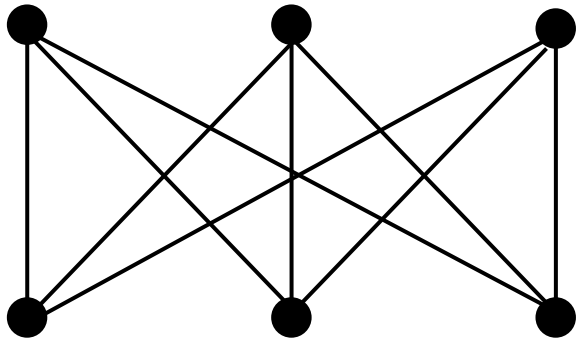
Lecture 12. Graphs and Numbers

DR. YARASLAU ZADVORNY

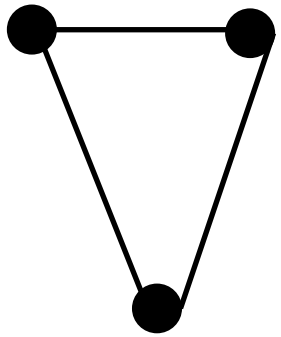
Is the graph $K_{3,3}$ planar?



How did we prove that K_5 is not planar?

The sum of degrees of faces equals to $2E$ where E is the number of edges.

In particular, $3F \leq 2E$.



How did we prove that K_5 is not planar?

The sum of degrees of faces equals to 2E where E is the number of edges.

In particular, $3F \leq 2E$.

Theorem. $E \leq 3V - 6$.

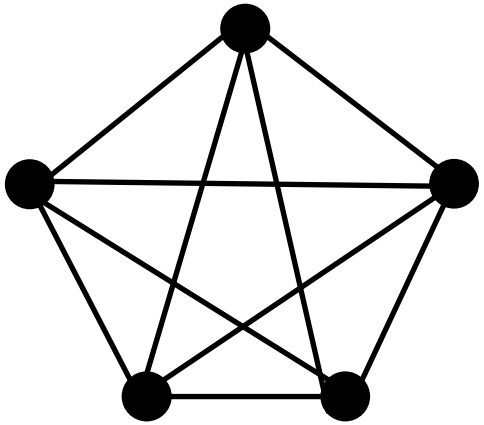
$$V - E + F = 2$$

$$3V + 3F = 6 + 3E$$

$$3V + 2E \geq 6 + 3E$$

$$3V \geq 6 + E$$

$$3V - 6 \geq E$$

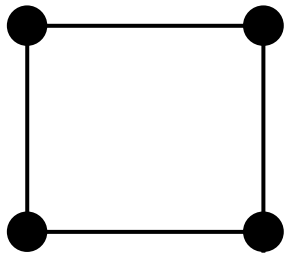


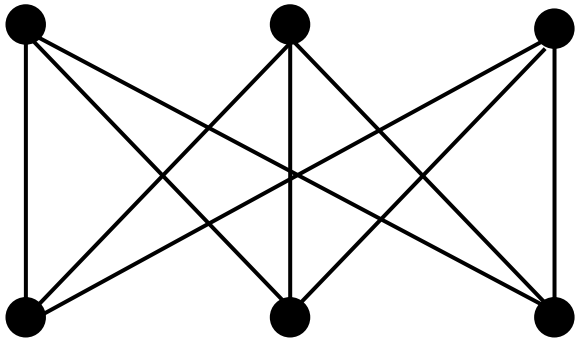
Consequense. The graph K_5 is not a planar graph because for this graph $V = 5$ and $E = 10$.

Is the graph $K_{3,3}$ planar?

The sum of degrees of faces equals to $2E$ where E is the number of edges.

In particular, for a bipartite graph, $4F \leq 2E$.





Is the graph $K_{3,3}$ planar?

The sum of degrees of faces equals to $2E$ where E is the number of edges.

In particular, for a bipartite graph, $4F \leq 2E$.

