Greatest common divisor

Tuesday, June 29, 2021 2:27 PM

To understand what elements of $\mathbb{Z}_n$ have multiplicative inverse, we need to recall basic properties of greatest common divisor of integers. In particular, we recall Euclid's algorithm.

The greatest common divisor of two non-zero integers a and b is, as its name suggests,

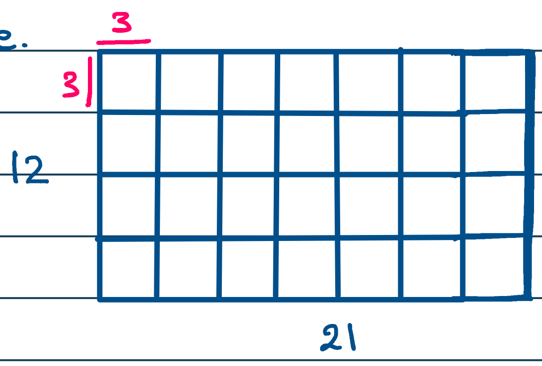
$$\max\{d \in \mathbb{Z} \mid d \mid a, \ d \mid b\},$$

and it is denoted by $\gcd(a,b)$.

Notice that if a is a non-zero integer and $d \mid a$, then $d \leq |a|$. Hence $\gcd(a,b) \leq \min\{|a|,|b|\}$ if a, b are two non-zero integers.

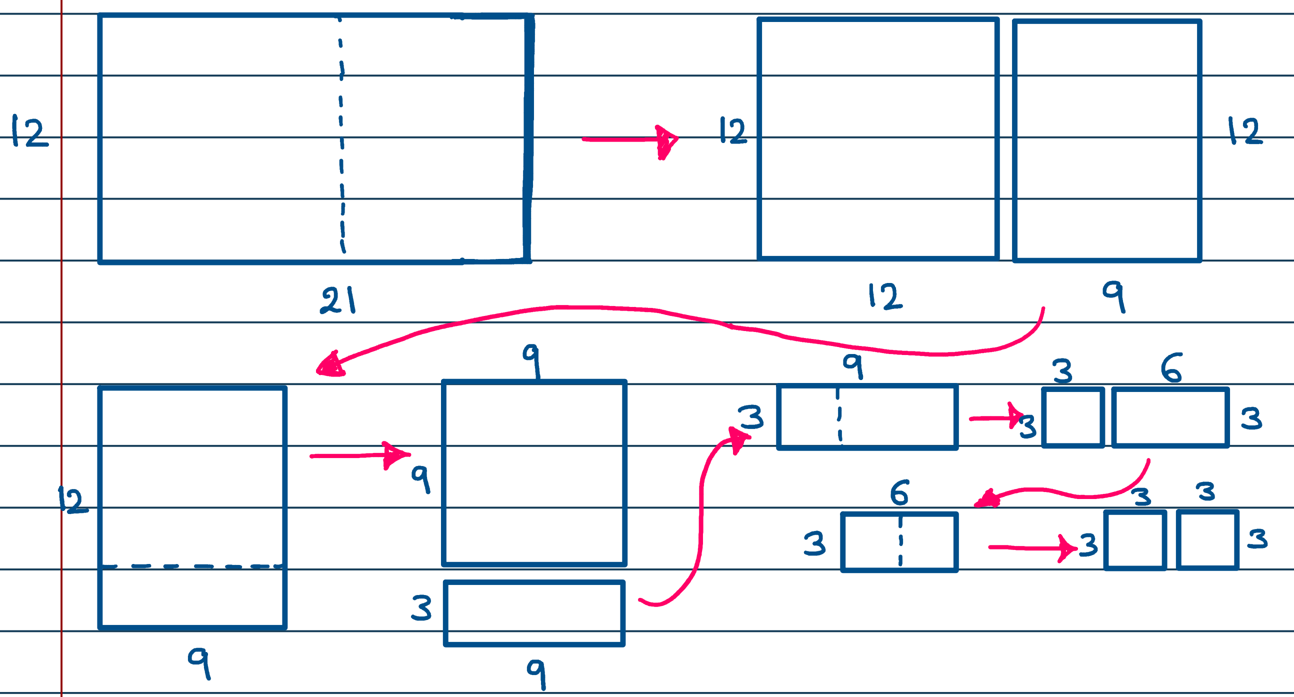
Pictorially $\gcd(a,b)$ is the size of the largest square tile which can cover an $a \times b$ rectangle.

