



WHUSpot Beamer Template

Tony Xiang

Wuhan University

June 11, 2019



What Are Prime Numbers?



Definition

A **prime number** is a number that has exactly two divisors.

- ▶ 2 is prime (two divisors: 1 and 2).



What Are Prime Numbers?



Definition

A **prime number** is a number that has exactly two divisors.

- ▶ 2 is prime (two divisors: 1 and 2).
- ▶ 3 is prime (two divisors: 1 and 3).



What Are Prime Numbers?



Definition

A **prime number** is a number that has exactly two divisors.

- ▶ 2 is prime (two divisors: 1 and 2).
- ▶ 3 is prime (two divisors: 1 and 3).
- ▶ 4 is not prime (**three** divisors: 1, 2 and 4)



There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.



Theorem

There is no largest prime number.

Proof.

1. Suppose p were the largest prime number.
2. Consider the number $q = p + 1$.
3. But q is greater than 1, thus divisible by some prime number not in the first p numbers.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.





There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.



Theorem

There is no largest prime number.

Proof.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p numbers.
3. $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.





There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.



Theorem

There is no largest prime number.

Proof.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p numbers.
3. Then $q + 1$ is not divisible by any of them.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.





There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.



Theorem

There is no largest prime number.

Proof.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p numbers.
3. Then $q + 1$ is not divisible by any of them.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.



The proof used *reductio ad absurdum*.



What's Still To Do?



Answered Questions

How many primes are there?

Open Questions

Is every even number the sum of two primes?



What's Still To Do?



- ▶ Answered Questions
 - ▶ How many primes are there?
- ▶ Open Questions
 - ▶ Is every even number the sum of two primes?



What's Still To Do?



Answered Questions

How many primes are there?

Open Questions

Is every even number the sum of two primes? [1]



An Algorithm For Finding Primes Numbers.

```
int main (void)
{
    std::vector<bool> is_prime (100, true);
    for (int i = 2; i < 100; i++)

        return 0;
}
```






An Algorithm For Finding Primes Numbers.

```
int main (void)
{
    std::vector<bool> is_prime (100, true);
    for (int i = 2; i < 100; i++)
        if (is_prime[i])
        {
            // ...
        }
    return 0;
}
```





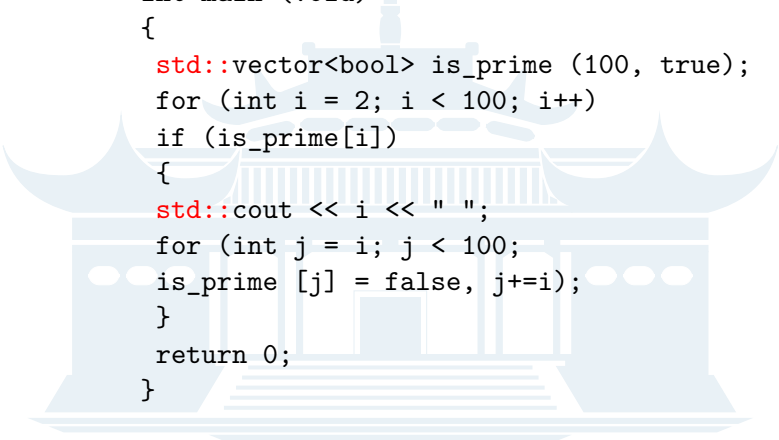
An Algorithm For Finding Primes Numbers.



```
int main (void)
{
    std::vector<bool> is_prime (100, true);
    for (int i = 2; i < 100; i++)
        if (is_prime[i])
        {
            std::cout << i << " ";
            for (int j = i; j < 100;
                is_prime [j] = false, j+=i);
        }
    return 0;
}
```



An Algorithm For Finding Primes Numbers.



```
int main (void)
{
    std::vector<bool> is_prime (100, true);
    for (int i = 2; i < 100; i++)
        if (is_prime[i])
        {
            std::cout << i << " ";
            for (int j = i; j < 100;
                is_prime [j] = false, j+=i);
        }
    return 0;
}
```

Note the use of `std::`.



$\langle + - \rangle$ on a frame

Theorem

$$A = B.$$





$\langle + - \rangle$ on a frame

Theorem

$A = B.$

Proof.





$\langle + - \rangle$ on a frame

Theorem

$$A = B.$$

Proof.

- ▶ Clearly, $A = C$.
- ▶ Thus $A = B$.





$\langle + - \rangle$ on a frame

Theorem

$$A = B.$$

Proof.

