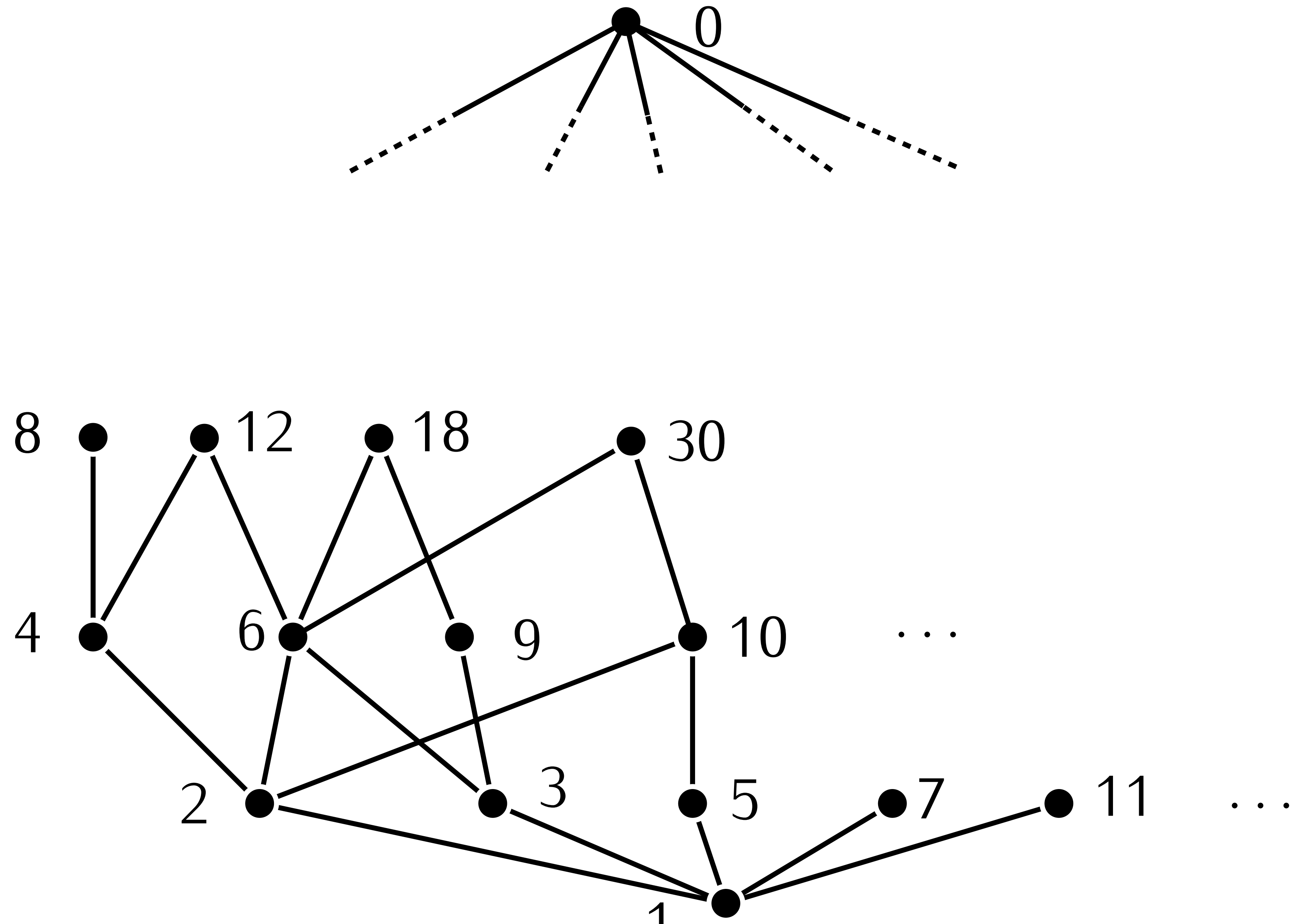
Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe

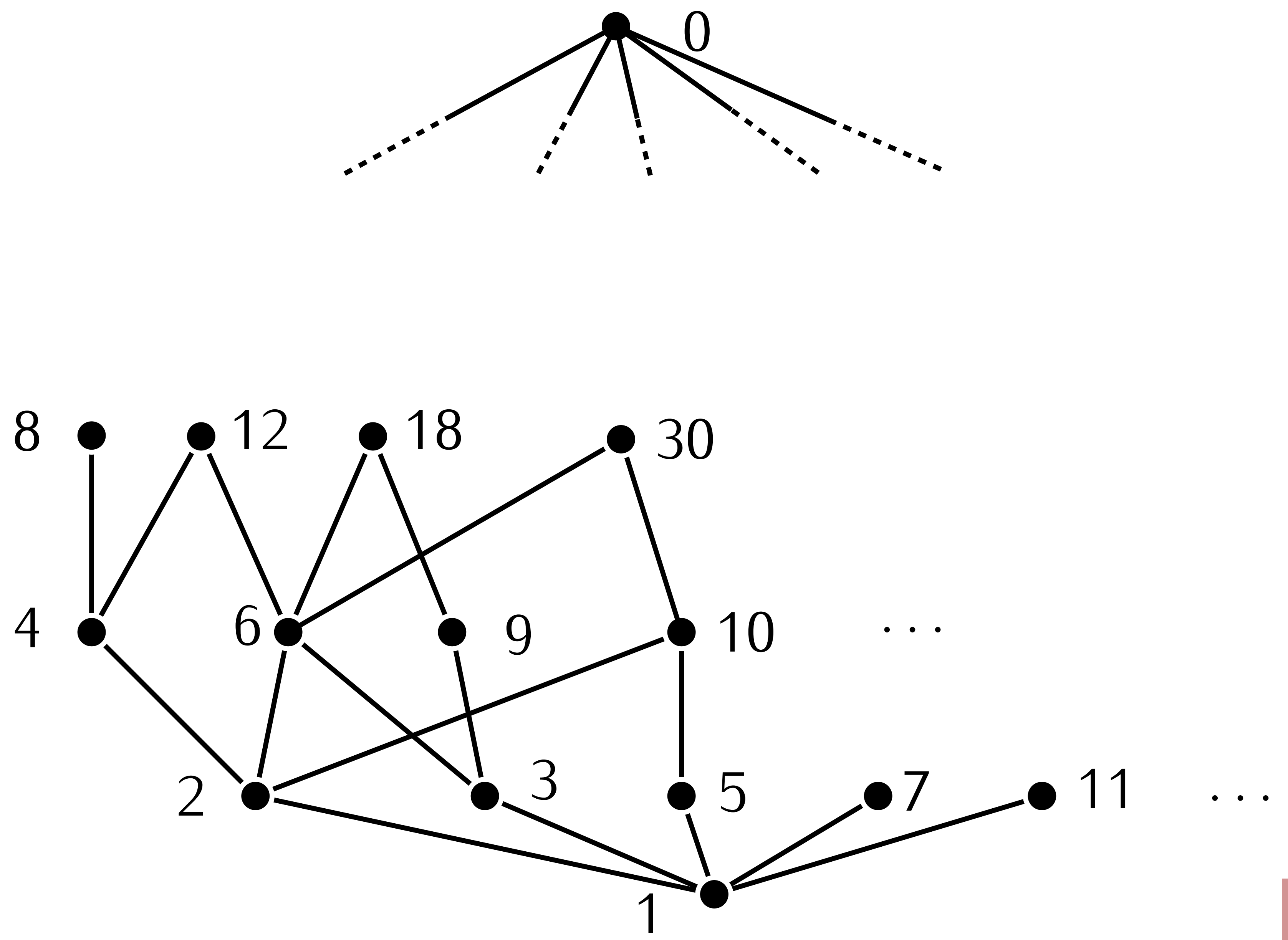
Research Group for Theoretical Computer Science


0
8
12
18
30
4
6
9
10
...
2
3
5
7
11
...
1

Definition. Let $S \subseteq \mathbb{N}_0$, and $d \in \mathbb{N}_0$. We say:

- d is a common divisor of S if for all $s \in S$, we have d divides s
- d is a greatest common divisor of S if it is a common divisor and for every common divisor d' of S, we have d' divides d

We write $a \wedge b$ for the greatest common divisor (gcd) of $\{a, b\}$.



Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. If d divides a and b, then d divides every element of `remainder`.

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. If d divides a and b, then d divides every element of `remainder`.

Proof by induction: `remainders` $= (r_0, r_1, \ldots, r_k, 0)$
For every $i \in \{0, \ldots, k\}$, d divides r_i
True for $i = 0, 1$ by assumption
For $i \geq 2$:

$$r_i = q \cdot r_{i+1} + r_{i+2}$$

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. If d divides a and b, then d divides every element of `remainder`.

Proof by induction: `remainders` $= (r_0, r_1, \ldots, r_k, 0)$
For every $i \in \{0, \ldots, k\}$, d divides r_i
True for $i = 0, 1$ by assumption
For $i \geq 2$:

$$r_i = q \cdot r_{i+1} + r_{i+2}$$

divisible by d
$r_i = d \cdot x$

divisible by d
$(r_{i+1} = d \cdot y)$

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. If d divides a and b, then d divides every element of `remainder`.

Proof by induction: $\texttt{remainders} = (r_0, r_1, \dots, r_k, 0)$
For every $i \in \{0, \dots, k\}$, d divides r_i
True for $i = 0, 1$ by assumption
For $i \geq 2$:

$$r_i = q \cdot r_{i+1} + r_{i+2}$$

divisible by d
$r_i = d \cdot x$

divisible by d
$(r_{i+1} = d \cdot y)$

So $r_{i+2} = d \cdot (x - qy)$ is divisible by d. $\square$

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. e divides a and b.

