Divisibility in $\mathbb{Z}$

UNIVERSITY OF TORONTO

January 28th, 2021

Divisibility – 1

Definition: divisibility

Given $a, b \in \mathbb{Z}$, we write $b|a$ if $\exists k \in \mathbb{Z},\ a = bk$.
We say that *"a is divisible by b"* or *"b is divisor of a"* or *"a is a multiple of b"*.

Divisibility – 1

Definition: divisibility

Given $a, b \in \mathbb{Z}$, we write $b|a$ if $\exists k \in \mathbb{Z},\ a = bk$.
We say that *"a is divisible by b"* or *"b is divisor of a"* or *"a is a multiple of b"*.

Examples

- $(-5)|10$
- $5 \nmid (-11)$

Divisibility – 1

Definition: divisibility

Given $a, b \in \mathbb{Z}$, we write $b|a$ if $\exists k \in \mathbb{Z},\ a = bk$.
We say that *"a is divisible by b"* or *"b is divisor of a"* or *"a is a multiple of b"*.

Examples

- $(-5)|10$
- $5 \nmid (-11)$

Remarks

- When $b \neq 0$, $b|a$ if and only if the remainder of the Euclidean division of a by b is 0.
- Any integer is a divisor of 0, i.e $\forall b \in \mathbb{Z},\ b|0$.
  Indeed, $0 = b \times 0$.
- Any integer is divisible by 1 and itself, i.e. $\forall a \in \mathbb{Z},\ 1|a$ and $a|a$.
  Indeed, $a = 1 \times a = a \times 1$.
- The only integer divisible by 0 is 0, i.e. $\forall a \in \mathbb{Z},\ 0|a \implies a = 0$.
  Indeed, then $a = 0 \times k$ for some $k \in \mathbb{Z}$ and hence $a = 0$.

Divisibility – 2

Proposition

1. $\forall a, b \in \mathbb{Z},\ \big(a|b \text{ and } b|a\big) \implies |a| = |b|$
2. $\forall a, b, c \in \mathbb{Z},\ \big(a|b \text{ and } b|c\big) \implies a|c$
3. $\forall a, b, c, d \in \mathbb{Z},\ \big(a|b \text{ and } c|d\big) \implies ac|bd$
4. $\forall a, b, c, \lambda, \mu \in \mathbb{Z},\ \big(a|b \text{ and } a|c\big) \implies a|(\lambda b + \mu c)$
5. $\forall a \in \mathbb{Z},\ a|1 \implies |a| = 1$

Divisibility – 3

Proof.

1. $\forall a, b \in \mathbb{Z},\ \big(a|b \text{ and } b|a\big) \implies |a| = |b|$
   Let $a, b \in \mathbb{Z}$ satisfying $a|b$ and $b|a$. If $a = 0$ then $b = 0$ (from $0|b$). So we may assume that $a \neq 0$.
   There exist $k, l \in \mathbb{Z}$ such that $b = ak$ and $a = bl$. Then $a = bl = akl$, thus $1 = kl$ since $a \neq 0$.
   Therefore, $1 = |1| = |kl| = |k| \times |l|$. Since $|k|, |l| \in \mathbb{N}$, we get that $|k| = |l| = 1$.
   Finally, $|a| = |bl| = |b| \times |l| = |b| \times 1 = |b|$.
2. $\forall a, b, c \in \mathbb{Z},\ \big(a|b \text{ and } b|c\big) \implies a|c$
   Let $a, b, c \in \mathbb{Z}$ satisfying $a|b$ and $b|c$. Then $b = ak$ and $c = bl$ for some $k, l \in \mathbb{Z}$.
   Therefore $c = bl = akl$, so $a|c$.
3. $\forall a, b, c, d \in \mathbb{Z},\ \big(a|b \text{ and } c|d\big) \implies ac|bd$
   Let $a, b, c, d \in \mathbb{Z}$ satisfying $a|b$ and $c|d$. Then $b = ak$ and $d = cl$ for some $k, l \in \mathbb{Z}$.
   Therefore $bd = ackl$, so $ac|bd$.
4. $\forall a, b, c, \lambda, \mu \in \mathbb{Z},\ \big(a|b \text{ and } a|c\big) \implies a|(\lambda b + \mu c)$
   Let $a, b, c \in \mathbb{Z}$ satisfying $a|b$ and $a|c$. Then $b = ka$ and $c = la$ for some $k, l \in \mathbb{Z}$.
   Hence $\lambda b + \mu c = \lambda ka + \mu la = (\lambda k + \mu l)a$. Thus $a|(\lambda b + \mu c)$.
5. $\forall a \in \mathbb{Z},\ a|1 \implies |a| = 1$
   Let $a \in \mathbb{Z}$. Assume that $a|1$. Then $a|1$ and $1|a$. So by the first item, $|a| = 1$. ∎

