIS IMPLIES THAT $d|d^*$. SIMILARLY, SINCE $d^*|-a$ AND $d^*|b$ WE HAVE $d^*|(-1)(-a)=a$ AND $d^*|b$. THUS, $d^*|d$. SINCE $d^*,d>0$ AND $d^*|d$, $d|d^*$ WE HAVE $d=d^*$.

(iii) WE OBSERVE THAT $1|a$ AND $1|1$. THEN, 1 IS A COMMON DIVISOR OF a AND 1. SUPPOSE THAT $c|a$ AND $c|1$. THEN $|c|\leq 1$. WE THEREFORE HAVE $(a,1)=1$.

(iv) LET $a\in\mathbb{Z}$, $a\neq 0$. NOTE THAT $a|a$ AND SO, $|a|\,|\,a$. IN ADDITION, $|a|\,|\,0$. SO, $|a|$ IS A COMMON DIVISOR OF a AND 0. SUPPOSE NOW THAT $c|a$ AND $c|0$. THEN $|c|\leq |a|$ AND SO, $c\leq |a|$. THEREFORE, $(a,0)=|a|$.

(v) LET $b\in\mathbb{Z}$, $b\neq 0$. SINCE $b|b$ AND $b|a$ WE OBSERVE $|b|\,|\,b$ AND $|b|\,|\,a$. THEN $|b|$ IS A COMMON DIVISOR OF a AND b. SUPPOSE NOW THAT $c|a$ AND $c|b$. THEN $|c|\leq |b|$ AND SO, $c\leq |c|\leq |b|$. THIS SHOWS THAT $(a,b)=|b|$.

EXERCISE 3: LET $a,b\in\mathbb{Z}$ ODD INTEGERS. PROVE THAT
$$(a^4+b^4-2,16)=16.$$

SOLUTION: BY EX. 2(V) IT SUFFICES TO PROVE $16\,|\,a^4+b^4-2$.
FROM THE BINOMIAL THEOREM WE OBSERVE
$$(2x+y)^4=\sum_{k=0}^{4}\binom{4}{k}(2x)^k y^{4-k}$$

$$= \binom{4}{0} y^4 + \binom{4}{1} \cdot 2xy^3 + \binom{4}{2} \cdot 4x^2y^2 + \binom{4}{3} \cdot 8x^3y + \binom{4}{4} \cdot 16x^4$$

$$= y^4 + 8xy^3 + 24x^2y^2 + 32x^3y + 16x^4.$$

WE NOW OBSERVE THERE EXIST $q, s \in \mathbb{Z}$ SUCH THAT $a = 2q+1$ AND $b = 2s+1$ BY THE ALGORITHM DIVISION THEOREM. WE THEREFORE HAVE

$$a^4 = (2q+1)^4 = 16q^4 + 32q^3 + 24q^2 + 8q + 1,$$
$$b^4 = (2s+1)^4 = 16s^4 + 32s^3 + 24s^2 + 8s + 1.$$

THEN,

$$a^4 + b^4 - 2 = 16q^4 + 32q^3 + 24q^2 + 8q + 16s^4 + 32s^3 + 24s^2 + 8s,$$
$$a^4 + b^4 - 2 = 16(q^4 + 2q^3 + s^4 + 2s^3) + (24q^2 + 8q) + (24s^2 + 8s).$$

WE NEXT CLAIM THAT $16 \mid 24m^2 + 8m$ FOR EVERY $m \in \mathbb{Z}$.