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. e divides a and b.

$$
\begin{aligned}
b &= q_2 \times a + r_2 \\
a &= q_3 \times r_2 + r_3 \\
r_2 &= q_4 \times r_3 + r_4 \\
&\vdots \\
r_{k-2} &= q_k \times r_{k-1} + r_k \\
r_{k-1} &= q_{k+1} \times r_k + 0
\end{aligned}
$$

this is e

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. e divides a and b.

$$
\begin{aligned}
b &= q_2 \times a + r_2 \\
a &= q_3 \times r_2 + r_3 \\
r_2 &= q_4 \times r_3 + r_4 \\
&\vdots \\
r_{k-2} &= q_k \times r_{k-1} + r_k \\
r_{k-1} &= q_{k+1} \times r_k + 0
\end{aligned}
$$

e divides r_{k-1}

this is e

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. e divides a and b.

$$\begin{aligned} b &= q_2 \times a + r_2 \\ a &= q_3 \times r_2 + r_3 \\ r_2 &= q_4 \times r_3 + r_4 \\ &\vdots \\ r_{k-2} &= q_k \times r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} \times r_k + 0 \end{aligned}$$

e divides r_{k-2}

e divides r_{k-1}

this is e

```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Theorem. For any $a, b \in \mathbb{N}_0$, the number e given by `euclid` is $\gcd(a, b)$.

Two things to prove:

- e divides a and b
- every d that divides a and b also divides e

Lemma. e divides a and b.

$$
\begin{aligned}
b &= q_2 \times a + r_2 & \quad & e \text{ divides } b \\
a &= q_3 \times r_2 + r_3 & & e \text{ divides } a \\
r_2 &= q_4 \times r_3 + r_4 & & e \text{ divides } r_2 \\
&\vdots \\
r_{k-2} &= q_k \times r_{k-1} + r_k & & e \text{ divides } r_{k-2} \\
r_{k-1} &= q_{k+1} \times r_k + 0 & & e \text{ divides } r_{k-1}
\end{aligned}
$$

this is e

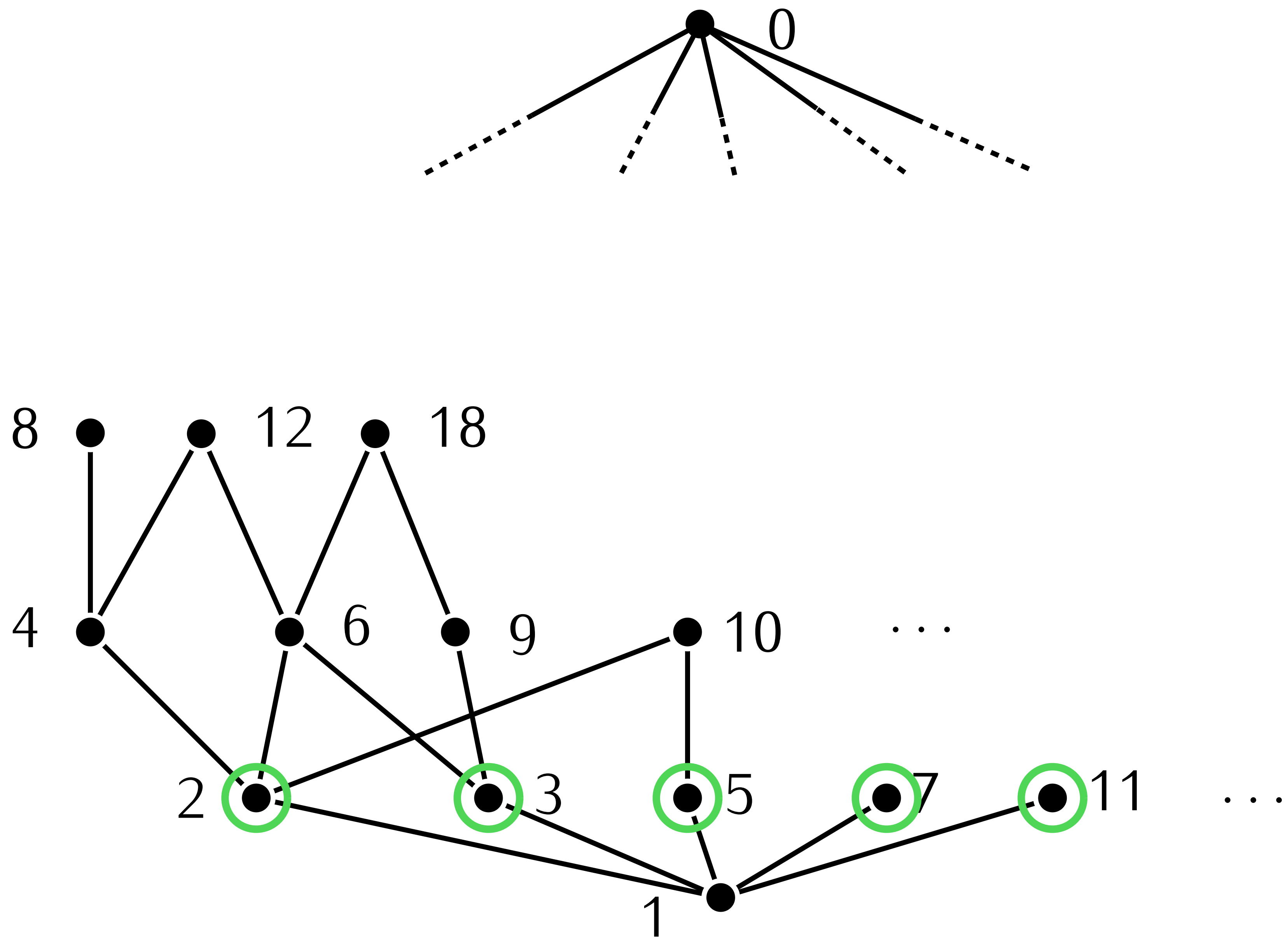
```
def euclid(a,b):
  if a > b:
    a,b = b,a # swap a and b
  if a == 0:
    return b

  remainders = [b,a]
  while remainders[-1] != 0:
    b = remainders[-2]
    a = remainders[-1]
    q,r = divmod(b,a)
    remainders.append(r)