Greatest common divisor – 1

Theorem

Given $a, b \in \mathbb{Z}$ not both zero, the set common divisors of a and b admits a greatest element denoted $\gcd(a, b)$ and called the *greatest common divisor of a and b*.

Greatest common divisor – 1

Theorem

Given $a, b \in \mathbb{Z}$ not both zero, the set common divisors of a and b admits a greatest element denoted $\gcd(a, b)$ and called the *greatest common divisor of a and b*.

Proof. Let $a, b \in \mathbb{Z}$ not both zero. We set $S = \left\{d \in \mathbb{Z} \ : \ d|a \text{ and } d|b\right\}$.

- S is non-empty since it contains 1.
- Without loss of generality, let assume that $a \neq 0$.
  Let $d \in S$ then $a = dk$ for some $k \in \mathbb{Z}$. Note that $k \neq 0$ (otherwise $a = dk = 0$), hence $1 \leq |k|$.
  Thus $d \leq |d| \leq |d| \times |k| = |dk| = |a|$.
  Hence S is bounded from above by $|a|$.

Therefore, S admits a greatest element (as an non-empty subset of $\mathbb{Z}$ bounded from above). ■

Greatest common divisor – 1

Theorem

Given $a, b \in \mathbb{Z}$ not both zero, the set common divisors of a and b admits a greatest element denoted $\gcd(a, b)$ and called the *greatest common divisor of a and b*.

Proof. Let $a, b \in \mathbb{Z}$ not both zero. We set $S = \left\{ d \in \mathbb{Z} \ : \ d|a \text{ and } d|b \right\}$.

- S is non-empty since it contains 1.
- Without loss of generality, let assume that $a \neq 0$.
  Let $d \in S$ then $a = dk$ for some $k \in \mathbb{Z}$. Note that $k \neq 0$ (otherwise $a = dk = 0$), hence $1 \leq |k|$.
  Thus $d \leq |d| \leq |d| \times |k| = |dk| = |a|$.
  Hence S is bounded from above by $|a|$.

Therefore, S admits a greatest element (as an non-empty subset of $\mathbb{Z}$ bounded from above). ■

Remark

Note that $\gcd(a, b) \geq 1$ since 1 is a common divisor of a and b (particularly $\gcd(a, b) \in \mathbb{N}$).

Greatest common divisor – 2

Given $a, b \in \mathbb{Z}$ not both zero and $d \in \mathbb{N} \setminus \{0\}$, how do we prove that $d = \gcd(a, b)$?

Quite often the strategy is the following:

1. Prove: $d|a$.
2. Prove: $d|b$.
3. Prove: $\forall \delta \in \mathbb{N}, \left(\delta|a \text{ and } \delta|b\right) \implies \delta|d$.

Indeed, then d is a common divisor of a and b by the first two steps.
And it is the greatest one by the last step, as we show below.
Let $\delta \in \mathbb{Z}$ be a common divisor of a and b.

