Summary last week

- A countably infinite if enumeration $\mathbb{N} \to A$; countable if finite or countably infinite.
- countability preserved by subset, image, union, cartesian product
- non-countability of infinite sequences, $2^{\mathbb{N}}$, $\mathcal{P}(\mathbb{N})$, $\mathbb{R}$ by diagonalisation (Cantor)
- injections $f : A \to B$, $g : B \to A$, then exists bijection $A \to B$ (Schröder–Bernstein)
- collections $|\_|$ of equinumerous sets partially ordered by injections; $\mathbb{N} < \mathbb{R}$.

Summary last week

- A countably infinite if enumeration $\mathbb{N} \to A$; countable if finite or countably infinite.
- countability preserved by subset, image, union, cartesian product
- non-countability of infinite sequences, $2^{\mathbb{N}}$, $\mathcal{P}(\mathbb{N})$, $\mathbb{R}$ by diagonalisation (Cantor)
- injections $f : A \to B$, $g : B \to A$, then exists bijection $A \to B$ (Schröder–Bernstein)
- collections $|\_|$ of equinumerous sets partially ordered by injections; $\mathbb{N} < \mathbb{R}$.
- equivalence relation if reflexive, transitive, and symmetric
- if $\sim$ equivalence on A, then $[a] = \{b \mid a \sim b\}$ is equivalence class of $a \in A$
- b representative of $[a]$ if $b \in [a]$
- B system of representatives if for all $a \in A$, unique representative b of $[a]$ in B
- bijection between partitionings P and equivalences $a \sim b$ if $\exists B \in P, a, b \in B$.
- reflexive, transitive relation $\leq$ induces equivalence relation $\leq \cap \geq$

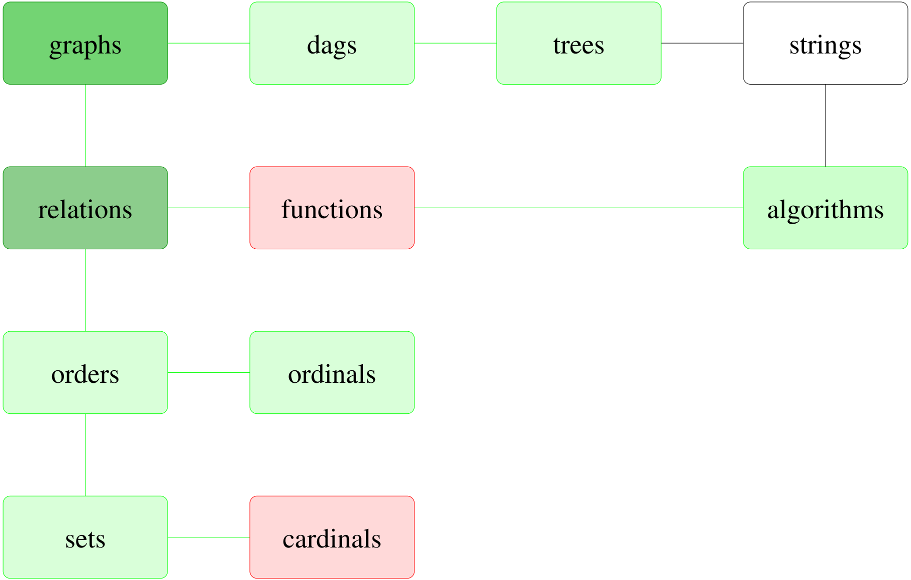
Summary last week

- A countably infinite if enumeration $\mathbb{N} \to A$; countable if finite or countably infinite.
- countability preserved by subset, image, union, cartesian product
- non-countability of infinite sequences, $2^{\mathbb{N}}$, $\mathcal{P}(\mathbb{N})$, $\mathbb{R}$ by diagonalisation (Cantor)
- injections $f : A \to B$, $g : B \to A$, then exists bijection $A \to B$ (Schröder–Bernstein)
- collections $|\_|$ of equinumerous sets partially ordered by injections; $\mathbb{N} < \mathbb{R}$.
- equivalence relation if reflexive, transitive, and symmetric
- if $\sim$ equivalence on A, then $[a] = \{b \mid a \sim b\}$ is equivalence class of $a \in A$
- b representative of $[a]$ if $b \in [a]$
- B system of representatives if for all $a \in A$, unique representative b of $[a]$ in B
- bijection between partitionings P and equivalences $a \sim b$ if $\exists B \in P, a, b \in B$.
- reflexive, transitive relation $\leq$ induces equivalence relation $\leq \cap \geq$
- algorithm for $\gcd(x, y)$ with $x, y \in \mathbb{Z}$ by subtraction, division modulo (Euclid)
- extended algorithm for u, v with $\gcd(x, y) = u \cdot x + v \cdot y$ (Bézout); $\mathrm{lcm}(x, y) = \frac{x \cdot y}{\gcd(x,y)}$

Course themes

- directed and undirected graphs
- relations and functions
- orders and induction
- trees and dags
- finite and infinite counting
- elementary number theory
- Turing machines, algorithms, and complexity
- decidable and undecidable problem

Discrete structures



Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1) $77 = 1 \cdot 77 + 0 \cdot 30$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

$$
\begin{array}{lrrrl}
(1) & 77 = & 1 \cdot 77 + & 0 \cdot 30 & \\
(2) & 30 = & 0 \cdot 77 + & 1 \cdot 30 & \\
(3) & 77 - 30 = & (1 - 0) \cdot 77 + & (0 - 1) \cdot 30 & (1) - (2)
\end{array}
$$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77+$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77+$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77+$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77+$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77+$	$3 \cdot 30$	$(2) - (4)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77 +$	$3 \cdot 30$	$(2) - (4)$
(6)	$4 =$	$2 \cdot 77 +$	$(-5) \cdot 30$	$(4) - (5)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77 +$	$3 \cdot 30$	$(2) - (4)$
(6)	$4 =$	$2 \cdot 77 +$	$(-5) \cdot 30$	$(4) - (5)$
(7)	$9 =$	$(-3) \cdot 77 +$	$8 \cdot 30$	$(5) - (6)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77 +$	$3 \cdot 30$	$(2) - (4)$
(6)	$4 =$	$2 \cdot 77 +$	$(-5) \cdot 30$	$(4) - (5)$
(7)	$9 =$	$(-3) \cdot 77 +$	$8 \cdot 30$	$(5) - (6)$
(8)	$5 =$	$(-5) \cdot 77 +$	$13 \cdot 30$	$(7) - (6)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ *not zero, there exist* $u, v \in \mathbb{Z}$ *with* $\gcd(a,b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77 +$	$3 \cdot 30$	$(2) - (4)$
(6)	$4 =$	$2 \cdot 77 +$	$(-5) \cdot 30$	$(4) - (5)$
(7)	$9 =$	$(-3) \cdot 77 +$	$8 \cdot 30$	$(5) - (6)$
(8)	$5 =$	$(-5) \cdot 77 +$	$13 \cdot 30$	$(7) - (6)$
(9)	$1 =$	$(-7) \cdot 77 +$	$18 \cdot 30$	$(8) - (6)$