  return remainders[-2]
```

Prime numbers

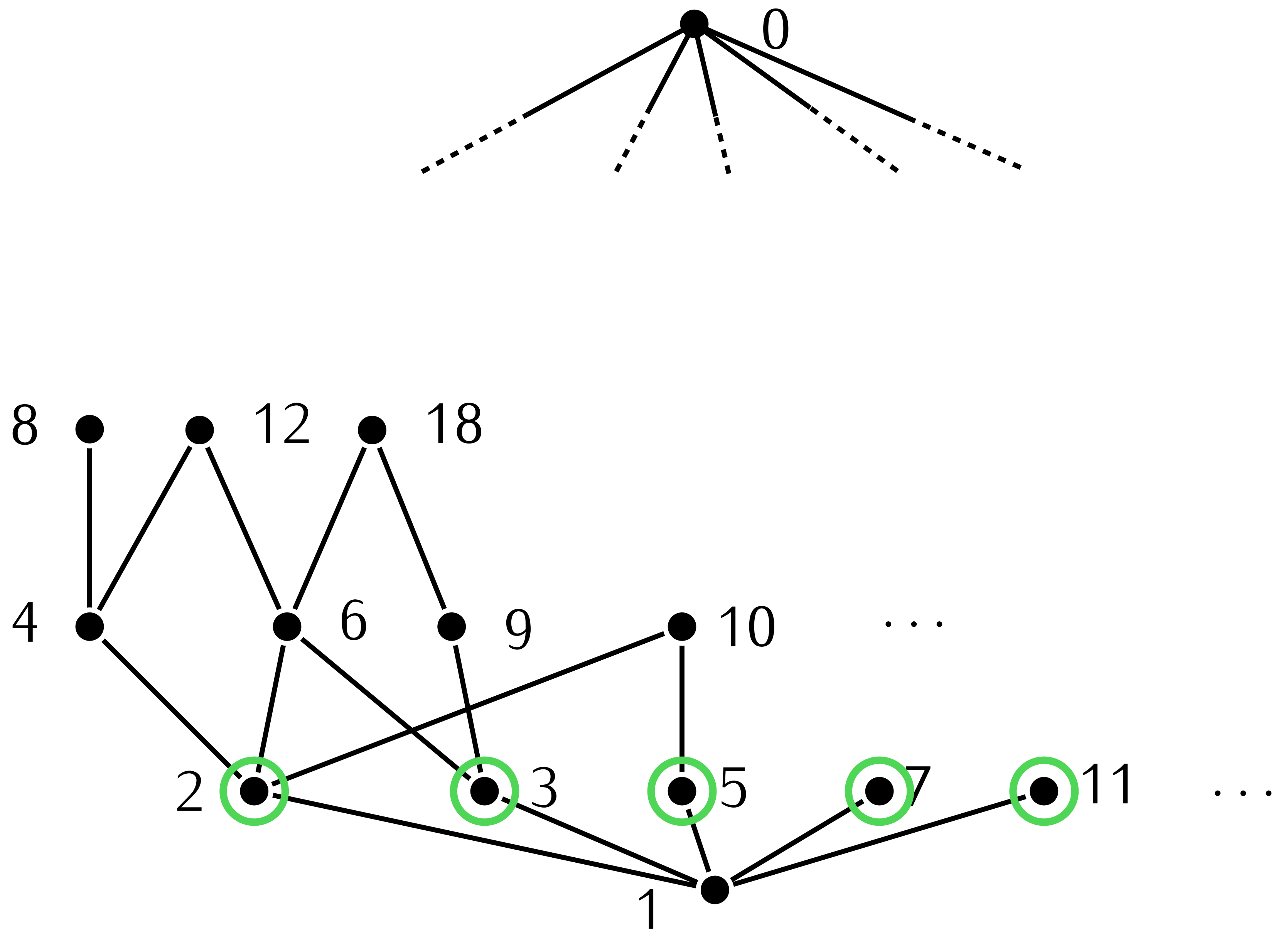
Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.



(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

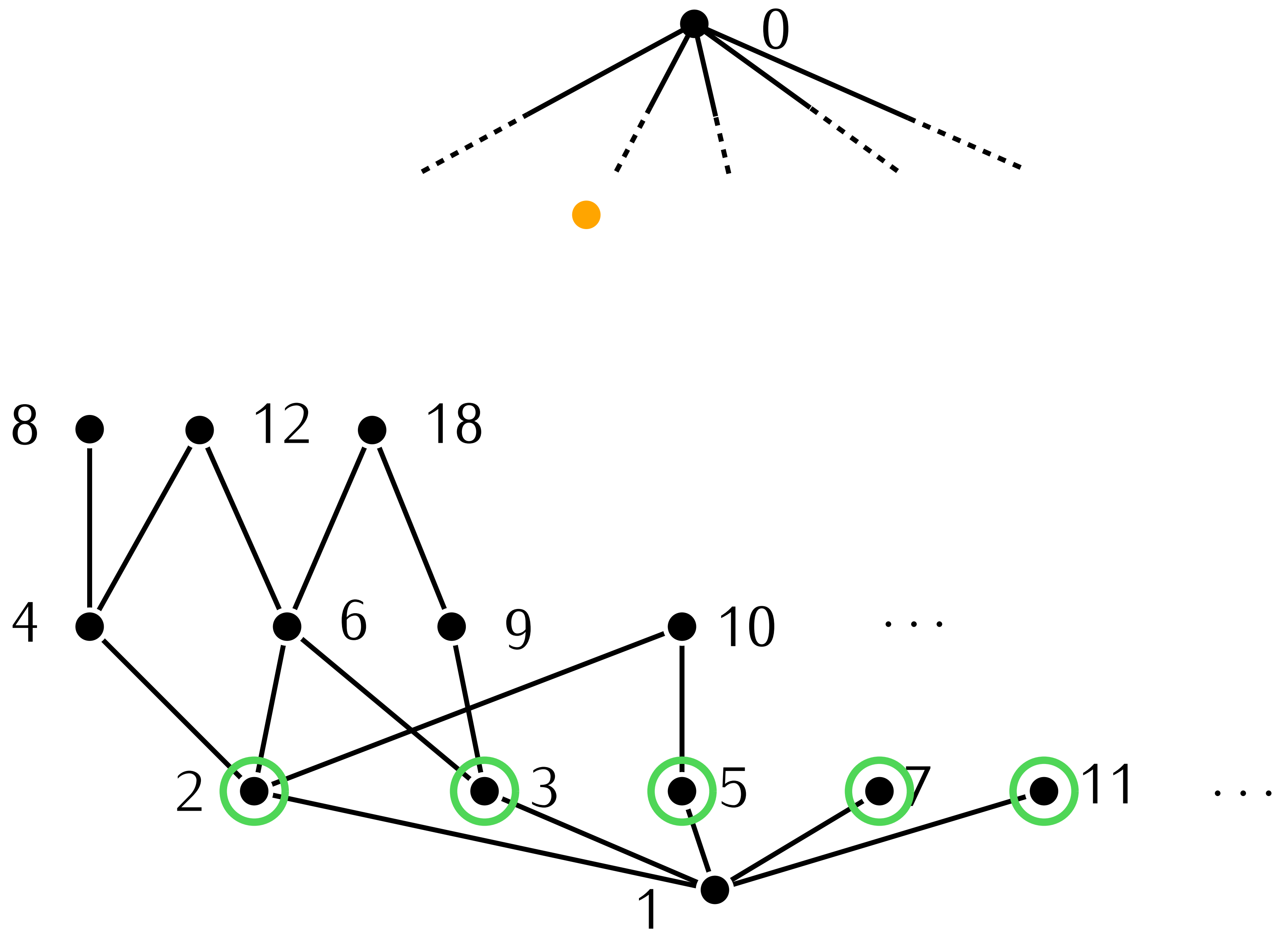
Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.



(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

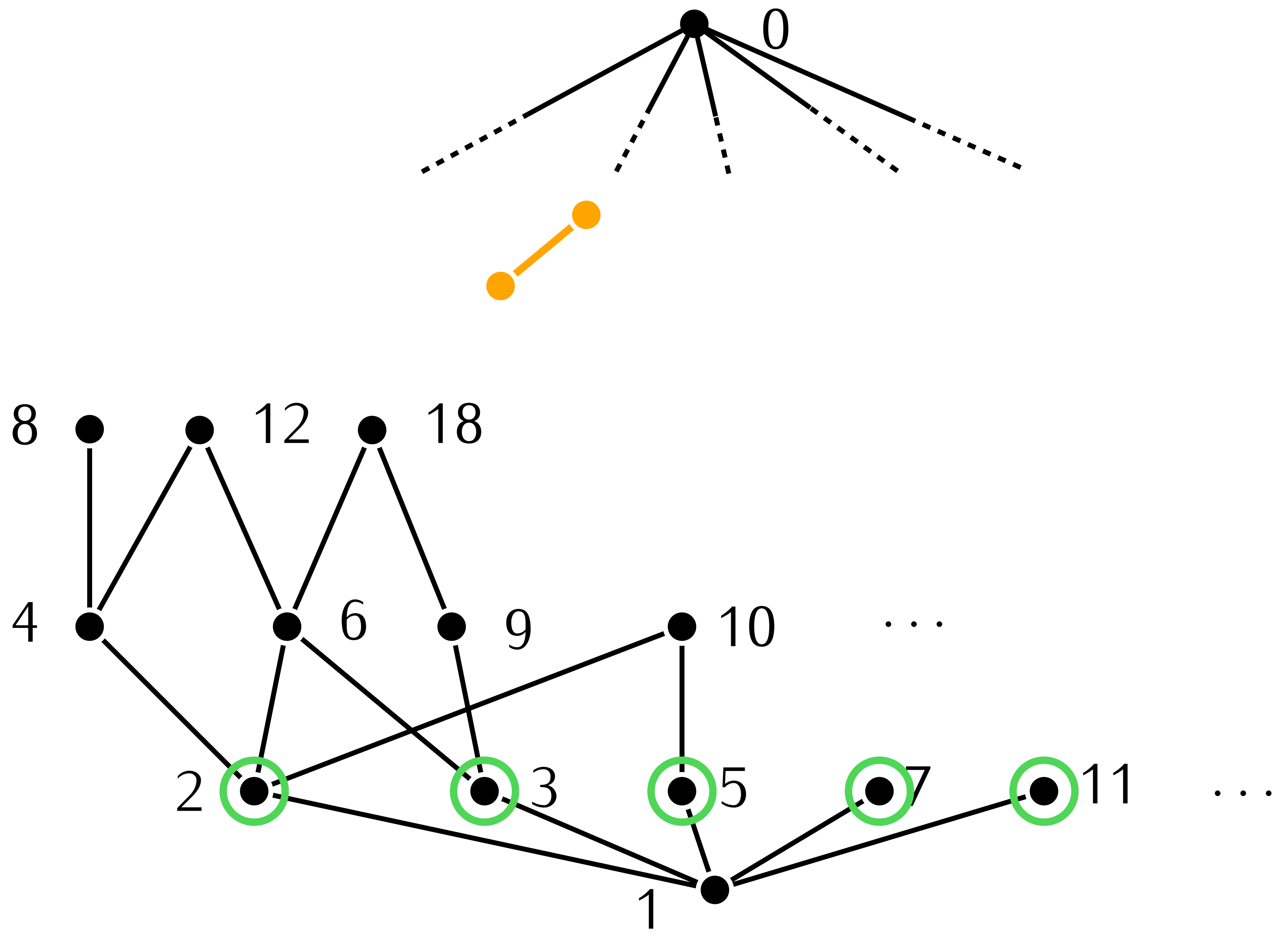
Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.



(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

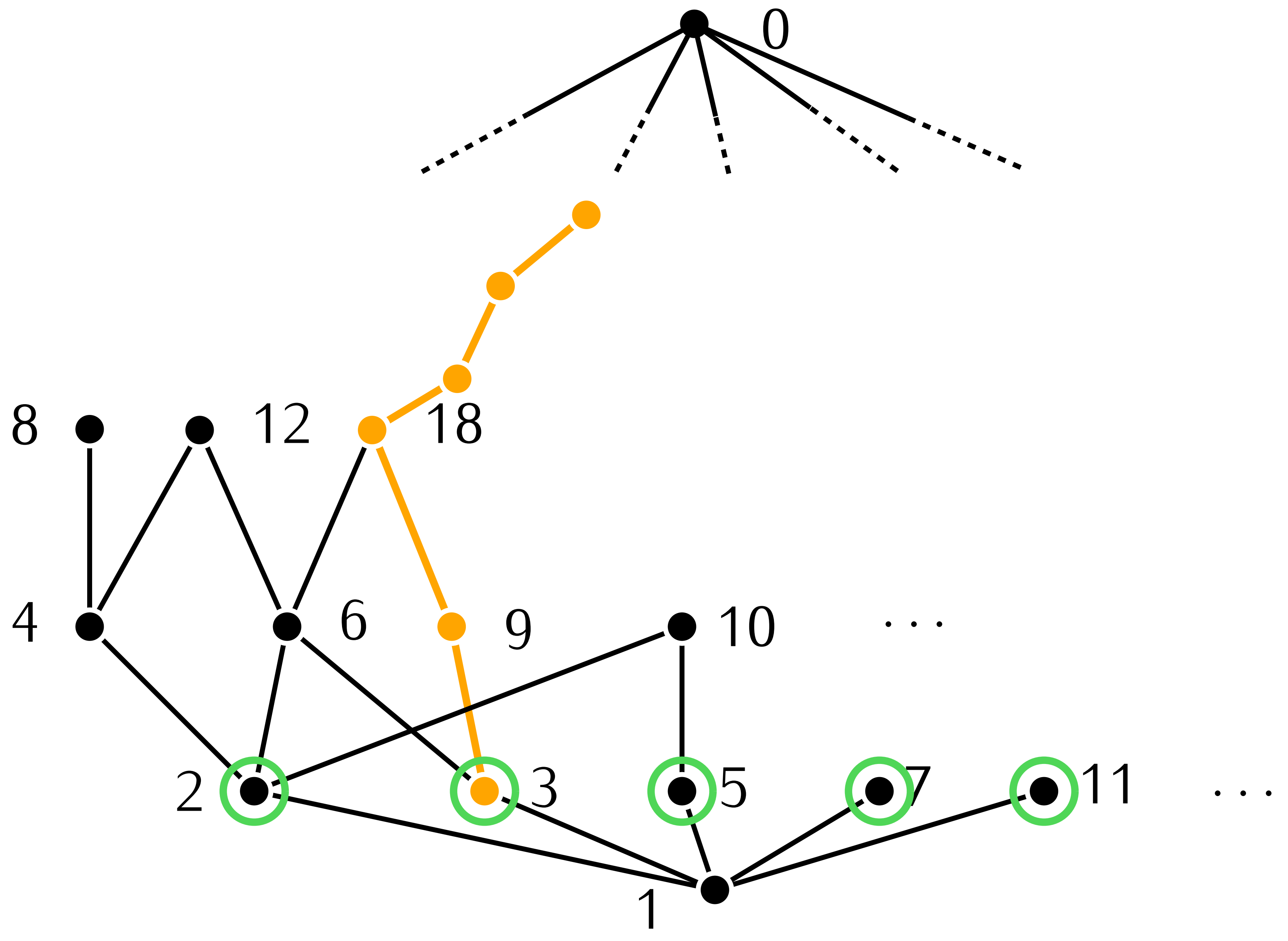
Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.



(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

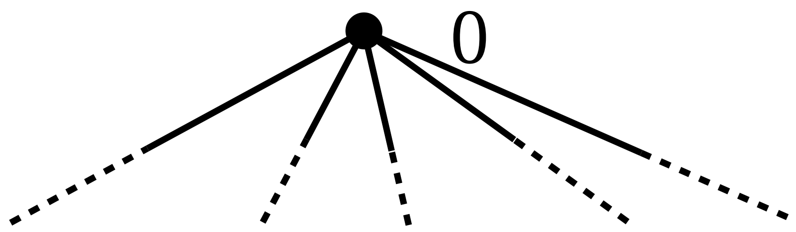


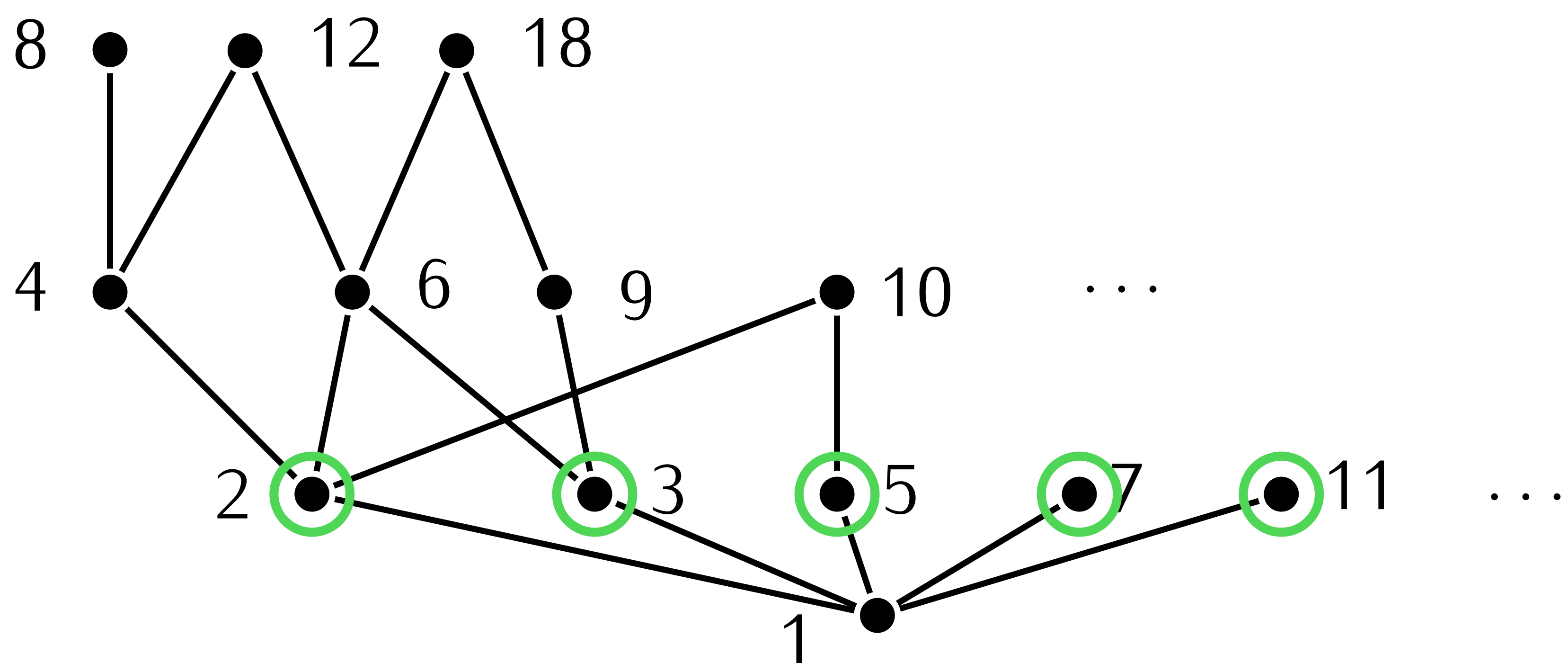
(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.



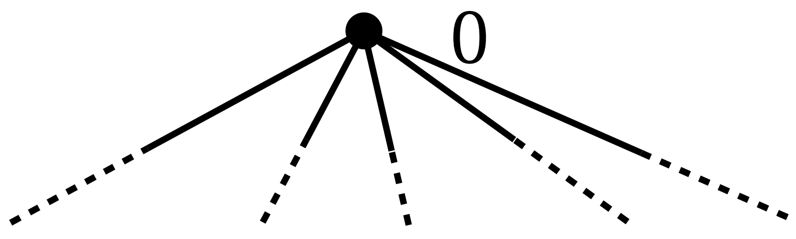


(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

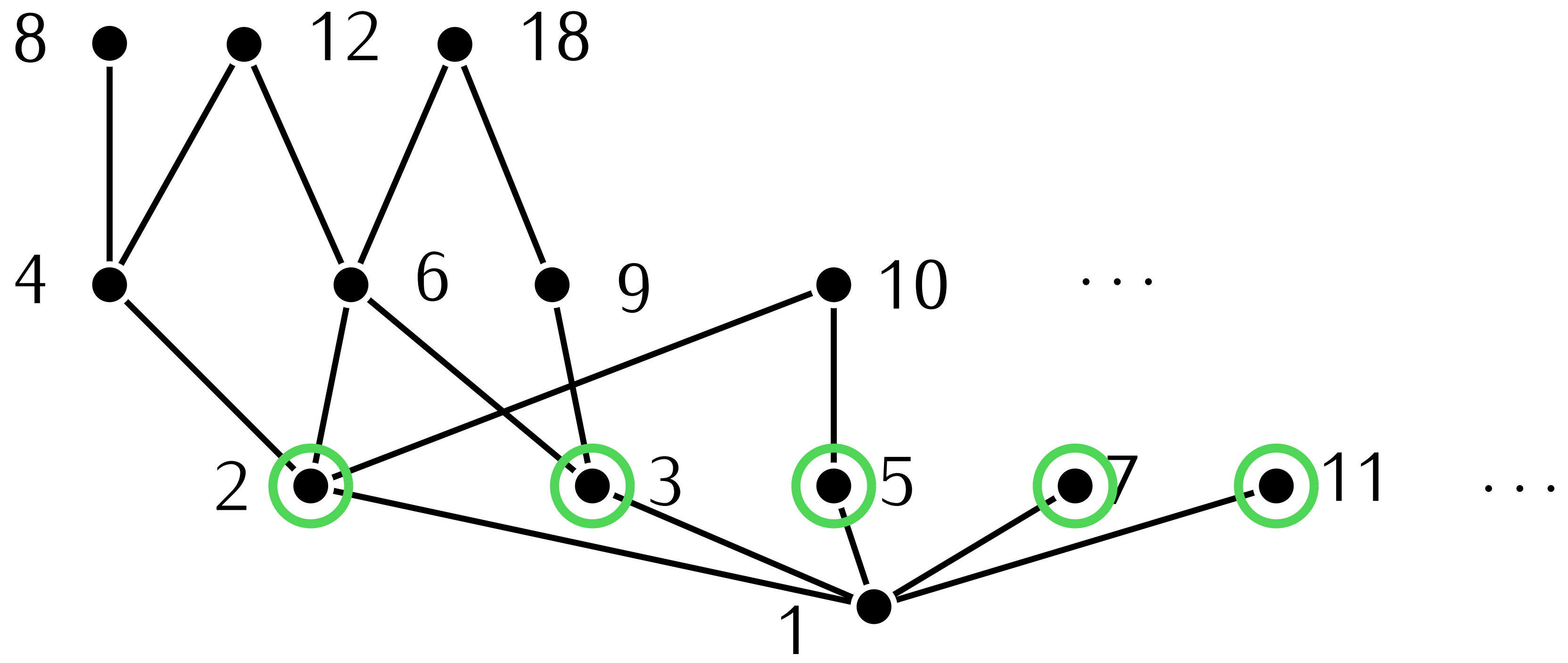
Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.



- Let $p_1, \ldots, p_k$ be any list of prime numbers.



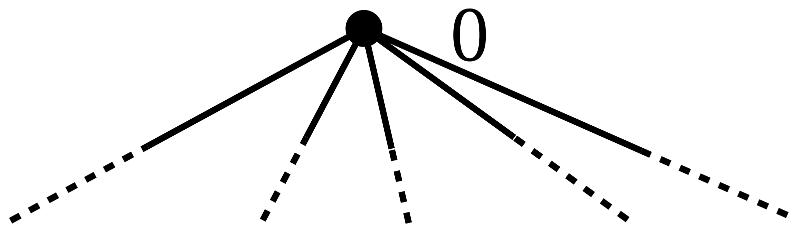
(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

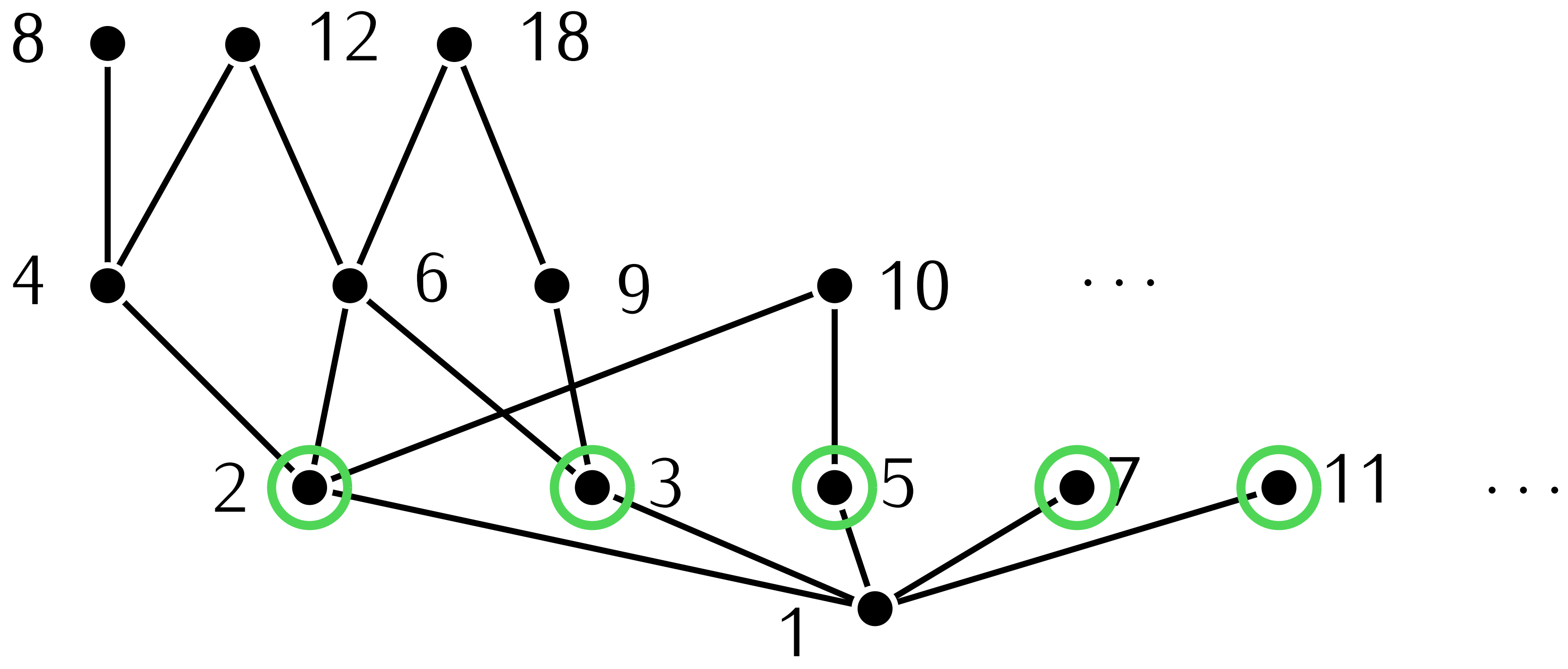
Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.

- Let $p_1, \ldots, p_k$ be any list of prime numbers.
- Define $N = p_1 \ldots p_k + 1$



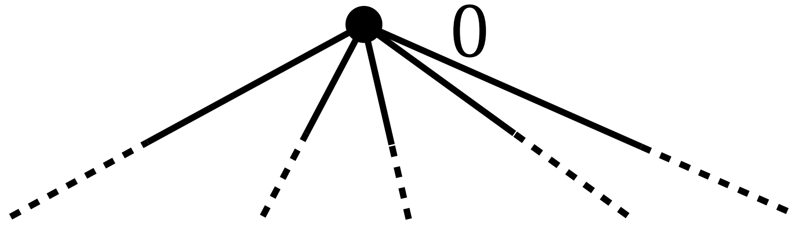


(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

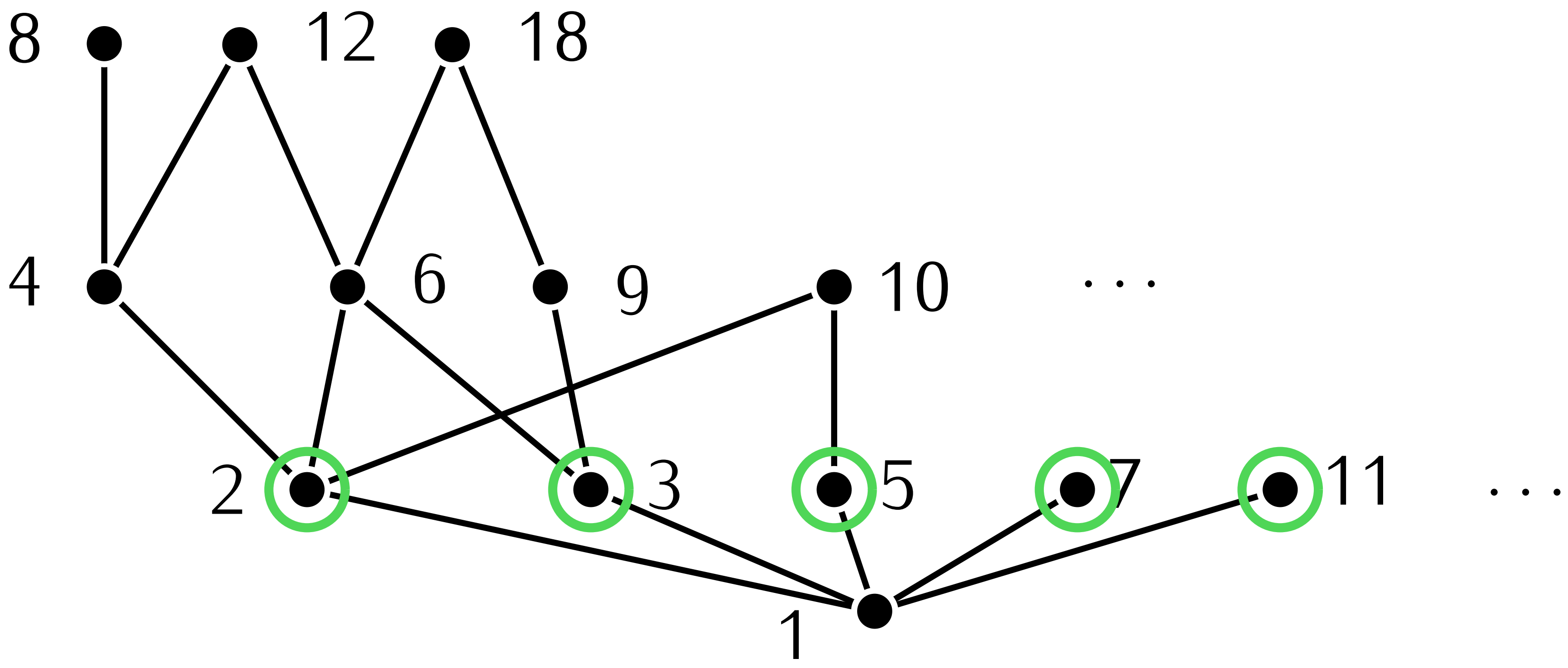
Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.



- Let $p_1, \ldots, p_k$ be any list of prime numbers.
- Define $N = p_1 \ldots p_k + 1$
- N is divisible by a prime p



(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.

- Let $p_1, \ldots, p_k$ be any list of prime numbers.
- Define $N = p_1 \ldots p_k + 1$
- N is divisible by a prime p
- $N = (p_1 \ldots p_{k-1})p_k + 1$ and $1 < p_k$, so p is not p_k

(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.

- Let $p_1, \ldots, p_k$ be any list of prime numbers.
- Define $N = p_1 \ldots p_k + 1$
- N is divisible by a prime p
- $N = (p_1 \ldots p_{k-1})p_k + 1$ and $1 < p_k$, so p is not p_k
- Similarly for every $i \in \{1, \ldots, k-1\}$, N is not divisible by p_i.
  So $p \notin \{p_1, \ldots, p_k\}$

(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Every number $n \in \mathbb{N}$ that is not 1 is divisible by a prime number.