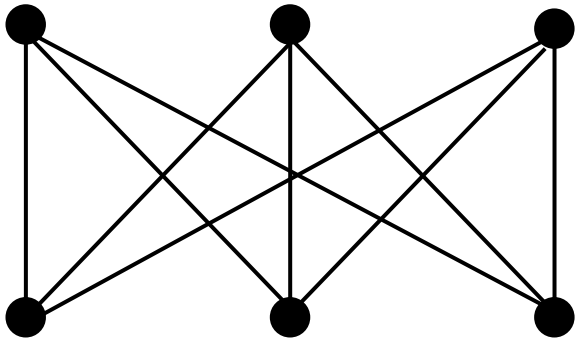
$$V - E + F = 2$$

$$4V + 4F = 8 + 4E$$

$$4V + 2E \geq 8 + 4E$$

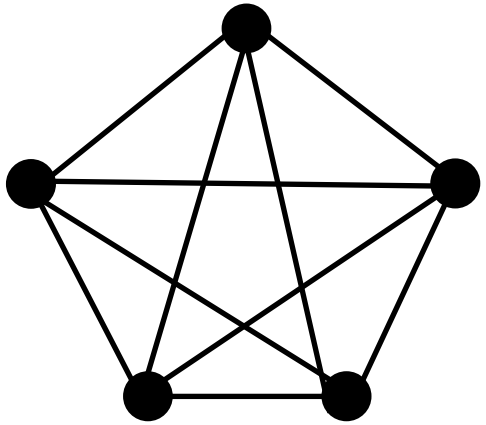
$$4V \geq 8 + 2E$$

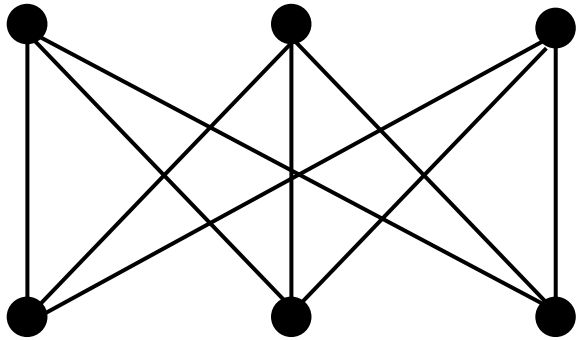
$$2V - 4 \geq E$$



Consequense. The graph $K_{3,3}$ is not a planar graph because for this graph $V = 6$ and $E = 9$.

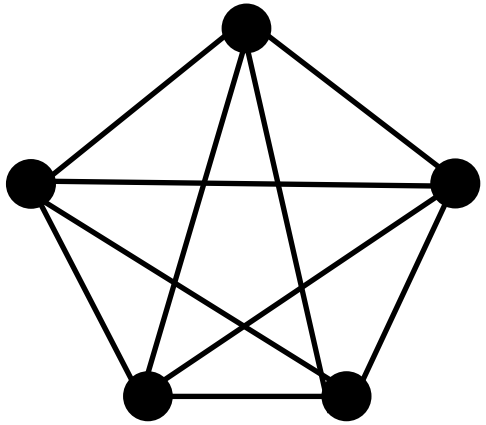
Kuratowski's theorem

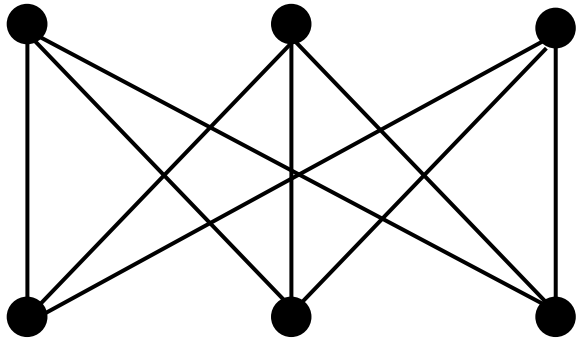




Kuratowski's theorem

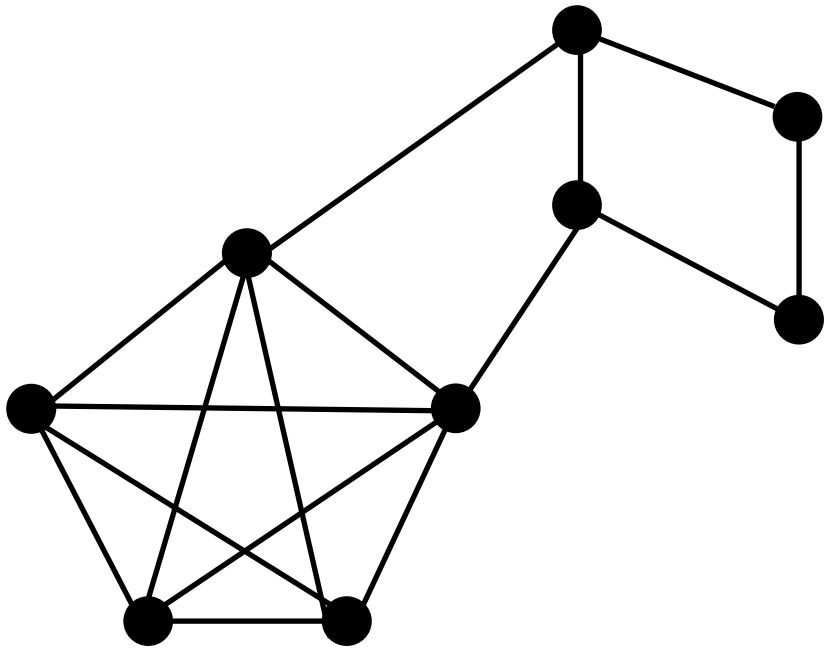
A graph is planar if and only if it doesn’t contain a subgraph that is homeomorphic to K_5 or to $K_{3,3}$.





