$54 = (-2)(-24) + 6$, with $0 \leq 6 < |-24|$.

Theorem: If $a = qb + r$, with $0 \leq r < |b|$, then

$$q = \begin{cases} \lfloor \frac{a}{b} \rfloor & \text{if } b > 0 \\ \lceil \frac{a}{b} \rceil & \text{if } b < 0 \end{cases}$$

proof: Let $b > 0$. Now, by definition

$x - 1 < \lfloor x \rfloor \leq x$ for any x.

Now, we assume that $x = \frac{a}{b}$ and $k = \lfloor x \rfloor$..

Then $\frac{a}{b} - 1 < k \leq \frac{a}{b}$

$\Rightarrow a - b < kb \leq a$

$\Rightarrow -a \leq -kb \leq -a + b$ (multiplying by -1).

$\Rightarrow 0 \leq a - kb < b$ (Adding a).

Now letting $r = a - kb$, we have $a = kb + r$ with $0 \leq r < |b|$. By uniqueness q, $q = k = \lfloor \frac{a}{b} \rfloor$.

Now, consider $b < 0$. Now by definition. $x < \lceil x \rceil \leq x + 1$ for any x. Let $x = \frac{a}{b}$

$k = \lceil x \rceil$. Then $\frac{a}{b} < k \leq \frac{a}{b} + 1$

$\Rightarrow a < kb \leq a + b$

$\Rightarrow 0 < kb - a \leq b$

$\Rightarrow 0 > a - kb \geq -b$.

so letting $r = a - kb$, we have.

$\Rightarrow a = kb + r$ with $0 \leq r \leq |b|$

Now, by uniqueness q, $q = k = \lceil x \rceil$

as asserted. proved

Q. Given three consecutive integer $a, a+1, a+2$ prove that one of them is divisible by 3.

Soln, By Division algorithm, we can write $a = bq + r$. $0 \leq r < b$.

$\Rightarrow a = 3q + r \quad 0 \leq r < 3$.

If $r = 0$, $a = 3q$

If $r = 1$, $a = 3q + 1 \Rightarrow a + 2 = 3q + 3$.

If $r = 2$ $a = 3q + 2 \Rightarrow a + 1 = 3q + 3$

GCD (Definition): Let a and b be given integers with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a,b)$ is the unique integer d satisfying the following

(a) $d \mid a$ and $d \mid b$

(b) If $c \mid a$, and $c \mid b$, then $c \leq d$.

Lemma (Bezout's lemma): If a and b are two integers, not both zero, then their gcd can be written as $ax+by$ for some integers x and y.

proof: consider the set

$$S = \{ ax+by > 0 \mid x, y \in \mathbb{Z} \}.$$

The set S is clearly nonempty. as

$$a \cdot a + b \cdot b > 0 \in S.$$

Now, by well-ordering principle S has a least element d. As $d \in S$, we can write $d = ax_0 + by_0$, for some integer x_0 and y_0. It is enough to show that d is the gcd of a and b. observe that if $c \mid a$ and $c \mid b$ c is a common

divisor of a and b, then $c \mid ax+by$ for any choice of integers x and y. Therefore $c \mid d$, and in particular $c \leq d$. Next, we will show that d divides a and b. Now by division algorithm $a = dq + r$ for some $0 \leq r < d$. Then $r = a - dq$

$$\Rightarrow r = a - (ax_0 + by_0)q$$

$$\Rightarrow r = a(1 - x_0 q) + b(-y_0 q).$$

If $r > 0$, r will be an element in S which is smaller than d. This is a contradiction to the minimality of d in S. Hence $r = 0$ and so $d \mid a$. Similarly, $d \mid b$. Thus $d = ax_0 + by_0$ is the gcd. proved

---

If a and b are integers such that $a \mid b$ what is the greatest common divisor of a and b?

Suppose a is a non-zero integer gcd $(a, 0)$?

Thm: Let a and b be integers, not both zero. Then a true integer d is the gcd of a and b if and only if

(1) $d|a$, $d|b$

(2) $c|a$, $c|b \Rightarrow c|d$.

proof: Let $d = gcd(a,b) \Rightarrow d|a$ & $d|b$.

Therefore $d = ax_0 + by_0$ for some integers x_0 and y_0. Thus, if $c|a$ and $c|b$, then $c|(ax_0 + by_0) \Rightarrow c|d$.

Conversely, if an integer d satisfies the two properties mentioned above, then, any common divisor c of a and b will divides d, and hence will be less than d. Therefore, d is the gcd of a and b.

Lemma: If $a = bq + r$, then $gcd(a,b) = gcd(b,r)$.

proof: Let $d = gcd(a,b)$, and $d_1 = gcd(b,r)$.

Then $d|a$, and $d|b \Rightarrow d|(a - qb)$

$\Rightarrow d|r$. Thus d is a common divisor of b and r. Hence $d|d_1$

Similarly, $d_1 | b$ and $d_1 | r \Rightarrow d_1 | (bq + r)$.
i.e. d_1 divides both a and b. Then $d_1 | d$
Thus $d = d_1$ as both d and d_1 are +ve by our definition of gcd. ###

Euclid's algorithm is an efficient way of computing the gcd of two integers by repeated application of the above lemma. At each step the size of the integers concerned gets reduced

Now, from division algorithm:

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b$$

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

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

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \qquad 0 \leq r_{n+1} < r_n$$

As we have a decreasing sequence of non-negative integers $b > r_1 > r_2 > \cdots > r_n > r_{n+1}$ we must have $r_{n+1} = 0$ for some n. Then by applying the previous lemma repeatedly we finally find that

$$\gcd(a,b) = \gcd(r,b) = \gcd(r_2, r_1) = \cdots$$
$$= \gcd(r_{n-1}, r_{n-2}) = r_n.$$

Thus, the last non-zero remainder r_n in the above process gives us the remainder.

Ex(1). find the gcd of 630 and 196.

(2)