Thm. **FTA** Any pos. integer $n > 1$ has a unique prime factorization,

$$n = p_1 p_2 \cdots p_k \quad (\text{w/ repetition})$$

$$= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (\text{w/o rep., } p_i \neq p_j \text{ for } i \neq j)$$

pf: By strong induction:

$\exists$ by

(1) $n = 2$ is prime

(2) Assume $n \geq 2$ & $\forall m$, $2 \leq m \leq n$

$$m = \prod_p p^{e(p)} \quad \text{unique exists}$$

& consider $n+1$. Either $n+1$ is prime (& we are done) or not, & $n+1 = ab$ w/ $1 < a, b \leq n \Rightarrow$

$$a = \prod_p p^{e(p)}, \quad b = \prod_q q^{e(q)} \Rightarrow n+1 = ab = \prod_{p,q} p^{e(p)} q^{e(q)}$$

Now for <u>uniqueness</u>: When $n=2$, we are done, so suppose $n>2$, and suppose

$$n = p_1 \cdots p_k$$
$$= a_1 \cdots a_\ell$$

Then

$$p_1 \mid a_1 \cdots a_\ell \implies p_1 \mid a_i \text{ for at least one } i=1,\dots,\ell$$

$$\implies p_1 = a_i \quad \text{bec. } a_i \text{ is prime } \& \ p_1 > 1$$

Therefore

$$p_2 \cdots p_k = a_1 \cdots a_{i-1} a_{i+1} \cdots a_\ell$$

Now use induction hypothesis:

$\forall s=2,\dots,k$, $p_s = a_r$ for some $r = 1,\dots,i-1,i+1,\dots,\ell$

$\implies k=\ell$ & by relabeling

$p_j = a_j \ \forall j=1,\dots,k=\ell$

<u>ex.</u> $24 = 8 \cdot 3 = 2^3 \cdot 3^1$

<u>ex.</u> $32 = 2^5$

<u>ex.</u> $78 = 6 \cdot 13 = 2^1 \cdot 3^1 \cdot 13^1$

etc.

I. Greatest Common Divisor

(1) What is it?

(2) How can we find it?

Def A divisor of an integer $n \in \mathbb{Z}$ is another integer $d \in \mathbb{Z}$ s.t.

$$\boxed{n = dk \text{ for some } k \in \mathbb{Z}}$$

In this case, both d & k are divisors, & we write $\boxed{d \mid n}$ & $k \mid n$.

ex. 8 is a divisor of 72, because

$$\underbrace{72}_{n} = \underbrace{8}_{d} \cdot \underbrace{9}_{k}$$

Remark: There is always at least one divisor, $d = 1$ for any $a, b \in \mathbb{Z}$.

QED

<u>Notation</u>: Let's transfer the problem to sets:

Define the <u>set of all common divisors of a & $b \in \mathbb{Z}$</u>;

$$\boxed{D(a,b) \overset{def}{=} \{ d \in \mathbb{Z} \mid d|a \text{ and } d|b \}}$$

$\boxtimes$

<u>Observation</u>: $D(a,b) \neq \emptyset$ bec. $1 \in D(a,b)$. $\boxtimes$

<u>Thm. 1.2 (Apostol)</u> For all $a, b \in \mathbb{Z}$, there exists <u>a</u> divisor $d \in D(a,b)$ s.t.

$$\boxed{d = am + bn \text{ for some } m, n \in \mathbb{Z}}$$

<u>ex.</u> Let $a = 24$, $b = 18$. Then,

$$D(24, 18) = \{ \pm 1, \pm 2, \pm 3, \pm 6 \}$$

and

$$\begin{array}{ccccccc} 6 & = & 24 & \cdot & 1 & + & 18 \cdot (-1) \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ d & & a & & m & & b \quad n \end{array}$$

But notice that the other divisors do <u>not</u> have expressions of the form

$$d = am + bn \text{ for } m, n \in \mathbb{Z}$$

e.g.