Theorem (Bézout's lemma)

for $a, b \in \mathbb{Z}$ not zero, there exist $u, v \in \mathbb{Z}$ with $\gcd(a, b) = u \cdot a + v \cdot b$

Example ($1 = \gcd(77, 30)$)

(1)	$77 =$	$1 \cdot 77 +$	$0 \cdot 30$	
(2)	$30 =$	$0 \cdot 77 +$	$1 \cdot 30$	
(3)	$47 =$	$1 \cdot 77 +$	$(-1) \cdot 30$	$(1) - (2)$
(4)	$17 =$	$1 \cdot 77 +$	$(-2) \cdot 30$	$(3) - (2)$
(5)	$13 =$	$(-1) \cdot 77 +$	$3 \cdot 30$	$(2) - (4)$
(6)	$4 =$	$2 \cdot 77 +$	$(-5) \cdot 30$	$(4) - (5)$
(7)	$9 =$	$(-3) \cdot 77 +$	$8 \cdot 30$	$(5) - (6)$
(8)	$5 =$	$(-5) \cdot 77 +$	$13 \cdot 30$	$(7) - (6)$
(9)	$1 =$	$(-7) \cdot 77 +$	$18 \cdot 30$	$(8) - (6)$

may stop at 1 since 1 is least possible divisor, it's trivial. $u = -7$ and $v = 18$

indeed $1 = \gcd(77, 30) = (-7) \cdot 77 + 18 \cdot 30 = -539 + 540$

The divisibility order $\mid$ (recall from weeks 4 and 5)

Lemma

divisibility $\mid$ *is a well-founded partial order on the positive natural numbers* $\mathbb{N}_{>0}$

The divisibility order $|$

Lemma

divisibility $|$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

The divisibility order $\mid$

Lemma

divisibility $\mid$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

- reflexivity: $x \mid x$ since $x \cdot 1 = x$

The divisibility order $|$

Lemma

divisibility $|$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

- reflexivity: $x \mid x$ since $x \cdot 1 = x$
- transitivity: if $x \mid y$ and $y \mid z$, then $x \cdot y' = y$ and $y \cdot z' = z$ for some y', z'. Hence setting $x' := y' \cdot z'$, we have $x \cdot x' = x \cdot y' \cdot z' = y \cdot z' = z$, so $x \mid z$

The divisibility order $|$

Lemma

divisibility $|$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

- reflexivity: $x \mid x$ since $x \cdot 1 = x$
- transitivity: if $x \mid y$ and $y \mid z$, then $x \cdot y' = y$ and $y \cdot z' = z$ for some y', z'. Hence setting $x' := y' \cdot z'$, we have $x \cdot x' = x \cdot y' \cdot z' = y \cdot z' = z$, so $x \mid z$
- anti-symmetry: if $x \mid y$ and $y \mid x$, then $x \leq y$ and $y \leq x$, hence $x = y$ by anti-symmetry of $\leq$

The divisibility order $|$

Lemma

divisibility $|$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

- reflexivity: $x \mid x$ since $x \cdot 1 = x$
- transitivity: if $x \mid y$ and $y \mid z$, then $x \cdot y' = y$ and $y \cdot z' = z$ for some y', z'. Hence setting $x' := y' \cdot z'$, we have $x \cdot x' = x \cdot y' \cdot z' = y \cdot z' = z$, so $x \mid z$
- anti-symmetry: if $x \mid y$ and $y \mid x$, then $x \leq y$ and $y \leq x$, hence $x = y$ by anti-symmetry of $\leq$
- well-founded: if $\ldots x'' \mid x' \mid x$ were an infinite descending chain, then so would $\ldots x'' < x' < x$, contradicting well-foundedness of $\leq$ ∎

The divisibility order $\mid$

Lemma

divisibility $\mid$ is a well-founded partial order on the positive natural numbers $\mathbb{N}_{>0}$

Proof.

note: if $x \mid y$ then $x + \ldots + x = y$ hence $x \leq y$ (for y positive)

- reflexivity: $x \mid x$ since $x \cdot 1 = x$
- transitivity: if $x \mid y$ and $y \mid z$, then $x \cdot y' = y$ and $y \cdot z' = z$ for some y', z'. Hence setting $x' := y' \cdot z'$, we have $x \cdot x' = x \cdot y' \cdot z' = y \cdot z' = z$, so $x \mid z$
- anti-symmetry: if $x \mid y$ and $y \mid x$, then $x \leq y$ and $y \leq x$, hence $x = y$ by anti-symmetry of $\leq$
- well-founded: if $\ldots x'' \mid x' \mid x$ were an infinite descending chain, then so would $\ldots x'' < x' < x$, contradicting well-foundedness of $\leq$ ∎

$\Rightarrow$ proofs by well-founded induction on $\mid$ for statements on $\mathbb{N}_{>0}$ and $\mathbb{N}_{>1} = \mathbb{N} - \{0, 1\}$

Definition

- p is prime if $p \in \mathbb{N}_{>1}$ and for all x, y, if $p \mid x \cdot y$ then $p \mid x$ or $p \mid y$
- p is irreducible or indecomposable if $p \in \mathbb{N}_{>1}$ and p only has trivial divisors

Definition

- p is prime if $p \in \mathbb{N}_{>1}$ and for all x, y, if $p \mid x \cdot y$ then $p \mid x$ or $p \mid y$
- p is irreducible or indecomposable if $p \in \mathbb{N}_{>1}$ and p only has trivial divisors

Lemma

for $p \in \mathbb{N}_{>1}$, we have p is prime iff p is indecomposable iff p is $\mid$-minimal (on $\mathbb{N}_{>1}$)

Definition

- p is prime if $p \in \mathbb{N}_{>1}$ and for all x, y, if $p \mid x \cdot y$ then $p \mid x$ or $p \mid y$
- p is irreducible or indecomposable if $p \in \mathbb{N}_{>1}$ and p only has trivial divisors

Lemma

for $p \in \mathbb{N}_{>1}$, we have p is prime iff p is indecomposable iff p is $\mid$-minimal

Proof.

- Assume p prime and suppose $p = x \cdot y$. By p being prime $p \mid x$ or $p \mid y$, say w.l.o.g. $p \mid x$. By $x \mid p$, then $x = p$ and $y = 1$, so both are trivial hence p is indecomposable

Definition

- p is prime if $p \in \mathbb{N}_{>1}$ and for all x, y, if $p \mid x \cdot y$ then $p \mid x$ or $p \mid y$
- p is irreducible or indecomposable if $p \in \mathbb{N}_{>1}$ and p only has trivial divisors

Lemma

for $p \in \mathbb{N}_{>1}$, we have p is prime iff p is indecomposable iff p is $\mid$-minimal

Proof.

