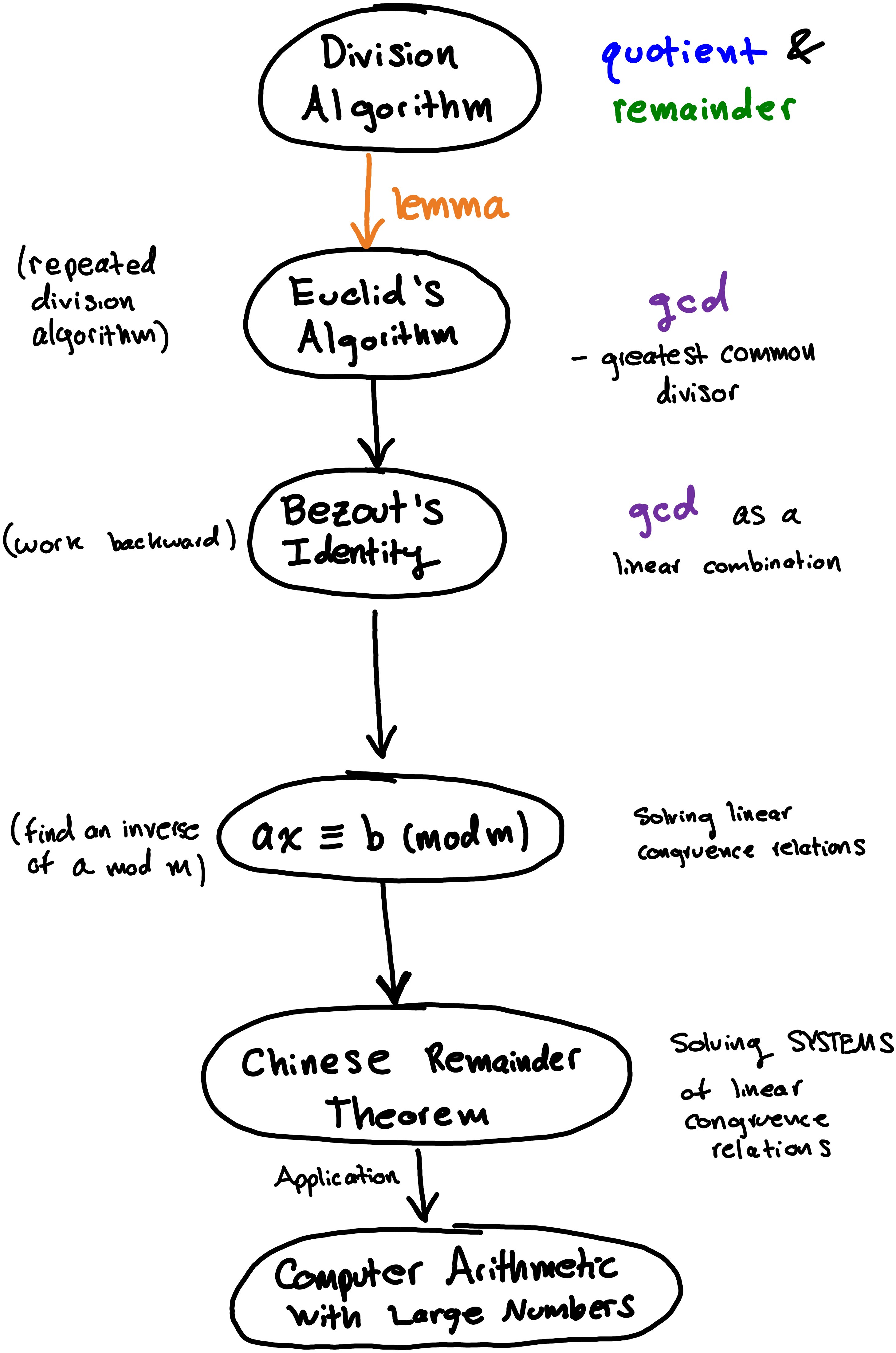

Division Algorithm
quotient & remainder
lemma
(repeated division algorithm)
Euclid's Algorithm
gcd
- greatest common divisor
(work backward)
Bezout's Identity
gcd as a linear combination
(find an inverse of a mod m)
ax ≡ b (mod m)
Solving linear congruence relations
Chinese Remainder Theorem
Solving SYSTEMS of linear congruence relations
Application
Computer Arithmetic with Large Numbers

A Note on Notation: Typically we prefer the notation '$|$' for "such that" in sets $\{ \blacksquare \mid \blacksquare \}$ however, we do not wish to confuse this vertical line for an instance of "divides" which we also write using a vertical line. Therefore if either $\blacksquare$ or $\blacksquare$ contain a "divides" symbol we use a colon ':' to express the phrase "such that."