$$1 = ax + by$$
$$= 24x + 18y$$
$$= \underbrace{2(12x + 9y)}_{\text{even}}$$

odd

$$\cancel{2} = ax + by$$
$$= 24x + 18y$$
$$= \cancel{2}(12x + 9y)$$

$$\Leftrightarrow 1 = 12x + 9y$$
$$\Leftrightarrow 1 = \underbrace{3(4x + 3y)}_{\text{div. by } 3}$$

not divis. by 3

$$3 = ax + by$$
$$= 24x + 18y$$
$$\Leftrightarrow 1 = 8x + 6y$$
$$= \underbrace{2(4x + 3y)}_{\text{even}}$$

odd

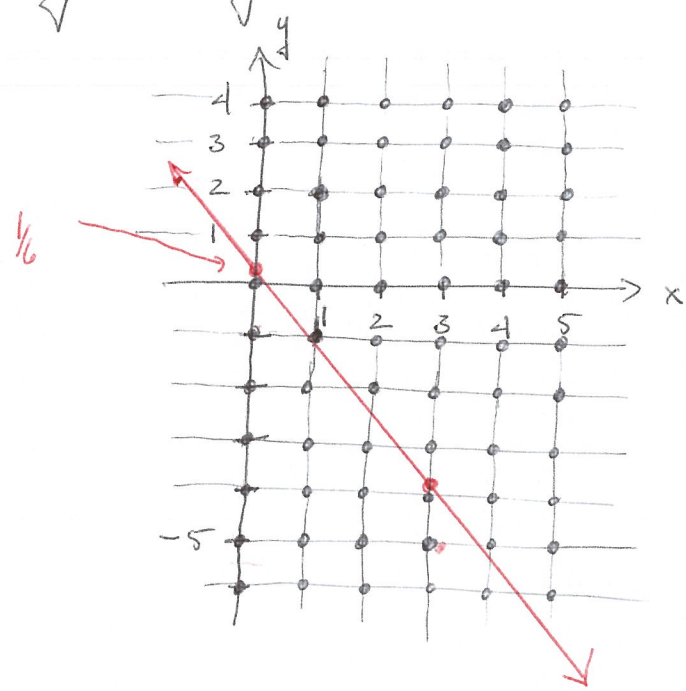
So none of $\pm 1, \pm 2, \pm 3$ have <u>integer</u> <u>soln's</u> to

$$ax + by = d$$

Why? In the xy-plane, the line

$$ax + by = d \quad \text{for } d \in D(a,b)$$

may or may not intersect $(m,n) \in \mathbb{Z}^2 \subseteq \mathbb{R}^2$,



e.g. $3 = 24x + 18y$

$\iff 1 = 8x + 6y$

$\iff y = -\frac{4}{3}x + 1/6$

never touches a single black dot $\bullet\ (m,n)$, $m,n \in \mathbb{Z}$.

Thus, only $d = \pm 6 = \max D(a,b) \overset{\text{def}}{=} \gcd(a,b)$

seems to work in this case. $\boxtimes$

pf of Thm. 12:

Case 1 $a, b \geq$: Let $n = a+b$ and let us use induction on $n \in \mathbb{N}$.

(1) $n = 0$ (base case): Let $\underbrace{d = 0}_{\in D(0,0)} = m = \underbrace{n}_{= a+b \iff a=b=0}$,

so

$$0 = 0 \cdot 0 + 0 \cdot 0$$

$$d = am + bn, \quad m, n \in \mathbb{Z}$$

$= 0$

(2) (inductive step, using strong induction):

Suppose $\forall k = 0, 1, \ldots, n$ the statement of the thm. holds true ($k = a+b$, $d \in D(a,b)$ $\Rightarrow \exists m, n \in \mathbb{Z}$ s.t. $d = am + bn$), & consider the case $k = n+1 = a+b$.