Theorem. There are infinitely many prime numbers.

- Let $p_1, \ldots, p_k$ be any list of prime numbers.
- Define $N = p_1 \ldots p_k + 1$
- N is divisible by a prime p
- $N = (p_1 \ldots p_{k-1})p_k + 1$ and $1 < p_k$, so p is not p_k
- Similarly for every $i \in \{1, \ldots, k-1\}$, N is not divisible by p_i.
  So $p \notin \{p_1, \ldots, p_k\}$
- $p_1, \ldots, p_k$ cannot be a list of all the primes $\square$

(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

Definition. A number $p \in \mathbb{N}_0$ is prime if it is > 1 and it is only divisible by 1 and itself.

Theorem. Let p be a prime number and $a, b \in \mathbb{Z}$. If p divides ab, then it divides a or it divides b.

(*) Being prime can be defined for $p \in \mathbb{Z}$ as well

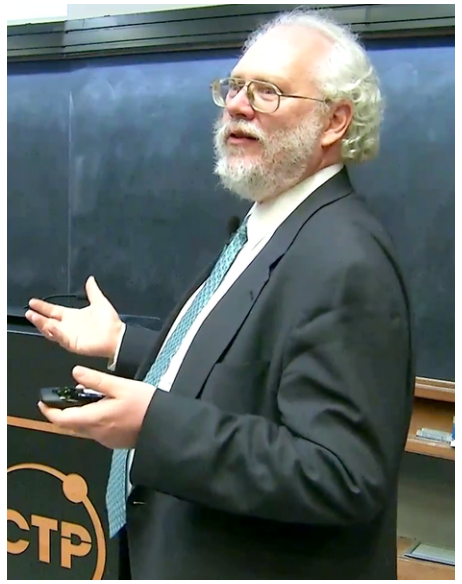
Theorem. Let $n \in \mathbb{N}$ be such that $n \geq 2$.
There exist prime numbers $p_1 < \cdots < p_k$ and $e_1, \ldots, e_k \in \mathbb{N}$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$.
Moreover this decomposition is unique.

Theorem. Let $n \in \mathbb{N}$ be such that $n \geq 2$.
There exist prime numbers $p_1 < \cdots < p_k$ and $e_1, \ldots, e_k \in \mathbb{N}$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$.