Greatest Common Divisors

let $a, b \in \mathbb{N}$

"such that" (see note above)

$$\mathrm{Div}(a) := \{x : x \mid a\} \quad \text{(set of divisors of } a\text{)}$$

$$\mathrm{Div}(b) := \{x : x \mid b\} \quad \text{(set of divisors of } b\text{)}$$

$$1 \in \underbrace{\mathrm{Div}(a) \cap \mathrm{Div}(b)}_{\neq \emptyset \text{ non-empty}} \quad \text{(set of common divisors of } a \text{ \& } b\text{)}$$

$\Rightarrow$

$$\gcd(a,b) := \max\left(\mathrm{Div}(a) \cap \mathrm{Div}(b)\right)$$

(the greatest common divisor)

Note: If $X \subseteq \mathbb{N}$, and $X \neq \emptyset$, $|X| < \infty$ then $\max X$ exists.

e.g.

$$\mathrm{Div}(12) = \{1,2,3,4,6,12\}$$

$$\mathrm{Div}(18) = \{1,2,3,6,9,18\}$$

$$\mathrm{Div}(12) \cap \mathrm{Div}(18) = \{1,2,3,6\}$$

$$\max\left(\mathrm{Div}(12) \cap \mathrm{Div}(18)\right) = 6$$

$$\Rightarrow \gcd(12,18) = 6$$

A Second approach to GCDs

Recall that "a divides b" defines a relation on the natural numbers $\mathbb{N}$. What properties did it have?

pre-order

partial order

order

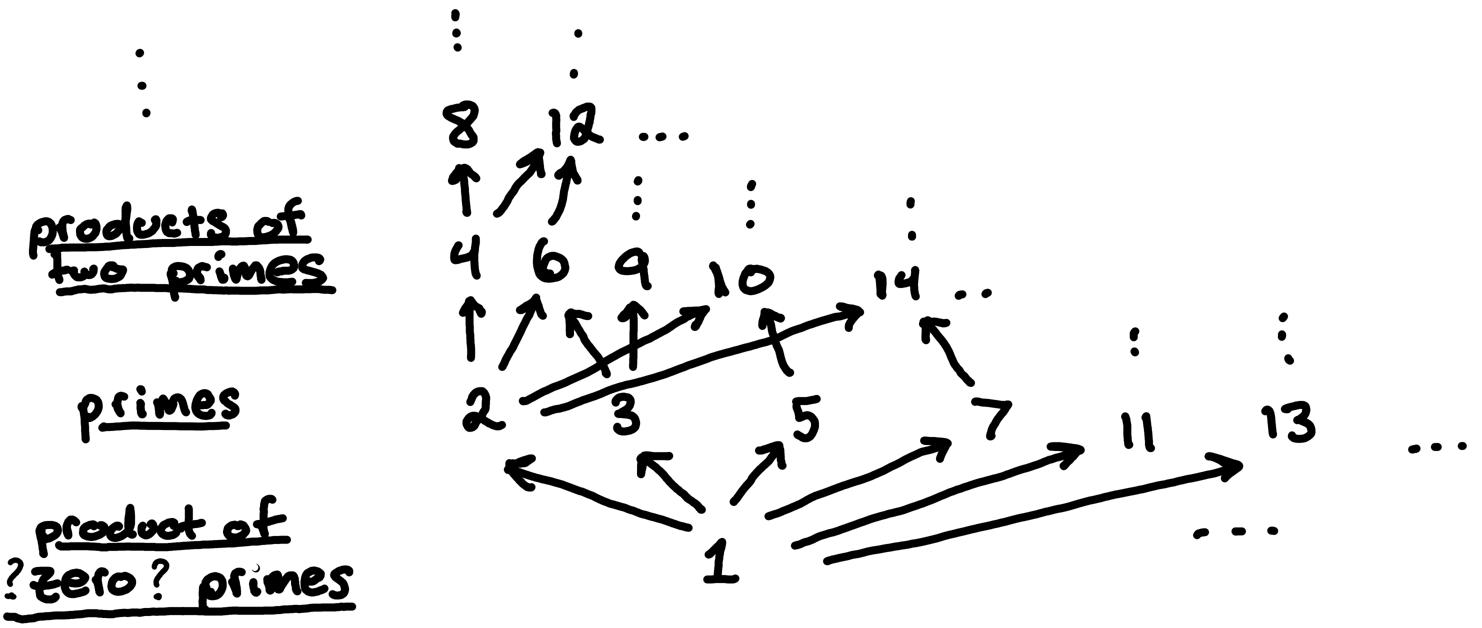
(i) Reflexive: $a \mid a$ since $a = 1 \cdot a$

(ii) Transitive: $a \mid b \wedge b \mid c \Rightarrow a \mid c$
since $ax = b \wedge by = c$
implies $a(xy) = c$