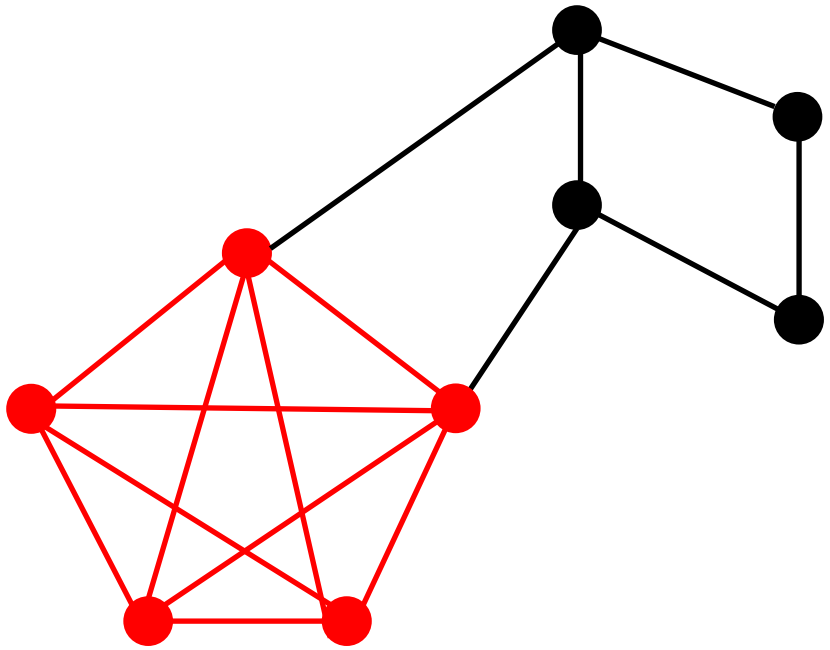
Kuratowski's theorem

A graph is planar if and only if it doesn’t contain a subgraph that is homeomorphic to K_5 or to $K_{3,3}$.



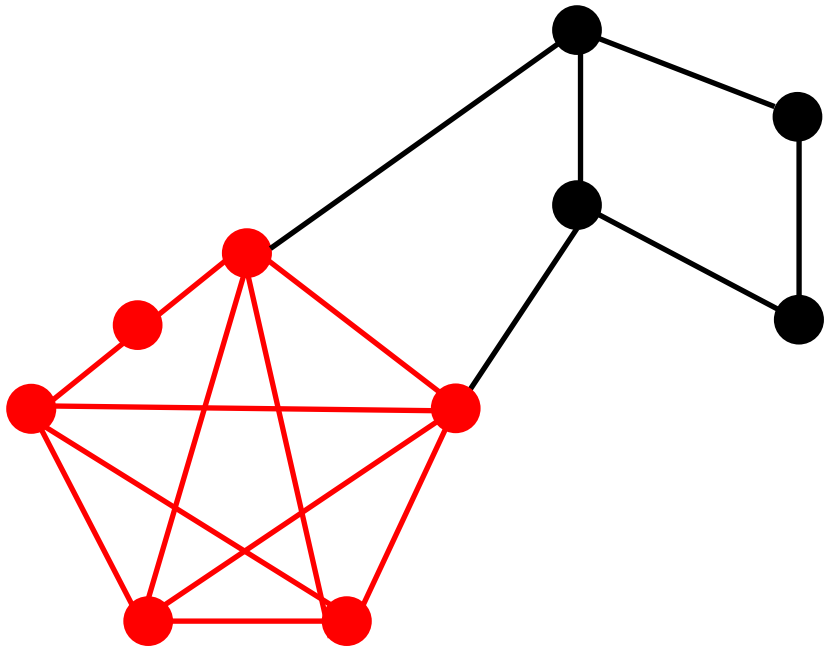
Kuratowski's theorem

A graph is planar if and only if it doesn't contain a subgraph that is homeomorphic to K_5 or to $K_{3,3}$.