WOLOG we may assume $a \geq b$ (else relabel)

(a) $\underline{b=0} \Longrightarrow k=n+1=a$, & we can take $d=a$, $m=1$, $n=0$,

$$\begin{aligned} d &= a \\ &= a\cdot 1 + 0\cdot 0 \\ &= am + bn \end{aligned}$$

(b) $\underline{b \geq 1}$ $\Longrightarrow$

$(1 \leq b \leq a \leq n+1)$

$$0 \leq a-b \leq n+1-b \leq n+1-1 = n$$

so we can use the induction hypothesis on $\boxed{a' \overset{\text{def}}{=} a-b}$, $\boxed{b' \overset{\text{def}}{=} b}$: $\exists\, m,n \in \mathbb{Z}$, $\underline{d \in D(a',b')} = D(a-b,b)$, s.t.

$$\boxed{\begin{aligned} d = a'm + b'n &= (a-b)m + bn \\ &= am + b(n-m) \end{aligned}}$$

Now, $\boxed{d \in D(a',b') = D(a-b,b)} \Longrightarrow$

$d \mid (a-b)$ & $d \mid b \Longrightarrow$

$d \mid (a-b+b = a)$ $\boxed{\Longrightarrow d \in D(a,b)}$

(i)

$D(a-b,b) \subseteq D(a,b)$ and $\forall d \in D(a-b,b)$ $\exists\, m,n \in \mathbb{Z}$ s.t.

$d = am + b(n-m)$
$= am + bl$

But of course we have the reverse inclusion as well

$$D(a-b, b) \supseteq D(a,b)$$

since

$$d \in D(a,b) \implies d \mid a \ \& \ d \mid b$$
$$\implies d \mid (a-b)$$
$$\implies d \in D(a-b, b)$$

(pf: $d \in D(a,b) \implies a = dk,\ b = dl$
$(k, l \in \mathbb{Z})$
$\implies a - b = dk - dl$
$= d\underbrace{(k-l)}_{\in \mathbb{Z}}$)

Hence

$$D(a,b) = D(a-b, b)$$

& $d \in D(a,b) \implies d = \underbrace{am + b(n-m)}_{\in \mathbb{Z}}$

so the statement holds true for

$k = n+1$, whether $b = 0$ or $b \geq 1$
$= a+b$ & $a \geq b$

OR both

<u>Case 2</u>: <u>$a < 0$</u> OR <u>$b < 0$</u>:

Apply case 1 to $|a|$ & $|b| \geq 0$,

$$d \in D(a,b) \iff d \in D(|a|, |b|)$$

so

$$d = |a|m + |b|n \text{ for some } m, n \in \mathbb{Z}$$

If $a < 0$, $|a|m = (-a)m = a(-m)$, so

$$d = a(-m) + |b|n$$

& if $b < 0$, repeat,

$$d = a(-m) + b(-n)$$

else, if $b \geq 0$, leave n alone, $|b| = b \Rightarrow$

$$d = a(-m) + bn$$

& sim. w/ $a \geq 0$, $b < 0$. QED

Observation: We could put a different partial order on $D(a,b)$, namely divisibility

$$e \le f \overset{def}{\iff} e \mid f$$

ex. $D(24,18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$= \{-6, -3, -2, -1, 1, 2, 3, 6\}$

so

$e, f \in D(24,18)$ satisfying $e \mid f$ are

$e = \pm 1$, f any element, $e \mid f$

$e = \pm 2$, $f = \pm 2, \pm 6$, $e \mid f$

$e = \pm 3$, $f = \pm 3, \pm 6$, $e \mid f$

$e = \pm 6$, $f = \pm 6$, $e \mid f$

$\Rightarrow$ $\pm 1 \le$ any f

$\pm 2 \le \pm 2, \pm 6$ etc

W.r.t. this "$\le$" $\overset{def}{=}$ $\mid$, $\boxed{\pm 6 = \max D(24,18).}$

Thm. 1.3 (Apostol) $\forall a, b \in \mathbb{Z}$, there is only one (uniqueness!) greatest common divisor (w.r.t. the usual $\leq$ as well as w.r.t. $|$) satisfying

