37181 DISCRETE MATHEMATICS

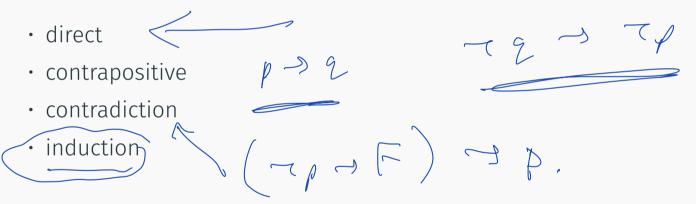
©Murray Elder, UTS Lecture 3: proofs



- proof methods:
 - direct
 - contrapositive
 - \cdot contradiction

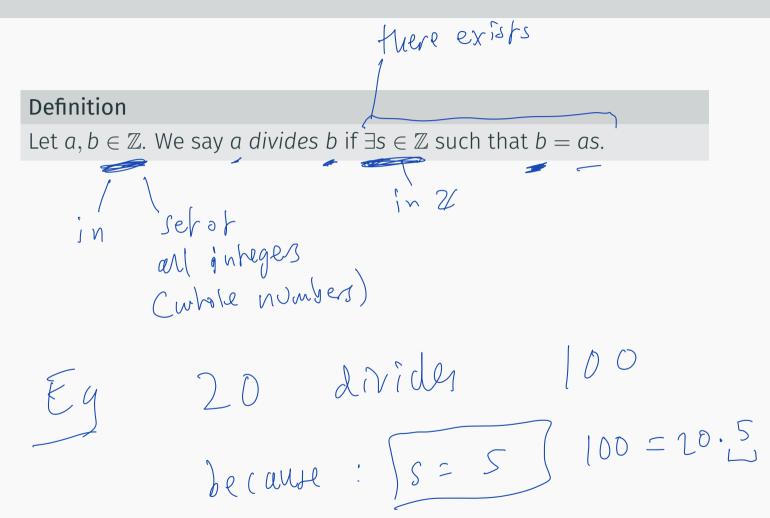
Proofs in mathematics or computer science are based on the argument forms we started to learn last week.

To start with, the main types of proof styles are:



If you do more math or theoretical computer science you will see more styles.

DIVIDES

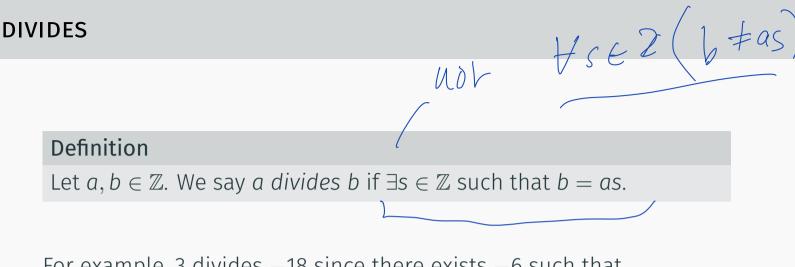


DIVIDES

Definition Let $a, b \in \mathbb{Z}$. We say a divides b if $\exists s \in \mathbb{Z}$ such that b = as.

For example, 3 divides –18 since

 $-18 = 3 \cdot (-6)$



For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since $if \quad b = a \cdot 5 \quad 14 \cdot 35$ s = 14 = 123hot in k

Definition

Let $a, b \in \mathbb{Z}$. We say a divides b if $\exists s \in \mathbb{Z}$ such that b = as.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ 14 \neq 3s.

Definition

Let $a, b \in \mathbb{Z}$. We say a divides b if $\exists s \in \mathbb{Z}$ such that b = as.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ 14 \neq 3s.