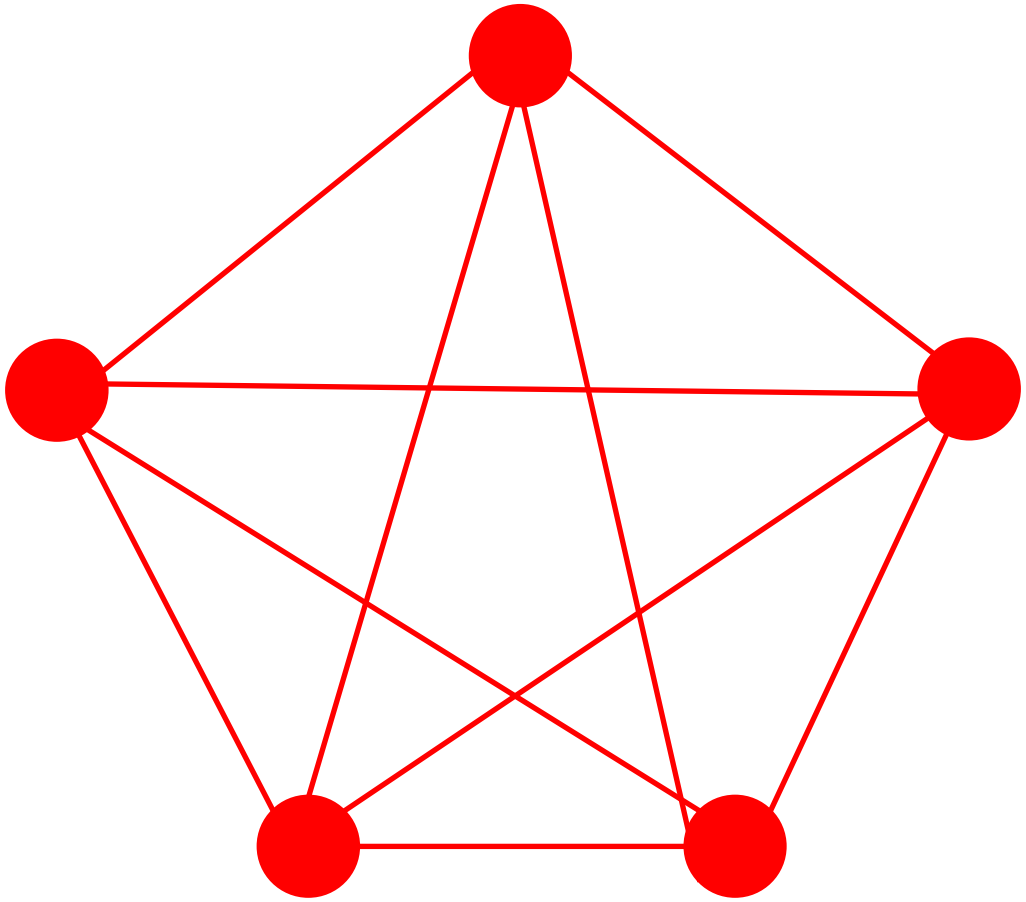


Kuratowski's theorem

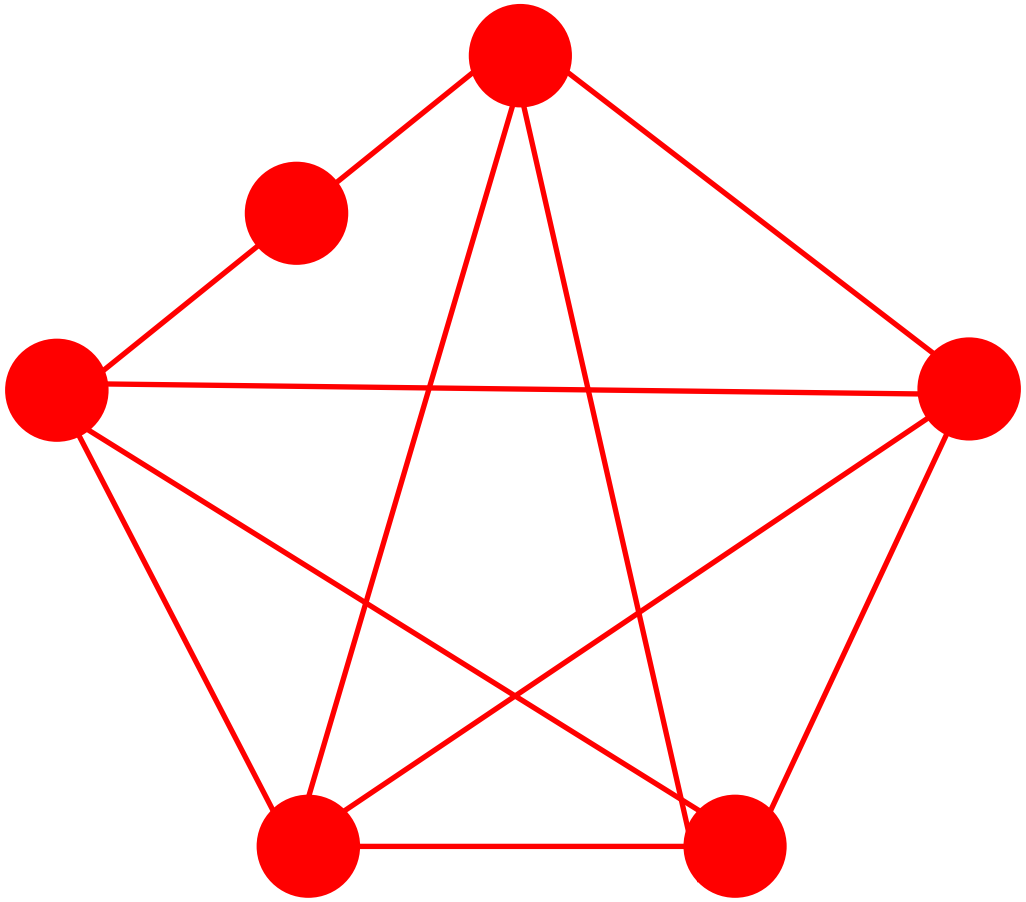
A graph is planar if and only if it doesn't contain a subgraph that is homeomorphic to K_5 or to $K_{3,3}$.



