2016

Ex:- If a, b, c are positive integers such that $\gcd(a, b) = 1 = \gcd(a, c)$ then prove that $\gcd(a, bc) = 1$.

Soln: Given $\gcd(a, b) = 1 = \gcd(a, c)$

Let $\gcd(a, bc) = d$, $d > 1$.

Then $d \mid a$, $d \mid bc$.

If $d \mid b$ then $\gcd(a, b) \geq d > 1$, which is a contradiction.

If $d \mid c$, then $\gcd(a, c) \geq d > 1$, which is a contradiction. So neither $d \mid b$ nor $d \mid c$.

$\Rightarrow d \nmid bc$ which is a contradiction as $d \mid bc$.

Hence $\gcd(a, bc) = d$, $d > 1$ is not possible

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

2016

Ex. Show that every square number is of the form $5k-1, 5k, 5k+1$ where k is some positive integers.

Soln: Let a be any positive integer. Then a is either of the form $5q, 5q+1, 5q+2, 5q+3$ ~~$5k, 5k+1, 5k+2,$~~ or $5q+4$ ~~$5k+3$~~ or ~~$5k+4$~~, where q is some integer.

Case 1 If $a = 5q$, then $a^2 = 25q^2 = 5.(5q^2) = 5k$ where, $k = 5q^2$

Case 2. If $a = 5q+1$, then $a^2 = (5q+1)^2$

$= 25q^2 + 10q + 1$

$= 5(5q^2 + 2q) + 1$

$= 5k + 1$, $k = 5q^2 + 2q$

Case 3.

Ex. If $a \mid (b+c)$, then either $a \mid b$ or $a \mid c$.
Justify whether it is true or false.

Soln: It is not true because for
$a = 2,\ b = 3,\ c = 5$ we have
$a = 2 \mid (b+c) = (3+5) = 8$ but neither $2 \mid 3$ nor $2 \mid 5$

~~2016~~ Ex. ~~If gcd $(x, y) \neq 1$ and $xy \neq 1, 2$, then~~
~~x and y are~~

2015 Ex. For all integers $n \geq 0$, $7^n - 1$ is divisible by 6 (State whether true or false)

Soln. Hint. $7^n - 1 = 7^n - 1^n$
$= (7-1)\ (\qquad)$

It is true.

Use
$a^n - b^n = (a-b)$
$= (a-b)(a^{n-1} + ba^{n-2} \ldots)$

2015 Ex. If a and b are positive integers such that $\gcd(a, b) = 1$, then show that $\gcd(a+b, a-b) = 1$ or 2.

Soln. Given $\gcd(a, b) = 1$.
Let $\gcd(a+b, a-b) = d$.
Then $d \mid a+b$, $d \mid a-b$

If $k > 0$, then
$\gcd(ka, kb)$
$= k \gcd(a, b)$

$\therefore d \mid (a+b)+(a-b)$ and $d \mid (a+b)-(a-b)$
$\Rightarrow d \mid 2a$ and $d \mid 2b$
$\Rightarrow d$ is a common divisor of $2a$ and $2b$
$\therefore d \leq \gcd(2a, 2b) = 2\gcd(a, b) = 2.1$
$\Rightarrow d \leq 2$
Hence $d = 1$ or 2.

#

2014 For any integer n, $4 \mid (n^2+2)$.
(State whether true or false)

2018. **Ex.** If a is a nonzero integer, then show that $\gcd(a, 0) = |a|$

Soln Let a be any non zero integer.

Case 1 If $a > 0$ then $|a| = a$.

Also $a \mid 0$, $a \mid a \Rightarrow |a| \mid 0$, $|a| \mid a$.

$\therefore \gcd(a, 0) = |a|$ as no integer greater than a can divide a.

Case 2. If $a < 0$, then $|a| = -a$, which is positive.

But $|a| = -a \mid 0$ and $|a| = -a \mid a$.

$\Rightarrow |a|$ is a common divisor of 0 and a.

Also no positive integer greater than $-a$ can divide a. So $\gcd(a, 0) = |a|$.

#

2018 **Ex.** For integers a and b if $(a, 4) = 2$, $(b, 4) = 2$, then show that $(a+b, 4) = 4$.

Soln. Given $(a, 4) = 2$, $(b, 4) = 2$.

$\therefore 2 \mid a$, and $2 \mid b$.

$\Rightarrow a = 2k_1$ and $b = 2k_2$ where k_1 and k_2 are odd integers otherwise if k_1 is an even integer then $a = 2k_1 = 2 \cdot 2k$, $k_1 = 2k$, k is an integer $\Rightarrow a = 4k$. $\Rightarrow$ ~~$(a, 4) =$~~ $4 \mid a$

$\Rightarrow 4$ is a common divisor of a and 4. $\Rightarrow$ $\gcd(a, 4) \geq 4$ which is a contradiction as $(a, 4) = 2$.

$\therefore a + b = 2k_1 + 2k_2 = 2(k_1 + k_2)$

$= 2 \times$ an even integer [$\because$ both k_1 & k_2 odd

$= 2 \times 2m$, m is an integer

$= 4m$

$\Rightarrow 4 \mid (a+b) \Rightarrow \gcd(a+b, 4) = 4$. #

show that $a \mid \gcd(a, b)\gcd(a, c)$.

2.4 THE EUCLIDEAN ALGORITHM

The greatest common divisor of two integers can, of course, be found by listing all their positive divisors and choosing the largest one common to each; but this is cumbersome for large numbers. A more efficient process, involving repeated application of the Division Algorithm, is given in the seventh Book of the *Elements*. Although there is historical evidence that this method predates Euclid, today it is referred to as the *Euclidean Algorithm*.

The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say, at the $(n+1)$th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:

$$\begin{aligned}
a &= q_1 b + r_1 & 0 &< r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

We argue that r_n, the last nonzero remainder that appears in this manner, is equal to $\gcd(a, b)$. Our proof is based on the lemma below.

Lemma. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - qb)$, or $d \mid r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c \mid (qb + r)$, whence $c \mid a$. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$.

Using the result of this lemma, we simply work down the displayed system of equations, obtaining

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

as claimed.

Theorem 2.3 asserts that $\gcd(a, b)$ can be expressed in the form $ax + by$, but the proof of the theorem gives no hint as to how to determine the integers x and y. For this, we fall back on the Euclidean Algorithm. Starting with the next-to-last equation arising from the algorithm, we write

$$r_n = r_{n-2} - q_n r_{n-1}$$

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain

$$\begin{aligned} r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3} \end{aligned}$$

This represents r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing backward through the system of equations, we successively eliminate the remainders r_{n-1}, $r_{n-2}, \ldots, r_2, r_1$ until a stage is reached where $r_n = \gcd(a, b)$ is expressed as a linear combination of a and b.

Example 2.3. Let us see how the Euclidean Algorithm works in a concrete case by calculating, say, $\gcd(12378, 3054)$. The appropriate applications of the Division Algorithm produce the equations

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$$6 = \gcd(12378, 3054)$$

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders