Principles of Abstract Interpretation
MIT press
Ch. **30**, Basic number theory

Patrick Cousot

pcousot.github.io

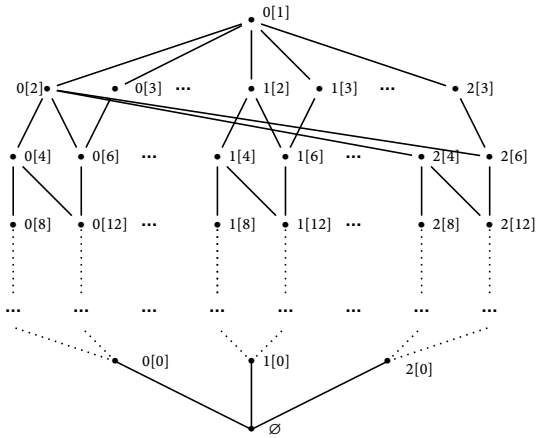
PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-30--number-theory-PrAbsInt.pdf

Chapter 30

Ch. **30**, Basic number theory

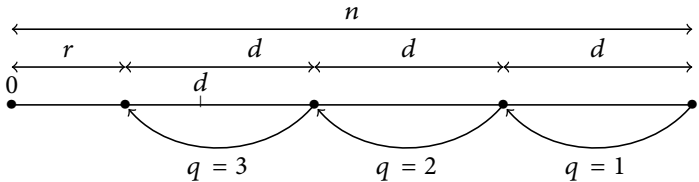
- We recall basic number theory results on Euclidean division, congruences, GCD, LCM, *etc*.
- This will allow us to define the complete lattice of congruences used in program congruence analysis ($c[m] \triangleq \{c + k.m \mid k \in \mathbb{Z}\}$)



Euclidean division

Euclidean division

- The *Euclidean division* of an integer $n \in \mathbb{Z}$ by the *divisor* $d \in \mathbb{Z} \setminus \{0\}$ is the unique pair $\langle q, r \rangle$ of a *quotient* q and *rest* r such that $n = qd + r$ with $0 \leqslant r < |d|$.



- If $r = 0$ then d *divides* n (or n is a *multiple* of d) *i.e.* $\exists q \,.\, n = qd$
- This is written $d \,/\, n$.

en.wikipedia.org/wiki/Euclid
en.wikipedia.org/wiki/Euclidean_division

Euclidean division algorithm

Euclidean division of $n \in \mathbb{N}$ by $d \in \mathbb{N}^+$ by repeated subtractions

```
# let divide n d = (* n>=0 && d>0 *)
   if n<0 || d <= 0 then failwith "divide: incorrect parameter";
   let q = ref 0 and r = ref n in
      while !r >= d do
         q := !q + 1; r := !r - d
      done;
      (!q,!r) ;;
```

```
# divide 14 3 ;;
- : int * int = (4, 2)
```

- `let x = ref e` declares a mutable variable `x` initialized to the value of expression `e`
- `!x` denotes the value of `x`
- `x := e'` is an assignment of the value of expression `e'` to the mutable variable `x`

Integer division algorithm of $n \in \mathbb{Z}$ by $d \in \mathbb{Z} \setminus \{0\}$

```
let rec Euclid n d =
   if d = 0 then if n=0 then (0,0)
                 else failwith "Euclid: division by 0"
   else if d < 0 then
      let (q,r) = Euclid n (-d) in (-q,r)
   else if n < 0 then
      let (q,r) = Euclid (-n) d in
         if r = 0 then (-q, 0)
         else (-q-1,d-r)
   else divide n d
```

```
# Euclid 0 0;;
- : int * int = (0, 0).
# Euclid 17 (-7);;
- : int * int = (-2, 3).
# Euclid (-17) (-7);;
- : int * int = (3, 4)
# Euclid (-17) 7;;
- : int * int = (-3, 4)
```

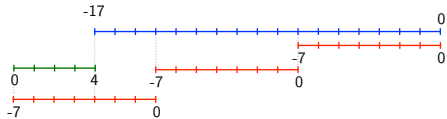
```
# Euclid 1 0;;
 Exception: Failure "Euclid: division by 0".
Euclid 15 (-3);;
 - : int * int = (-5, 0)
# Euclid (-15) 3 ;;
 - : int * int = (-5, 0)
# Euclid 17 7;;
 - : int * int = (2, 3)
```

en.wikipedia.org/wiki/Division_algorithm

Integer division algorithm

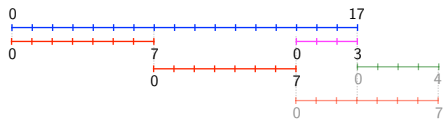
- Negative arguments

```
# Euclid (-17) (-7);;
- : int * int = (3, 4)
```



is calculated from

```
# Euclid 17 7;;
- : int * int = (2, 3)
```



Divisibility is preserved by linear combinations (Exercise 30.4)

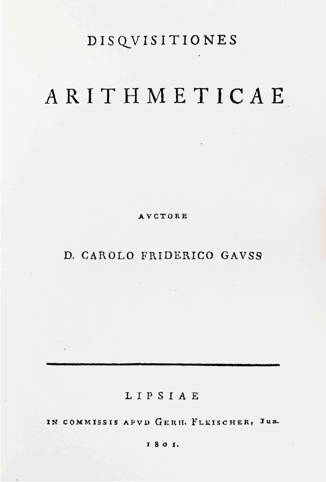
If d divides $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then d divides any integral linear combination $ux + vy$ for all $u, v \in \mathbb{Z}$

Proof

- By hypothesis, $\exists k, l \in \mathbb{Z} \,.\, x = kd \wedge y = ld$
- So $ux + vx = (uk + vl)d$ proving that $ux + vy$ is a multiple of d. □

en.wikipedia.org/wiki/Linear_combination

Congruences



DISQVISITIONES

ARITHMETICAE

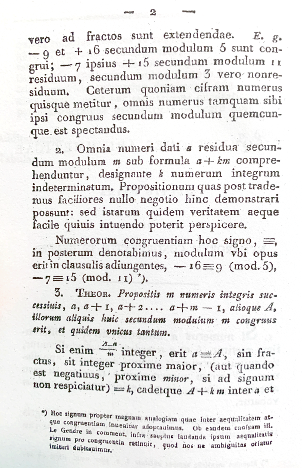
AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.



— 2 —

vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2. Omnia numeri dati a residua secundum modulum m sub formula $a+km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post trademus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quiuis intuendo poterit perspicere.

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum vbi opus erit in clausulis adiungentes, $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11) *).

3. THEOR. *Propositis m numeris integris successiuis, $a, a+1, a+2 \ldots . a+m-1$, alioque A, illorum aliquis huic secundum modulum m congruus erit, et quidem vnicus tantum.*

Si enim $\frac{A-a}{m}$ integer, erit $a \equiv A$, sin fractus, sit integer proxime maior, (aut quando est negatiuus, proxime *minor*, si ad signum non respiciatur) $= k$, cadetque $A+km$ inter a et

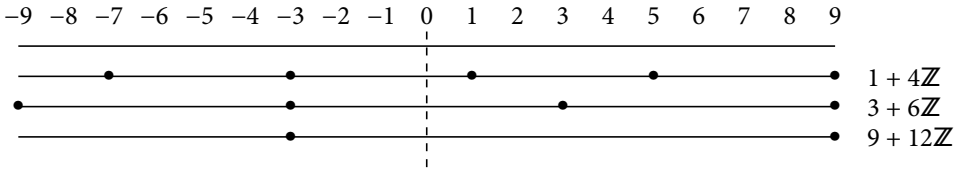
*) Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam inuenitur adoptauimus. Ob eandem caussam ill. Le Gendre in comment. infra saepius laudanda ipsum aequalitatis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur imitari dubitauimus.