SUPPOSE FIRST THAT m IS EVEN. THEN $m = 2k$, $k \in \mathbb{Z}$. SO, $24m^2 + 8m = 8m(3m+1) = 8 \cdot 2k \cdot (3 \cdot 2k + 1) = 16k(6k+1)$. AS $k(6k+1) \in \mathbb{Z}$, THIS SHOWS $16 \mid 24m^2 + 8m$. ASSUME NEXT THAT m IS ODD. THEN $m = 2k+1$, $k \in \mathbb{Z}$. THEREFORE,

$$24m^2 + 8m = 8m(3m+1) = 8(2k+1)(3(2k+1)+1)$$
$$= 8(2k+1)(6k+4) = 8 \cdot 2(2k+1)(3k+2)$$
$$= 16(2k+1)(3k+2) \quad \text{WITH } (2k+1)(3k+2) \in \mathbb{Z}.$$

SO, $16 \mid 24m^2 + 8m$. THIS PROVES OUR CLAIM.

HENCE, USING THAT CLAIM, WE CAN CONCLUDE THERE EXIST $q', s' \in \mathbb{Z}$ SUCH THAT

$$24q^2 + 8q = 16q', \quad 24s^2 + 8s = 16s'.$$

THUS,

$$a^4 + b^4 - 2 = 16(q^4 + 2q^3 + s^4 + 2s^3) + 16q' + 16s' = 16w$$

FOR SOME $w \in \mathbb{Z}$. THIS PROVES $16 \mid a^4+b^4-2$.
HENCE, $(a^4+b^4-2, 16) = |16| = 16$.

EXERCISE 4: PROVE THAT, FOR A POSITIVE INTEGER m AND ANY INTEGER a, THE NUMBER $\gcd(a, a+m)$ DIVIDES m. IN PARTICULAR, $\gcd(a, a+1) = 1$.

SOLUTION: LET $d = (a, a+m)$. THEN, $d \mid a$ AND $d \mid a+m$. SO, $d \mid (a+m) - a$ WHICH IMPLIES $d \mid m$. IN PARTICULAR, IF $m=1$, WE HAVE $d \mid 1$ AND SO $d \in \{-1, 1\}$. SINCE $d > 0$, WE HAVE $d = 1$.

EXERCISE 5: LET $a, b \in \mathbb{Z}$. PROVE THE FOLLOWING HOLD:

(i) THERE EXIST INTEGERS x AND y FOR WHICH $c = ax+by$ IFF $\gcd(a,b) \mid c$.

(ii) IF THERE EXIST INTEGERS x AND y FOR WHICH $ax+by = \gcd(a,b)$ THEN $\gcd(x,y) = 1$.

SOLUTION: LET $d = (a,b)$.

(i) SUPPOSE THERE EXIST INTEGERS x AND y SUCH THAT $c = ax+by$. SINCE $d \mid a$ AND $d \mid b$ WE HAVE $d \mid ax$, $d \mid by$. THEREFORE, $d \mid ax+by$ WHICH MEANS $d \mid c$. CONVERSELY, BY EX. (1), WE KNOW THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT $as+bt = d$. AS $d \mid c$ THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $c = dk$. THEREFORE,

$$c = d.k = (as+bt)k = a(sk) + b(tk).$$

TAKING $x := sk \in \mathbb{Z}$, $y := tk \in \mathbb{Z}$ WE HAVE $c = ax+by$. THE RESULT FOLLOWS.

(ii) OBSERVE THE NUMBERS $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ SINCE $d \mid a, d \mid b$.

THEN, THERE EXIST $x, y \in \mathbb{Z}$ SUCH THAT $\frac{a}{d}x + \frac{b}{d}y = 1$.
LET $d^* = (x, y)$. NOTE $d^* > 0$, $d^* | x$ AND $d^* | y$. THUS, $d^* \mid \frac{a}{d}x$, $d^* \mid \frac{b}{d}y$ AND SO $d^* \mid \frac{a}{d}x + \frac{b}{d}y = 1$. THEREFORE, $d^* \in \{-1, 1\}$. SINCE $d^* > 0$, WE HAVE $d^* = 1$.

DEFINITION: TWO INTEGERS a AND b, NOT BOTH OF WHICH ARE ZERO, ARE SAID TO BE RELATIVELY PRIME OR COPRIME IF $\gcd(a,b) = 1$.