- Assume p prime and suppose $p = x \cdot y$. By p being prime $p \mid x$ or $p \mid y$, say w.l.o.g. $p \mid x$. By $x \mid p$, then $x = p$ and $y = 1$, so both are trivial hence p is indecomposable
- Assume p indecomposable and suppose $x \mid p$ with $x \in \mathbb{N}_{>1}$, i.e. $x \cdot y = p$ for some y. By p being indecomposable, then x, y are trivial, so $p = x$ and p is $\mid$-minimal

Definition

- p is prime if $p \in \mathbb{N}_{>1}$ and for all x, y, if $p \mid x \cdot y$ then $p \mid x$ or $p \mid y$
- p is irreducible or indecomposable if $p \in \mathbb{N}_{>1}$ and p only has trivial divisors

Lemma

for $p \in \mathbb{N}_{>1}$, we have p is prime iff p is indecomposable iff p is $\mid$-minimal

Proof.

- Assume p prime and suppose $p = x \cdot y$. By p being prime $p \mid x$ or $p \mid y$, say w.l.o.g. $p \mid x$. By $x \mid p$, then $x = p$ and $y = 1$, so both are trivial hence p is indecomposable
- Assume p indecomposable and suppose $x \mid p$ with $x \in \mathbb{N}_{>1}$, i.e. $x \cdot y = p$ for some y. By p being indecomposable, then x, y are trivial, so $p = x$ and p is $\mid$-minimal
- Assume p $\mid$-minimal and suppose $p \mid x \cdot y$, i.e. $p \cdot d = x \cdot y$ for some d. Either $p \mid x$ or else $\gcd(p, x) = 1$ by p being $\mid$-minimal. Then $1 = u \cdot p + v \cdot x$ for some u, v (Bézout): $y = y \cdot 1 = y \cdot (u \cdot p + v \cdot x) = y \cdot u \cdot p + y \cdot v \cdot x = y \cdot u \cdot p + v \cdot p \cdot d = (y \cdot u + v \cdot d) \cdot p$ hence $p \mid y$. That is, either $p \mid x$ or $p \mid y$, so p is prime ∎

Theorem (Fundamental theorem of arithmetic, FTA)

every natural number greater than one can be written as a product of prime numbers, its prime factors, which are unique up to their order.

Theorem (Fundamental theorem of arithmetic, FTA)

every natural number greater than one can be written as a product of prime numbers, its prime factors, which are unique up to their order.

Proof.

- we first show that $\forall x \in \mathbb{N}_{>1}$ there exists a collection of prime numbers p_l such that $x = \prod p_l$, by induction on x well-foundedly ordered by $|$.
  recall from week 5.

Theorem (Fundamental theorem of arithmetic, FTA)

every natural number greater than one can be written as a product of prime numbers, its prime factors, which are unique up to their order.

Proof.

- we first show that $\forall x \in \mathbb{N}_{>1}$ there exists a collection of prime numbers p_I such that $x = \prod p_I$, by induction on x well-foundedly ordered by $|$.
  If x is not prime itself, then $x = y \cdot z$ for y, z non-trivial (by the lemma), hence $y = \prod q_J$ and $z = \prod r_K$ for collections of primes q_J and r_K by the IH twice.
  Combining both, $x = \prod q_J \cdot \prod r_K$, i.e. we may take the concatenation of q_J and r_K.

Theorem (Fundamental theorem of arithmetic, FTA)

every natural number greater than one can be written as a product of prime numbers, its prime factors, which are unique up to their order.

Proof.

- we first show that $\forall x \in \mathbb{N}_{>1}$ there exists a collection of prime numbers p_I such that $x = \prod p_I$, by induction on x well-foundedly ordered by $|$.
  If x is not prime itself, then $x = y \cdot z$ for y, z non-trivial (by the lemma), hence $y = \prod q_J$ and $z = \prod r_K$ for collections of primes q_J and r_K by the IH twice.
  Combining both, $x = \prod q_J \cdot \prod r_K$, i.e. we may take the concatenation of q_J and r_K.
- next we show uniqueness, i.e. if $\prod p_I = \prod q_J$ then the collections of prime numbers p_I and q_J are the same up to order, by mathematical induction on $\#I$.

Theorem (Fundamental theorem of arithmetic, FTA)

every natural number greater than one can be written as a product of prime numbers, its prime factors, which are unique up to their order.

Proof.

- we first show that $\forall x \in \mathbb{N}_{>1}$ there exists a collection of prime numbers p_I such that $x = \prod p_I$, by induction on x well-foundedly ordered by $|$.
  If x is not prime itself, then $x = y \cdot z$ for y, z non-trivial (by the lemma), hence $y = \prod q_J$ and $z = \prod r_K$ for collections of primes q_J and r_K by the IH twice.
  Combining both, $x = \prod q_J \cdot \prod r_K$, i.e. we may take the concatenation of q_J and r_K.
- next we show uniqueness, i.e. if $\prod p_I = \prod q_J$ then the collections of prime numbers p_I and q_J are the same up to order, by mathematical induction on $\#I$.
  Suppose $i \in I$. Then $p_i \mid \prod p_I = \prod q_J$, so $\exists j \in J$ such that $p_i \mid q_j$ hence $p_i = q_j$ (by the lemma twice). Therefore, $\prod p_{I-\{i\}} = \frac{\prod p_I}{p_i} = \frac{\prod q_J}{q_j} = \prod q_{J-\{j\}}$, and by the IH $p_{I-\{i\}}$ and $q_{J-\{j\}}$ are the same up to order, hence so are p_I and q_J. ∎

Theorem

there are infinitely many prime numbers.

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

- set $n := \prod_{i=1}^{k} p_i$, so that $p_i \mid n$ for each i.

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

- set $n := \prod_{i=1}^{k} p_i$, so that $p_i \mid n$ for each i.
- by FTA $n + 1$ has prime factorisation, with primes among $p_1, \ldots, p_k$ by assumption

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

- set $n := \prod_{i=1}^{k} p_i$, so that $p_i \mid n$ for each i.
- by FTA $n + 1$ has prime factorisation, with primes among $p_1, \ldots, p_k$ by assumption
- if $p_i \mid n + 1$, then also $p_i \mid (n + 1) - n = 1$; contradicting p_i is prime. ∎

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

- set $n := \prod_{i=1}^{k} p_i$, so that $p_i \mid n$ for each i.
- by FTA $n + 1$ has prime factorisation, with primes among $p_1, \ldots, p_k$ by assumption
- if $p_i \mid n + 1$, then also $p_i \mid (n + 1) - n = 1$; contradicting p_i is prime. ∎

Remark

there are countably many primes since subset of $\mathbb{N}$.

Theorem

there are infinitely many prime numbers.