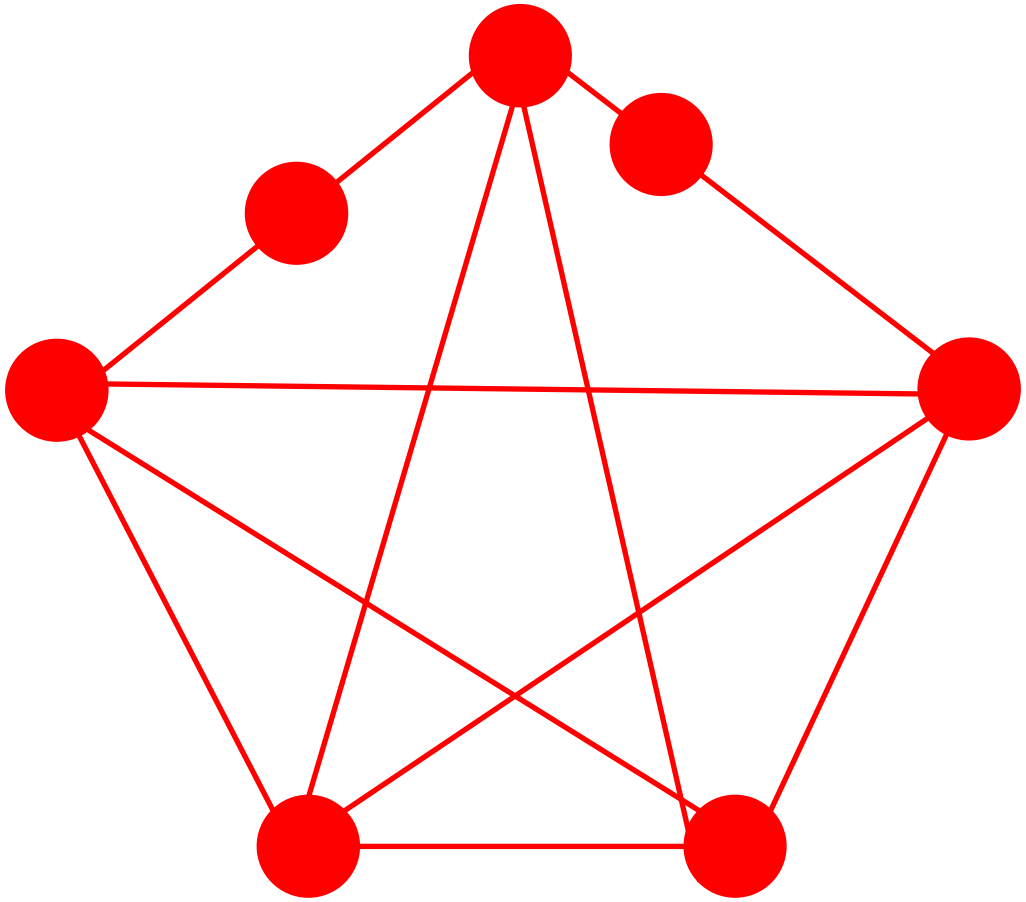
Homeomorpisms of graphs



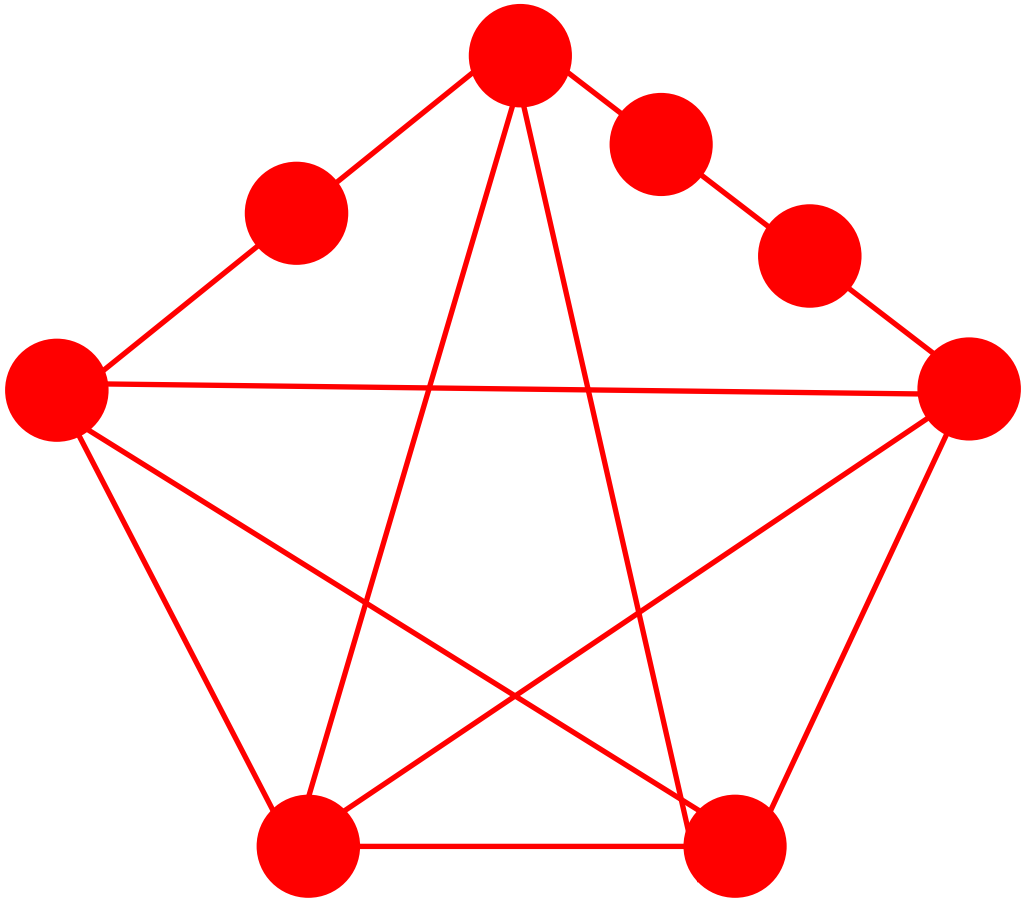
Homeomorpisms of graphs



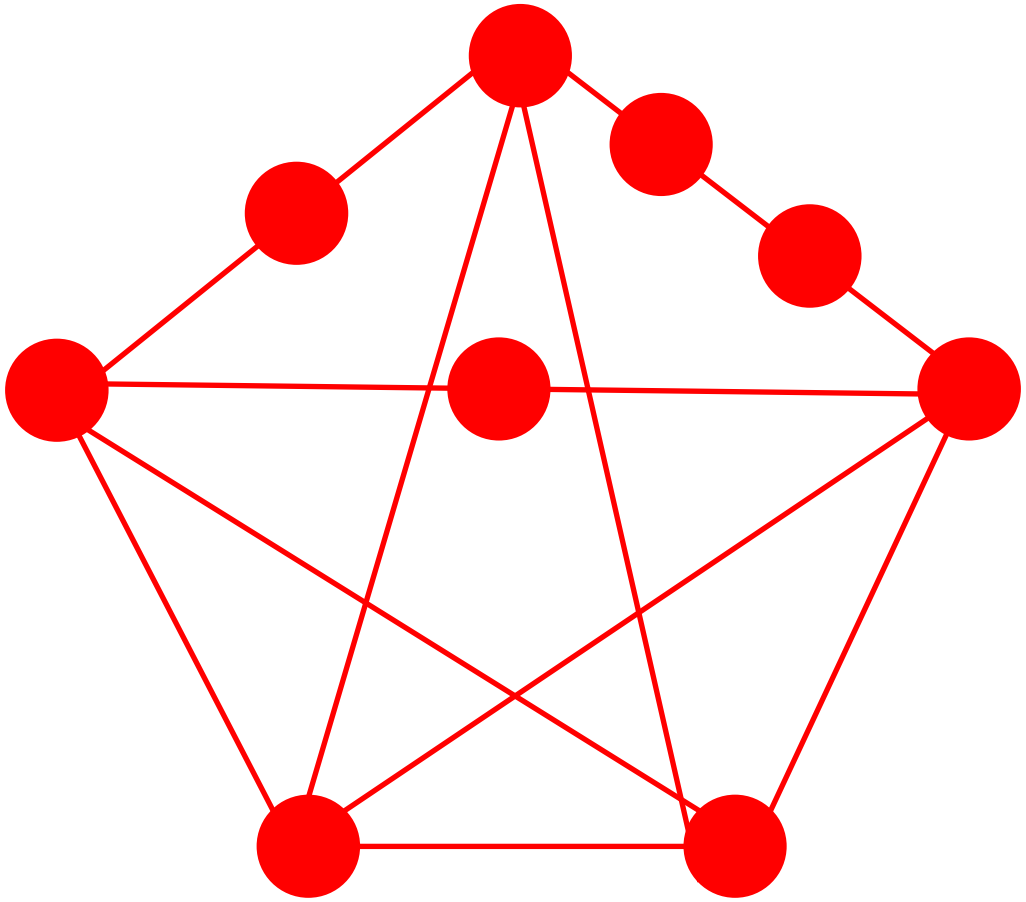
Homeomorpisms of graphs



Homeomorpisms of graphs