SOME IMPORTANT RESULTS

LET $a, b \in \mathbb{Z}$, NOT BOTH ZERO. THE FOLLOWING HOLD:

R(i) $\gcd(a,b) = 1$ IFF $ax + by = 1$ FOR SOME $x, y \in \mathbb{Z}$.

R(ii) IF $\gcd(a,b) = d$ THEN $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

R(iii) LET $c \in \mathbb{Z}$. IF $a | c$ AND $b | c$, WITH $\gcd(a,b) = 1$ THEN $ab | c$.

R(iv) LET $c \in \mathbb{Z}$. IF $a | bc$ WITH $\gcd(a,b) = 1$ THEN $a | c$.

EXERCISE 6: LET $a \in \mathbb{Z}$. SHOW THE FOLLOWING:

(i) $\gcd(2a+1, 9a+4) = 1$.

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

(iii) IF a IS ODD THEN $\gcd(3a, 3a+2) = 1$.

SOLUTION: LET $a \in \mathbb{Z}$.

(i) BY R(i) ABOVE, IT SUFFIES TO PROVE THERE EXIST $m, n \in \mathbb{Z}$ SUCH THAT $(2a+1)m + (9a+4)n = 1$.

WE OBSERVE $(2a+1)m + (9a+4)n = a \cdot (2m+9n) + (m+4n) = 1$.

THEREFORE, WE MAY TAKE $m, n \in \mathbb{Z}$ SUCH THAT

$$\begin{cases} 2m + 9n = 0 \\ m + 4n = 1 \end{cases} \iff \begin{cases} 2m + 9n = 0 \\ 2m + 8n = 2 \end{cases} \iff \begin{cases} n = -2 \\ m = 9 \end{cases}.$$

SO, WE HAVE $(2a+1)\cdot 9 + (9a+4)\cdot(-2) = 9-8 = 1$.

THUS, BY R(i), $\gcd(2a+1, 9a+4) = 1$ FOR ALL $a \in \mathbb{Z}$.

(ii) LET $d = (5a+2, 7a+3)$. THEN, WE OBSERVE

$$\begin{cases} d \mid 5a+2 \\ d \mid 7a+3 \end{cases} \Rightarrow \begin{cases} d \mid (5a+2)\cdot 7 \\ d \mid (7a+3)\cdot 5 \end{cases} \Rightarrow \begin{cases} d \mid 35a+14 \\ d \mid 35a+15 \end{cases}$$

WE THUS HAVE $d \mid (35a+15)-(35a+14)$, THAT IS $d \mid 1$.

SO, $d \in \{-1, 1\}$. SINCE $d > 0$ WE HAVE $d = 1$.

(iii) SUPPOSE THAT $a \in \mathbb{Z}$ IS ODD. LET $d = (3a, 3a+2)$. THEN $d \mid 3a$ AND $d \mid 3a+2$. THIS IMPLIES THAT $d \mid (3a+2) - 3a$, THAT IS $d \mid 2$. SINCE $d > 0$ WE HAVE $d \in \{1, 2\}$. SUPPOSE THAT $d = 2$. THEN $2 \mid 3a$. BY R(iv) ABOVE, SINCE $\gcd(2,3) = 1$, WE HAVE $2 \mid a$. THIS SHOWS THAT a IS EVEN CONTRADICTING THAT a IS odd. THEREFORE $d \neq 2$ AND SO $d = 1$.

EXERCISE 7: PROVE THE FOLLOWING HOLD:

(i) THE PRODUCT OF ANY THREE CONSECUTIVE INTEGERS IS DIVISIBLE BY 6.

(ii) THE PRODUCT OF ANY FOUR CONSECUTIVE INTEGERS IS DIVISIBLE BY 24.

(iii) THE PRODUCT OF ANY FIVE CONSECUTIVE INTEGERS IS DIVISIBLE BY 120.

SOLUTION:

(i) LET $a \in \mathbb{Z}$. WE NEED TO PROVE THAT $6 \mid a(a+1)(a+2)$.

WE FIRST ASSUME THAT $a \in \mathbb{N}$. WE WILL PROVE THAT $6 \mid a(a+1)(a+2)$ FOR ALL $a \in \mathbb{N}$. LET $S = \{a \in \mathbb{N} : 6 \mid a(a+1)(a+2)\}$. NOTE THAT $1\cdot(1+1)\cdot(1+2) = 1\cdot 2\cdot 3 = 1\cdot 6$. THIS SHOWS THAT $1 \in S$. GIVEN $h \in \mathbb{N}$,

$n > 1$, ASSUME THAT $n \in S$. THEN $n(n+1)(n+2) = 6q$ FOR SOME $q \in \mathbb{N}$. WE NEED TO SHOW THAT $n+1 \in S$. NOTE THAT

$$(n+1)(n+2)(n+3) = n(n+1)(n+2) + 3(n+1)(n+2)$$
$$= 6q + 3(n+1)(n+2)$$

NOW, OBSERVE $(n+1)(n+2)$ IS EVEN SINCE $n+1$ AND $n+2$ ARE TWO CONSECUTIVE INTEGERS AND SO, ONE OF THEM IS EVEN. SO, $(n+1)(n+2) = 2q'$ FOR SOME $q' \in \mathbb{N}$. THEREFORE,

$$(n+1)(n+2)(n+3) = 6q + 3.2q' = 6(q+q') \quad \text{WITH } q+q' \in \mathbb{Z}.$$

THEN $6 \mid (n+1)(n+2)(n+3)$ AND SO, $n+1 \in S$. BY THE PRINCIPLE OF MATHEMATICAL INDUCTION, $S = \mathbb{N}$. THIS MEANS THAT $a(a+1)(a+2)$ IS DIVISIBLE BY 6 FOR EVERY $a \in \mathbb{N}$.

NOW, OBSERVE $a.(a+1).(a+2) = 0$ WHENEVER $a \in \{-2,-1,0\}$ AND SO $6 \mid a(a+1)(a+2)$ FOR EVERY INTEGER $a \geq -2$.

ASSUME NOW THAT $a < -2$. THEN $a.(a+1)(a+2) < 0$. NOTE

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

SINCE $-a-2 > 0$, BY THE ABOVE COMMENTS, THE PRODUCT

$$(-a-2).(-a-2+1).(-a-2+2) = (-a-2)(-a-1)(-a) = 6.t \quad , t \in \mathbb{N}.$$

THEREFORE, $a(a+1)(a+2) = (-1).6t = 6.(-t)$, $-t \in \mathbb{Z}$.

THIS SHOWS THAT $a(a+1)(a+2)$ IS DIVISIBLE BY 6 FOR EVERY $a \in \mathbb{Z}$.

(ii) LET $a \in \mathbb{Z}$. WE WILL SHOW THAT $24 \mid a(a+1)(a+2)(a+3)$ FOR EVERY $a \in \mathbb{Z}$. WE FIRST CLAIM THAT $24 \mid a(a+1)(a+2)(a+3)$ FOR

EVERY $a \in \mathbb{N}$. TO PROVE THIS WE PROCEED BY INDUCTION.

IF $a=1$ THEN $1.(1+1).(1+2).(1+3) = 4! = 24$ AND $24/24$.

GIVEN $h \in \mathbb{N}, h>1$, ASSUME $h(h+1)(h+2)(h+3) = 24q$, $q \in \mathbb{N}$.

WE WILL PROVE THAT $24 \mid (h+1)(h+2)(h+3)(h+4)$. NOTE THAT

$$\begin{aligned}(h+1)(h+2)(h+3)(h+4) &= h(h+1)(h+2)(h+3) + 4(h+1)(h+2)(h+3) \\ &= 24q + 4(h+1)(h+2)(h+3)\end{aligned}$$

NOTE THAT $h+1, h+2, h+3$ ARE 3 CONSECUTIVE INTEGERS. SO, BY (i), THERE EXISTS $q' \in \mathbb{N}$ SUCH THAT $(h+1)(h+2)(h+3) = 6q'$.