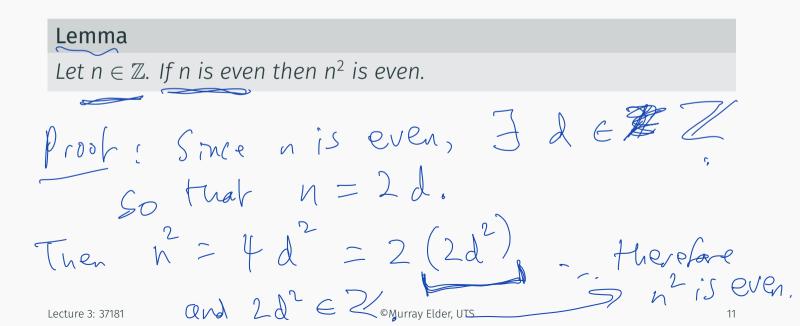
Notation: *a* | *b* means "*a* divides *b*"

Recall that an integer *n* is even if

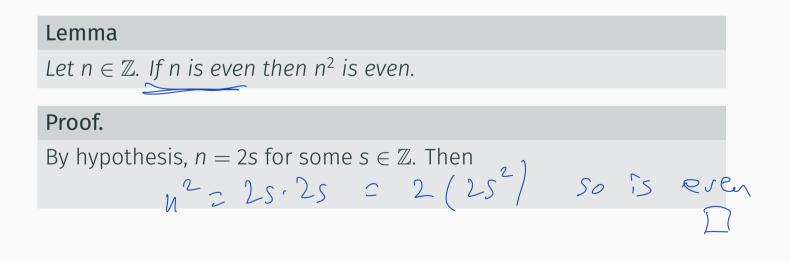
Recall that an integer *n* is even if 2 | n, that is, it can be written as n = 2d for some $d \in \mathbb{Z}$.

 \mathbf{N}

Recall that an integer *n* is even if 2 | n, that is, it can be written as n = 2d for some $d \in \mathbb{Z}$.



Recall that an integer *n* is *even* if 2 | n, that is, it can be written as n = 2d for some $d \in \mathbb{Z}$.



DIRECT

Sometimes it is easy to show step-by-step that p implies q (or using syllogism $(p \rightarrow r)$ and $(r \rightarrow s)$ and $(s \rightarrow t)$ and $(t \rightarrow q)$).

Recall that an integer *n* is *even* if 2 | n, that is, it can be written as n = 2d for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof.

By hypothesis, n = 2s for some $s \in \mathbb{Z}$. Then $n^2 = (2s)^2 = 4s^2 = 2(2s^2)$ is even.

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof. By hypothesis, 3 s + 2 so that n = 25. $n^{3} = (2s)^{3} = 2(4s^{2})$ = 2(4s^{2}) Then

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof.

By hypothesis, n = 2s for some $s \in \mathbb{Z}$. Then $n^3 = (2s)^3 = 2(4s^3)$ is even.

YOUR TURN

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof. h² is even, so 3 s E Z $n^2 = 25$ 50 N= W2 2s

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

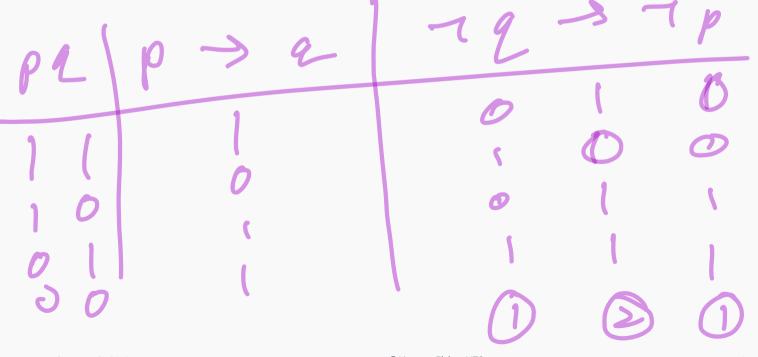
? direct doesn't work



CONTRAPOSITIVE

Recall that $p \rightarrow q$ is logically equivalent to (has the same truth values as) $\neg q \rightarrow \neg p$.

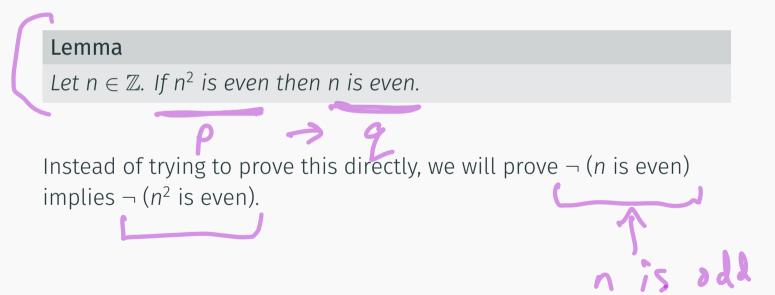
Check this with a truth table.



CONTRAPOSITIVE

Recall that $p \rightarrow q$ is logically equivalent to (has the same truth values as) $\neg q \rightarrow \neg p$.

Check this with a truth table.



Recall that $p \rightarrow q$ is logically equivalent to (has the same truth values as) $\neg q \rightarrow \neg p$.

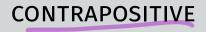
Check this with a truth table.

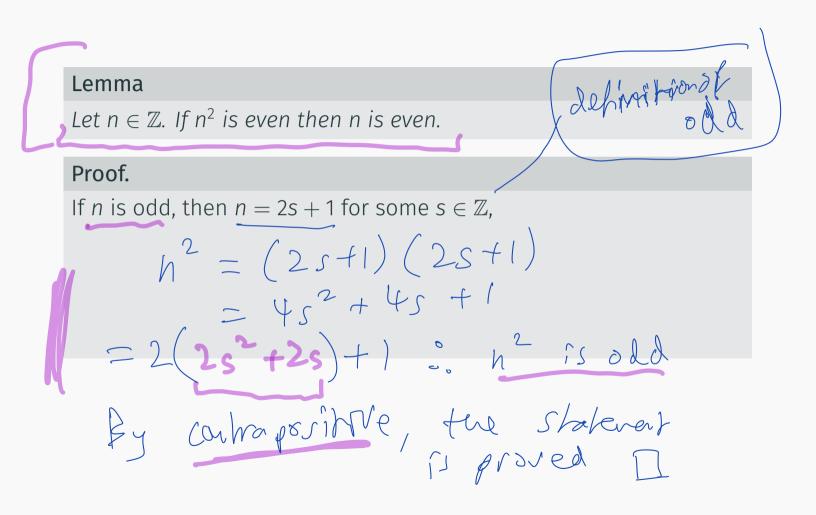
Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Instead of trying to prove this directly, we will prove \neg (*n* is even) implies \neg (*n*² is even).

In other words, if n is odd then n^2 is odd.





CONTRAPOSITIVE $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then n = 2s + 1 for some $s \in \mathbb{Z}$, so $n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

Lemma

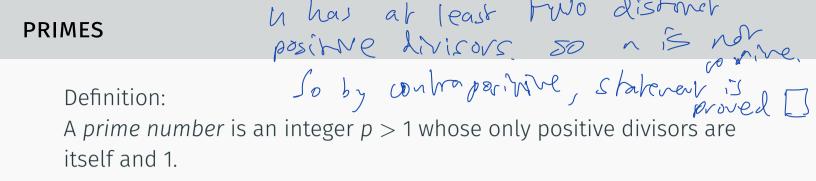
Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

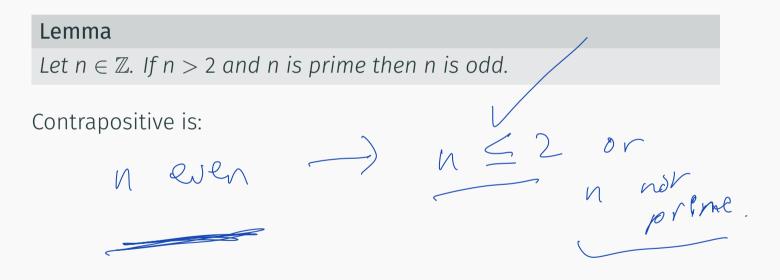
Proof.

