Competitive
Programming and
Mathematics
Society

Number Theory

Workshop 2, Week 6, Term 1, 2021

CPMSoc Mathematics

Table of contents

CPMSOC

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.
- In number theory, we restrict ourselves to discrete quantities, like integers or natural numbers.

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.
- In number theory, we restrict ourselves to discrete quantities, like integers or natural numbers.
- This generally makes the questions harder.

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.
- In number theory, we restrict ourselves to discrete quantities, like integers or natural numbers.
- This generally makes the questions harder.

Theorem (Fermat's Last Theorem, 1637-1995)

$a^n + b^n = c^n$ has no integer solutions for $n > 2$.

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.
- In number theory, we restrict ourselves to discrete quantities, like integers or natural numbers.
- This generally makes the questions harder.

Theorem (Fermat's Last Theorem, 1637-1995)

$a^n + b^n = c^n$ *has no integer solutions for* $n > 2$.

- Key topics in number theory include divisibility, primality, and partitioning.

What is Number Theory?

- In algebra, we usually deal with continuous quantities, like real or complex numbers.
- In number theory, we restrict ourselves to discrete quantities, like integers or natural numbers.
- This generally makes the questions harder.

Theorem (Fermat's Last Theorem, 1637-1995)

$a^n + b^n = c^n$ *has no integer solutions for* $n > 2$.

- Key topics in number theory include divisibility, primality, and partitioning.
- Key techniques include modular arithmetic and algebraic manipulations.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$
  - $0 \equiv 3 \pmod{3}, 1 \equiv 4 \pmod{3}, 2 \equiv 5 \pmod{3}, 3 \equiv 6 \pmod{3}, \ldots$

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$
  - $0 \equiv 3 \pmod{3}, 1 \equiv 4 \pmod{3}, 2 \equiv 5 \pmod{3}, 3 \equiv 6 \pmod{3}, \ldots$
- Modular equivalence, written as $\equiv$, is similar to $=$ in a number of ways, so we say it is an equivalence relation.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$
  - $0 \equiv 3 \pmod{3}, 1 \equiv 4 \pmod{3}, 2 \equiv 5 \pmod{3}, 3 \equiv 6 \pmod{3}, \ldots$
- Modular equivalence, written as $\equiv$, is similar to $=$ in a number of ways, so we say it is an equivalence relation.
- It is transitive:
  $3 \equiv 7 \pmod{4}$ and $7 \equiv 15 \pmod{4}$ implies $3 \equiv 15 \pmod{4}$, just as
  $a = b, b = c \implies a = c$.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$
  - $0 \equiv 3 \pmod{3}, 1 \equiv 4 \pmod{3}, 2 \equiv 5 \pmod{3}, 3 \equiv 6 \pmod{3}, \ldots$
- Modular equivalence, written as $\equiv$, is similar to $=$ in a number of ways, so we say it is an equivalence relation.
- It is transitive:
  $3 \equiv 7 \pmod{4}$ and $7 \equiv 15 \pmod{4}$ implies $3 \equiv 15 \pmod{4}$, just as $a = b, b = c \implies a = c$.
- It is reflexive:
  $a \equiv a \pmod{n}$, just as $a = a$.

Modular Arithmetic

- We say that $a \equiv b \pmod{n}$ when it matches any of these equivalent definitions:
  1. $a - b = kn$ for some integer k.
  2. $a = kn + b$ for some integer k.
  3. a and b have the same remainder when divided by n.
  - $4 \equiv 13 \equiv -5 \pmod{9}$
  - $0 \equiv 3 \pmod{3}, 1 \equiv 4 \pmod{3}, 2 \equiv 5 \pmod{3}, 3 \equiv 6 \pmod{3}, \ldots$
- Modular equivalence, written as $\equiv$, is similar to $=$ in a number of ways, so we say it is an equivalence relation.
- It is transitive:
  $3 \equiv 7 \pmod{4}$ and $7 \equiv 15 \pmod{4}$ implies $3 \equiv 15 \pmod{4}$, just as $a = b, b = c \implies a = c$.
- It is reflexive:
  $a \equiv a \pmod{n}$, just as $a = a$.
- It is symmetric:
  $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$, just as $a = b \implies b = a$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.
- If p is prime, then for every a ($p \nmid a$) there exists b such that $ab \equiv 1 \pmod{p}$.