THEREFORE, $24 \mid (h+1)(h+2)(h+3)(h+4)$ SINCE

$$(h+1)(h+2)(h+3)(h+4) = 24q + 4.6q' = 24(q+q') \text{ WITH } q+q' \in \mathbb{Z}.$$

THIS PROVES OUR CLAIM.

WE NEXT OBSERVE $24 \mid a(a+1)(a+2)(a+3)$ FOR EVERY INTEGER $a \in \{0, -1, -2, -3\}$ SINCE $a(a+1)(a+2)(a+3) = 0 = 24.0$.

ASSUME NOW THAT $a < -3$. THEN, $-a-3 > 0$ AND SO THE PRODUCT $(-a-3)(-a-3+1)(-a-3+2)(-a-3+3) = (-a)(-a-1)(-a-2)(-a-3)$ IS DIVISIBLE BY 6. THEN, $6 \mid (-a)(-a-1)(-a-2)(-a-3)$. SO,

$6 \mid (-1).(-a).(-1).(-a-1).(-1).(-a-2).(-1).(-a-3)$. THAT IS,

$6 \mid a.(a+1)(a+2)(a+3)$. THIS SHOWS THE PRODUCT $a(a+1)(a+2)(a+3)$ IS DIVISIBLE BY 24 FOR EVERY $a \in \mathbb{Z}$.

THE RESULT FOLLOWS.

(iii) SIMILAR TO (i)-(ii) ABOVE AND THEREFORE IT IS LEFT AS AN EXERCISE.

EXERCISE 8: Let $a \in \mathbb{Z}$ be an odd integer. Show that the product $a(a^2-1)$ is divisible by 24.

SOLUTION: Let $a \in \mathbb{Z}$ be an odd integer. Then, by the division algorithm theorem, $a = 4q+r$ for some $q, r \in \mathbb{Z}$ with $r \in \{0,1,2,3\}$. Since a is odd, $r \notin \{0,2\}$ and so, $r \in \{1,3\}$. Then $a^2 = (4q+r)^2 = 16q^2 + 8qr + r^2$. If $r=1$, we get $a^2 = 16q^2+8q+1 = 8(2q^2+q)+1$ while if $r=3$, we have $a^2 = 16q^2+24q+9 = 8(2q^2+3q+1)+1$. Therefore, there exists $k \in \mathbb{Z}$ such that $a^2 = 8k+1$. That is, $a^2-1 = 8k$. Then, $8 \mid a^2-1$ which implies $8 \mid a(a^2-1)$. On the other hand, observe $a(a^2-1) = a(a+1)(a-1) = (a-1)a(a+1)$ is the product of 3 consecutive integers. Then, by Ex.6(i), it is divisible by 6. Since $3 \mid 6$ and $6 \mid a(a^2-1)$ we have $3 \mid a(a^2-1)$. Note that $(3,8)=1$. So, by R(iii) above, $3 \cdot 8 \mid a(a^2-1)$. That is $24 \mid a(a^2-1)$.

EXERCISE 9: Confirm the following properties of the greatest common divisor:

(i) If $(a,b)=1$ and $(a,c)=1$ then $(a,bc)=1$.
(ii) If $(a,b)=1$ and $c \mid a$ then $(b,c)=1$.
(iii) If $(a,b)=1$ then $(ac,b) = (c,b)$.
(iv) If $(a,b)=1$ and $c \mid a+b$ then $(a,c)=(b,c)=1$.
(v) If $(a,b)=1$, $d \mid ac$ and $d \mid bc$ then $d \mid c$.
(vi) If $(a,b)=1$ then $(a^2,b^2)=1$.

SOLUTION: LET $a, b, c \in \mathbb{Z}$ DIFFERENT FROM 0.