- If $\delta \leq 0$ then $\delta \leq d$.
- If $\delta > 0$ then $d = \delta k$ for some $k \in \mathbb{Z}$.
  Note that $k \geq 1$ since $d, \delta > 0$.
  Thus $\delta \leq \delta k = d$

Bézout's identity – 1

Theorem: Bézout's identity

Given $a, b \in \mathbb{Z}$ not both zero, there exist $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Bézout's identity – 1

Theorem: Bézout's identity

Given $a, b \in \mathbb{Z}$ not both zero, there exist $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Example

$\gcd(15, 25) = 5 = 15 \times 2 + 25 \times (-1)$

Bézout's identity – 1

Theorem: Bézout's identity

Given $a, b \in \mathbb{Z}$ not both zero, there exist $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Example

$\gcd(15, 25) = 5 = 15 \times 2 + 25 \times (-1)$

Remarks

- The couple (u, v) is not unique:
$$\begin{aligned} 5 &= 15 \times 27 + 25 \times (-16) \\ &= 15 \times 2 \quad + 25 \times (-1) \end{aligned}$$
- The converse is false: $2 = 3 \times 4 + 5 \times (-2)$ but $\gcd(3, 5) = 1 \neq 2$.
Nonetheless, we will see later that there is a partial converse when $\gcd(a, b) = 1$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ : \ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ :\ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ : \ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.
- Let's prove that $d = \gcd(a, b)$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ :\ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.
- Let's prove that $d = \gcd(a, b)$.
  - Euclidean division: $\exists q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < |d| = d$.
    Assume by contradiction that $r \neq 0$.
    Then $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$ is in S.
    Contradiction with d being the least element of S.
    Hence $r = 0$ and $a = dq$, i.e. $d | a$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ :\ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.
- Let's prove that $d = \gcd(a, b)$.
  - Euclidean division: $\exists q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < |d| = d$.
    Assume by contradiction that $r \neq 0$.
    Then $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$ is in S.
    Contradiction with d being the least element of S.
    Hence $r = 0$ and $a = dq$, i.e. $d|a$.
  - Similarly $d|b$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\}\ :\ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.
- Let's prove that $d = \gcd(a, b)$.
  - Euclidean division: $\exists q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < |d| = d$.
    Assume by contradiction that $r \neq 0$.
    Then $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$ is in S.
    Contradiction with d being the least element of S.
    Hence $r = 0$ and $a = dq$, i.e. $d|a$.
  - Similarly $d|b$.
  - Let $\delta \in \mathbb{N}$ be another common divisor of a and b.
    Then there $\exists k, l \in \mathbb{Z},\ a = \delta k,\ b = \delta l$. Hence $d = au + bv = \delta(ku + lv)$.
    Therefore $\delta|d$.

Bézout's identity – 2

Proof of Bézout's identity. Let $a, b \in \mathbb{Z}$ not both zero. We want to show $\exists u, v \in \mathbb{Z},\ au + bv = \gcd(a, b)$.

- Set $S = \{n \in \mathbb{N} \setminus \{0\} \ : \ \exists u, v \in \mathbb{Z},\ n = au + bv\}$.
- Note that $|a| + |b| > 0$ since at least one is non-zero.
  Then $|a| + |b| = a \times (\pm 1) + b \times (\pm 1) \in S$. So $S \neq \varnothing$.
  Thus, by the well-ordering principle, S admits a least element d.
  Since $d \in S$, $d = au + bv$ for some $u, v \in \mathbb{Z}$.
- Let's prove that $d = \gcd(a, b)$.
  - Euclidean division: $\exists q, r \in \mathbb{Z}$ such that $a = dq + r$ and $0 \leq r < |d| = d$.
    Assume by contradiction that $r \neq 0$.
    Then $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$ is in S.
    Contradiction with d being the least element of S.
    Hence $r = 0$ and $a = dq$, i.e. $d|a$.
  - Similarly $d|b$.
  - Let $\delta \in \mathbb{N}$ be another common divisor of a and b.
    Then there $\exists k, l \in \mathbb{Z},\ a = \delta k,\ b = \delta l$. Hence $d = au + bv = \delta(ku + lv)$.
    Therefore $\delta | d$.
- According to Slide 6, we proved that d is the greatest common divisor of a and b. ■