(iii) Anti-Symmetric: $a \mid b \wedge b \mid a \Rightarrow a = b$

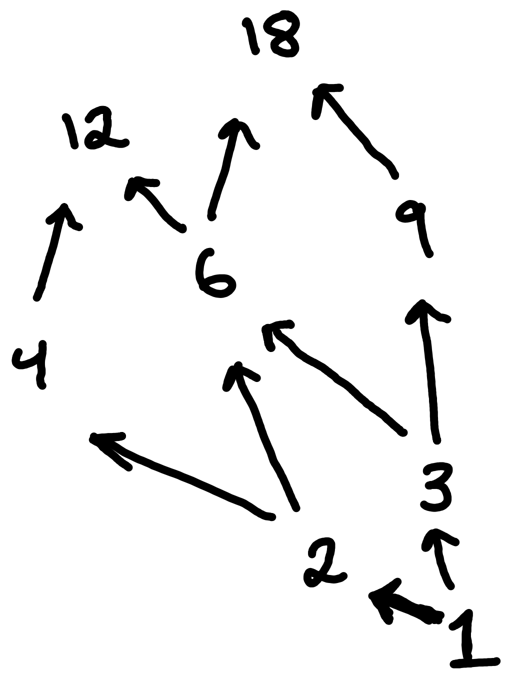
$$a \mid b \wedge b \mid a \;\Downarrow\; a \leq b \wedge b \leq A \;\Nearrow\; a = b$$

Thus, we can draw the Hasse diagram of the poset $(\mathbb{N}, \mid)$ & hope to understand what GCDs are geometrically (i.e. pictorially). Here is a small portion of the diagram.

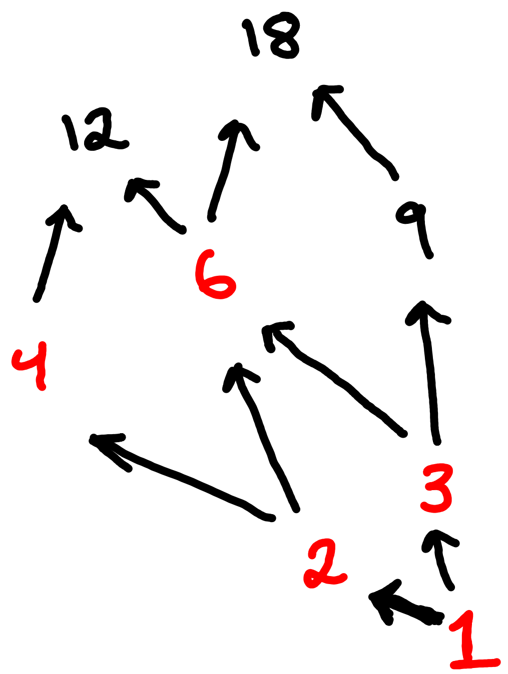


this picture gets crowded and unwieldy rather quickly, so it is useful to omit parts deemed not immediately relevant to the task at hand.

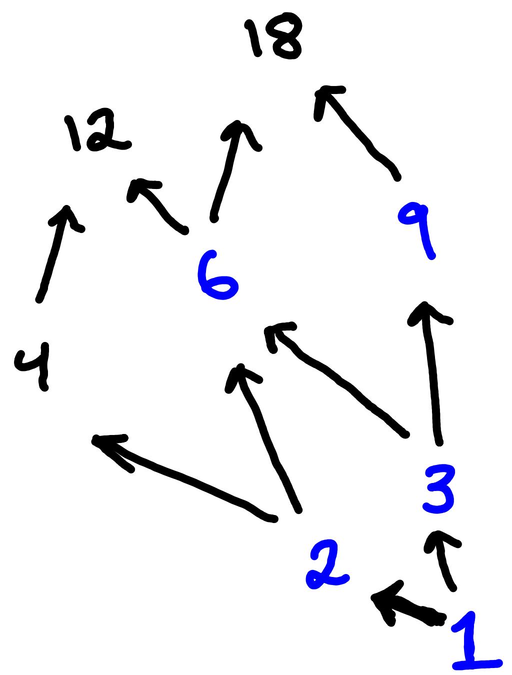
Here is the minimal piece of the diagram needed to understand the calculation of $\gcd(12,18)$.



Coloring all divisors of 12 red we see

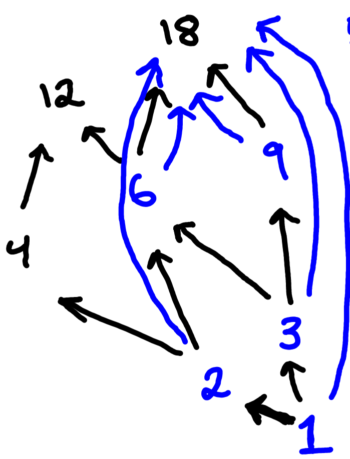


Similarly, we might color the divisors of 18 blue to get



It is not difficult to "see" the set of divisors of a number in this poset, indeed, $\mathrm{Div}(n) = \{$all numbers that can reach n travelling along arrows of the diagram$\}$. To say this in another way, $\mathrm{Div}(n)$ is the collection of numbers appearing as the starting point of a path (of directed arrows) ending @ n.

e.g.