(i) SINCE $(a,b)=1$ AND $(a,c)=1$, THERE EXIST $m, n, p, q \in \mathbb{Z}$ SUCH THAT $am+bn=1$ AND $ap+cq=1$. THEN, WE CAN WRITE

$$1 = 1.1 = (am+bn)(ap+cq) = amap + amcq + bnap + bncq$$
$$= a(map + mcq + bnp) + bc(nq).$$

HENCE, THERE EXIST $x, y \in \mathbb{Z}$, $x := map+mcq+bnp$, $y := nq$ SUCH THAT $ax+bcy=1$. THIS SHOWS $(a,bc)=1$.

(ii) SINCE $(a,b)=1$, THERE EXIST $x, y \in \mathbb{Z}$ SUCH THAT $ax+by=1$. NOTICE $a=cq$, $q \in \mathbb{Z}$ AS $c|a$. WE THUS HAVE

$$1 = ax+by = cqx+by = by + c.(qx).$$

THIS SHOWS THAT $(b,c)=1$.

(iii) LET $d=(ac,b)$ AND $d^*=(c,b)$. SINCE $d^*|c$, $d^*|b$ THEN $d^*|ac$ AND $d^*|b$. SO, d^* IS A COMMON DIVISOR OF ac AND b. THEN, $d^*|d$. OBSERVE THERE EXIST $s,t \in \mathbb{Z}$ SUCH THAT $as+bt=1$ SINCE $(a,b)=1$. IN ADDITION, AS $d|ac$ AND $d|b$ WE CAN WRITE $ac=dk$, $b=dl$ FOR SOME $k, l \in \mathbb{Z}$. NOTICE $d^*=cp+bq$ FOR SOME $p,q \in \mathbb{Z}$. THEREFORE, WE HAVE

$$d^* = d^*.1 = (cp+bq).(as+bt)$$
$$= cpas + cpbt + bq(as+bt)$$
$$= ac(ps) + b(cpt+q(as+bt))$$
$$= dk(ps) + dl(cpt+q(as+bt)) = d.u \text{ FOR SOME } u \in \mathbb{Z}.$$

THIS SHOWS THAT $d|d^*$. SINCE $d>0$, $d^*>0$ WE HAVE $d=d^*$.

(iv) LET $d=(a,c)$ AND $d^*=(b,c)$. WE KNOW THAT $(a,b)=1$ AND $c|a+b$. SINCE $d|c$ AND $c|a+b$ WE GET $d|a+b$. SINCE

$d \mid a$ WE HAVE $d \mid (a+b)-a$, THAT IS $d \mid b$. SO, d IS A COMMON DIVISOR OF a AND b THEN $d \leq (a,b)=1$ WHICH MEANS $d=1$.

SIMILARLY, AS $d^* \mid c$ AND $c \mid a+b$ WE GET $d^* \mid a+b$ AND SO $d^* \mid (a+b)-b = a$. SINCE $d^* \mid a$ AND $d^* \mid c$ WE HAVE $d^* \leq d = 1$.

THIS SHOWS $d = d^* = 1$.

(V) SUPPOSE $(a,b)=1$, $d \mid ac$, $d \mid bc$. THEN THERE EXIST INTEGERS m, n, k, ℓ SUCH THAT $am+bn=1$, $dk=ac$, $d\ell=bc$.

THEREFORE, WE CAN WRITE

$$c = c \cdot 1 = c(am+bn) = (ac)m + (bc)n = dkm + d\ell n = d(km+\ell n).$$

THIS SHOWS THAT $d \mid c$.

(VI) SUPPOSE $(a,b)=1$. BY (iii) ABOVE WE GET

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

SO, IF $(a,b)=1$ THEN $(a^2,b)=1$. NOTE THAT $(b,a)=(a,b)=1$. THEN $(b^2,a)=1$. SO, $(a^2,b)=(b^2,a)=1$. WE NEXT APPLY (iii) ABOVE AGAIN. SINCE $(a,b^2)=1$ THEN

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

EXERCISE 10: LET t_m DENOTE THE m-TH TRIANGULAR NUMBER. FOR WHAT VALUES OF m DOES t_m DIVIDE $t_1+t_2+\ldots+t_m$?