Properties of the gcd – 1

Proposition

$\forall a \in \mathbb{Z} \setminus \{0\}, \operatorname{gcd}(a, 0) = |a|$

Properties of the gcd – 1

Proposition

$\forall a \in \mathbb{Z} \setminus \{0\}, \gcd(a,0) = |a|$

Proof.
By definition, $\gcd(a,0)$ is the greatest divisor of a.
Since $a = |a| \times (\pm 1)$, we know that $|a|$ is a divisor of a. We have to check that it is the greatest one.
Let d be a non-negative divisor of a, then $a = dk$ for some $k \in \mathbb{Z}$.
Since $a \neq 0$, we know that $k \neq 0$.
Hence $1 \leq |k|$ from which we get that $d \leq d|k| = |d| \times |k| = |dk| = |a|$. ∎

Properties of the gcd – 2

Proposition

Let $a, b \in \mathbb{Z}$ not both zero, then

1. $\gcd(a, b) = \gcd(b, a)$
2. $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$
3. $\forall \delta \in \mathbb{Z},\ \left(\delta | a \text{ and } \delta | b\right) \implies \delta | \gcd(a, b)$
4. $\forall \lambda \in \mathbb{Z} \setminus \{0\},\ \gcd(\lambda a, \lambda b) = |\lambda| \gcd(a, b)$
5. $\forall k \in \mathbb{Z},\ \gcd(a + kb, b) = \gcd(a, b)$

Properties of the gcd – 2

Proposition

Let $a, b \in \mathbb{Z}$ not both zero, then

1. $\gcd(a,b) = \gcd(b,a)$
2. $\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$
3. $\forall \delta \in \mathbb{Z}, \ \left(\delta | a \text{ and } \delta | b\right) \implies \delta | \gcd(a,b)$
4. $\forall \lambda \in \mathbb{Z} \setminus \{0\}, \ \gcd(\lambda a, \lambda b) = |\lambda| \gcd(a,b)$
5. $\forall k \in \mathbb{Z}, \ \gcd(a+kb, b) = \gcd(a,b)$

Proof.

3. Let $a, b \in \mathbb{Z}$. Let $\delta \in \mathbb{Z}$. Assume that $\delta | a$ and $\delta | b$.
   By Bézout's theorem, $\gcd(a,b) = au + bv$ for some $u, v \in \mathbb{Z}$.
   Since $\delta | a$ and $\delta | b$, we have that $\delta \big| au + bv = \gcd(a,b)$.

4. Let $a, b \in \mathbb{Z}$ let $\lambda \in \mathbb{Z} \setminus \{0\}$. Since $|\lambda|$ divides λa and λb, then it divides $\gcd(\lambda a, \lambda b)$ by the third item.
   Hence $\gcd(\lambda a, \lambda b) = |\lambda| \times d$ for some $d \in \mathbb{Z}$. Let's prove that $d = \gcd(a,b)$.
   Let $n \in \mathbb{Z}$, then $n \big| a, b \Leftrightarrow |\lambda| n \big| \lambda a, \lambda b \Leftrightarrow |\lambda| n \big| \gcd(\lambda a, \lambda b) \Leftrightarrow n \big| d$.

5. Let $a, b, k \in \mathbb{Z}$. $\gcd(a,b) | a, b$ hence $\gcd(a,b) | a + kb$. Thus $\gcd(a,b) | \gcd(a+kb, b)$.
   Similarly, $\gcd(a+kb, b) | a+kb, b$ hence $\gcd(a+kb,b) | a + kb - kb = a$. Thus $\gcd(a+kb,b) | \gcd(a,b)$.
   Hence $|\gcd(a+kb,b)| = |\gcd(a,b)|$. Since they are both non-negative, we get $\gcd(a+kb,b) = \gcd(a,b)$. ∎

How to compute the gcd? Euclid's algorithm! – 1

Result: $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ not both zero.