(1) $d \geq 0$

(2) $d \in D(a,b)$

(3) $e \in D(a,b)$ $\Longrightarrow e | d$ (i.e. $d = \max D(a,b)$ w.r.t. $|$)

pf: By Thm. 1.2, $\exists d \in \mathbb{Z}$ satisfying (2) & (3), bec. $\exists d \in D(a,b)$ s.t.

existence

$$d = am + bn, \quad m, n \in \mathbb{Z}$$

$\Longrightarrow$ if $e \in D(a,b)$ then $e | d$ ($e |$ RHS $\Rightarrow$ $e |$ LHS too)

and of course $-d$ also satisfies (2)–(3), so choose whichever of $\pm d \geq 0$. More generally

uniqueness

for any d' satisfying (2) – (3), i.e. $d' \in D(a,b)$ & $e \in D(a,b) \Rightarrow e \mid d'$, then apply this to $e = d$: $d \mid d'$. Reversing the roles of d & d' $\Rightarrow d' \mid d$, so

$$d' = \pm d \quad \text{or} \quad |d'| = |d|$$

so there is <u>only</u> <u>one</u> $d \geq 0$ satisfying (2) – (3).

QED

Thm (Division Algorithm) For all $a, b \in \mathbb{Z}$, w/ $b > 0$, there exist $q, r \in \mathbb{Z}$, satisfying

$$a = \underbrace{q}_{\text{quotient}}b + \underbrace{r}_{\text{remainder}} \quad \text{and} \quad 0 \le r < b$$

i.e.

$$\frac{a}{b} = q + \frac{r}{b}$$

ex. $\frac{29}{7} = 4 + \frac{1}{7}$ or $\underset{a}{27} = \underset{q}{4} \cdot \underset{b}{7} + \underset{r}{1}$

ex. $-\frac{32}{5} = -7 + \frac{3}{5}$ or $\underset{a}{-32} = \underset{q}{(-7)} \cdot \underset{b}{5} + \underset{r}{3}$

pf: Let $K = \{ z \in \mathbb{Z} \mid z = a - xb,\ x \in \mathbb{Z} \}$ and let $L = \{ z \in K \mid z \ge 0 \}$. Then, let's show

$$\min L = r = a - qb \text{ for some } q \in \mathbb{Z}$$

First, $L \neq \emptyset$, bec. $a - xb \ge 0$ is solvable in $\mathbb{Z}$

(just find $x \in \mathbb{Z}$ s.t. $\frac{b}{a} \geq x$). Secondly, by the well-ordering property of $\mathbb{N}$, L has a least element, call it r,

$$r \overset{\text{def}}{=} \min L$$

(so $r = a - qb$ for some $q \in \mathbb{Z}$)

Now, we claim that

$$0 \leq r < b$$

for if we suppose not we run into a contradiction:

Suppose

$$r \geq b$$

Since $b > 0$,

$$\begin{aligned} r &> r - b \\ &= (a - qb) - b \\ &= a - (q+1)b \end{aligned}$$

But $r \geq b \implies r - b \geq 0$, so

$$0 \leq \underbrace{a - (q+1)b}_{\text{call it } s \in L} = r - b \underbrace{< r}_{s < r \ \& \ s \in L} = \min L$$

contrad.

QED

1.2.4 Euclidean Algorithm and Continued Fractions

If $a, b \in \mathbb{Z}$ and $b \geq 1$, Lemmas 1.15 and 1.16 assure us that there exists a greatest common divisor $d = \gcd(a, b)$, but as yet we have no method of finding one given arbitary integers a and b. The Euclidean algorithm remedies this deficiency. It's method makes use of the division algorithm, Lemma 1.14: there exist integers q and r, with $0 \leq r < b$ such that

$$a = bq + r$$

If d is any common divisor of a and b, that is $d|a$ and $d|b$, then $d|r$ as well, and conversely if $d|b$ and $d|r$, then $d|a$. Hence,