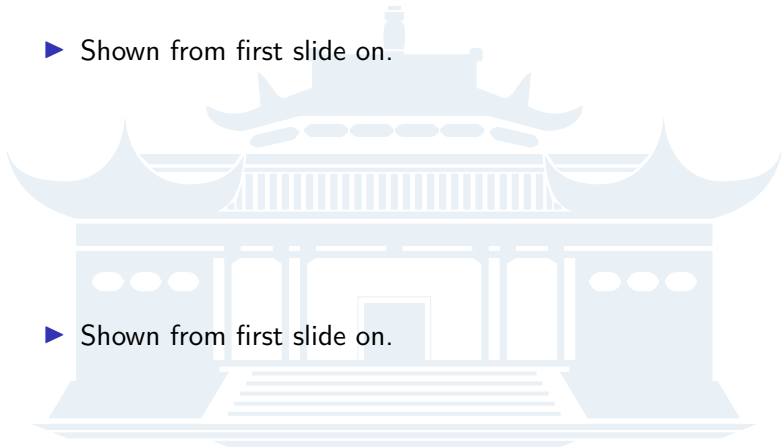
- ▶ Clearly, $A = C$.
- ▶ As shown earlier, $C = B$.
- ▶ Thus $A = B$.





Overlays

- ▶ Shown from first slide on.



- ▶ Shown from first slide on.



Overlays

- ▶ Shown from first slide on.
- ▶ Shown from second slide on.
 - ▶ Shown from second slide on.



- ▶ Shown from first slide on.



Overlays

- ▶ Shown from first slide on.
- ▶ Shown from second slide on.
 - ▶ Shown from second slide on.
 - ▶ Shown from third slide on.
- ▶ Shown from third slide on.
- ▶ Shown from first slide on.





Overlays

- ▶ Shown from first slide on.
- ▶ Shown from second slide on.
 - ▶ Shown from second slide on.
 - ▶ Shown from third slide on.

- ▶ Shown from third slide on.
- ▶ Shown from fourth slide on.

Shown from fourth slide on.

- ▶ Shown from first slide on.





Overlays

- ▶ Shown from first slide on.
- ▶ Shown from second slide on.
 - ▶ Shown from second slide on.
 - ▶ Shown from third slide on.
- ▶ Shown from third slide on.
- ▶ Shown from fourth slide on.

Shown from fourth slide on.

- ▶ Shown from first slide on.
- ▶ Shown from fifth slide on.





Part I

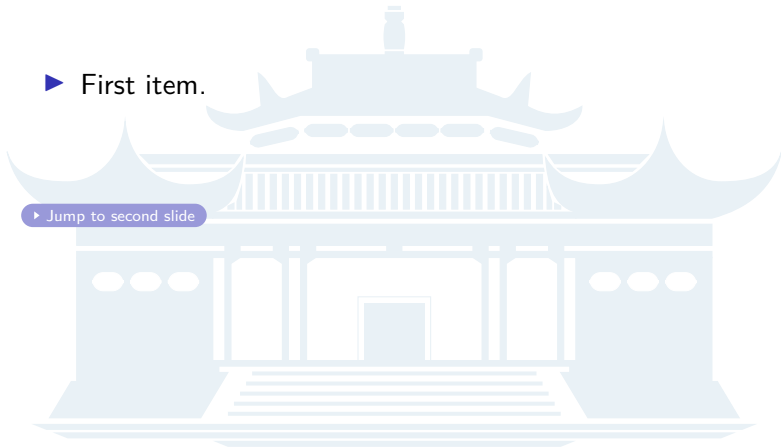
Review of Previous Lecture





► First item.

► Jump to second slide





- ▶ First item.
- ▶ Second item.

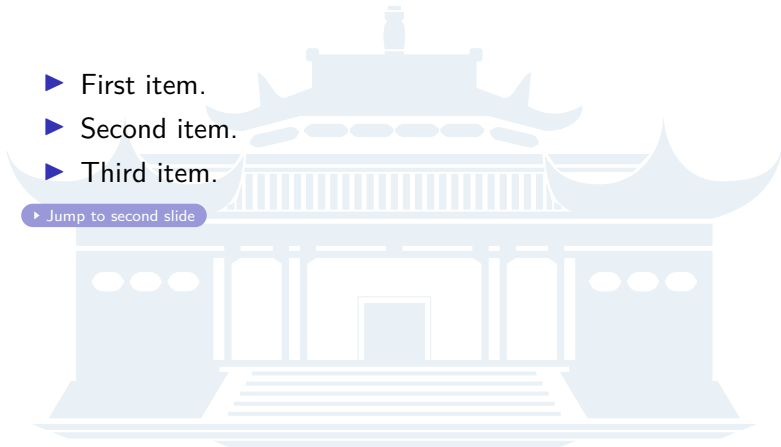
▶ Jump to second slide





- ▶ First item.
- ▶ Second item.
- ▶ Third item.