Moreover this decomposition is unique.

- Important in math (building blocks for all numbers)
  There are still many open questions about prime numbers (Goldbach's conjecture, Twin Prime conjecture, Riemann's hypothesis)
- Important in crypto (RSA)
- It seems hard to compute $p_1, \ldots, p_k$ if given $n \in \mathbb{N}$

Theorem. Let $n \in \mathbb{N}$ be such that $n \geq 2$.
There exist prime numbers $p_1 < \cdots < p_k$ and $e_1, \ldots, e_k \in \mathbb{N}$ such that $n = p_1^{e_1} \cdots p_k^{e_k}$.
Moreover this decomposition is unique.

- Important in math (building blocks for all numbers)
  There are still many open questions about prime numbers (Goldbach's conjecture, Twin Prime conjecture, Riemann's hypothesis)
- Important in crypto (RSA)
- It seems hard to compute $p_1, \ldots, p_k$ if given $n \in \mathbb{N}$
- **Theoretically,** there is a quantum algorithm that can do this and **break RSA**.

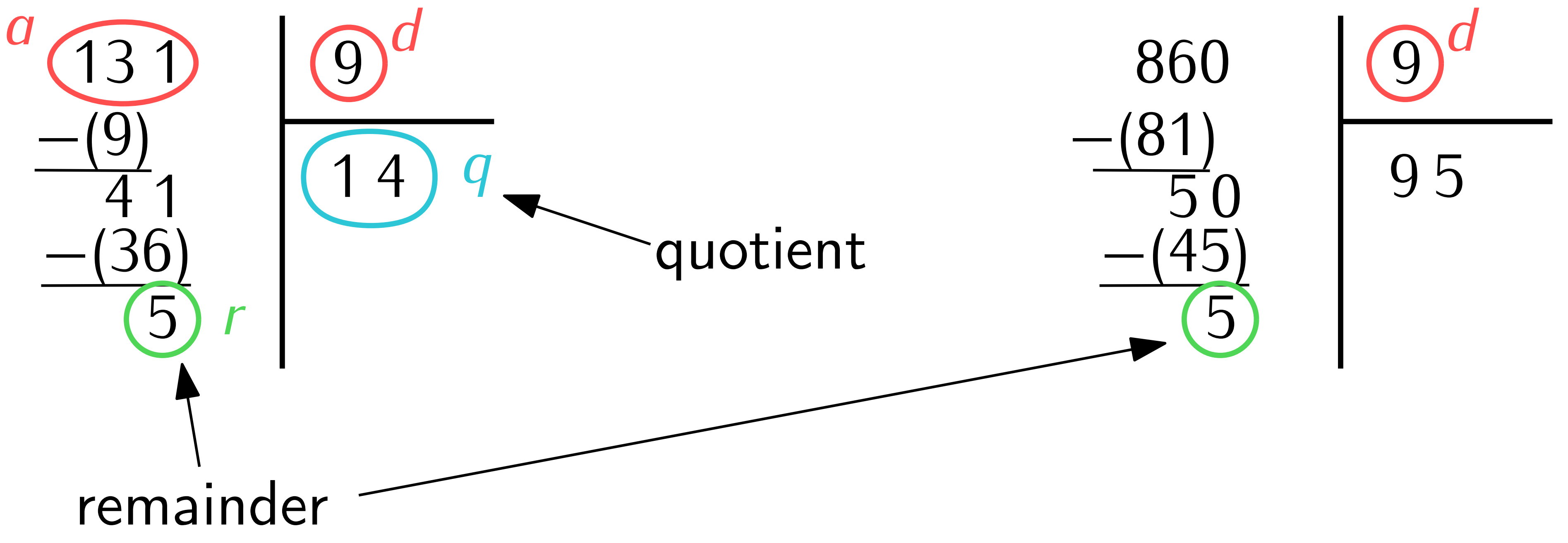


Peter Shor

Modular arithmetic

Theorem. For all $a, d \in \mathbb{Z}$ such that $a \neq 0$, there exists a unique pair $(q, r) \in \mathbb{Z}^2$ such that:

- $a = q \cdot d + r$
- $r \in \{0, \ldots, |d| - 1\}$



Almost the same as `divmod` in Python:

```
divmod(131,9) # (14,5)
divmod(10,-3) # (-4,-2)
```

- If remainder is 0: we say d divides a
  a is a multiple of d

Notation: $d \mid a$

- Define $b \equiv_d b'$ by "they have the same remainder in the division by d"
  $131 \equiv_9 860$

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d"
We then say that b and b' are congruent modulo d.

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d"
We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d" We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Methods: to check if $1075 \equiv 364 \bmod 72$

Compute $1075 - 364 = 711$
Check if 711 is divisible by 72

Divide 1075 by 72: $1075 = 14 \times 72 + 67$
Divide 364 by 72: $364 = 5 \times 72 + 4$
Check if the remainders are equal

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Methods: to check if $1075 \equiv 364 \bmod 72$

Compute $1075 - 364 = 711$
Check if 711 is divisible by 72

Divide 1075 by 72: $1075 = 14 \times 72 + 67$
Divide 364 by 72: $364 = 5 \times 72 + 4$
Check if the remainders are equal

Which of the following are true?

- $14 \equiv 6 \bmod 2$
- $3 \equiv 1 \bmod 4$
- $61 \equiv 5 \bmod 7$

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d"
We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Equivalence relation Equivalence class Set of equivalence classes

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d" We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Equivalence relation	Equivalence class	Set of equivalence classes
$\equiv_d$	$[5]_{\equiv_d}$	$\mathbb{Z}/\equiv_d$

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Equivalence relation	Equivalence class	Set of equivalence classes
$\equiv_d$	$\cancel{[5]_{\equiv_d}}$ $[5]_d$	$\cancel{\mathbb{Z}/\equiv_d}$ $\mathbb{Z}/d\mathbb{Z}$

Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

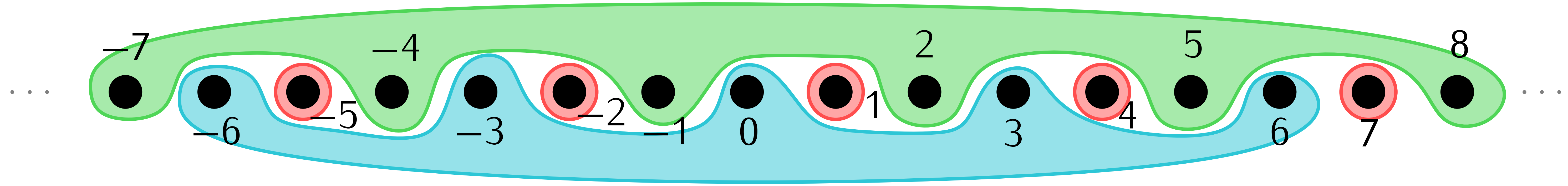
Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Equivalence relation	Equivalence class	Set of equivalence classes
$\equiv_d$	$\cancel{[5]_{\equiv_d}}$ $[5]_d$	$\cancel{\mathbb{Z}/\equiv_d}$ $\mathbb{Z}/d\mathbb{Z}$

There are exactly d equivalence classes: $|\mathbb{Z}/d\mathbb{Z}| = d$



Definition. Let $d \geq 2$. Define $b \equiv_d b'$ by "b and b' have the same remainder in the division by d". We then say that b and b' are congruent modulo d.

Equivalently: $b \equiv_d b'$ if $b - b'$ is divisible by d

Notation. Other common notations for the same thing: $b \equiv b' \bmod d$ or $b = b' \bmod d$

Theorem. $\equiv_d$ is an equivalence relation.

Equivalence relation	Equivalence class	Set of equivalence classes
$\equiv_d$	$\cancel{[5]_{\equiv_d}}$ $[5]_d$	$\cancel{\mathbb{Z}/\equiv_d}$ $\mathbb{Z}/d\mathbb{Z}$

Examples.
- $d = 12$: $\mathbb{Z}/d\mathbb{Z}$ is $\{[1]_{12}, [2]_{12}, \ldots, [12]_{12}\}$ hours on a clock
- $d = 7$: $\{[1]_7, [2]_7, \ldots, [7]_7\}$ days of the week
- $d = 2$: $\{[0]_2, [1]_2\}$ parity

Algebra: study of **operations** and **equations** on *stuff*

Number theory

Boolean algebra

Numbers: $+, \times, 1/x, 1, 0$

Matrices: $+, \times, M^{-1}, I, 0$

Sets: $\cap, \cup, \times, \Delta, \emptyset, \ldots$

Functions: $\circ, f^{-1}, \mathrm{Id}_A$

Booleans: $\wedge, \vee, \Rightarrow, \neg, \top, \bot$

Relations: $\circ, R^T, \mathrm{Id}, \cup, \cap, \times, \ldots$

Linear algebra

Relational algebra

Modular integers: $+, \times, [a]_d^{-1}, [1]_d, [0]_d$

$$\text{Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{N}_0 \text{ or } \mathbb{Z}$$

$$\textbf{Modular} \text{ Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{Z}/d\mathbb{Z}$$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

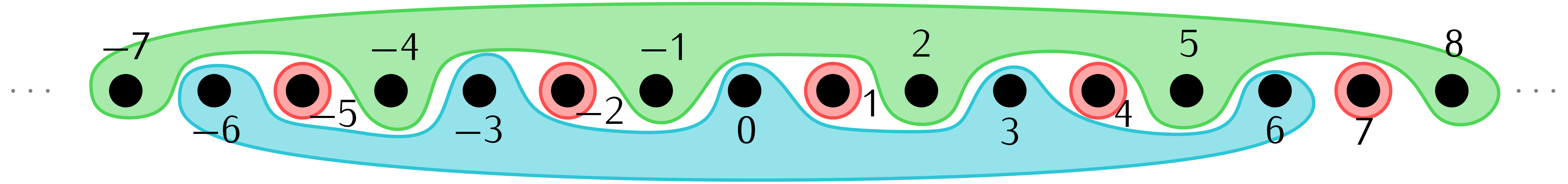
- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

Arithmetic = study of $+$ and $\times$ over $\mathbb{N}_0$ or $\mathbb{Z}$

Modular Arithmetic = study of $+$ and $\times$ over $\mathbb{Z}/d\mathbb{Z}$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

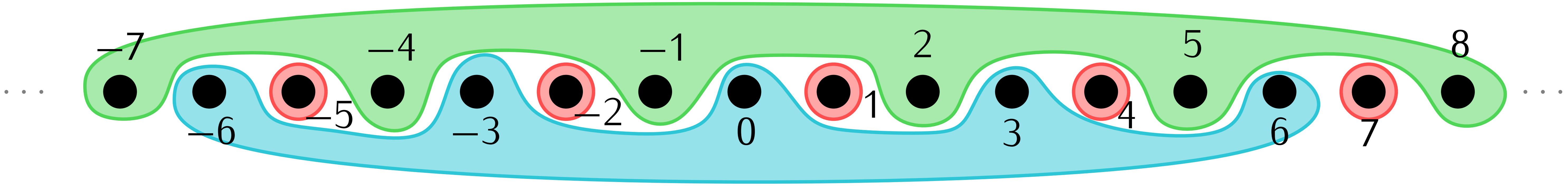


Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{N}_0$ or $\mathbb{Z}$

Modular Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{Z}/d\mathbb{Z}$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a+b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$



Note that this is a **definition** and it depends on d:

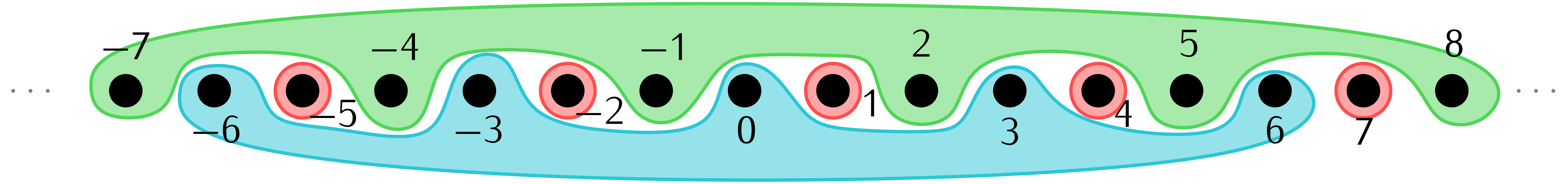
$\boxed{\{\dots,-1,2,5,\dots\}} + \boxed{\{\dots,-3,0,3,\dots\}} =$ $\boxed{\{\dots,-1,2,5,\dots\}} + \boxed{\{\dots,-2,1,4,\dots\}} =$

$$\text{Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{N}_0 \text{ or } \mathbb{Z}$$

$$\textbf{Modular}\text{ Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{Z}/d\mathbb{Z}$$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$



Note that this is a **definition** and it depends on d:

$\{\ldots, -1, 2, 5, \ldots\} + \{\ldots, -3, 0, 3, \ldots\} =$ $\{\ldots, -1, 2, 5, \ldots\} + \{\ldots, -2, 1, 4, \ldots\} =$

The usual rules of addition and multiplication are true in modular arithmetic:

- $[a]_d + [b]_d = [b]_d + [a]_d$ and $[a]_d \times [b]_d = [b]_d \times [a]_d$
- $[0]_d + [a]_d = [a]_d$
- $[a]_d \times ([b]_d + [c]_d) = [a]_d \times [b]_d + [a]_d \times [c]_d$

Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{N}_0$ or $\mathbb{Z}$

Modular Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{Z}/d\mathbb{Z}$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a+b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

Which day of the week will it be in one week?

Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{N}_0$ or $\mathbb{Z}$

Modular Arithmetic $=$ study of $+$ and $\times$ over $\mathbb{Z}/d\mathbb{Z}$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

~~Which day of the week will it be in one week?~~
Which day of the week will it be in one month (January 15, 2026)?

$$\text{Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{N}_0 \text{ or } \mathbb{Z}$$

$$\textbf{Modular} \text{ Arithmetic} = \text{study of } + \text{ and } \times \text{ over } \mathbb{Z}/d\mathbb{Z}$$

Definition. We define addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ as follows:

- $[a]_d + [b]_d$ is defined to be $[a + b]_d$
- $[a]_d \times [b]_d$ is defined to be $[a \times b]_d$

~~Which day of the week will it be in one week?~~

~~Which day of the week will it be in one month (January 15, 2026)?~~

Which day of the week was it two months ago (October 15, 2025)?

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a - b]_d$, easy

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a - b]_d$, easy
- Division: $[b]_d/[a]_d = [b/a]_d$?!

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a-b]_d$, easy
- Division: $[b]_d/[a]_d = \cancel{[b/a]_d}$?!

The usual division that we know (for numbers in $\mathbb{Q}$, for example) satisfies: $\frac{b}{a} = b \times \boxed{\frac{1}{a}}$ and $a \times \boxed{\frac{1}{a}} = 1$

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a-b]_d$, easy
- Division: $[b]_d/[a]_d = \cancel{[b/a]_d}$?!

The usual division that we know (for numbers in $\mathbb{Q}$, for example) satisfies: $\frac{b}{a} = b \times \boxed{\frac{1}{a}}$ and $a \times \boxed{\frac{1}{a}} = 1$

Definition. Let $a \in \mathbb{Z}$. An inverse of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a-b]_d$, easy
- Division: $[b]_d/[a]_d = \cancel{[b/a]_d}$?!

The usual division that we know (for numbers in $\mathbb{Q}$, for example) satisfies: $\frac{b}{a} = b \times \boxed{\frac{1}{a}}$ and $a \times \boxed{\frac{1}{a}} = 1$

Definition. Let $a \in \mathbb{Z}$. An inverse of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