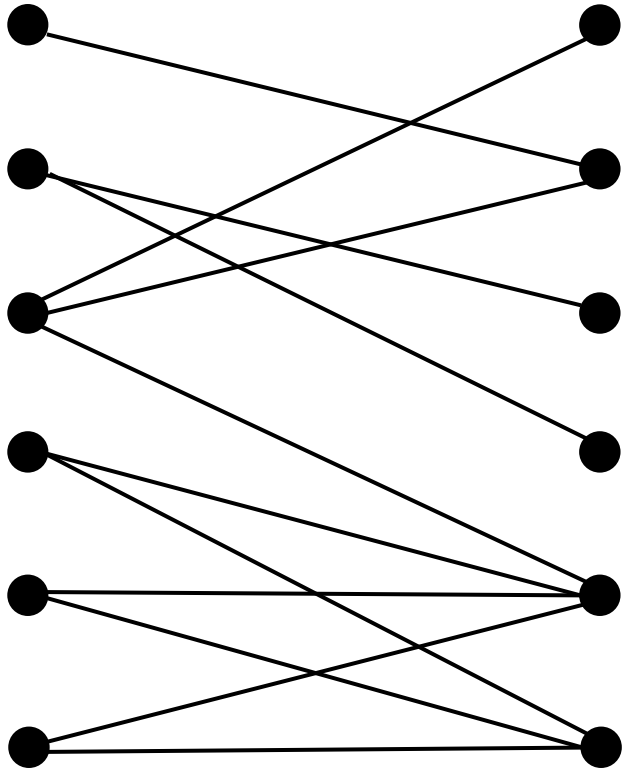


Homeomorpisms of graphs



Hall's Marriage Theorem

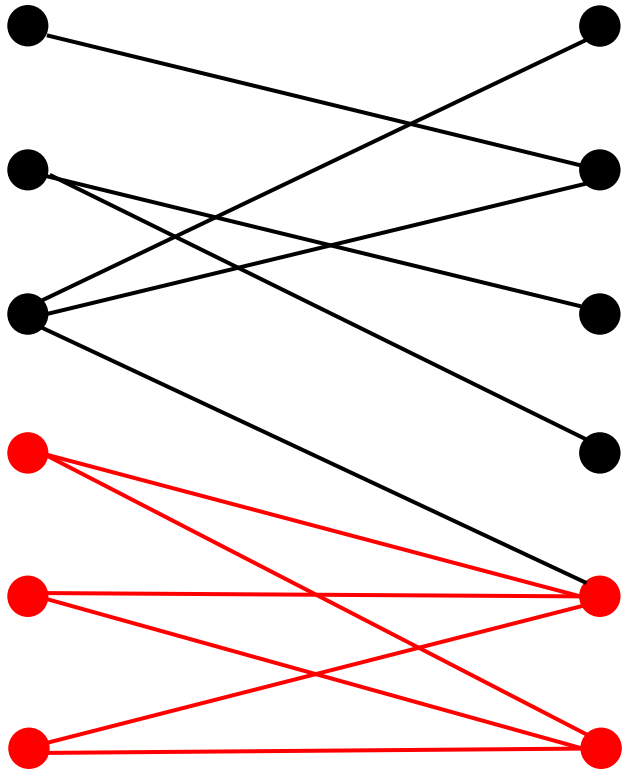
In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.



Hall's Marriage Theorem

In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.

If for any k boys the union of the sets of their girlfriends contains at least k girls, then each boy can choose a wife from among his girlfriends.