Proof.

for a proof by contradiction, suppose $p_1, \ldots, p_k$ were the finite list of primes

- set $n := \prod_{i=1}^{k} p_i$, so that $p_i \mid n$ for each i.
- by FTA $n + 1$ has prime factorisation, with primes among $p_1, \ldots, p_k$ by assumption
- if $p_i \mid n + 1$, then also $p_i \mid (n + 1) - n = 1$; contradicting p_i is prime. ∎

Remark

there are countably many primes since subset of $\mathbb{N}$.

Remark

FTA links numbers wrt addition $(+, -)$ to numbers wrt multiplication $(\cdot, \div)$. Connections between both hard in general, cf. Goldbach's conjecture: if $n > 2$, then $n = p_i + p_j$.

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ *can be uniquely written as* $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ *given a long enough initial segment* p_k *of the prime numbers in ascending order, and collection* e_k *of exponents*

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^k p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Example

- $77 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1$ exponents $e = (0, 0, 0, 1, 1)$ and $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Example

- $77 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1$ exponents $e = (0, 0, 0, 1, 1)$ and $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$
- $77 \cdot 28 = 2^{0+2} \cdot 3^{0+0} \cdot 5^{0+0} \cdot 7^{1+1} \cdot 11^{1+0} = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^1 = 2156$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Example

- $77 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1$ exponents $e = (0,0,0,1,1)$ and $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$
- $77 \cdot 28 = 2^{0+2} \cdot 3^{0+0} \cdot 5^{0+0} \cdot 7^{1+1} \cdot 11^{1+0} = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^1 = 2156$
- $77 \div 28 = 2^{0 \dot{-} 2} \cdot 3^{0 \dot{-} 0} \cdot 5^{0 \dot{-} 0} \cdot 7^{1 \dot{-} 1} \cdot 11^{1 \dot{-} 0} = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^1 = 11$
  $x \div y$ cut-off division ($= \frac{x}{y}$ iff $y \mid x$), $x \dot{-} y$ cut-off subtraction ($= x - y$ iff $y \leq x$)

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Example

- $77 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1$ exponents $e = (0, 0, 0, 1, 1)$ and $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$
- $77 \cdot 28 = 2^{0+2} \cdot 3^{0+0} \cdot 5^{0+0} \cdot 7^{1+1} \cdot 11^{1+0} = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^1 = 2156$
- $77 \div 28 = 2^{0 \dot{-} 2} \cdot 3^{0 \dot{-} 0} \cdot 5^{0 \dot{-} 0} \cdot 7^{1 \dot{-} 1} \cdot 11^{1 \dot{-} 0} = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^1 = 11$
  $x \div y$ cut-off division ($= \frac{x}{y}$ iff $y \mid x$), $x \dot{-} y$ cut-off subtraction ($= x - y$ iff $y \leq x$)
- $\gcd(77, 28) = 2^{\min(0,2)} \cdot 3^{\min(0,0)} \cdot 5^{\min(0,0)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 7$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Example

- $77 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1$ exponents $e = (0,0,0,1,1)$ and $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$
- $77 \cdot 28 = 2^{0+2} \cdot 3^{0+0} \cdot 5^{0+0} \cdot 7^{1+1} \cdot 11^{1+0} = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^2 \cdot 11^1 = 2156$
- $77 \div 28 = 2^{0 \dot{-} 2} \cdot 3^{0 \dot{-} 0} \cdot 5^{0 \dot{-} 0} \cdot 7^{1 \dot{-} 1} \cdot 11^{1 \dot{-} 0} = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^1 = 11$
  $x \div y$ cut-off division ($= \frac{x}{y}$ iff $y \mid x$), $x \dot{-} y$ cut-off subtraction ($= x - y$ iff $y \leq x$)
- $\gcd(77, 28) = 2^{\min(0,2)} \cdot 3^{\min(0,0)} \cdot 5^{\min(0,0)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 7$
- $\mathrm{lcm}(77, 28) = 2^{\max(0,2)} \cdot 3^{\max(0,0)} \cdot 5^{\max(0,0)} \cdot 7^{\max(1,1)} \cdot 11^{\max(1,0)} = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1 = 308$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Corollary

$p_n^e \cdot p_n^f = p_n^{e+f}$, $p_n^e \div p_n^f = p_n^{e \dot{-} f}$, $\mathrm{gcd}(p_n^e, p_n^f) = p_n^{\mathrm{min}(e,f)}$, *and* $\mathrm{lcm}(p_n^e, p_n^f) = p_n^{\mathrm{max}(e,f)}$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ *can be uniquely written as* $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ *given a long enough initial segment* p_k *of the prime numbers in ascending order, and collection* e_k *of exponents*

Corollary

$p_n^e \cdot p_n^f = p_n^{e+f}$, $p_n^e \div p_n^f = p_n^{e \dot{-} f}$, $\gcd(p_n^e, p_n^f) = p_n^{\min(e,f)}$, *and* $\operatorname{lcm}(p_n^e, p_n^f) = p_n^{\max(e,f)}$

Corollary

for $a, b \in \mathbb{Z}$ *not zero,* $\operatorname{lcm}(a, b) = \frac{|a| \cdot |b|}{\gcd(a,b)}$

Operations on numbers via exponents of prime factors

Corollary (to FTA)

any $n \in \mathbb{N}_{>0}$ can be uniquely written as $p_k^e := \prod_{i=1}^{k} p_i^{e_i}$ given a long enough initial segment p_k of the prime numbers in ascending order, and collection e_k of exponents

Corollary

$p_n^e \cdot p_n^f = p_n^{e+f}$, $p_n^e \div p_n^f = p_n^{e \dot{-} f}$, $\mathrm{gcd}(p_n^e, p_n^f) = p_n^{\min(e,f)}$, *and* $\mathrm{lcm}(p_n^e, p_n^f) = p_n^{\max(e,f)}$

Corollary

for $a, b \in \mathbb{Z}$ not zero, $\mathrm{lcm}(a,b) = \frac{|a| \cdot |b|}{\mathrm{gcd}(a,b)}$

Proof.

writing $|a| = p_n^e$ and $|b| = p_n^f$ for n large enough, by the previous corollary:

$\mathrm{lcm}(a,b) = \mathrm{lcm}(p_n^e, p_n^f) = p_n^{\max(e,f)} = p_n^{e+f-\min(e,f)} = \frac{(p_n^e) \cdot (p_n^f)}{\mathrm{gcd}(p_n^e, p_n^f)} = \frac{|a| \cdot |b|}{\mathrm{gcd}(a,b)}$

using $\max(x,y) = x + y - \min(x,y)$ for natural numbers x, y. ∎

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.

caveat: not known whether one-way functions exist

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.

RSA: $p \cdot q$ easy to compute, factoring hard;

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.

RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline, omitting some conditions

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key := (e, n), private key := (d)

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key $:= (e, n)$, private key $:= (d)$
3. encrypt message m into cypher text $c := m^e \pmod{n}$

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key $:= (e, n)$, private key $:= (d)$
3. encrypt message m into cypher text $c := m^e \pmod{n}$
4. decrypt cypher text c into original message $m \equiv c^d \pmod{n}$

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key $:= (e, n)$, private key $:= (d)$
3. encrypt message m into cypher text $c := m^e \pmod{n}$
4. decrypt cypher text c into original message $m \equiv c^d \pmod{n}$

correct: $c^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k\cdot(p-1)\cdot(q-1)} \equiv m \cdot (m^{(p-1)\cdot(q-1)})^k \overset{Euler}{\equiv} m \cdot 1 \equiv m \,(\operatorname{mod} n)$

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key $:= (e, n)$, private key $:= (d)$
3. encrypt message m into cypher text $c := m^e \pmod{n}$
4. decrypt cypher text c into original message $m \equiv c^d \pmod{n}$

correct: $c^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k\cdot(p-1)\cdot(q-1)} \equiv m \cdot (m^{(p-1)\cdot(q-1)})^k \overset{Euler}{\equiv} m \cdot 1 \equiv m \,(\bmod\, n)$
secure: to decrypt c given (e, n), need (d) so $\phi = (p-1) \cdot (q-1)$ given $p \cdot q$; factoring!

Number theory (factorisation, modulo) application: RSA

Cryptography

may be based on one-way functions f, easy to compute f, hard to compute f^{-1}.
RSA: $p \cdot q$ easy to compute, factoring hard; not hard on quantum computers (Shor)

RSA outline

1. choose large primes p,q. set $n := p \cdot q$ and $\phi := (p-1) \cdot (q-1)$
2. choose e,d such that $e \cdot d \equiv 1 \pmod{\phi}$; public key $:= (e, n)$, private key $:= (d)$
3. encrypt message m into cypher text $c := m^e \pmod{n}$
4. decrypt cypher text c into original message $m \equiv c^d \pmod{n}$

correct: $c^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k\cdot(p-1)\cdot(q-1)} \equiv m \cdot (m^{(p-1)\cdot(q-1)})^k \overset{\text{Euler}}{\equiv} m \cdot 1 \equiv m \pmod{n}$
secure: to decrypt c given (e, n), need (d) so $\phi = (p-1) \cdot (q-1)$ given $p \cdot q$; factoring!

RSA ingredients developed on following slides:

modulo, Euler (RSA case), fast exponentiation, Chinese remainder (speed-up)

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same
- congruence modulo n is equivalence relation

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same
- congruence modulo n is equivalence relation
- congruence modulo n is $+,\cdot$-congruence: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same
- congruence modulo n is equivalence relation
- congruence modulo n is $+,\cdot$-congruence: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$
- equivalence class of a is congruence or residue class: $\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same
- congruence modulo n is equivalence relation
- congruence modulo n is $+$,$\cdot$-congruence: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$
- equivalence class of a is congruence or residue class: $\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$
- $\mathbb{Z}/n\mathbb{Z}$ is the set of all congruence classes modulo n

Modulo

Definition (modulo some positive natural number n)

- integers a, b are congruent modulo n, denoted by $a \equiv b \pmod{n}$ if remainders $a \bmod n$ and $b \bmod n$ after division by n are the same
- congruence modulo n is equivalence relation
- congruence modulo n is $+,\cdot$-congruence: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$
- equivalence class of a is congruence or residue class: $\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$
- $\mathbb{Z}/n\mathbb{Z}$ is the set of all congruence classes modulo n

Remark

As system of representatives we usually employ the smallest non-negative remainders $\{0, 1, 2, \ldots, n-1\}$ or the absolutely-smallest remainders

$$\begin{cases} \{-n/2 + 1, \ldots, -1, 0, 1, \ldots, n/2\} & \text{if } n \text{ is even} \\ \{-(n-1)/2, \ldots, -1, 0, 1, \ldots, (n-1)/2\} & \text{if } n \text{ is odd.} \end{cases}$$

Modulo (continued)

Example

We have $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$; moreover $\overline{0} = \{0, 5, 10, 15, \ldots\} = \overline{5}$, and $\overline{2} + \overline{4} = \overline{6} = \overline{1}$ and $\overline{4} \cdot \overline{4} \cdot \overline{3} = \overline{4 \cdot 4} \cdot \overline{3} = \overline{1} \cdot \overline{3} = \overline{3}$.

Modulo (continued)

Example

We have $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$; moreover $\overline{0} = \{0, 5, 10, 15, \ldots\} = \overline{5}$, and $\overline{2} + \overline{4} = \overline{6} = \overline{1}$ and $\overline{4} \cdot \overline{4} \cdot \overline{3} = \overline{4 \cdot 4} \cdot \overline{3} = \overline{1} \cdot \overline{3} = \overline{3}$.

Lemma

The functions

$$+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, (\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a + b},$$

$$\cdot\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, (\overline{a}, \overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b},$$

are well-defined ■

Modulo (continued)

Example

We have $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$; moreover $\overline{0} = \{0, 5, 10, 15, \ldots\} = \overline{5}$, and $\overline{2} + \overline{4} = \overline{6} = \overline{1}$ and $\overline{4} \cdot \overline{4} \cdot \overline{3} = \overline{4 \cdot 4} \cdot \overline{3} = \overline{1} \cdot \overline{3} = \overline{3}$.

Lemma

The functions

$$+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,,\ (\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a + b}\,,$$

$$\cdot\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\,,\ (\overline{a}, \overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}\,,$$

are well-defined ∎

Example

In many programming languages there is a data type for integers corresponding to $\mathbb{Z}/2^{2^n}\mathbb{Z}$ for some $n \geq 3$. For example `unsigned int` in C corresponds to $n = 5$ resp. $n = 6$. For $n = 5$, i.e. a 32-bits architecture, the sum of $2^{2^5} - 1 = 2^{32} - 1$ and 1 is 0.

Inverses modulo

Definition

A congruence class $\overline{a}$ modulo n is invertible, if there is a congruence class $\overline{b}$ modulo n such that $\overline{a} \cdot \overline{b} \equiv \overline{1} \pmod{n}$, i.e. if $a \cdot b - 1 = k \cdot n$ for some k.

Inverses modulo

Definition

A congruence class $\overline{a}$ modulo n is invertible, if there is a congruence class $\overline{b}$ modulo n such that $\overline{a} \cdot \overline{b} \equiv \overline{1} \pmod{n}$, i.e. if $a \cdot b - 1 = k \cdot n$ for some k.

Lemma

$\overline{a}$ modulo n is invertible for non-zero a iff $\gcd(a, n) = 1$; in that case, we can compute using Bézout's lemma, integers u, v such that $u \cdot a + v \cdot n = 1$ and $\overline{a}^{-1} = \overline{u}$

Inverses modulo

Definition

A congruence class $\overline{a}$ modulo n is invertible, if there is a congruence class $\overline{b}$ modulo n such that $\overline{a} \cdot \overline{b} \equiv \overline{1} \pmod{n}$, i.e. if $a \cdot b - 1 = k \cdot n$ for some k.