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

Now, we can repeat the argument to find q' and r', with $0 \leq r' < r$ such that $b = rq' + r'$, and with

$$\gcd(a, b) = \gcd(b, r) = \gcd(r, r')$$

Proceeding thus we get a decreasing sequence of nonegative integers, which must therefore be finite,

$$r \geq r' \geq r'' \geq \cdots \geq r^{(n)} = 0$$

The greatest common divisor of a and b, therefore, is

$$\gcd(a, b) = g(b, r) = \gcd(r^{(n-1)}, r^{(n)})$$

To give this algorithm a consistent indexing we take

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_2 &= r \end{aligned}$$

and all the other r_k are determined by the division algorithm at each step, until we reach $r_{n+1} = 0$, which gives $\gcd(r_{n-1}, r_n) = \gcd(a, b)$:

$$\begin{aligned} r_0 &= q_0 r_1 + r_2 \\ r_1 &= q_1 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-2} + r_n \\ r_{n-1} &= r_n q_{n-1} \end{aligned}$$

The natural number n is called the **length** of the Euclidean algorithm for a and b, the sequence $(q_0, q_1, \ldots, q_{n-1})$ is called the **sequence of partial quotients** for a and b, and the sequence $(r_2, r_3, \ldots, r_n)$ is called the **sequence of remainders**. For example, to find $\gcd(932, 574)$, we proceed thus: $r_0 = 932$, $r_1 = 574$, and since $\frac{932}{574} = 1\frac{358}{574}$, we have $q_0 = 1$ and $r_2 = 358$, so that

$$932 = 574 \cdot 1 + 358$$

Now, $\frac{574}{358} = 1\frac{1}{216}$, so $r_3 = 216$ and $q_1 = 1$, or

$$574 = 358 \cdot 1 + 216$$

Proceeding thus we get

$$\begin{aligned}
932 &= 574 \cdot 1 + 358 \\
574 &= 358 \cdot 1 + 216 \\
358 &= 216 \cdot 1 + 142 \\
216 &= 142 \cdot 1 + 74 \\
142 &= 74 \cdot 1 + 68 \\
74 &= 68 \cdot 1 + 6 \\
68 &= 6 \cdot 11 + 2 \\
6 &= 2 \cdot 3
\end{aligned}$$

So

$$2 = r_n = \gcd(6, 2) = \gcd(932, 574)$$

The sequence of partial quotients for 932 and 574 is $(1, 1, 1, 1, 1, 1, 11, 3)$ and the sequence of remainders is $(358, 216, 142, 74, 68, 6, 2)$, with the last being the gcd. The length of the algorithm for 932 and 574 is $n = 8$.

Here is a MATLAB implementation of the Euclidean algorithm:

```
true=1; false=0;

fprintf('Enter a positive integer n:\n\n')
n=input('');
a=n;
fprintf('\n\n')
fprintf('and another positive integer m:\n\n')
m=input('');
b=m;
fprintf('\n\n')

if n<m
    nn=m;
    m=n;
    n=nn;
    ok=true;
elseif n==m
    ok=false;
    fprintf('The greatest common denominator of %d and %d is %d.\n\n',a,b,n)
else
    ok=true;
end

while n>m & ok==true
    k=floor(n/m);
```

```
    r=n-m*k;
    n=m;
    m=r;
    if r==0
        fprintf('The Euclidean Algorithm gives gcd(%d,%d)=%d\n\n',a,b,n)
    else
        ok=true;
    end
end
```