$a \leftarrow |a|$

$b \leftarrow |b|$

while $b \neq 0$ **do**

  $r \leftarrow a\%b$ *(the remainder of the Euclidean division* $a = bq + r$ *with* $0 \leq r < b$*)*

  $a \leftarrow b$

  $b \leftarrow r$

end

return a

How to compute the gcd? Euclid's algorithm! – 1

Result: $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ not both zero.
$a \leftarrow |a|$
$b \leftarrow |b|$
while $b \neq 0$ **do**
    $r \leftarrow a\%b$ *(the remainder of the Euclidean division* $a = bq + r$ *with* $0 \leq r < b$*)*
    $a \leftarrow b$
    $b \leftarrow r$
end
return a

Why does it work?

1. **Initialization:** $\gcd(|a|, |b|) = \gcd(a, b)$ so we reduce to the case $a, b \geq 0$.
2. **Inductive step:** $\gcd(a, b) = \gcd(bq + r, b) = \gcd(r, b) = \gcd(b, r)$.
   At the end of the loop, $a > 0$ and $b \geq 0$ is decreasing since $0 \leq b < r$.
   So $b = 0$ after finitely many steps.
3. **Termination:** then $\gcd(a, b) = \gcd(a, 0) = a$ since $a > 0$.

How to compute the gcd? Euclid's algorithm! – 1

Result: $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ not both zero.
$a \leftarrow |a|$
$b \leftarrow |b|$
while $b \neq 0$ **do**
    $r \leftarrow a\%b$ *(the remainder of the Euclidean division* $a = bq + r$ *with* $0 \leq r < b$*)*
    $a \leftarrow b$
    $b \leftarrow r$
end
return a

Why does it work?

1. **Initialization:** $\gcd(|a|, |b|) = \gcd(a, b)$ so we reduce to the case $a, b \geq 0$.
2. **Inductive step:** $\gcd(a, b) = \gcd(bq + r, b) = \gcd(r, b) = \gcd(b, r)$.
   At the end of the loop, $a > 0$ and $b \geq 0$ is decreasing since $0 \leq b < r$.
   So $b = 0$ after finitely many steps.
3. **Termination:** then $\gcd(a, b) = \gcd(a, 0) = a$ since $a > 0$.

See the lecture notes for a version without pseudo-code.

How to compute the gcd? Euclid's algorithm! – 2

We want to compute $\gcd(600, -136)$:

$$\begin{array}{ccccccc|ll}
 & & & & & & & a_0 = 600, & b_0 = 136 \\
600 & = & 136 & \times & 4 & + & 56 & a_1 = 136, & b_1 = 56 \\
136 & = & 56 & \times & 2 & + & 24 & a_2 = 56, & b_2 = 24 \\
56 & = & 24 & \times & 2 & + & 8 & a_3 = 24, & b_3 = 8 \\
24 & = & 8 & \times & 3 & + & 0 & a_4 = 8, & b_4 = 0
\end{array}$$

Hence $\gcd(600, -136) = 8$.

How to compute the gcd? Euclid's algorithm! – 2

We want to compute $\gcd(600,-136)$:

$$\begin{array}{ccccccc|ll} & & & & & & & a_0 = 600, & b_0 = 136 \\ 600 & = & 136 & \times & 4 & + & 56 & a_1 = 136, & b_1 = 56 \\ 136 & = & 56 & \times & 2 & + & 24 & a_2 = 56, & b_2 = 24 \\ 56 & = & 24 & \times & 2 & + & 8 & a_3 = 24, & b_3 = 8 \\ 24 & = & 8 & \times & 3 & + & 0 & a_4 = 8, & b_4 = 0 \end{array}$$

Hence $\gcd(600,-136)=8$.

Remark

Then it is possible to obtain a suitable Bézout's identity going backward.

$$\begin{aligned} 8 &= 56 + 24\times(-2) && \text{since } 8 = 56 - 24\times 2 \\ &= 56 + (136 + 56\times(-2))\times(-2) && \text{since } 24 = 136 - 56\times 2 \\ &= 136\times(-2) + 56\times 5 && \\ &= 136\times(-2) + (600 + 136\times(-4))\times 5 && \text{since } 56 = 600 - 136\times 4 \\ 8 &= 600\times 5 + (-136)\times 22 && \end{aligned}$$