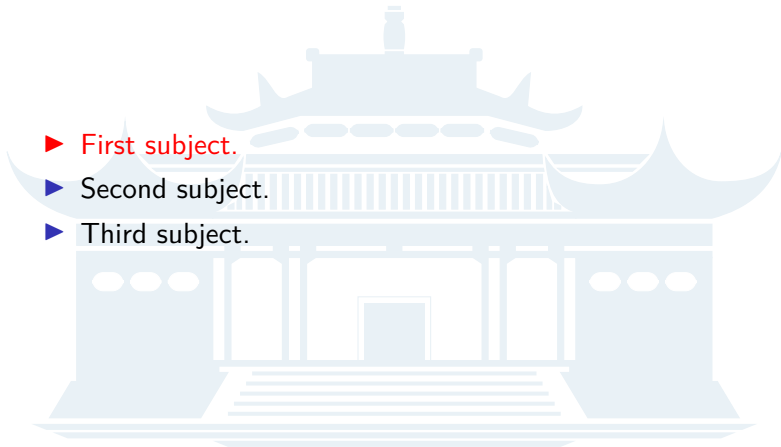
▶ [Jump to second slide](#)





repeating a frame

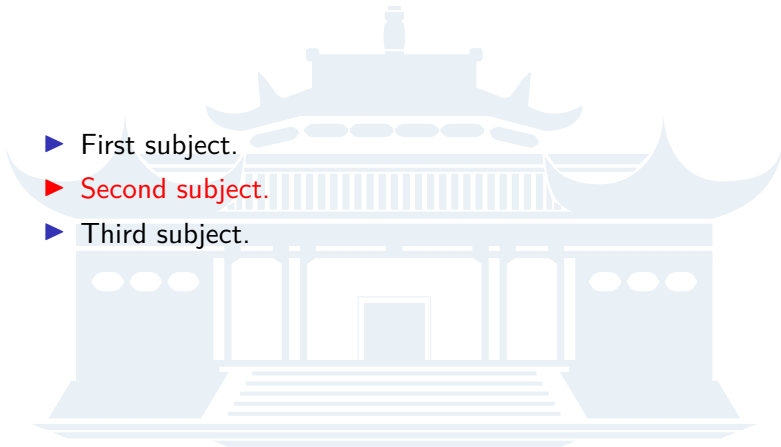
- ▶ First subject.
- ▶ Second subject.
- ▶ Third subject.





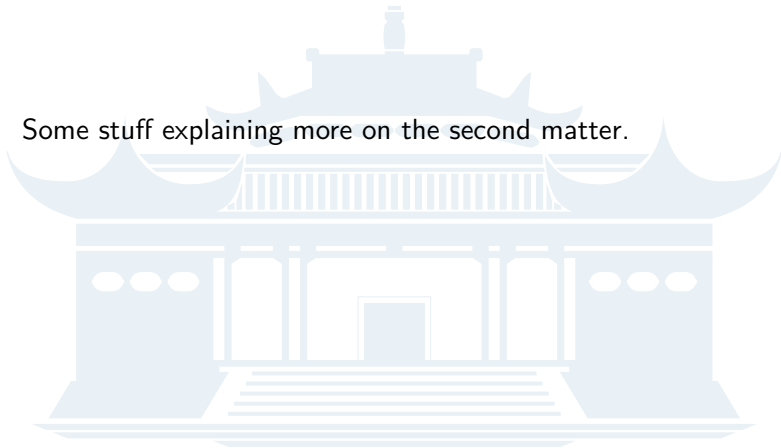
repeating a frame

- ▶ First subject.
- ▶ Second subject.
- ▶ Third subject.





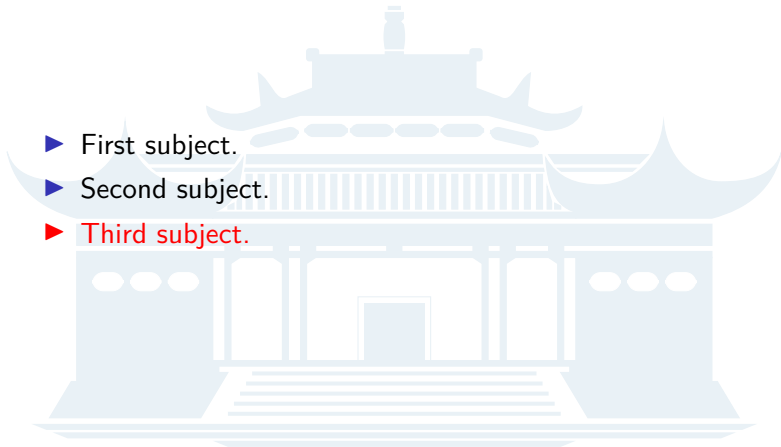
Some stuff explaining more on the second matter.





repeating a frame

- ▶ First subject.
- ▶ Second subject.
- ▶ Third subject.





► Eggs





- ▶ Eggs
- ▶ Plants





- ▶ Eggs
- ▶ Plants
- ▶ Animals





[Goldbach, 1742] Christian Goldbach.

A problem we should try to solve before the ISPN '43 deadline,

Letter to Leonhard Euler, 1742.