Congruence classes (Section **30.2**)

- The *congruence class* of c modulo m is

$$c + m\mathbb{Z} \triangleq \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \,.\, z = c + km\}$$

- This is the set of all integers z equal to $c \in \mathbb{Z}$ modulo $m \in \mathbb{Z}$



- So m *divides* $z - c$, written $m \,/\, z - c$ or $z \equiv c \pmod{m}$.
- c is called the *residue* of z modulo m [Gavss, 1801, p. 2].
- For a given modulo m, the relation $x \equiv y \pmod{m}$ is an equivalence relation.

en.wikipedia.org/wiki/Carl_Friedrich_Gauss
en.wikipedia.org/wiki/Congruence_relation
en.wikipedia.org/wiki/Modular_arithmetic

Canonical congruences (Section **30.3**)

- The same set $c + m\mathbb{Z}$ can be defined by different residues and moduli.
- For example $2 + 4\mathbb{Z} = 6 + -4\mathbb{Z}$ since if $z = 2 + 4k$ then $z = 6 + (-4)(1 - k)$.
- A canonical representation is obtained by requiring $m \geqslant 0$ and, if $m \neq 0$, by requiring c to be the least residue such that $0 \leqslant c < m$.
- For example, $c + 1\mathbb{Z} = \mathbb{Z}$ since $\forall z \in \mathbb{Z} \,.\, \forall c \in \mathbb{Z} \,.\, z = c + 1(z - c) \Rightarrow z \equiv c \pmod 1$. Since $z = 0 + 1(z - 0)$, the least residue is 0 with $0 + 1\mathbb{Z} = \mathbb{Z}$.
- We use $\varnothing$ for the empty set which cannot be represented by a congruence class.
- In the following we leave implicit that any congruence we consider has to be normalized into one of

$$\mathbb{P}^{\equiv} \triangleq \{c + m\mathbb{Z} \mid (m = 0) \vee (m > 0 \wedge 0 \leqslant c < m)\} \cup \{\varnothing\}.$$

Greatest common divisor

Greatest common divisor

- The set of common divisors of two integers x and y, not both 0,
  - contains 1, so is not empty
  - is bounded by $|x|$ (by def. divisibility)

  so the divisors have a largest/highest/greatest element
- This greatest divisor is called the *greatest common divisor* of x and y.
- If $x = y = 0$ then all integers divide them so there is no greatest divisor
- By convention, we define $0 \gcd 0 = 0$.

en.wikipedia.org/wiki/Greatest_common_divisor

Definition of the greatest common divisor

- The *greatest common divisor* of two integers, not both 0, is the largest positive integer which divides both integers.

$$x \gcd y \triangleq \max\{z \in \mathbb{N} \mid z \,/\, x \wedge z \,/\, y\} \qquad x \neq 0 \vee y \neq 0$$
$$0 \gcd 0 \triangleq 0$$

Definition of the greatest common divisor

- The *greatest common divisor* of two integers, not both 0, is the largest positive integer which divides both integers.

$$x \gcd y \triangleq \max\{z \in \mathbb{N} \mid z \,/\, x \wedge z \,/\, y\} \qquad x \neq 0 \vee y \neq 0$$
$$0 \gcd 0 \triangleq 0$$

$x \gcd y = y \gcd x$
$(x = y) \Rightarrow (x \gcd y = x = y)$
$(x > y) \Rightarrow (x \gcd y = (x - y) \gcd y)$

$$\begin{array}{ll} & x = kz \wedge y = k'z \\ \Leftrightarrow & x = kz = y + (x - y) \wedge y = k'z \qquad \text{(with } x - y > 0 \text{ since } x > y\text{)} \\ \Leftrightarrow & kz = k'z + (x - y) \wedge y = k'z \qquad (y = k'z) \\ \Leftrightarrow & (x - y) = (k - k')z + \wedge y = k'z \end{array}$$

so $x \gcd y = \max\{z \in \mathbb{N} \mid z \,/\, x \wedge z \,/\, y\} = \max\{z \in \mathbb{N} \mid z \,/\, (x - y) \wedge z \,/\, y\} = (x - y) \gcd y$

Greatest common divisor algorithm

The following algorithm computes $x \gcd y$, $x, y \in \mathbb{Z}$.

```
# let rec gcd x y = if (x=0) && (y=0) then 0
                    else if (x=0) then y
                    else if (y=0) then x
                    else if (x<0) || (y<0) then gcd (abs x) (abs y)
                    else if x > y then gcd (x-y) y
                    else if x = y then x
                    else gcd x (y-x)


# gcd 9 15;;
  gcd 9 6;;
  gcd 3 6;;
  gcd 3 3;;
- : int = 3
#
```

en.wikipedia.org/wiki/Euclidean_algorithm

Bachet-Bézout identity

Bachet-Bézout identity

The following theorem is due to Claude-Gaspard Bachet de Méziriac [Méziriac, 1624, proposition XVIII] and was generalized by Étienne Bézout [Bézout, 1764] to polynomials.