Lemma

$\overline{a}$ modulo n is invertible for non-zero a iff $\gcd(a, n) = 1$; in that case, we can compute using Bézout's lemma, integers u, v such that $u \cdot a + v \cdot n = 1$ and $\overline{a}^{-1} = \overline{u}$

Proof.

if $\gcd(a, n) = 1$ and $u \cdot a + v \cdot n = 1$, then $\overline{1} = \overline{u} \cdot \overline{a} + \overline{v} \cdot \overline{n} = \overline{u} \cdot \overline{a}$. vice versa, if $\overline{a}$ invertible, then $\overline{a} \cdot \overline{b} = \overline{1}$ for some b, hence $\overline{a \cdot b - 1} = \overline{0}$; and therefore $n \mid (a \cdot b - 1)$. thus $\gcd(a, n) = 1$, as $\gcd(a, n)$ divides n hence $a \cdot b - 1$, and a hence $a \cdot b$ ∎

Inverses modulo

Definition

A congruence class $\overline{a}$ modulo n is invertible, if there is a congruence class $\overline{b}$ modulo n such that $\overline{a} \cdot \overline{b} \equiv \overline{1} \pmod{n}$, i.e. if $a \cdot b - 1 = k \cdot n$ for some k.

Lemma

$\overline{a}$ modulo n is invertible for non-zero a iff $\gcd(a, n) = 1$; in that case, we can compute using Bézout's lemma, integers u, v such that $u \cdot a + v \cdot n = 1$ and $\overline{a}^{-1} = \overline{u}$

Proof.

if $\gcd(a, n) = 1$ and $u \cdot a + v \cdot n = 1$, then $\overline{1} = \overline{u} \cdot \overline{a} + \overline{v} \cdot \overline{n} = \overline{u} \cdot \overline{a}$. vice versa, if $\overline{a}$ invertible, then $\overline{a} \cdot \overline{b} = \overline{1}$ for some b, hence $\overline{a \cdot b - 1} = \overline{0}$; and therefore $n \mid (a \cdot b - 1)$. thus $\gcd(a, n) = 1$, as $\gcd(a, n)$ divides n hence $a \cdot b - 1$, and a hence $a \cdot b$ ∎

Corollary (cancellation by multiplication with $\overline{a}^{-1}$)

if $0 < a < p$ and $a \cdot b \equiv a \cdot c \pmod{p}$ with p prime, then $b \equiv c \pmod{p}$

Theorem (Fermat's little theorem, FLT)

for prime p, and integer a with $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$

Theorem (Fermat's little theorem, FLT)

for prime p, and integer a with $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$

Proof.

by cancellation of $\overline{1 \cdot 2 \cdots (p-1)}$ from

$$\overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{a^{p-1}} = \overline{1 \cdot a} \cdot \overline{2 \cdot a} \cdots \overline{(p-1) \cdot a} = \overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{1}$$

where we use cancellation again to show $\overline{1 \cdot a}, \overline{2 \cdot a}, \ldots, \overline{(p-1) \cdot a}$ are all distinct and also from $\overline{0}$, so that they must be a permutation of the congruence classes $\overline{1}, \overline{2}, \ldots, \overline{(p-1)}$, to conclude their products are the same (double counting). ∎

Theorem (Fermat's little theorem, FLT)

for prime p, and integer a with $p \nmid a$*, we have* $a^{p-1} \equiv 1 \pmod{p}$

Proof.

by cancellation of $\overline{1 \cdot 2 \cdots (p-1)}$ from

$$\overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{a^{p-1}} = \overline{1 \cdot a} \cdot \overline{2 \cdot a} \cdots \overline{(p-1) \cdot a} = \overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{1}$$

where we use cancellation again to show $\overline{1 \cdot a}, \overline{2 \cdot a}, \ldots, \overline{(p-1) \cdot a}$ are all distinct and also from $\overline{0}$, so that they must be a permutation of the congruence classes $\overline{1}, \overline{2}, \ldots, \overline{(p-1)}$, to conclude their products are the same (double counting). ∎

Corollary (Euler's theorem, RSA case)

for all primes p, q*, and integers a with* $\gcd(a, p \cdot q) = 1$, $a^{(p-1)\cdot(q-1)} \equiv 1 \pmod{p \cdot q}$

Theorem (Fermat's little theorem, FLT)

for prime p, and integer a with $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$

Proof.

by cancellation of $\overline{1 \cdot 2 \cdots (p-1)}$ from

$$\overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{a^{p-1}} = \overline{1 \cdot a} \cdot \overline{2 \cdot a} \cdots \overline{(p-1) \cdot a} = \overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{1}$$

where we use cancellation again to show $\overline{1 \cdot a}, \overline{2 \cdot a}, \ldots, \overline{(p-1) \cdot a}$ are all distinct and also from $\overline{0}$, so that they must be a permutation of the congruence classes $\overline{1}, \overline{2}, \ldots, \overline{(p-1)}$, to conclude their products are the same (double counting). ∎

Corollary (Euler's theorem, RSA case)

for all primes p, q, *and integers a with* $\gcd(a, p \cdot q) = 1$, $a^{(p-1)\cdot(q-1)} \equiv 1 \pmod{p \cdot q}$

Proof.

By FTA and $p, q \mid a^{(p-1)\cdot(q-1)} - 1$, from FLT twice, with a^{p-1}, q resp. a^{q-1}, p. ∎

Fast exponentiation

Example

We compute: $3^9 = 3^{(1001)_2} = 3^{2^3} \cdot 3^{2^0} = 3^8 \cdot 3^1 = ((3^2)^2)^2 \cdot 3 = 19683$. The computation uses 4 multiplications, of which 3 are for squaring.

Fast exponentiation

Example

We compute: $3^9 = 3^{(1001)_2} = 3^{2^3} \cdot 3^{2^0} = 3^8 \cdot 3^1 = ((3^2)^2)^2 \cdot 3 = 19683$. The computation uses 4 multiplications, of which 3 are for squaring.

Theorem (exponentiation by squaring)

Let a be an integer and let n be a positive integer with binary representation $b_k b_{k-1} \cdots b_0$ where $b_k = 1$; in symbols $(b_k b_{k-1} \cdots b_0)_2 = n$. We can then compute the power a^n by squaring (and possibly multiplying) k-times:

> *Set $x = a$.*
>
> *For i from $k-1$ down to 0 repeat:*
>
> *Set $x = x^2$.*
>
> *If $b_i = 1$, set $x = x * a$.*

Fast exponentation (continued)

Proof.