We could proceed differently and get similar results using fractions, even though we have not formally introduced fractions; nonetheless, we can still state the following result and come back to it with more formal credentials later:

$$
\begin{aligned}
\frac{932}{574} &= 1+\frac{358}{574} = 1+\frac{1}{\frac{574}{358}} = 1+\frac{1}{\frac{358+216}{358}} \\
&= 1+\frac{1}{1+\frac{216}{358}} = 1+\frac{1}{1+\frac{1}{\frac{358}{216}}} = 1+\frac{1}{1+\frac{1}{\frac{216+142}{216}}} \\
&= 1+\frac{1}{1+\frac{1}{1+\frac{142}{216}}} = 1+\frac{1}{1+\frac{1}{1+\frac{1}{\frac{216}{142}}}} = 1+\frac{1}{1+\frac{1}{1+\frac{1}{\frac{142+74}{142}}}} \\
&= 1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{74}{142}}}} \\
&= 1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{68}{74}}}}} \\
&= 1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{6}{68}}}}}}
\end{aligned}
$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{11 + \cfrac{1}{3}}}}}}}$$

This is called a **finite continued fraction**, and the numbers 1, 1, 1, 1, 1, 1, 11 and 3 appearing in the left of each of the denominators, from top to bottom, are in this context called the **partial quotients** of the continued fraction. They are the same numbers appearing in the sequence of partial quotients $(1, 1, 1, 1, 1, 1, 11, 3)$ in the Euclidean algorith, not uncoincidentally, for we get them by the same method. Special notation is used for continued fractions:

$$\begin{aligned}
\langle a_0, a_1, \ldots, a_n \rangle &= a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+} \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\vdots \\ a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}
\end{aligned}$$

We see that there is a connection between finite continued fractions and the Euclidean algorithm. To formally establish this link requires an induction argument, which is provided in the proof of the following theorem.

Theorem 1.26 (Euclidean Algorithm) *If $a, b \in \mathbb{Z}$ and $b \geq 1$, and the Euclidean algorithm for a and b has length n and a sequence of partial quotients $(q_0, q_1, \ldots, q_{n-1})$, then*

$$\frac{a}{b} = \langle q_0, q_1, \ldots, q_{n-1} \rangle$$

Proof: The proof is by induction on n. For $n = 1$ we have $a = r_0$, $b = r_1$, and $r_0 = qr_1$, so $\frac{a}{b} = \frac{r_0}{r_1} = q_0 = \langle q_0 \rangle$. For $n = 2$ we have

$$\begin{aligned}
r_0 &= r_1 q_0 + r_2 \\
r_1 &= r_2 q_1
\end{aligned}$$

so

$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{r_2}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{q_1} = \langle q_0, q_1 \rangle$$

Now suppose the theorem holds for some $n \geq 2$. Then, if the Euclidean algorithm for a

and b, $b \geq 1$, has length $n+1$, with

$$\begin{aligned} r_0 &= r_1 q_0 + r_2 \\ r_1 &= r_2 q_1 + r_3 \\ &\vdots \\ r_n &= r_{n+1} q_n \end{aligned}$$

if we clip the first equation in it we get a length n algorithm

$$\begin{aligned} r_1 &= r_2 q_1 + r_3 \\ &\vdots \\ r_n &= r_{n+1} q_n \end{aligned}$$

where $a' = r_1$ and $b' = r_2 \geq 1$ ($r_2 \geq 0$ because we chose $n \geq 2$), so we may use the induction hypothesis to conclude that

$$\frac{r_1}{r_2} = \langle q_1, q_2, \ldots, q_n \rangle$$

whence

$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{r_2}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{\langle q_1, \ldots, q_n \rangle} = \langle q_0, q_1, \ldots, q_n \rangle$$

Hence the statement holds for $n+1$ whenever it does for n, so by induction it holds for all $n \in \mathbb{N}$. ■

Theorem 1.27 (Euclid's Theorem) *There are infinitely many primes.*

Proof: Suppose there are only a finite number of primes, say $p_1, \ldots, p_n \in \mathbb{N}$. Then the number $N = \prod_{i=1}^{n} p_i + 1$ is not prime, and since there are only a finite number of primes, one of the primes, p_i, divides N. But if $p_i | N$, then, since $p_i | \prod_{i=1}^{n} p_i$ we must have that $p_i | (N - \prod_{i=1}^{n} p_i)$, or $p_i | 1$, which is a contradiction because $p_i > 1$. Hence there cannot be finitely may primes. ■