5 paths ending @ 18

⇕

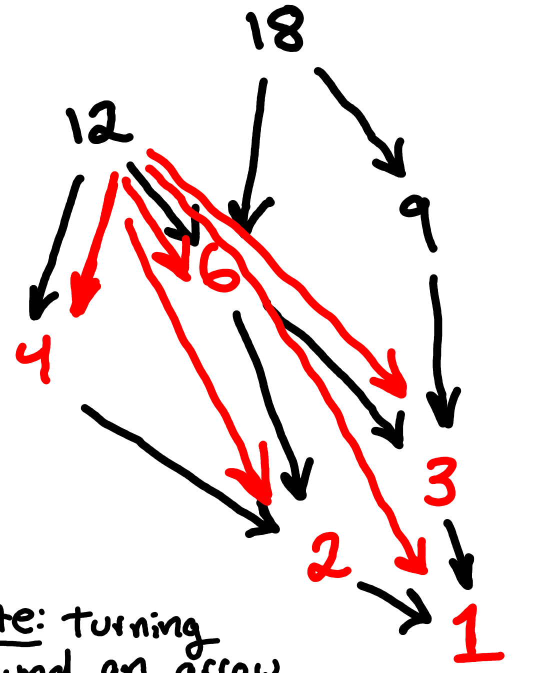
5 divisors of 18

To shorten what must be said, we can summarize as follows

$\mathrm{Div}(n) = \{$numbers "pointing to" $n\}$.

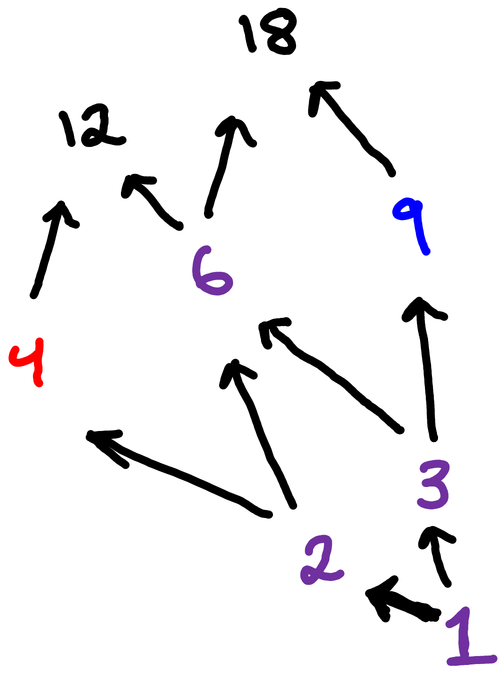
One might also choose to turn the arrows arround, in which case

$\mathrm{Div}(n) = \{$numbers n "points to"$\}$



Note: turning around an arrow indicating a "divides" relation results in an arrow indicating the relation "is a multiple of"

If we color the divisors of 12 red, and at the same time color the divisors of 18 blue, letting two colors mix to form purple when they coincide, we get.



$\mathrm{Div}(12) \cap \mathrm{Div}(18)$

By definition, the purple numbers are common divisors of 12 & 18.

$$\mathrm{Div}(12) = \{x : x \mid 12\}$$
$$= \{x \mid x \rightarrow 12\}$$

$$\mathrm{Div}(18) = \{x \quad x \mid 18\}$$
$$= \{x \mid x \rightarrow 18\}$$

Lastly, we must figure out how to "see" which of the purple numbers is largest from the Hasse diagram. By positioning numbers higher on the page when they are larger in absolute value, we can easily spot this maximum of the numbers colored purple earlier i.e., the GCD

Since the purple number farthest up the page is the GCD (of the numbers in question, 12 & 18 in our case) & any purple number is a divisor of both 12 & 18, all purple numbers point to the one furthest up the page!

gcd(a,b) is said to be "the last number pointing to both a & b" in the sense that

$$\begin{tikzcd} a & & b \\ & \gcd(a,b) \arrow[ul] \arrow[ur] & \end{tikzcd} \qquad \text{\& whenever} \qquad \begin{tikzcd} a & & b \\ & x \arrow[ul] \arrow[ur] & \end{tikzcd}$$

one has $x \longrightarrow \gcd(a,b)$. Concisely,

$$\begin{tikzcd} & & a \\ x \arrow[r, dashed] \arrow[urr] \arrow[drr] & \gcd(a,b) \arrow[ur] \arrow[dr] & \\ & & b \end{tikzcd}$$

the dashed arrow is the one guaranteed by "context" (the context being the solid arrows). The origin of this description of GCDs is category theory If you are curious, the relevant terms to look up are "product" or "limit." Turning all arrows around produces the definition of a "coproduct" or "colimit."

Q: What happens if we turn the arrows around in the poset $(\mathbb{N}, |)$ then find the last number pointing to a & b ? What is the relationship between this number & gcd(a,b) ?

These questions will be answered at another time. For now, we pave the way for this future discussion with an observation

<u>Observe:</u> Organizing the naturals by height on the page according to the # of prime factors (counting with multiplicity so $4=2^2$ has <u>two</u> prime factors) the last row with at least one purple number has at most one purple number.