Theorem 30.7 Let a and b be integers.

(1) There exist (non-unique) Bézout coefficients $x, y \in \mathbb{Z}$ such that $ax+by = a \gcd b$.

(2) Moreover, $a \gcd b$ is the smallest positive integer that can be written as $ax + by$.

(3) Any integer of the form $ax + by$ is a multiple of the greatest common divisor $a \gcd b$. □

$9 \gcd 15 = 3$

$9 \times 2 + 15 \times (-1) = 3 \qquad x = 2, y = -1$

$9 \times (-3) + 15 \times 2 = 3 \qquad x = 3, y = 2$

en.wikipedia.org/wiki/Bézout's_identity, en.wikipedia.org/wiki/Étienne_Bézout, en.wikipedia.org/wiki/Claude_Gaspar_Bachet_de_Méziriac

Proof of Theorem 30.7

- If $a = b = 0$ then $ax + by = a \gcd b = 0 \gcd 0 = 0$ by choosing *e.g.* $x = y = 0$.
- If $a = 0$, $b \neq 0$ then $ax + by = by = 0 \gcd b = b$ by choosing $y = 1$.
- Same when $b = 0$ and $a \neq 0$.
- Otherwise $a \neq 0$ and $b \neq 0$.

Case $a \neq 0$ and $b \neq 0$

- Let $S = \{ax + by \in \mathbb{N}^+ \mid x, y \in \mathbb{Z}\}$ be the set of integral positive linear combinations of a and b.
- $|a| \in S$ so S is not empty.
- Because $S \subseteq \mathbb{N}^+$, S is well-founded, and therefore S has a minimal element $m \in S$.
- By def. of S, there exists $u, v \in \mathbb{Z}$ such that $m = au + bv$.
- By Euclidean division we have $a = mq + r$ where $0 \leqslant r < m$. Assume by contradiction that $r > 0$.
- Then $r = a - mq = a - (au + bv)q = a(1 - qu) + b(vq) > 0$ proving that $r \in S$ (for $x = 1 - qu$ and $y = vq$) in contradiction with $r < m$ and m is the minimum of S.
- So $r = 0$ proving that m divides a.
- Similarly m divides b.

- By definition $a \gcd b$ is the greatest divisor of both a and b so $m \leqslant a \gcd b$.
- $a \gcd b$ divides both a and b
- So $a \gcd b$ divides $au + bv = m$
- So $a \gcd b \leqslant m$.
- By antisymmetry, $au + bv = m = a \gcd b$.
- Proving (1).

(2)

- If $i = ax + by > 0$ then $i \in S$ so $a \gcd b = m \leqslant i$ since m is minimal in S,
- So $a \gcd b$ is the smallest positive integer that can be written as $ax + by$.

(3)

- If $i = ax + by \in S$ then $a \gcd b$ divides a and b so divides $ax + by = i$
- So i is a multiple of $a \gcd b$. □

Extended Euclidean division

Extended Euclidean division

Compute the Bézout coefficients of any two integers a and b (using Euclid division). Assume that $a \geqslant b \geqslant 0$.

$r_0 = a$	$x_0 = 1$	$y_0 = 0$
$r_1 = b$	$x_1 = 0$	$y_1 = 1$
r_2 s.t. $r_0 = r_1 q_1 + r_2,\ 0 < r_2 < r1$	$x_2 = x_0 - x_1 q_1$	$y_2 = y_0 - y_1 q_1$
...		
r_{k+1} s.t. $r_{k-1} = r_k q_k + r_{k+1},\ 0 < r_{k+1} < r_k$	$x_{k+1} = x_{k-1} - x_k q_k$	$y_{k+1} = y_{k-1} - y_k q_k$
...		
r_ℓ s.t. $r_{\ell-1} = r_\ell q_\ell + r_{\ell+1},\ r_{\ell+1} = 0$	$x_\ell = x_{\ell-2} - x_{\ell-1} q_{\ell-1}$	$y_\ell = y_{\ell-2} - y_{\ell-1} q_{\ell-1}$
$r_{\ell+1} = 0$	$x_{\ell+1} = x_{\ell-1} - x_\ell q_\ell$	$y_{\ell+1} = y_{\ell-1} - y_\ell q_\ell$