SOLUTION: RECALL THAT $t_m = \binom{m+1}{2} = \frac{m(m+1)}{2}$ AND THE SUM

$$\sum_{k=1}^{m} t_k = \frac{m(m+1)(m+2)}{6} = \frac{m(m+1)}{2} \cdot \frac{m+2}{3} = t_m \cdot \frac{m+2}{3}.$$

THIS MEANS THAT t_m DIVIDES THE SUM $t_1+t_2+\ldots+t_m$ IFF THE

NUMBER $\frac{m+2}{3} \in \mathbb{N}$. BY THE ALGORITHM DIVISION THEOREM, WE CAN WRITE $m = 3q + r$ WITH $q, r \in \mathbb{N}$, $r \in \{0, 1, 2\}$. NOTE THAT $m+2 = 3q+r+2$. SO, IF $3 \mid m+2$ THEN $3 \mid r+2$ WHICH IMPLIES $r = 1$. THEREFORE $m = 3q+1$, $q \in \mathbb{N}$.

EXERCISE 11: LET $a, b, c \in \mathbb{Z}$, DIFFERENT FROM 0. IF $a \mid bc$ SHOW THAT $a \mid (a,b)(a,c)$.

SOLUTION: LET $d = (a,b)$ AND $d^* = (a,c)$. THEN, $d = as + bt$ AND $d^* = ap + cq$ FOR SOME $s, t, p, q \in \mathbb{Z}$. MOREOVER, THERE EXISTS $\ell \in \mathbb{Z}$ SUCH THAT $bc = a\ell$ SINCE $a \mid bc$. HENCE,

$$
\begin{aligned}
dd^* &= (as+bt)(ap+cq) = (as+bt)ap + (as+bt)cq \\
&= ap \cdot (as+bt) + as \cdot cq + btcq \\
&= a\left[p(as+bt) + scq\right] + bc \cdot tq \\
&= a\left[p(as+bt) + scq\right] + a\ell \cdot tq = a \cdot w \text{ For some } w \in \mathbb{Z}.
\end{aligned}
$$

WE THEREFORE HAVE $a \mid dd^*$.

EXERCISE 12: LET $a, b \in \mathbb{Z}$ NOT BOTH ZERO. IF $(a,b) = 1$ PROVE THAT $(a^n, b^m) = 1$ FOR EVERY $n, m \in \mathbb{N}$.

SOLUTION: LET $a, b \in \mathbb{Z}$ NOT BOTH ZERO SUCH THAT $(a,b) = 1$. THEN THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT $as + bt = 1$. WE FIRST SHOW THAT $(a^n, b) = 1$ FOR EVERY $n \in \mathbb{N}$. LET S DENOTE THE SET $S := \{n \in \mathbb{N} : (a^n, b) = 1\}$. NOTE THAT $1 \in S$

SINCE $(a,b)=1$. ASSUME NEXT THAT $n\in S$ FOR SOME $n\in\mathbb{N}$, $n>1$. THEN $(a^n,b)=1$. BY EX. 9(iii) WE HAVE

$$(a^{n+1},b)=(a^n\cdot a,b)=(a,b)=1.$$

THIS SHOWS THAT $n+1\in S$ AND SO $S=\mathbb{N}$ BY THE PRINCIPLE OF MATHEMATICAL INDUCTION.