To find this tile, each time we cut the largest possible from one of the edges. We stop when we get a square!



Basic of divisibility

Tuesday, June 29, 2021 3:29 PM



The above process is essentially Euclid's algorithm. We will make the process more formal and prove why it works.

<u>Lemma</u>. Suppose $a, b, d \in \mathbb{Z}$. Then

- $d \mid a,\ d \mid b \Rightarrow d \mid ra + sb$ for every $r, s \in \mathbb{Z}$
- $d \mid b,\ d \mid a-b \Rightarrow d \mid a$

<u>Pf.</u>
- $\left.\begin{array}{l} d \mid a \Rightarrow a = kd \text{ for some } k \in \mathbb{Z} \\ d \mid b \Rightarrow b = ld \text{ for some } l \in \mathbb{Z} \end{array}\right\} \Rightarrow$

  $ra + sb = rkd + sld = \underbrace{(rk + sl)}_{\text{in } \mathbb{Z}} d \Rightarrow d \mid ra + sb.$
- $d \mid b,\ d \mid a-b \Rightarrow d \mid (1)(b) + (1)(a-b) \Rightarrow d \mid a.$ ■

The following is a corollary of the above lemma.

Steps of Euclid's algorithm

Tuesday, June 29, 2021 3:29 PM

Corollary. Suppose a, b are two positive integers. Then

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

Pf. We show that d is a common divisor of a and b if and only if d is a common divisor of b and $a-b$.

$d \mid a,\ d \mid b \Rightarrow d \mid (1)(a) + (-1)(b) \Rightarrow d \mid a-b.$

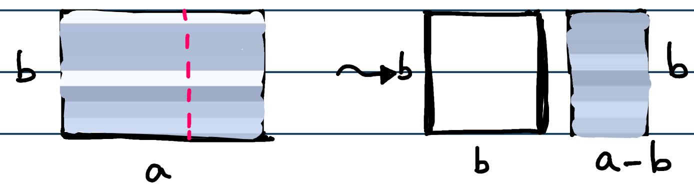
Hence $d \mid b$ and $d \mid a-b$.

If $d \mid b$ and $d \mid a-b$, then $d \mid a$ by the previous lemma.

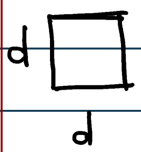
Hence $\gcd(a,b) = \max\{d \in \mathbb{Z} \mid d \mid a,\ d \mid b\}$

$$= \max\{d \in \mathbb{Z} \mid d \mid b,\ d \mid a-b\} = \gcd(b, a-b). \qquad \blacksquare$$

The above corollary justifies the steps in the pictorial argument:



By cutting, we do not change the gcd of the sides. So repeating this process we end up getting a square



, and $\gcd(d,d) = d$, which means sides of this square is the gcd of the sides of the initial rectangle.

Next we point out the connection with Euclid's algorithm.

Euclid's algorithm

Tuesday, June 29, 2021 3:29 PM

__Lemma__. Suppose n is a non-zero integer. If $a \overset{n}{\equiv} a'$, then

$$\gcd(a,n) = \gcd(a',n).$$

__Pf.__ Since $a \overset{n}{\equiv} a'$, $a - a' = nk$ for some $k \in \mathbb{Z}$.

- $d \mid n$ and $d \mid a' \Rightarrow d \mid (k)n + (1)a' \Rightarrow d \mid a$. (I)
- $d \mid n$ and $d \mid a \Rightarrow d \mid (1)a + (-k)n \Rightarrow d \mid a'$. (II)

By (I), (II), $\{d \in \mathbb{Z} \mid d \mid n, d \mid a\} = \{d \in \mathbb{Z} \mid d \mid n, d \mid a'\}$. Hence $\gcd(n,a) = \gcd(n,a')$. ∎

Euclid's algorithm is a fast way of finding the gcd of two positive integers. Similar to the pictorial method, Euclid's algorithm gives us a process through which the gcd stays the same, but we get smaller and smaller pairs.