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.
- If p is prime, then for every a ($p \nmid a$) there exists b such that $ab \equiv 1 \pmod{p}$.
- If p is prime, then $a^p \equiv a \pmod{p}$ (Fermat's little theorem).

Modular Arithmetic

Modular equivalence has some other fun properties.

- $n \equiv 0 \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{kn}$.
- If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.
- If p is prime, then for every a ($p \nmid a$) there exists b such that $ab \equiv 1 \pmod{p}$.
- If p is prime, then $a^p \equiv a \pmod{p}$ (Fermat's little theorem).
- p is prime iff $(p-1)! \equiv -1 \pmod{p}$ (Wilson's theorem).

Modular Arithmetic

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.
3. If this were a perfect square, then we could write $4^k \left(3 + 4^{k'} x\right) = n^2$ for some $n \in \mathbb{Z}$.

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.
3. If this were a perfect square, then we could write $4^k \left(3 + 4^{k'} x\right) = n^2$ for some $n \in \mathbb{Z}$.
4. However, we then have some integer $u = 2^{-k} n$ where $u^2 = 3 + 4^{k'} x \equiv 3 \pmod 4$.

Modular Arithmetic

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \dots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.
3. If this were a perfect square, then we could write $4^k \left(3 + 4^{k'} x\right) = n^2$ for some $n \in \mathbb{Z}$.
4. However, we then have some integer $u = 2^{-k} n$ where $u^2 = 3 + 4^{k'} x \equiv 3 \pmod 4$.
5. For any perfect square, we have $n^2 \equiv 0^2, 1^2, 2^2$, or $3^2 \equiv 0$ or $1 \pmod 4$.

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.
3. If this were a perfect square, then we could write $4^k \left(3 + 4^{k'} x\right) = n^2$ for some $n \in \mathbb{Z}$.
4. However, we then have some integer $u = 2^{-k} n$ where $u^2 = 3 + 4^{k'} x \equiv 3 \pmod 4$.
5. For any perfect square, we have $n^2 \equiv 0^2, 1^2, 2^2$, or $3^2 \equiv 0$ or $1 \pmod 4$.
6. Since all perfect squares have remainder 0 or 1, we have a contradiction.

Modular Arithmetic

CPMSOC

Example

Can you find a set of 2000 distinct positive integers such that the sum of the members of every subset is not a perfect square?

1. Consider the set of integers given by $n_i = 3 \cdot 4^i$ for $i = 1, 2, \ldots, 2000$.
2. Now any sum of these integers can be written as $4^k \left(3 + 4^{k'} x\right)$ for some $k, k', x \in \mathbb{N}$.
3. If this were a perfect square, then we could write $4^k \left(3 + 4^{k'} x\right) = n^2$ for some $n \in \mathbb{Z}$.
4. However, we then have some integer $u = 2^{-k} n$ where $u^2 = 3 + 4^{k'} x \equiv 3 \pmod 4$.
5. For any perfect square, we have $n^2 \equiv 0^2, 1^2, 2^2$, or $3^2 \equiv 0$ or $1 \pmod 4$.
6. Since all perfect squares have remainder 0 or 1, we have a contradiction.
7. Thus, every subset sum is not a perfect square.

Divisibility

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.

Divisibility

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod{b}$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \not\mid 6$.

Divisibility

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod b$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \nmid 6$.
- Divisibility is similar to $\geq$ and $\leq$ in a number of ways, so we say it is a partial order relation.

Divisibility

CPMSOC

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod{b}$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \nmid 6$.
- Divisibility is similar to $\geq$ and $\leq$ in a number of ways, so we say it is a partial order relation.
- It is transitive:
  $2 \mid 4$ and $4 \mid 8$ implies $2 \mid 8$, just as $\pi \geq 3$ and $3 \geq e$ implies $\pi \geq e$.