If n is odd, then n = 2s + 1 for some $s \in \mathbb{Z}$, so $n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

Since the statement we have proved (the contrapositive) is logically equivalent to the original statement to be shown, we are done. \Box

52 PRIMES 37181 **Definition:** A prime number is an integer p > 1 whose only positive divisors are itself and 1. 1 4 2 Lemma Let $n \in \mathbb{Z}$. If n > 2 and n is prime then n is odd. Contapositive Uniresse RURN - N 15 Propr ver N = 25 some st 2 Discourse Suppose n>2, (if not, n 52 and meare done) then 2/h 50 9m and Lecture 3: 37181 ©Murray Elder, UTS A N. L I





PRIMES

Definition:

A prime number is an integer p > 1 whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If n > 2 and n is prime then n is odd.

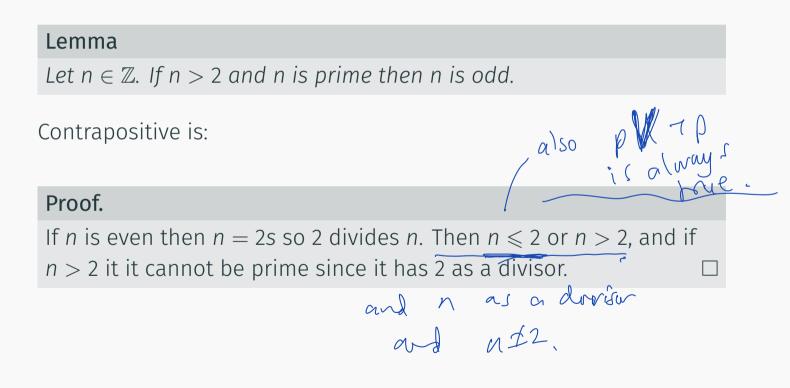
Contrapositive is:

Proof.

PRIMES

Definition:

A prime number is an integer p > 1 whose only positive divisors are itself and 1.



PRIMES

Definition:

A prime number is an integer p > 1 whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If n > 2 and n is prime then n is odd.

Contrapositive is:

Proof.

If *n* is even then n = 2s so 2 divides *n*. Then $n \leq 2$ or n > 2, and if n > 2 it it cannot be prime since it has 2 as a divisor.

Note in my proof, I added a hypothesis $q \lor \neg q$ half way!

Lecture 3: 37181

©Murray Elder, UTS

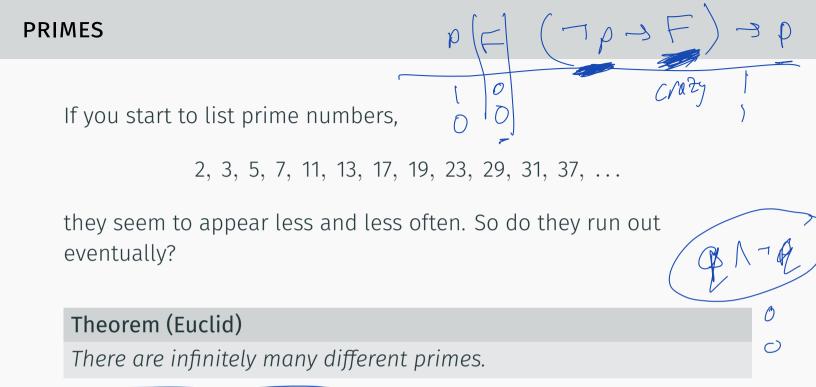
If you start to list prime numbers,

If you start to list prime numbers,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

they seem to appear less and less often. So do they run out eventually?

Kun out. Finite list.