<u>proof sketch:</u> If two numbers x & y have the same number of prime factors and $x|y$ then the prime factorization of x coincides with that of y and thus $x=y$. The observation follows from setting $y = \gcd(a,b)$ & x any common divisor of a & b at the same height as y in the poset $(\mathbb{N}, |)$ described above. $\square$

It is then reasonable to guess

$$\gcd(a,b) = \begin{array}{c}\text{product of all primes}\\ \text{a \& b have in common}\\ \text{with multiplicity.}\end{array}$$

Indeed this is what we will eventually prove.

The following are equivalent

(i) n is the greatest common divisor of a & b i.e, $\gcd(a,b) = n$

(ii) $\max(\mathrm{Div}(a) \cap \mathrm{Div}(b)) = \{n\}$.

(iii) n is the largest number to divide both a & b i.e., $n|a$ & $n|b$ and $\forall m$

$$m|a \ \& \ m|b \Rightarrow m|n.$$

(iv) n is the last thing pointing into both a & b in the poset $(\mathbb{N}, |)$ i.e., $m \to a$ & $m \to b \Rightarrow m \to n$

in category theory the GCD of a & b is the product of a & b in the poset category $(\mathbb{N}, |)$

$$\begin{tikzcd} & & a \\ m \arrow[urr, bend left] \arrow[drr] \arrow[r, dashed] & n \arrow[ur] \arrow[dr] & \\ & & b \end{tikzcd}$$

Such an n is called the "infimum" or "meet" of a & b in the poset $(\mathbb{N}, |)$

(vi) n is the product of all primes common to both a & b counted with multiplicity

i.e., $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

then $n = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}$.

(vii) n is the first thing both a & b point into if the relation defining the poset $(\mathbb{N}, |)$ is reversed i.e, if $x \longrightarrow y$ if and only if $y | x$ then

> In Category theory (if you are curious) "turning around arrows" is called "dualization" & the result is the "opposite category" & the diagram to the right defines n as the "coproduct" of a & b or the "colimit" of the diagram consisting of a & b.

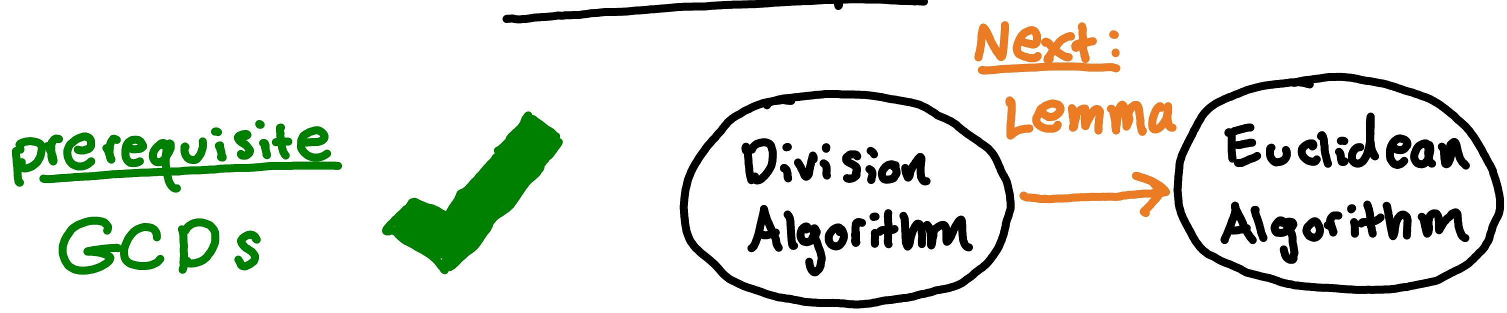
$$\begin{tikzcd} & & a \arrow[dll] \arrow[dl] \\ m & n \arrow[l, dashed] & \\ & & b \arrow[ul] \arrow[ull] \end{tikzcd}$$

Such an n is called the "supremum" or "join" of a & b in the poset $(\mathbb{N}, |)$ with the relation reversed, i.e, the inverse relation of $|$ on $\mathbb{N}$.

lastly, we restate the unanswered question from earlier before moving on.

Q: What would happen if we were to find the join of a & b in $(\mathbb{N}, |)$ without first taking the inverse relation (or equivalently, reversing the direction of arrows in the Hasse diagram)?