Divisibility

CPMSOC

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod{b}$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \not| 6$.
- Divisibility is similar to $\geq$ and $\leq$ in a number of ways, so we say it is a partial order relation.
- It is transitive:
  $2 \mid 4$ and $4 \mid 8$ implies $2 \mid 8$, just as $\pi \geq 3$ and $3 \geq e$ implies $\pi \geq e$.
- It is reflexive:
  $7|7$, just as $\pi \geq \pi$.

Divisibility

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod{b}$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \not| 6$.
- Divisibility is similar to $\geq$ and $\leq$ in a number of ways, so we say it is a partial order relation.
- It is transitive:
  $2 \mid 4$ and $4 \mid 8$ implies $2 \mid 8$, just as $\pi \geq 3$ and $3 \geq e$ implies $\pi \geq e$.
- It is reflexive:
  $7|7$, just as $\pi \geq \pi$.
- It is antisymmetric:
  $4 \mid 8$ implies $8 \not| 4$, just as $x \geq y$ implies $y \not\geq x$ unless $y = x$.
  If $a \mid b$, then $b \not| a$ unless $b = a$.

Divisibility

CPMSOC

- We say $a \mid b$ ("a divides b") when $b = ka = ka + 0$ for some integer k.
- Alternatively, when $a \equiv 0 \pmod{b}$.
  $2 \mid 4 \mid 12$ and $2 \mid 6 \mid 12$ but $4 \not| 6$.
- Divisibility is similar to $\geq$ and $\leq$ in a number of ways, so we say it is a partial order relation.
- It is transitive:
  $2 \mid 4$ and $4 \mid 8$ implies $2 \mid 8$, just as $\pi \geq 3$ and $3 \geq e$ implies $\pi \geq e$.
- It is reflexive:
  $7|7$, just as $\pi \geq \pi$.
- It is antisymmetric:
  $4 \mid 8$ implies $8 \not| 4$, just as $x \geq y$ implies $y \not\geq x$ unless $y = x$.
  If $a \mid b$, then $b \not| a$ unless $b = a$.
- Divisibility is not a total order, since $4 \not| 7$ and $7 \not| 4$, while at least one of $x \geq y$ or $y \geq x$ must always be true.

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.
2. So $1^n + 2^n + 3^n + 4^n = 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod 5$

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.
2. So $1^n + 2^n + 3^n + 4^n = 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod 5$
3. Otherwise when $n \equiv 1 \pmod 4$:
   $1^{4k+1} + 2^{4k+1} + 3^{4k+1} + 4^{4k+1} \equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \pmod 5$

Divisibility

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.
2. So $1^n + 2^n + 3^n + 4^n = 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod 5$
3. Otherwise when $n \equiv 1 \pmod 4$: $1^{4k+1} + 2^{4k+1} + 3^{4k+1} + 4^{4k+1} \equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \pmod 5$
4. When $n \equiv 2 \pmod 4$: $1^{4k+2} + 2^{4k+2} + 3^{4k+2} + 4^{4k+2} \equiv 1 + 4 + 9 + 16 \equiv 30 \equiv 0 \pmod 5$

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.
2. So $1^n + 2^n + 3^n + 4^n = 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod 5$
3. Otherwise when $n \equiv 1 \pmod 4$:
   $1^{4k+1} + 2^{4k+1} + 3^{4k+1} + 4^{4k+1} \equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \pmod 5$
4. When $n \equiv 2 \pmod 4$: $1^{4k+2} + 2^{4k+2} + 3^{4k+2} + 4^{4k+2} \equiv 1 + 4 + 9 + 16 \equiv 30 \equiv 0 \pmod 5$
5. When $n \equiv 3 \pmod 4$: $1^{4k+3} + 2^{4k+3} + 3^{4k+3} + 4^{4k+3} \equiv 1 + 8 + 27 + 64 \equiv 100 \equiv 0 \pmod 5$

Divisibility

CPMSOC

Example

Show that for any non-negative integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