Theorem 30.8 $r_\ell = a x_\ell + b y_\ell = a \gcd b$.

en.wikipedia.org/wiki/Extended_Euclidean_algorithm

Proof of Theorem 30.8 — Termination

- By the correctness of Euclid's algorithm, the sequence $\langle r_k,\ k \in \mathbb{N} \rangle$ is well-defined
- It is positive and strictly decreasing so finite.
- The sequence continues while $r_k > 0$
- So it must end at some limit r_ℓ with $r_{\ell+1} = 0$. □

— $r_\ell = a \gcd b$

- By recurrence, we have $a \gcd b = r_0 \gcd r_1 = \ldots = r_k \gcd r_{k+1} = \ldots = r_\ell \gcd r_\ell + 1 = r_\ell \gcd 0 = r_\ell$
  - For the basis, $r_0 = a$ and $r_1 = b$
  - For the induction step,

$$\begin{aligned} & r_{k-1} \gcd r_k \\ = \; & r_k q_k + r_{k+1} \gcd r_k && \text{(since } r_{k-1} = r_k q_k + r_{k+1}\text{)} \\ = \; & r_k \gcd r_{k+1} && \text{(simplification)} \end{aligned}$$

- Recall that divisibility is preserved by linear combinations (Exercise 30.4)
- It follows that the common divisors of r_{k-1} and r_k are the same as the common divisors of r_k and r_{k+1}.
- For the limit, $r_{\ell+1} = 0$ so $r_\ell = a \gcd b$.

— Let us prove by recurrence that $\forall k \in [0, \ell + 1] \,.\, ax_k + by_k = r_k$.

- For the basis, we have $ax_0 + by_0 = a \times 1 + b \times 0 = a = r_0$.
- For the induction step, we have

$$
\begin{aligned}
& ax_{k+1} + by_{k+1} \\
&= a(x_{k-1} - x_k q_k) + b(y_{k-1} - y_k q_k) && \text{(def. } x_{k+1} \text{ and } y_{k+1}\text{)} \\
&= ax_{k-1} + by_{k-1} - (ax_k + by_k)q_k \\
&= r_{k-1} - r_k q_k && \text{(ind. hyp.)} \\
&= r_{k+1} && \text{(def. } r_{k+1}\text{)}
\end{aligned}
$$

— In conclusion, combining the two previous results

- $r_\ell = a \gcd b$
- $\forall k \in [0, \ell + 1] \,.\, ax_k + by_k = r_k$.

we have $ax_\ell + by_\ell = a \gcd b$. □

Extended Euclidean division algorithm (Exercise 30.9)

The following algorithm returns $a \gcd b = ax + by$.

```
let rec bezout a b =
  if a=0 || b=0 then (0,0,0)
  else if a<0 then let (r,x,y) = bezout (-a) b in (r,-x,y)
  else if b<0 then let (r,x,y) = bezout a (-b) in (r,x,-y)
  else let r = ref a and r' = ref b
  and x  = ref 1 and  y  = ref 0
  and x' = ref 0 and  y' = ref 1 in
     while !r' <> 0 do
        (* r = ax+by et r' = ax'+by' *)
        let (q,_) = divide !r !r'
        and nr = !r and nx = !x and ny = !y in (* a,b > 0 *)
           r := !r'; x := !x'; y := !y';
           r' := nr - q*(!r'); x' := nx - q*(!x'); y' := ny - q*(!y)
     done;
     (!r, !x, !y) (* r = (a gcd b) = ax+by *)
```

Least common multiple

Least common multiple

The *least common multiple* of two integers is the least natural number which is divisible by both integers.

$$x \operatorname{lcm} y \triangleq \min\{z \in \mathbb{N} \mid x \,/\, z \wedge y \,/\, z\} \qquad x, y \neq 0$$

en.wikipedia.org/wiki/Least_common_multiple

Exercise 30.10

A congruence holds for two different moduli if and only if it holds for their least common multiple.