WE NOW FIX $m\in\mathbb{N}$ AND CONSIDER THE SET $T:=\{m\in\mathbb{N}:(a^m,b^m)=1\}$. IT FOLLOWS FROM THE ABOVE COMMENTS THAT $1\in T$ SINCE $(a^m,b)=1$. ASSUME NEXT THAT $n\in T$ FOR SOME $n\in\mathbb{N}$, $n>1$. THEN $(a^m,b^n)=1$. BY EX. 9(iii) WE HAVE

$$(a^m,b^{n+1})=(b^{n+1},a^m)=(b^n\cdot b,a^m)=(b,a^m)=(a^m,b)=1.$$

THIS SHOWS THAT $n+1\in T$ AND SO $T=\mathbb{N}$.

THEREFORE $(a^m,b^m)=1$ FOR EVERY $m,m\in\mathbb{Z}$.

AS AN EXERCISE, PROVE EXERCISE 12 WITHOUT INDUCTION BUT USING LINEAR COMBINATIONS AND THE BINOMIAL THEOREM.

EXERCISE 13: LET $a,b\in\mathbb{Z}$ NOT BOTH ZERO. LET $c\in\mathbb{Z}$, $c\neq 0$. PROVE THE FOLLOWING HOLD:

(i) $(ca,cb)=|c|\cdot(a,b)$

(ii) IF $(a,b)=d$ THEN $(a^m,b^m)=d^m$ FOR EVERY $m\in\mathbb{N}$.

SOLUTION:

(i) LET $a,b\in\mathbb{Z}$ NOT BOTH ZERO. LET $c\in\mathbb{Z}$, $c\neq 0$. LET $d=(ca,cb)$ AND $d^*=(a,b)$. NOTE THAT THERE EXIST $x,y\in\mathbb{Z}$ SUCH THAT $d^*=ax+by$. THIS IMPLIES THAT

$$|c|\cdot d^* = |c|(ax+by) = |c|ax + |c|by .$$

RECALL IF $w \mid z$ THEN $w \mid z.t$ FOR EVERY $t \in \mathbb{Z}$.
IN PARTICULAR, $w \mid z$ AND $w \mid -z$.
SINCE $d \mid ca$ AND $d \mid cb$ WE HAVE $d \mid |c|.a$ AND $d \mid |c|.b$.
SO, $d \mid |c|.ax$ AND $d \mid |c|by$. THIS SHOWS $d \mid |c|ax+|c|by$
WHICH MEANS $d \mid |c| d^*$.
WE NOW CLAIM THAT $|c|d^* \mid ca$. TO PROVE THIS, NOTE
$d^* \mid a$ AND SO $d^* \ell = a$, $\ell \in \mathbb{Z}$. THEN

$$|c| d^* \ell = |c| a = \begin{cases} ca & \text{IF } c>0 \\ (-c).a & \text{IF } c<0 \end{cases} .$$

SO, $|c| d^* \mid |c| a$ WHICH IMPLIES THAT $|c| d^* \mid ca$.
SINCE $d^* \mid b$ WE SIMILARLY HAVE $|c| d^* \mid |c| b$ AND SO $|c| d^* \mid cb$.
THEN, $|c| d^* \mid ca$ AND $|c| d^* \mid cb$ IMPLIES $|c| d^* \mid d$.
WE THEREFORE HAVE $d = |c| d^*$.

(ii) SUPPOSE $(a,b) = d$. THEN, $d = ax+by$ FOR $x,y \in \mathbb{Z}$.
NOTE $1 = \frac{a}{d} x + \frac{b}{d} y$ WHERE $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. THIS
SHOWS $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. SUPPOSE $\frac{a}{d} = \ell$, $\frac{b}{d} = m$.

THEN, $a = d\ell$ AND $b = dm$ WITH $(\ell, m) = 1$.
SO, FOR EVERY $n \in \mathbb{N}$,

$$(a^n, b^n) = \left((d\ell)^n, (dm)^n\right) = \left(d^n.\ell^n, d^n.m^n\right)$$
$$= \underset{\text{EX.13(i)}}{|d^n|.(\ell^n, m^n)} = \underset{\text{EX.12}}{|d|^n.1} = |d|^n = d^n .$$