1. If $4|n$, then $n = 4k$. Note that $1^4 \equiv 1 \pmod 5$, $2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.
2. So $1^n + 2^n + 3^n + 4^n = 1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \equiv 1 + 1 + 1 + 1 \equiv 4 \pmod 5$
3. Otherwise when $n \equiv 1 \pmod 4$: $1^{4k+1} + 2^{4k+1} + 3^{4k+1} + 4^{4k+1} \equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 0 \pmod 5$
4. When $n \equiv 2 \pmod 4$: $1^{4k+2} + 2^{4k+2} + 3^{4k+2} + 4^{4k+2} \equiv 1 + 4 + 9 + 16 \equiv 30 \equiv 0 \pmod 5$
5. When $n \equiv 3 \pmod 4$: $1^{4k+3} + 2^{4k+3} + 3^{4k+3} + 4^{4k+3} \equiv 1 + 8 + 27 + 64 \equiv 100 \equiv 0 \pmod 5$
6. Therefore, true! (by cases)

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.
  2. Whenever $p = ab$, $a = \pm 1$ or $b = \pm 1$.

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.
  2. Whenever $p = ab$, $a = \pm 1$ or $b = \pm 1$.

Theorem

Chebyshev said, and I'll say it again - there is always a prime between n and $2n$.

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.
  2. Whenever $p = ab$, $a = \pm 1$ or $b = \pm 1$.

Theorem

Chebyshev said, and I'll say it again - there is always a prime between n and $2n$.

- We say that a and b are coprime or relatively prime iff:

Primality and Coprimality

CPMSOC

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.
  2. Whenever $p = ab$, $a = \pm 1$ or $b = \pm 1$.

Theorem

Chebyshev said, and I'll say it again - there is always a prime between n and $2n$.

- We say that a and b are coprime or relatively prime iff:
  1. Whenever $c \mid a$ and $c \mid b$ we must have $c = 1, 0, -1$.

Primality and Coprimality

- We say that $p \neq 1, 0, -1$ is prime iff it matches any of these equivalent definitions:
  1. Whenever $p \mid ab$, $p \mid a$ or $p \mid b$.
  2. Whenever $p = ab$, $a = \pm 1$ or $b = \pm 1$.

Theorem

Chebyshev said, and I'll say it again - there is always a prime between n and $2n$.

- We say that a and b are coprime or relatively prime iff:
  1. Whenever $c \mid a$ and $c \mid b$ we must have $c = 1, 0, -1$.
  2. $GCD(a, b) = 1$. (sometimes written as $(a, b) = 1$)

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

1. Suppose n is not prime. Let $n = xy$ where $x, y \in \mathbb{N}$ and $x, y \geq 2$. Then $2^n - 1 = 2^{xy} - 1$.

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

1. Suppose n is not prime. Let $n = xy$ where $x, y \in \mathbb{N}$ and $x, y \geq 2$. Then $2^n - 1 = 2^{xy} - 1$.
2. We can write $2^{xy} - 1$ as $(2^x)^y - 1$ by index laws

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

1. Suppose n is not prime. Let $n = xy$ where $x, y \in \mathbb{N}$ and $x, y \geq 2$. Then $2^n - 1 = 2^{xy} - 1$.
2. We can write $2^{xy} - 1$ as $(2^x)^y - 1$ by index laws
3. $(2^x)^y - 1 = (2^x - 1)(2^{x(y-1)} + 2^{x(y-2)} + 2^{x(y-3)} + ... + 2^2 + 2 + 1)$

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

1. Suppose n is not prime. Let $n = xy$ where $x, y \in \mathbb{N}$ and $x, y \geq 2$. Then $2^n - 1 = 2^{xy} - 1$.
2. We can write $2^{xy} - 1$ as $(2^x)^y - 1$ by index laws
3. $(2^x)^y - 1 = (2^x - 1)(2^{x(y-1)} + 2^{x(y-2)} + 2^{x(y-3)} + ... + 2^2 + 2 + 1)$
4. Since $2^n - 1$ is divisible by $2^x - 1$, and $1 < 2^x - 1 < 2^n - 1$, it cannot be prime. This is a contradiction.