- By mathematical induction on k; for $k = 0$ $n = 1$ and the algorithm yields $a^1 = a$
- For $k > 0$ we write

$$n = \sum_{i=0}^{k} b_i 2^i = m \cdot 2 + b_0 \quad \text{with} \quad m = \sum_{i=1}^{k} b_i 2^{i-1} = \sum_{i=0}^{k-1} b_{i+1} 2^i$$

  By the induction hypothesis, the first $k - 1$ loops yield the value a^m; therefore, the last time ($i = 0$) yields

$$(a^m)^2 \cdot a^{b_0} = a^n$$

Fast exponentation (continued)

Proof.

- By mathematical induction on k; for $k = 0$ $n = 1$ and the algorithm yields $a^1 = a$
- For $k > 0$ we write

$$n = \sum_{i=0}^{k} b_i 2^i = m \cdot 2 + b_0 \quad \text{with} \quad m = \sum_{i=1}^{k} b_i 2^{i-1} = \sum_{i=0}^{k-1} b_{i+1} 2^i$$

By the induction hypothesis, the first $k - 1$ loops yield the value a^m; therefore, the last time ($i = 0$) yields

$$(a^m)^2 \cdot a^{b_0} = a^n$$

∎

Fast exponentation (continued)

Proof.

- By mathematical induction on k; for $k = 0$ $n = 1$ and the algorithm yields $a^1 = a$
- For $k > 0$ we write

$$n = \sum_{i=0}^{k} b_i 2^i = m \cdot 2 + b_0 \quad \text{with} \quad m = \sum_{i=1}^{k} b_i 2^{i-1} = \sum_{i=0}^{k-1} b_{i+1} 2^i$$

By the induction hypothesis, the first $k - 1$ loops yield the value a^m; therefore, the last time ($i = 0$) yields

$$(a^m)^2 \cdot a^{b_0} = a^n$$

∎

Remark

during exponentiation modulo some number n, no numbers $\geq n$ need to be used.

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \le x < p \cdot q$ *to pairs* (a, b) *with* $0 \le a < p$ *and* $0 \le b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0				
1					
2					

$$0 \mapsto (0, 0)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0				
1		1			
2					

$$1 \mapsto (1, 1)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0				
1		1			
2			2		

$$2 \mapsto (2, 2)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0			3	
1		1			
2			2		

$$3 \mapsto (0, 3)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$, *then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$, *is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0			3	
1		1			4
2			2		

$$4 \mapsto (1, 4)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0			3	
1		1			4
2	5		2		

$$5 \mapsto (2, 0)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	
1		1			4
2	5		2		

$$6 \mapsto (0, 1)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	
1		1	7		4
2	5		2		

$$7 \mapsto (1, 2)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	
1		1	7		4
2	5		2	8	

$$8 \mapsto (2, 3)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	9
1		1	7		4
2	5		2	8	

$$9 \mapsto (0, 4)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	9
1	10	1	7		4
2	5		2	8	

$$10 \mapsto (1, 0)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6		3	9
1	10	1	7		4
2	5	11	2	8	

$$11 \mapsto (2, 1)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$**)**

a \ b	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7		4
2	5	11	2	8	

$$12 \mapsto (0, 2)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$**)**

a \ b	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	

$$13 \mapsto (1, 3)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 5$)

a \ b	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

$$14 \mapsto (2, 4)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 3$**)**

a \ b	0	1	2
0	0		
1			
2			

$$0 \mapsto (0, 0)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 3$)

a \ b	0	1	2
0	0		
1		1	
2			

$$1 \mapsto (1, 1)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 3$**)**

a \ b	0	1	2
0	0		
1		1	
2			2

$$2 \mapsto (2, 2)$$

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Example ($p = 3, q = 3$**)**

a \ b	0	1	2
0	0		
1		1	
2			2

$3 \mapsto (0, 0)$ $\gcd(p, q) = 3 \neq 1$, crt not a bijection

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Proof.

sufficient to prove injectivity.

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Proof.

sufficient to prove injectivity. suppose $0 \leq x, x' < p \cdot q$. if $\mathrm{crt}(x) = \mathrm{crt}(x')$, then $x \equiv x' \pmod{p}$ and $x \equiv x' \pmod{q}$, hence $p, q \mid x - x'$. Thus

$$p \cdot q = \frac{p \cdot q}{1} = \frac{p \cdot q}{\gcd(p, q)} = \mathrm{lcm}(p, q) \mid x - x'$$

that is, solutions are $p \cdot q$ apart, so $x - x' = 0$ and $x = x'$.

Chinese remainder theorem, bijection

Theorem (Chinese Remainder, bijection)

if $\gcd(p, q) = 1$*, then the following function* crt *from numbers* $0 \leq x < p \cdot q$ *to pairs* (a, b) *with* $0 \leq a < p$ *and* $0 \leq b < q$*, is a bijection:*

$$x \mapsto (x \bmod p, x \bmod q)$$

Proof.

sufficient to prove injectivity. suppose $0 \leq x, x' < p \cdot q$. if $\mathrm{crt}(x) = \mathrm{crt}(x')$, then $x \equiv x' \pmod{p}$ and $x \equiv x' \pmod{q}$, hence $p, q \mid x - x'$. Thus

$$p \cdot q = \frac{p \cdot q}{1} = \frac{p \cdot q}{\gcd(p, q)} = \mathrm{lcm}(p, q) \mid x - x'$$

that is, solutions are $p \cdot q$ apart, so $x - x' = 0$ and $x = x'$. ■

Theorem (Chinese remainder theorem, Bézout)

Let p and q be positive integers such that $\gcd(p,q)=1$, and let a and b be arbitrary integers. The congruence system

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then has the unique solution $x \equiv vqa + upb \pmod{pq}$ where the integers u and v such that $up + vq = 1$ can be computed using Bézout's lemma.

Theorem (Chinese remainder theorem, Bézout)

Let p and q be positive integers such that $\gcd(p, q) = 1$, and let a and b be arbitrary integers. The congruence system

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then has the unique solution $x \equiv vqa + upb \pmod{pq}$ where the integers u and v such that $up + vq = 1$ can be computed using Bézout's lemma.

Proof.

- (existence) we show $x = v \cdot q \cdot a + u \cdot p \cdot b$ for $up + vq = 1$ satisfies equations: $x \equiv v \cdot q \cdot a + u \cdot p \cdot b \equiv v \cdot q \cdot a \equiv (1 - u \cdot p) \cdot a \equiv a - u \cdot p \cdot a \equiv a \pmod{p}$ and similarly for $x \equiv b \pmod{q}$
- (uniqueness)

Theorem (Chinese remainder theorem, Bézout)

Let p and q be positive integers such that $\gcd(p, q) = 1$, and let a and b be arbitrary integers. The congruence system

$$\begin{aligned} x &\equiv a \pmod p \\ x &\equiv b \pmod q \end{aligned}$$

then has the unique solution $x \equiv vqa + upb \pmod{pq}$ where the integers u and v such that $up + vq = 1$ can be computed using Bézout's lemma.