If you start to list prime numbers,

```
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
```

they seem to appear less and less often. So do they run out eventually?

Theorem (Euclid)

There are infinitely many different primes.

This time we have a statement p = "there are infinitely many primes", and we will prove that $\neg p$ implies a contradiction, *i.e.* use $(\neg p \rightarrow F) \rightarrow p$.

Assume

PROOF BY CONTRADICTION

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the

distinct primes:

 $p_1, p_2, \ldots, p_n.$

PROOF BY CONTRADICTION

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N = (p_1 p_2 \cdots p_n) + 1$$

$$N \text{ is bigger from every number pi}$$

$$Ou \quad \text{for } 18f \quad above. \quad \text{tree for e } N$$

$$Ou \quad \text{for } 18f \quad above. \quad \text{tree for e } N$$

$$Canvolv \quad be \quad prine.$$

$$But \text{ if } a - Af \quad either \quad a = p; \quad \text{for e } (E \in En)$$

$$Ecture 3: 37181$$

More of the prines in the list above h Suppose NTS not porse, then some Pill N 1 sign E ZC du N pi 2 p. P2 - Pi-i Pi+1 - In + 1 V mbe gla

Lemma IF n is not prive exists a prive Ler NEZ. fren freve nomber p $p \mid \mathcal{N}$. So that



PROOF BY CONTRADICTION

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

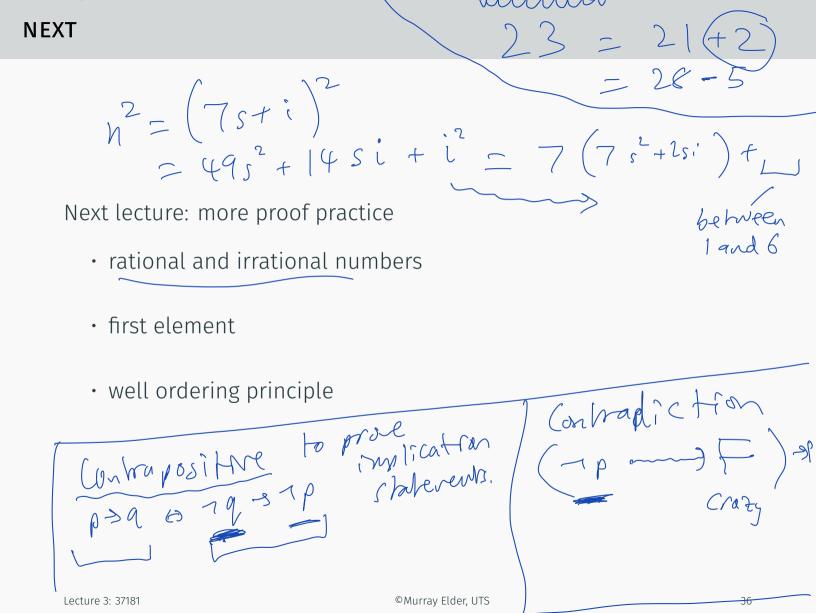
 $p_1, p_2, \ldots, p_n.$

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N=(p_1p_2\cdots p_n)+1$$

Is N prime or not?

EX IF n ; s divisible by T then n² is divisible by 7. Prod by hypothesis, JSEZ so that Dirett) h = 7sThen $h^2 = 49s^2 = 7(7s^2)$ - n is divible Ex2 prove that if n2 is divide 7 then n is drisible by ? Proof (Contra positive) Suppose n is ust divisible by 7 Then 3 s t 26 so that In - 7 n = 7 s + i $1 \le i \le 6$ 1, 2, 3, 4, 5, 6 $i \in \mathbb{Z}$



$$\begin{array}{c}
 \hline a \rightarrow b \\
 \hline \neg (a \rightarrow b) \\
 \hline \neg (a \rightarrow b) \\
 \hline a \wedge (a \rightarrow b) \\
 \hline A \\$$