Primality and Coprimality

CPMSOC

Example

Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

1. Suppose n is not prime. Let $n = xy$ where $x, y \in \mathbb{N}$ and $x, y \geq 2$. Then $2^n - 1 = 2^{xy} - 1$.
2. We can write $2^{xy} - 1$ as $(2^x)^y - 1$ by index laws
3. $(2^x)^y - 1 = (2^x - 1)(2^{x(y-1)} + 2^{x(y-2)} + 2^{x(y-3)} + ... + 2^2 + 2 + 1)$
4. Since $2^n - 1$ is divisible by $2^x - 1$, and $1 < 2^x - 1 < 2^n - 1$, it cannot be prime. This is a contradiction.
5. Thus, n must be prime!

Primality and Coprimality

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

Primality and Coprimality

CPMSOC

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

1. Since we want a factor of $a + b$, we keep the sum simple, so we can try $a = 2k + 1$, $b = 2k - 1$, for $k \in \mathbb{Z}$ and $k > 1$.

Primality and Coprimality

CPMSOC

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

1. Since we want a factor of $a + b$, we keep the sum simple, so we can try $a = 2k + 1$, $b = 2k - 1$, for $k \in \mathbb{Z}$ and $k > 1$.
2. In this case, we need to show that $(2k + 1)^{2k-1} + (2k - 1)^{2k+1}$ has a factor of $4k$.

Primality and Coprimality

CPMSOC

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

1. Since we want a factor of $a + b$, we keep the sum simple, so we can try $a = 2k + 1$, $b = 2k - 1$, for $k \in \mathbb{Z}$ and $k > 1$.
2. In this case, we need to show that $(2k + 1)^{2k-1} + (2k - 1)^{2k+1}$ has a factor of $4k$.
3. Notice that $(2k \pm 1)^2 = 4k^2 \pm 4k + 1$, so $(2k + 1)^{2k-1} = \left((2k + 1)^2\right)^{k-1}(2k + 1)$ can be expanded into the form $4kn + 2k + 1$ for some $n \in \mathbb{Z}$, and similarly for $(2k - 1)^{2k+1}$.

Primality and Coprimality

CPMSOC

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

1. Since we want a factor of $a + b$, we keep the sum simple, so we can try $a = 2k + 1$, $b = 2k - 1$, for $k \in \mathbb{Z}$ and $k > 1$.
2. In this case, we need to show that $(2k + 1)^{2k-1} + (2k - 1)^{2k+1}$ has a factor of $4k$.
3. Notice that $(2k \pm 1)^2 = 4k^2 \pm 4k + 1$, so $(2k + 1)^{2k-1} = \left((2k + 1)^2\right)^{k-1}(2k + 1)$ can be expanded into the form $4kn + 2k + 1$ for some $n \in \mathbb{Z}$, and similarly for $(2k - 1)^{2k+1}$.
4. Thus, $(2k + 1)^{2k-1} + (2k - 1)^{2k+1} = 4kn' + 2k + 1 + 2k - 1 = 4k(n' + 1)$ for some $n' \in \mathbb{Z}$, so $4k$ is a divisor.

Primality and Coprimality

CPMSOC

Example

Prove that there are infinitely many distinct pairs (a, b) of relatively prime integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

1. Since we want a factor of $a + b$, we keep the sum simple, so we can try $a = 2k + 1$, $b = 2k - 1$, for $k \in \mathbb{Z}$ and $k > 1$.
2. In this case, we need to show that $(2k + 1)^{2k-1} + (2k - 1)^{2k+1}$ has a factor of $4k$.
3. Notice that $(2k \pm 1)^2 = 4k^2 \pm 4k + 1$, so $(2k + 1)^{2k-1} = \left((2k + 1)^2\right)^{k-1} (2k + 1)$ can be expanded into the form $4kn + 2k + 1$ for some $n \in \mathbb{Z}$, and similarly for $(2k - 1)^{2k+1}$.
4. Thus, $(2k + 1)^{2k-1} + (2k - 1)^{2k+1} = 4kn' + 2k + 1 + 2k - 1 = 4k(n' + 1)$ for some $n' \in \mathbb{Z}$, so $4k$ is a divisor.
5. Since $\gcd(2k + 1, 2k - 1) = 1$, and we can take any $k > 1$, we have infinitely many distinct pairs satisfying the conditions.