Road Map



Lemma: Suppose $a = qb + r$ w/ $0 \leq r < b$

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

proof: Show that the set of common divisors agree in both cases

Suppose $d \mid a$ & $d \mid b$
then $d \mid r = a - qb$

$$\left.\begin{array}{l} \text{Suppose } d \mid a \ \&\ d \mid b \\ \text{then } d \mid r = a - qb \end{array}\right\} \quad \begin{array}{c} \mathrm{Div}(a) \cap \mathrm{Div}(b) \\ \rotatebox{90}{$\subseteq$} \\ \mathrm{Div}(b) \cap \mathrm{Div}(r) \end{array}$$

(is a subset of)

Conversely, if $d \mid b$ & $d \mid r$
then $d \mid a = qb + r$

$$\left.\begin{array}{l} \text{Conversely, if } d \mid b \ \&\ d \mid r \\ \text{then } d \mid a = qb + r \end{array}\right\} \quad \begin{array}{c} \mathrm{Div}(b) \cap \mathrm{Div}(r) \\ \rotatebox{90}{$\subseteq$} \\ \mathrm{Div}(a) \cap \mathrm{Div}(b) \end{array}$$

Hence $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(b) \cap \mathrm{Div}(r)$

$\Rightarrow$ they have the same maximum element

$\therefore \quad \gcd(a,b) = \gcd(b,r) \quad \square$

Euclid's Algorithm

Q: What is $\gcd(4620, 101)$?

1) Division Algorithm $\longrightarrow q_1$ & r_1
2) Use lemma to find gcd of smaller #s
3) Division Algorithm $\longrightarrow q_2$ & r_2

⋮

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1 \cdot 75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

← Stop once there is no remainder.

gcd is <u>remainder from second to last line</u>

<u>A:</u> $\gcd(4620, 101) = \gcd(101, 75)$

$= \gcd(75, 26) = \gcd(26, 23)$

$= \gcd(23, 3) = \gcd(3, 2) = 1$

<u>Def:</u> a and b are said to be relatively prime if $\gcd(a,b) = 1$

Hence 4620 & 101 are relatively prime.

Bezout's Identity

$$a, b \in \mathbb{Z}_{>0} \Rightarrow \exists\, s, t \in \mathbb{Z} \text{ s.t.}$$

$$\gcd(a,b) = sa + tb$$

$$
\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}
$$

flip $\longmapsto$

forget first line

$$
\begin{aligned}
&\cancel{2 = 2 \cdot 1 + 0} \\
3 &= 1 \cdot 2 + 1 \\
23 &= 7 \cdot 3 + 2 \\
26 &= 1 \cdot 23 + 3 \\
75 &= 2 \cdot 26 + 23 \\
101 &= 1 \cdot 75 + 26 \\
4620 &= 45 \cdot 101 + 75
\end{aligned}
$$

gcd

rearrange

$$
\begin{aligned}
3 = 1 \cdot 2 + 1 &\longmapsto 1 = 3 - 1 \cdot 2 \\
23 = 7 \cdot 3 + 2 &\longmapsto 2 = 23 - 7 \cdot 3 \\
26 = 1 \cdot 23 + 3 &\longmapsto 3 = 26 - 1 \cdot 23 \\
75 = 2 \cdot 26 + 23 &\longmapsto 23 = 75 - 2 \cdot 26 \\
101 = 1 \cdot 75 + 26 &\longmapsto 26 = 101 - 1 \cdot 75 \\
4620 = 45 \cdot 101 + 75 &\longmapsto 75 = 4620 - 45 \cdot 101
\end{aligned}
$$

$$1 = 3 - 1\cdot 2$$
$$2 = 23 - 7\cdot 3$$
$$3 = 26 - 1\cdot 23$$
$$23 = 75 - 2\cdot 26$$
$$26 = 101 - 1\cdot 75$$
$$75 = 4620 - 45\cdot 101$$

$$\begin{aligned}
1 &= 3 - 1\cdot(23 - 7\cdot 3) \\
&= 8\cdot 3 - 1\cdot 23 \\
&= 8\cdot(26 - 1\cdot 23) - 1\cdot 23 \\
&= 8\cdot 26 - 9\cdot 23 \\
&= 8\cdot 26 - 9\cdot(75 - 2\cdot 26) \\
&= 26\cdot 26 - 9\cdot 75 \\
&= 26\cdot(101 - 1\cdot 75) - 9\cdot 75 \\
&= 26\cdot 101 - 35\cdot 75 \\
&= 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)
\end{aligned}$$

$$\boxed{1 = 1601\cdot 101 - 35\cdot 4620}$$

Express remainders as linear combinations & replace this expression in the line above it

Linear Congruence

Solve for x if

$$ax \equiv b \pmod{m}$$

Note: There may not be a solution

e.g.

$$7x \equiv 1 \pmod{7}$$

has no solution since multiples of 7 are congruent to 0 mod 7.

Q: When can we guarantee a solution?

A: If $\gcd(a,m)=1$ (i.e. a & m are relatively prime) Then $\exists!$ solution to the linear congruence

$$ax \equiv b \pmod{m}$$

The main idea:

How would we find the answer to $ax=b$? We hope $a \neq 0$ so we may divide by it to get $a^{-1}b = (a^{-1}a)x = 1 \cdot x = x$.

Solve a simpler version of the problem then try to modify the solution to work in the original situation.

Multiplicative Inverses Mod m

If $\bar{a}a \equiv 1 \pmod{m}$

then we call $\bar{a}$ an inverse of a modulo m. This is the analogue of dividing by a in modular arithmetic.

Theorem: $\gcd(a,m)=1 \Rightarrow \exists!$ inverse of a modulo m.