Suppose $a \geq b$ are two positive integers. Let $a_0 := a$, $a_1 := b$. We divide a_0 by a_1:

$a_0 = a_1 \cdot q_1 + a_2$. Then $a_0 \overset{a_1}{\equiv} a_2$, and so by the above lemma, $\gcd(a_0, a_1) = \gcd(a_1, a_2)$. Next we divide a_1 by a_2 if $a_2 \neq 0$, and repeat this process till the remainder is 0.

Euclid's algorithm

Tuesday, June 29, 2021 3:29 PM

$a_0 = a_1 q_1 + a_2$, $\gcd(a_0, a_1) = \gcd(a_1, a_2)$, $a_1 > a_2$

$a_1 = a_2 q_2 + a_3$, $\gcd(a_1, a_2) = \gcd(a_2, a_3)$, $a_2 > a_3$

$\vdots \qquad \vdots \qquad \vdots$

$a_{n-1} = a_n q_n + 0$, $\gcd(a_{n-1}, a_n) = a_n$, $a_n > 0$

Hence $a_0 \geq a_1 > a_2 > \cdots > a_n > 0$ and $a_n = \gcd(a_0, a_1) = \gcd(a, b)$.

Notice that, for every $0 \leq i < n$,

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \begin{bmatrix} a_{i-1} \\ a_i \end{bmatrix} = \begin{bmatrix} (0)(a_{i-1}) + (1)(a_i) \\ (1)(a_{i-1}) + (-q_i)(a_i) \end{bmatrix} = \begin{bmatrix} a_i \\ a_{i-1} - a_i q_i \end{bmatrix} = \begin{bmatrix} a_i \\ a_{i+1} \end{bmatrix}.$$

Hence $$\begin{bmatrix} a_n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}.$$

Therefore $a_n = r a_0 + s a_1$ for some integers r, s. (*)

The following theorem follows.

<u>Theorem</u>. For every non-zero integers a and b, there are integers r and s such that $\gcd(a, b) = ra + sb$.

<u>Pf</u>. We notice that $\gcd(a, b) = \gcd(|a|, |b|)$. Now claim follows from (*). ∎

<u>Remark</u>. (*) gives us an algorithm to find an integer solution for $\gcd(a, b) = ax + by$.

Euclid's algorithm: an example

Tuesday, June 29, 2021 3:29 PM

<u>Ex.</u> Find gcd(197, 79) and write it as an integer linear combination of 197 and 79.

<u>Solution.</u> We follow Euclid's algorithm. Let $a_0 = 179$, $a_1 = 79$.

$197 = 79 \times 2 + 39$, $\quad q_1 = 2$, $\quad a_2 = 39$

$79 = 39 \times 2 + 1$, $\quad q_2 = 2$, $\quad a_3 = 1$

$39 = 1 \times 39 + 0$, $\quad q_3 = 39$, $\quad a_4 = 0$

So $\gcd(197, 79) = 1$ and

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} 197 \\ 79 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & -39 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -39 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} -2 & 5 \\ * & * \end{bmatrix}$$

This means $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 & 5 \\ * & * \end{bmatrix} \begin{bmatrix} 197 \\ 79 \end{bmatrix}$. Comparing the 1st components, we obtain that

$$1 = 197 \times (-2) + 79 \times (5). \qquad \blacksquare$$

Basic properties of gcd

Tuesday, June 29, 2021 3:29 PM

Here we review basic properties of gcd of two integers.

<u>Theorem</u>. Suppose a, b are two non-zero integers. Then if $\gcd(a,b)=d$, then $\gcd(\frac{a}{d}, \frac{b}{d})=1$.