Proof

$$
\begin{aligned}
& x \equiv y \pmod{m} \wedge x \equiv y \pmod{n} \\
\Leftrightarrow\ & m \mid (x - y) \wedge n \mid (x - y) && \text{⟅def. congruence⟆} \\
\Leftrightarrow\ & m \operatorname{lcm} n \mid (x - y) && \text{⟅the least common multiple divides all other common multiples⟆} \\
\Leftrightarrow\ & x \equiv y \pmod{m \operatorname{lcm} n} && \text{⟅def. congruence⟆} \quad \square
\end{aligned}
$$

Computing the least common multiple using the greatest common divisor

Lemma 1 $(x \gcd y)(x \operatorname{lcm} y) = |xy|$ □

en.wikipedia.org/wiki/Least_common_multiple

Proof of Lemma 1 Let $g = x \gcd y$.
$g \mid a$ and $g \mid b$ implies $g \mid ab$ that is $\exists n \in \mathbb{N} \,.\, gn = xy$.
— n is a multiplier

- $g \mid x$ and $g \mid y$ imply $\exists u, v \in \mathbb{Z} \,.\, gu = x \wedge vg = y$
- So $gn = xgv = guy$ hence $n = xv = uy$
- So $x \mid n$ and $y \mid n$
- Therefore n is a multiplier of x and y.

— n is the least multiplier

- Consider another one m such that $x \mid m$ and $y \mid m$
- Then $\exists r, s \in \mathbb{Z} \,.\, rx = m \wedge sy = m$.
- By Bachet-Bézout identity Theorem 30.7, we have $a, b \in \mathbb{Z}$ such that $xa + yb = x \gcd y = g$.
- It follows that $mg = mxa + myb = syxa + rxyb = xy(sa + rb) = gn(sa + rb)$
- So $m = n(sa + rb)$
- Therefore $n \mid m$
- Hence $n \leqslant |m|$
- Proving that $n = x \operatorname{lcm} y$.

— In conclusion, we have $xy = gn = x \gcd yx \operatorname{lcm} y$ so $|xy| = x \gcd yx \operatorname{lcm} y$ since $x \gcd y$ and $x \operatorname{lcm} y$ are positive. □

Least common multiple algorithm

The following `lcm` algorithm returns $x \operatorname{lcm} y$ for $x, y \in \mathbb{Z}$.

```
let lcm x y = if (x=0) && (y=0) then 0
              else (abs(x) / (gcd x y)) * abs(y)
```

Because $x \gcd y$ is a divisor of both x and y, computing the $x \operatorname{lcm} y$ by dividing before multiplying manipulates smaller integers:

$$\operatorname{lcm}(x, y) = \left(\frac{|x|}{x \gcd y}\right) \cdot |y| = \left(\frac{|y|}{x \gcd y}\right) \cdot |x|$$