Proof: $\gcd(a,m)=1 \Rightarrow \exists\, s,t$ such that $sa+tm=1$. Reduce both sides of the equation modulo m to see $sa \equiv 1 \pmod m$. Hence s is the inverse of a modulo m. $\square$

The Chinese Remainder Theorem

e.g. Solve for x if

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Spoiler Alert: $x=23$ works because

$23 \bmod 3 = 2$ (remainder after division)

$23 \bmod 5 = 3$

& $23 \bmod 7 = 2$

Method 1: (back substitution) ← Not the CRT

$x \equiv 2 \pmod 3 \iff \exists k \in \mathbb{Z}$ s.t. $x = 3k+2$

$x \equiv 3 \pmod 5 \iff 3k+2 \equiv 3 \pmod 5$

(Subtract 2 from both sides) $3k \equiv 1 \pmod 5$

(gcd$(3,5)=1 \Rightarrow$ can solve for k) $k \equiv 2 \pmod 5$

$2 \cdot 3 - 5 = 1$

$$\Updownarrow$$

$\exists \tilde{k} \in \mathbb{Z}$ s.t. $k = \underline{5\tilde{k}+2}$

$$\Rightarrow x = 3k+2 = 3(5\tilde{k}+2)+2$$

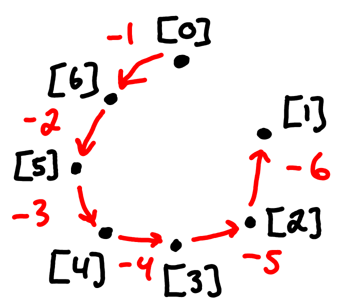
$$= 15\tilde{k}+6+2 = \underline{15\tilde{k}+8}$$

$x \equiv 2 \pmod 7$ Finally, we use the third congruence relation

$15\tilde{k}+8 \equiv 2 \pmod 7$ then solve

$15\tilde{k} \equiv -6 \pmod 7$

$15\tilde{k} \equiv 1 \pmod 7$



$\gcd(15,7)=1$ & $1 = 15 - 2\cdot 7$

Thus $\tilde{k} \equiv 1 \pmod 7 \Leftrightarrow \tilde{k} = 7\hat{k} + 1$

for some integer $\hat{k}$. Thus

$$x = 15\tilde{k} + 8 = 15(7\hat{k}+1) + 8 = 105\hat{k} + 23$$

We now have an expression for All solutions to the original system of linear congruences.

$$x \equiv 23 \pmod{105}$$

$\Rightarrow$ possible answers are

23 ← Smallest answer
128
233
.

Note:

$105 = 3\cdot 5\cdot 7$

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Theorem: (CRT)

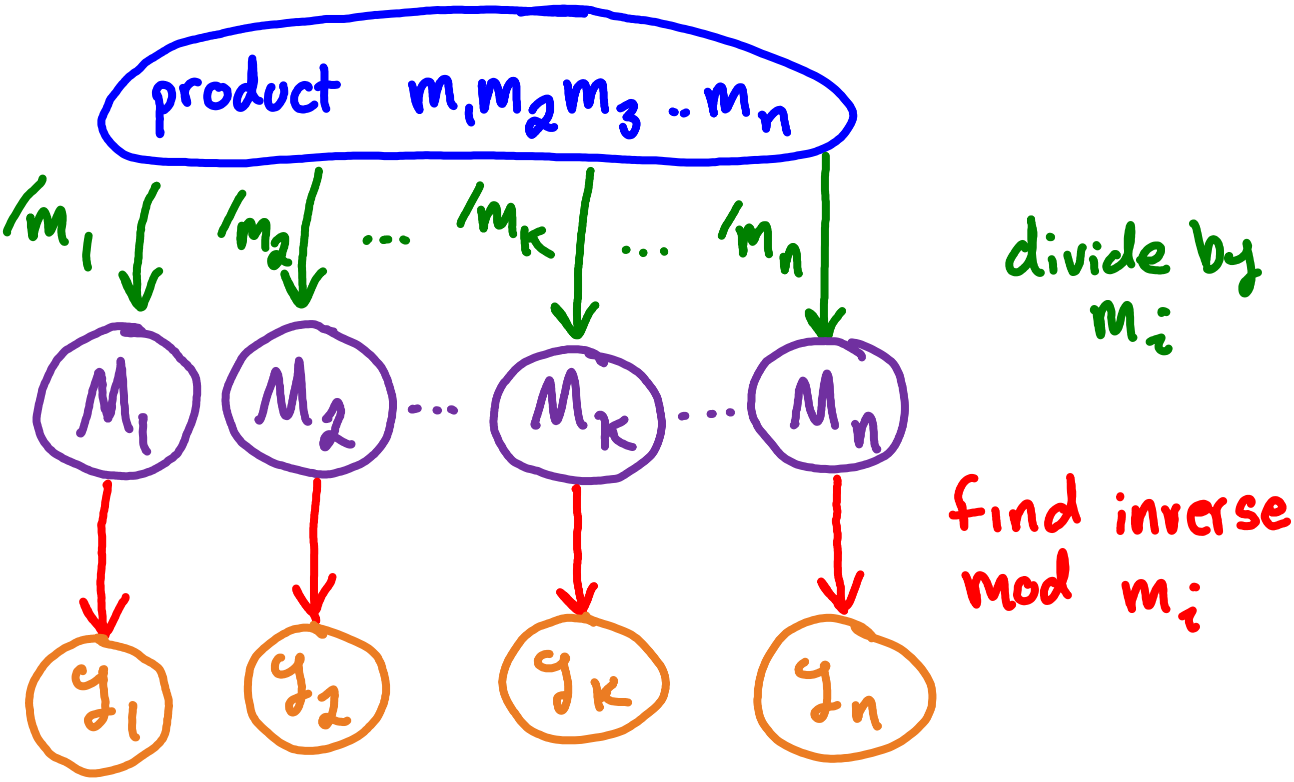
If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime (i.e. $\gcd(m_i, m_j) = 1 \;\forall i \neq j$) integers (all >1) & $a_1, a_2, \ldots, a_n$ are arbitrary integers, Then