Proof.

- (existence) we show $x = v \cdot q \cdot a + u \cdot p \cdot b$ for $up + vq = 1$ satisfies equations: $x \equiv v \cdot q \cdot a + u \cdot p \cdot b \equiv v \cdot q \cdot a \equiv (1 - u \cdot p) \cdot a \equiv a - u \cdot p \cdot a \equiv a \pmod p$ and similarly for $x \equiv b \pmod q$
- (uniqueness) as before: if both x, x' are solutions to the two equations, then $p, q \mid (x - x')$, hence $\mathrm{lcm}(p, q) = \frac{p \cdot q}{\gcd(p,q)} = p \cdot q \mid (x - x')$. That is, solutions are $p \cdot q$ apart, hence unique in $\{0, ..., p \cdot q - 1\}$.

Theorem (Chinese remainder theorem, Bézout)

Let p and q be positive integers such that $\gcd(p, q) = 1$, and let a and b be arbitrary integers. The congruence system

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then has the unique solution $x \equiv vqa + upb \pmod{pq}$ where the integers u and v such that $up + vq = 1$ can be computed using Bézout's lemma.

Proof.

- (existence) we show $x = v \cdot q \cdot a + u \cdot p \cdot b$ for $up + vq = 1$ satisfies equations: $x \equiv v \cdot q \cdot a + u \cdot p \cdot b \equiv v \cdot q \cdot a \equiv (1 - u \cdot p) \cdot a \equiv a - u \cdot p \cdot a \equiv a \pmod{p}$ and similarly for $x \equiv b \pmod{q}$
- (uniqueness) as before: if both x, x' are solutions to the two equations, then $p, q \mid (x - x')$, hence $\mathrm{lcm}(p, q) = \frac{p \cdot q}{\gcd(p,q)} = p \cdot q \mid (x - x')$. That is, solutions are $p \cdot q$ apart, hence unique in $\{0, ..., p \cdot q - 1\}$. ∎

Example

The following congruence system has the unique solution $x \equiv 16 \pmod{35}$

$$x \equiv 1 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Example

The following congruence system has the unique solution $x \equiv 16 \pmod{35}$

$$x \equiv 1 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

We compute integers u and v, such that $u \cdot 5 + v \cdot 7 = \gcd(5,7)$.

$A = (5,1,0)$	$B = (7,0,1)$	$q = 0$
$A = (7,0,1)$	$B = (5,1,0)$	$q = 1$
$A = (5,1,0)$	$B = (2,-1,1)$	$q = 2$
$A = (2,-1,-1)$	$B = (1,3,-2)$	$q = 2$

Hence $u = 3$, $v = -2$ and $\gcd(5,7) = 3 \cdot 5 - 2 \cdot 7 = 1$, and therefore

$$\underbrace{-2}_{v} \cdot \underbrace{7}_{q} \cdot \underbrace{1}_{a} + \underbrace{3}_{u} \cdot \underbrace{5}_{p} \cdot \underbrace{2}_{b} = 16$$

By the theorem, the solution $x \equiv 16 \pmod{35}$ is unique

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad \Longleftrightarrow \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad \Longleftrightarrow \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Proof.

$$\Leftarrow \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) + k \cdot p \cdot q \equiv a \pmod{p}$$

$$x \equiv a + p \cdot p' \cdot (b - a) + k \cdot p \cdot q \equiv a + b - a \equiv b \pmod{q}$$

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p,q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad\Longleftrightarrow\quad x \equiv a + p \cdot ((p' \cdot (b-a)) \bmod q) \pmod{p \cdot q}$$

Proof.

$\Leftarrow$ $x \equiv a + p \cdot ((p' \cdot (b-a)) \bmod q) + k \cdot p \cdot q \equiv a \pmod{p}$
$x \equiv a + p \cdot p' \cdot (b-a) + k \cdot p \cdot q \equiv a + b - a \equiv b \pmod{q}$

$\Rightarrow$ previous item shows rhs is a solution. now show it is unique modulo $p \cdot q$.
$0 \leq x, x' < p \cdot q$ being solutions entails $x \equiv x' \pmod{p}$ and $x \equiv x' \pmod{q}$, hence
$p, q \mid x - x'$. Thus, $p \cdot q = \frac{p \cdot q}{\gcd(p,q)} = \mathrm{lcm}(p,q) \mid x - x'$, so $x - x' = 0$ and $x = x'$. ∎

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad\iff\quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Example

Let $p = 3$, $q = 5$ (see above). Then $p' = 2$ ($3 \cdot 2 \equiv 1 \pmod{5}$). E.g. for $a = 1$ and $b = 2$, we obtain $x = 1 + 3 \cdot (2 \cdot (2 - 1) \bmod 5) = 7$, and 7 is indeed the number we find at coordinates $(a, b) = (1, 2)$ in the table on slide 17. For another example, at coordinate $(2, 1)$ in the table $x = 2 + 3 \cdot (2 \cdot (1 - 2) \bmod 5) = 2 + 3 \cdot (-2 \bmod 5) = 2 + 3 \cdot 3 = 11$.

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad \Longleftrightarrow \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Application to RSA

Speed up computation of $c^d \bmod (p \cdot q)$ for $\gcd(p, q) = 1$?

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p,q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \iff x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Application to RSA

Speed up computation of $c^d \bmod (p \cdot q)$ for $\gcd(p,q) = 1$?

1. compute $a := c^{d \bmod (p-1)} \bmod p$; by FLT $c^d \equiv a \pmod{p}$

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad \iff \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Application to RSA

Speed up computation of $c^d \bmod (p \cdot q)$ for $\gcd(p, q) = 1$?

1. compute $a := c^{d \bmod (p-1)} \bmod p$; by FLT $c^d \equiv a \pmod{p}$
2. compute $b := c^{d \bmod (q-1)} \bmod q$; by FLT $c^d \equiv b \pmod{q}$

Chinese remainder, RSA

Theorem (Chinese remainder, RSA)

Let $\gcd(p, q) = 1$ *and let* p' *be inverse of* p *modulo* q*, i.e.* $p \cdot p' \equiv 1 \pmod{q}$*. Then*

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned} \quad \Longleftrightarrow \quad x \equiv a + p \cdot ((p' \cdot (b - a)) \bmod q) \pmod{p \cdot q}$$

Application to RSA

Speed up computation of $c^d \bmod (p \cdot q)$ for $\gcd(p, q) = 1$?

1. compute $a := c^{d \bmod (p-1)} \bmod p$; by FLT $c^d \equiv a \pmod{p}$
2. compute $b := c^{d \bmod (q-1)} \bmod q$; by FLT $c^d \equiv b \pmod{q}$
3. compute $m := a + p \cdot ((p' \cdot (b - a)) \bmod q) \bmod (p \cdot q)$; by CRT $m \equiv c^d \pmod{p \cdot q}$.