<u>Pf</u>. Since $\gcd(a,b)=d$, $d \mid a$ and $d \mid b$ and

$$d = ra + bs \quad \text{for some } r,s\in\mathbb{Z}.$$

Hence $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ and $1 = r(\frac{a}{d}) + s(\frac{b}{d})$. (I)

Let $d' := \gcd(\frac{a}{d}, \frac{b}{d})$. Then $d' \mid \frac{a}{d}$, $d' \mid \frac{b}{d}$, and so $d' \mid r(\frac{a}{d}) + s(\frac{b}{d})$ (II). Therefore by (I) and (II), $d' \mid 1$.

Thus $d'=1$, which means $\gcd(\frac{a}{d}, \frac{b}{d})=1$. ∎

<u>Theorem</u>. Suppose a, b are two non-zero integers. If $d := \gcd(a,b)$ and d' is a common divisor of a and b, then $d' \mid d$.

<u>Pf</u>. Since $d = \gcd(a,b)$, $d = ra + sb$ for some $r,s\in\mathbb{Z}$.

Because $d' \mid a$ and $d' \mid b$, $d' \mid ra+sb$. Hence $d' \mid d$. ∎

<u>Theorem</u>. Suppose a,b,c are three non-zero integers. Then $\gcd(ac, bc) = |c| \gcd(a,b)$.

<u>Pf</u>. Suppose $d := \gcd(a,b)$. Then $d \mid a$ and $d \mid b$, and so

Basic properties of gcd

Tuesday, June 29, 2021 3:29 PM

$d|c|$ divides ac and $d|c|$ divides bc. Hence

$$d|c| \leq \gcd(ac, bc). \qquad \text{(I)}$$

On the other hand, $d = \gcd(a,b)$ implies that $d = ra + sb$ for some $r, s \in \mathbb{Z}$. Hence

$$d|c| = ra\,|c| + sb\,|c| = \pm\,(r(ac) + s(ac)). \qquad \text{(II)}$$

Notice that $\gcd(ac, bc)$ divides every integer linear combination of ac and bc. Hence by (II),

$$\gcd(ac, bc) \mid d|c|. \qquad \text{(III)}$$

By (I) and (III), $\gcd(ac, bc) = d|c|$, which means

$$\gcd(ac, bc) = |c| \gcd(a,b). \qquad ∎$$

Euclid's lemma. For $a, b, c \in \mathbb{Z} \setminus \{0\}$,

$$\left.\begin{array}{l} \gcd(a,b) = 1 \\ a \mid bc \end{array}\right\} \Rightarrow a \mid c.$$

(If a and b do not have any non-trivial common factors and a divides bc, then $a \mid c$. This lemma plays an important role in proving the uniqueness of factorization of integers into prime numbers.)

Euclid's lemma

Tuesday, June 29, 2021 3:29 PM

Pf. Since $\gcd(a,b)=1$, $\underbrace{1=ra+bs}_{(I)}$ for some $r,s\in\mathbb{Z}$.

Multiplying both sides of (I) by c, we obtain that

$$c = rc(a) + s(bc). \qquad \text{(II)}$$

Since $a|a$ and $a|bc$, a divides every integer linear combination of a and bc. Therefore by (II), $a|c$. ∎

An important corollary of Euclid's lemma is about prime numbers. Let's recall that an integer p is called prime if $p>1$ and p has exactly two positive divisors 1 and p.

This means if p is prime, $d\in\mathbb{Z}^+$, and $d|p$, then $d=1$ or p.

Here is an important corollary of Euclid's lemma.

Euclid's lemma: prime number case Suppose p is prime and a,b are two non-zero integers. Then

$$p|ab \text{ implies that either } p|a \text{ or } p|b.$$

Pf. If $p\nmid a$, then $\gcd(p,a)\neq p$. Hence $\gcd(p,a)=1$ as p has exactly two positive divisors 1 and p.

Since $\gcd(p,a)=1$ and $p|ab$, by Euclid's lemma, $p|b$. ∎