Definition (Reminder (?) from your Math 1 course)**.** Let M be an $n \times n$ matrix. An inverse of N is a matrix such that $MN = I_n$.

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a-b]_d$, easy
- Division: $[b]_d/[a]_d = \cancel{[b/a]_d}$?!

The usual division that we know (for numbers in $\mathbb{Q}$, for example) satisfies: $\frac{b}{a} = b \times \boxed{\frac{1}{a}}$ and $a \times \boxed{\frac{1}{a}} = 1$

Definition. Let $a \in \mathbb{Z}$. An inverse of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

Examples.
- 2 is an inverse of 2 modulo 3
- 3 is an inverse of 2 modulo 5
- inverse of 2 modulo 4?

We have defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$.
Can we define subtraction and division?

- Subtraction: $[a]_d - [b]_d = [a-b]_d$, easy
- Division: $[b]_d/[a]_d = \cancel{[b/a]_d}$?!

The usual division that we know (for numbers in $\mathbb{Q}$, for example) satisfies: $\frac{b}{a} = b \times \boxed{\frac{1}{a}}$ and $a \times \boxed{\frac{1}{a}} = 1$

Definition. Let $a \in \mathbb{Z}$. An inverse of a modulo d is a number $b \in \mathbb{Z}$ such that $a \times b \equiv_d 1$.

Examples.
- 2 is an inverse of 2 modulo 3
- 3 is an inverse of 2 modulo 5
- inverse of 2 modulo 4?

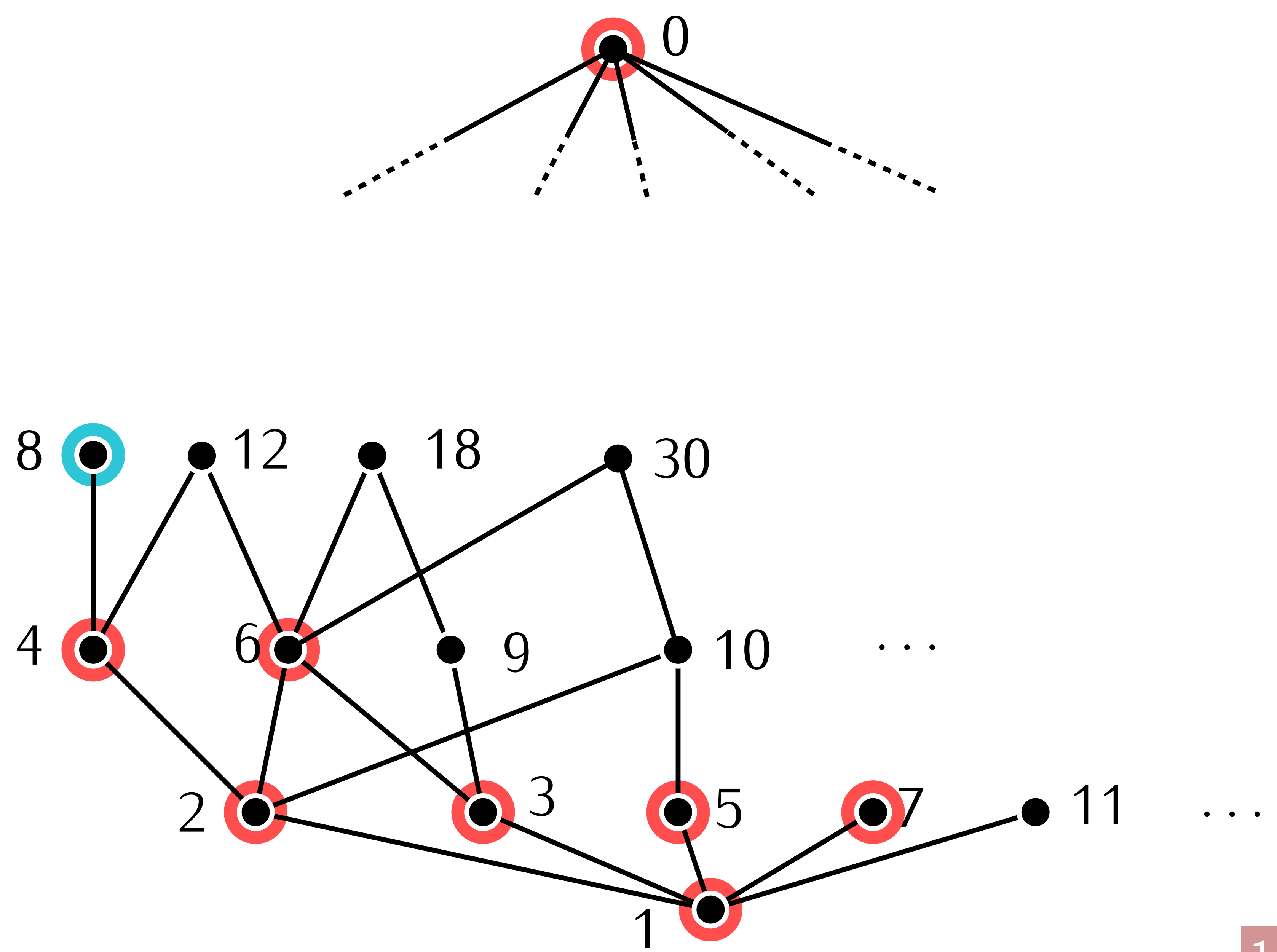
$\gcd(a, d) = 1$

Theorem. Let $a \in \mathbb{Z}$ and $d \geq 2$. Then a has an inverse modulo d if, and only if, a and d are coprime.

Theorem. Let $a \in \mathbb{Z}$ and $d \geq 2$. Then a has an inverse modulo d if, and only if, a and d are coprime.

$\gcd(a, d) = 1$

Which of the numbers in $\{0, \ldots, 7\}$ have an inverse modulo 8?

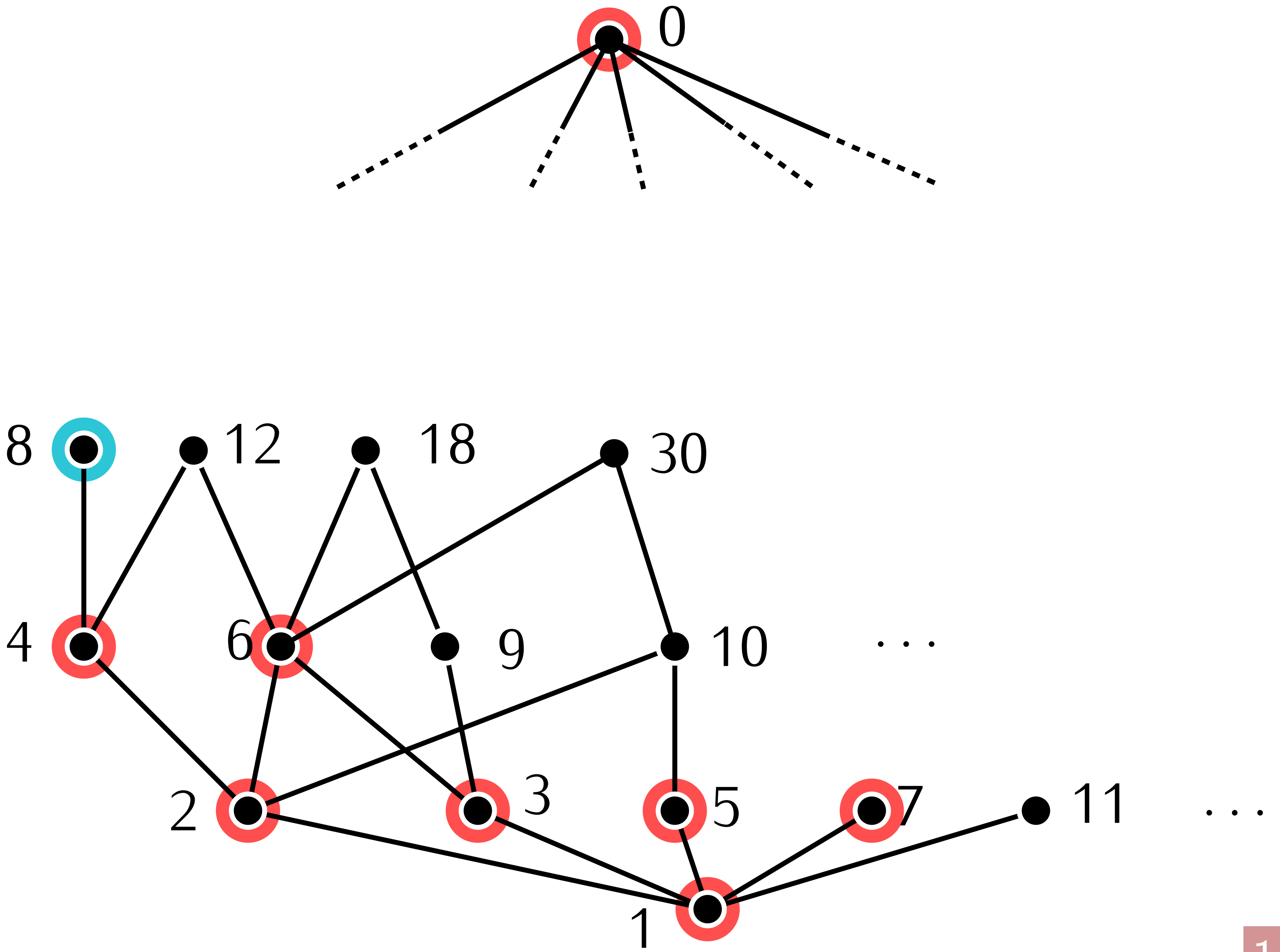


Theorem. Let $a \in \mathbb{Z}$ and $d \geq 2$. Then a has an inverse modulo d if, and only if, a and d are coprime.

$\gcd(a, d) = 1$

Which of the numbers in $\{0, \ldots, 7\}$ have an inverse modulo 8?

There are 4 numbers that have an inverse



Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \ldots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$$

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \dots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \dots, n-1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	$\{0\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3,4\}$	$\{1,5\}$	$\{1,2,3,4,5,6\}$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \ldots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	$\{0\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3,4\}$	$\{1,5\}$	$\{1,2,3,4,5,6\}$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Theorem. Let n have prime decomposition $p_1^{e_1} \times \cdots \times p_k^{e_k}$.
Then $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$.

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \ldots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	$\{0\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3,4\}$	$\{1,5\}$	$\{1,2,3,4,5,6\}$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Theorem. Let n have prime decomposition $p_1^{e_1} \times \cdots \times p_k^{e_k}$.
Then $\varphi(n) = \prod_{i=1}^{k} (p_i - 1)p_i^{e_i - 1}$.

Examples.
- $12 = 2^2 3$ so $\varphi(12) = (1 \times 2^1)(2 \times 3^0) = 4$
- $125 = 5^3$ so $\varphi(125) = 4 \times 5^2 = 100$

Definition. Let $n \geq 1$. Define $\varphi(n)$ to be the number of numbers in $\{0, \ldots, n-1\}$ that have an inverse modulo n.

$$\varphi(n) = |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$$

n	1	2	3	4	5	6	7	8	9
	$\{0\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3,4\}$	$\{1,5\}$	$\{1,2,3,4,5,6\}$	$\{1,3,5,7\}$	$\{1,2,4,5,7,8\}$
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Theorem. Let n have prime decomposition $p_1^{e_1} \times \cdots \times p_k^{e_k}$. Then $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}$.

What is $\varphi(60)$?

Examples.
- $12 = 2^2 3$ so $\varphi(12) = (1 \times 2^1)(2 \times 3^0) = 4$
- $125 = 5^3$ so $\varphi(125) = 4 \times 5^2 = 100$

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

What are the last 2 digits of 7^{582} (when written in base 10)?

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

What are the last 2 digits of 7^{582} (when written in base 10)?

$\log_{10}(7^{582}) = 582 \log_{10}(7) \approx 491.847\ldots$

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

What are the last 2 digits of 7^{582} (when written in base 10)?

$\log_{10}(7^{582}) = 582 \log_{10}(7) \approx 491.847\ldots$

$7^{582} = (d_{491} d_{490} \ldots d_2 \underline{d_1 d_0})_{10}$

what we want to know

Theorem. Let a and d be such that $\gcd(a, d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

What are the last 2 digits of 7^{582} (when written in base 10)?

$\log_{10}(7^{582}) = 582 \log_{10}(7) \approx 491.847\ldots$

$$7^{582} = (d_{491} d_{490} \ldots d_2 \underline{d_1 d_0})_{10} = d_{491} 10^{491} + \cdots + d_3 \times 1000 + d_2 \times 100 + d_1 \times 10 + d_0 = \sum_{i=0}^{491} d_i 10^i$$

what we want to know

Theorem. Let a and d be such that $\gcd(a,d) = 1$. Then $a^{\varphi(d)} \equiv 1 \bmod d$.

So $a \times a^{\varphi(d)-1} = a^{\varphi(d)} \equiv 1 \bmod d$

Proof: need some extra algebraic tools that we will see in a couple lectures

Application: compute large powers modulo a number

What are the last 2 digits of 7^{582} (when written in base 10)?

$\log_{10}(7^{582}) = 582 \log_{10}(7) \approx 491.847\ldots$

$$7^{582} = (d_{491} d_{490} \ldots d_2 \underline{d_1 d_0})_{10} = d_{491} 10^{491} + \cdots + d_3 \times 1000 + d_2 \times 100 + d_1 \times 10 + d_0 = \sum_{i=0}^{491} d_i 10^i$$

what we want to know: $7^{582} \equiv (d_1 \times 10 + d_0) \bmod 100$

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn - 1\}$.

Proof of existence:

Proof of uniqueness:

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:

$$um + vn = 1$$

Proof of uniqueness:

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x & = & a \bmod m \\ x & = & b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$

Proof of uniqueness:

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \ldots, mn-1\}$

Proof of uniqueness:

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \ldots, mn-1\}$

Proof of uniqueness:

- Define $f\colon \{0, \ldots, mn-1\} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \dots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \dots, mn-1\}$

Proof of uniqueness:

- Define $f \colon \{0, \dots, mn-1\} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is...

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn - 1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
  $$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \ldots, mn - 1\}$

Proof of uniqueness:

- Define $f\colon \{0, \ldots, mn - 1\} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is... surjective
- Since the domain and codomain have same size, f must be injective!

Theorem. Let m, n be coprime. For all $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x &= a \bmod m \\ x &= b \bmod n \end{cases}$$

There is exactly one such x in $\{0, \ldots, mn-1\}$.

Proof of existence:

- Let u, v be the Bézout coefficients for m, n:
$$um + vn = 1$$
- Define $x = umb + vna$
- Divide x by mn with remainder to get a solution in $\{0, \ldots, mn-1\}$

Proof of uniqueness:

- Define $f : \{0, \ldots, mn-1\} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $f(x) = ([x]_m, [x]_n)$
- We proved that f is... surjective
- Since the domain and codomain have same size, f must be injective!
- This means
  if $[x]_m = [y]_m$ and $[x]_n = [y]_n$, then $x = y$.