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Has a unique solution modulo $m := m_1 \cdot m_2 \cdot \ldots \cdot m_n$

(i.e. $\exists$ solution x with $0 \leq x < m$ & all other solutions are congruent modulo m to this solution)

<u>proof:</u>



$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$$
$$= \sum_{i=1}^{n} a_i M_i y_i$$

Check that x as defined above has the desired properties.

$$x \bmod m_1 =$$

$$a_1 M_1 y_1 + \cancel{a_2 M_2 y_2} + \dots + \cancel{a_n M_n y_n} \bmod m_1$$

all terms except M_1 have a factor of m_1

thus $x \bmod m_1 = a_1 M_1 y_1 \bmod m_1$

inverses modulo m_1

Therefore $x \bmod m_1 = a_1$

[i.e. $x \equiv a_1 \pmod{m_1}$] & similar reasoning proves $x \equiv a_i \pmod{m_i}\ \forall i.$ $\square$

<u>Lets now revisit that example:</u>

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

$3 \cdot 5 \cdot 7 = 105$

$105 \xrightarrow{/3} 35$, $105 \xrightarrow{/5} 21$, $105 \xrightarrow{/7} 15$

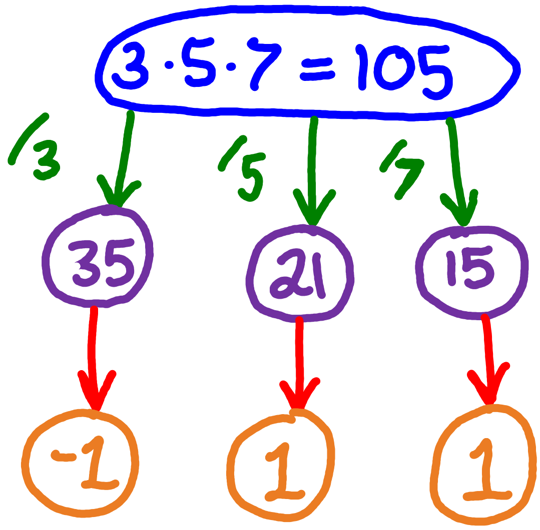
Next find inverses mod m_i

$\gcd(3, 35) = 1$ & $1 = 12 \cdot 3 - 1 \cdot 35$

$\gcd(5, 21) = 1$ & $1 = 1 \cdot 21 - 4 \cdot 5$

$\gcd(7, 15) = 1$ & $1 = 1 \cdot 15 - 2 \cdot 7$

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$



$$x := 2 \cdot 35 \cdot (-1) + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$

$$\text{(Simplify)} = -70 + 63 + 30 = \boxed{23}$$

Application: Computer Arithmetic w/ Large Integers

Computers generally run out of space to store numbers before running out of computing power. If we must carry out arithmetic w/ large numbers the Chinese Remainder Theorem (CRT) affords us the ability to exchange these numbers (which may be too big to store in the computer directly) for n-tuples of smaller numbers. The computer has an easier time computing with these n-tuples & the answer can be interpreted by translating back to a single large number by way of CRT.

(i) Select moduli $m_1, m_2, \dots, m_n$

↳ $m_i > 2 \quad \forall i \le n$

↳ $\gcd(m_i, m_j) = 1$ whenever $i \neq j$

↳ $m := m_1 m_2 \cdot \ldots \cdot m_n$ is larger than all #s we would like to do arithmetic with

(ii) Then $\forall x \le m \; \exists!$ n-tuple of integers representing x.

$$x \underset{\text{CRT}}{\overset{\text{reduce}}{\rightleftarrows}} (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_n)$$

(iii) Addition/Multiplication can be carried out component-wise

$$\boxed{\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}}$$

provided the m_i are pairwise relatively prime

★ the above is an isomorphism of "Rings" (whatever that means)