en.wikipedia.org/wiki/Least_common_multiple

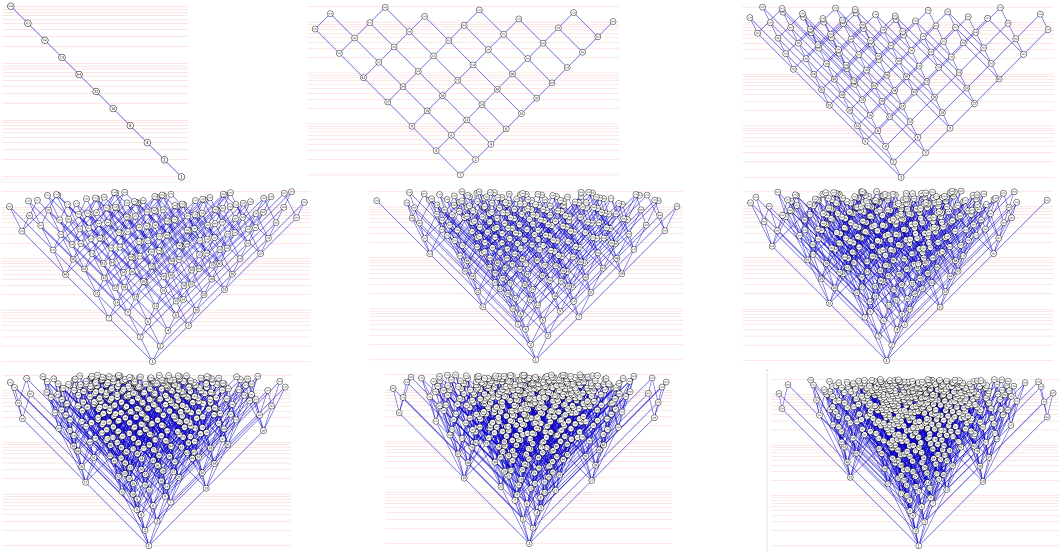
Divisibility lattice

Extend divisibility by

- $\forall x \,.\, x \,/\, 0$,
- $x \operatorname{lcm} 0 = 0 \operatorname{lcm} x = 0$,
- $x \gcd 0 = 0 \gcd x = x$.

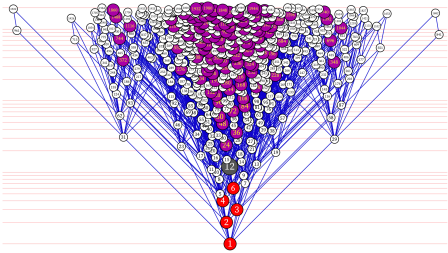
Then $\langle \mathbb{N},\ /,\ 1,\ 0,\ \operatorname{lcm},\ \gcd \rangle$ is a complete lattice

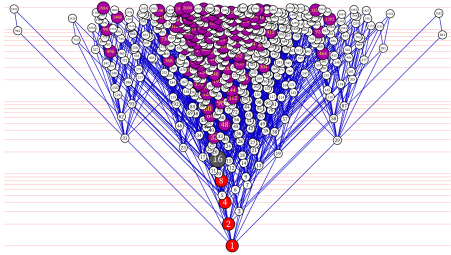
Multiples of $\{2\}$, $\{2,3\}$, $\{2,3,5\}$, ..., $\{2,3,5,7,11,13,17,19,23\}$, ..., divisibility lattice

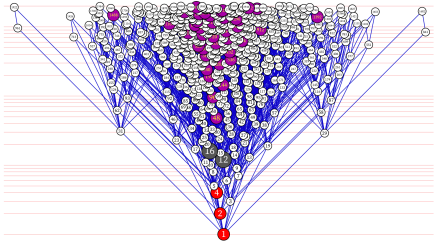


observablehq.com/@bryangingechen/divisibility-lattice

divisors, multiples, gcd, lcm







observablehq.com/@bryangingechen/divisibility-lattice

Conclusion

Conclusion

- The theory of congruences was initiated by Carl Friedrich Gauss [Gavss, 1801] (and we still use his notations), [Ore, 1948, Ch. 9].
- Mathematics books on congruences: [Hardy and Wright, 2008; Ore, 1948; Shoup, 2008; Vinogradov, 2016], *etc*.
- Congruences are used in the cartesian integer congruence static analysis of next Chapter **31**.

Bibliography I

Bézout, Étienne (1764). *Recherches sur le degré des équations résultantes de l'évanouissement des inconnues et sur les moyens qu'on doit employer pour trouver ces équations*. Mémoires de l'Académie Royale des Sciences, pp. 288–338.

Gavss, Carolo Friderico (1801). *Disqvisitiones Arithmeticæ*. English translation Arthur A. Clarke: Disquisitiones Arithmeticae, Yale University Press, 1966. Gerh. Fleischer, Lipsiae.

Hardy, Godfrey H. and Edward M. Wright (2008). *An introduction to theory of numbers*. 6th ed. Oxford University Press.

Méziriac, Claude-Gaspard Bachet de (1624). *Problèmes plaisans et délectables qui se font par les nombres*. 2nd ed. Pierre Rigaud & Associez. URL: http://gallica.bnf.fr/ark:/12148/bpt6k5818046p/f35.image.r=.langFR.

Ore, Oystein (1948). *Number Theory and its History*. Dover Books in Mathematics. Dover Pub., Inc., New York.

Bibliography II

Shoup, Victor (2008). *A computational introduction to number theory and algebra*. 2nd ed. Cambridge University Press. URL: http://www.shoup.net/ntb/ntb-v2.pdf.

Vinogradov, Ivan Matveevich (2016). *Elements of Number Theory*. Dover Publications.

Home work

Read Ch. **30** "Basic number theory", in particular the proofs, in

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you