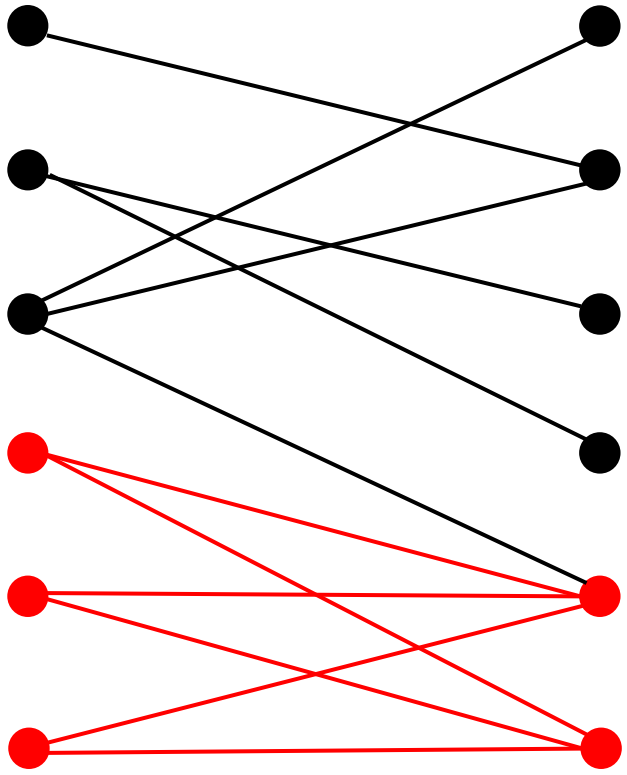


Hall's Marriage Theorem

In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.

If for any k boys the union of the sets of their girlfriends contains at least k girls, then each boy can choose a wife from among his girlfriends.

Why are we not worried about the girls?

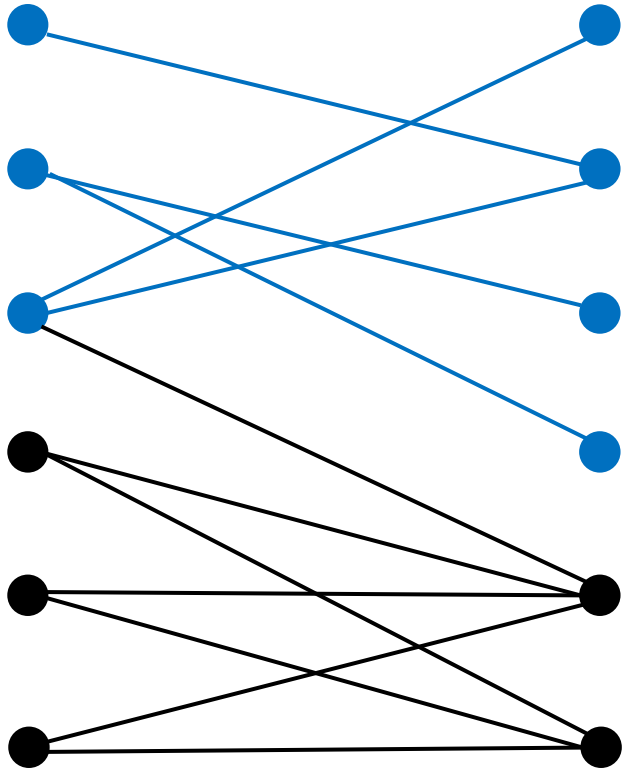


Hall's Marriage Theorem

In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.

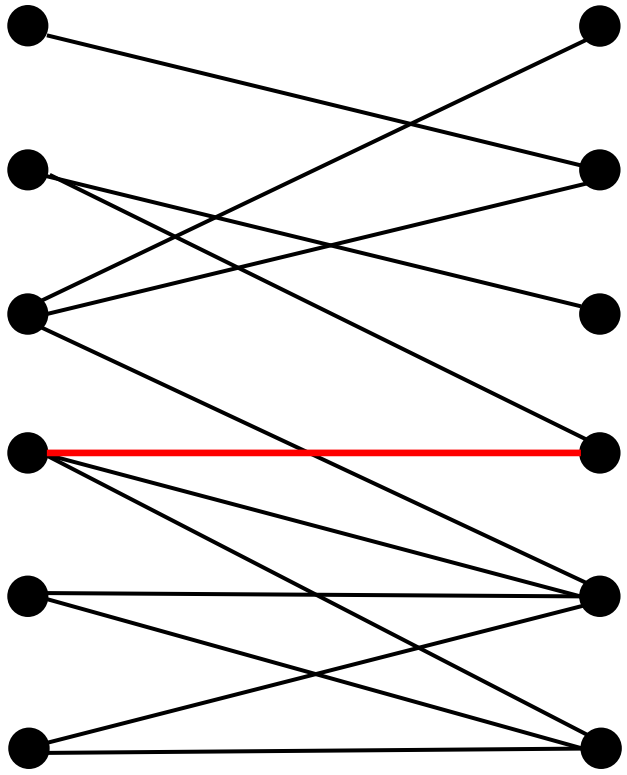
If for any k boys the union of the sets of their girlfriends contains at least k girls, then each boy can choose a wife from among his girlfriends.

Why are we not worried about the girls?



Hall's Marriage Theorem

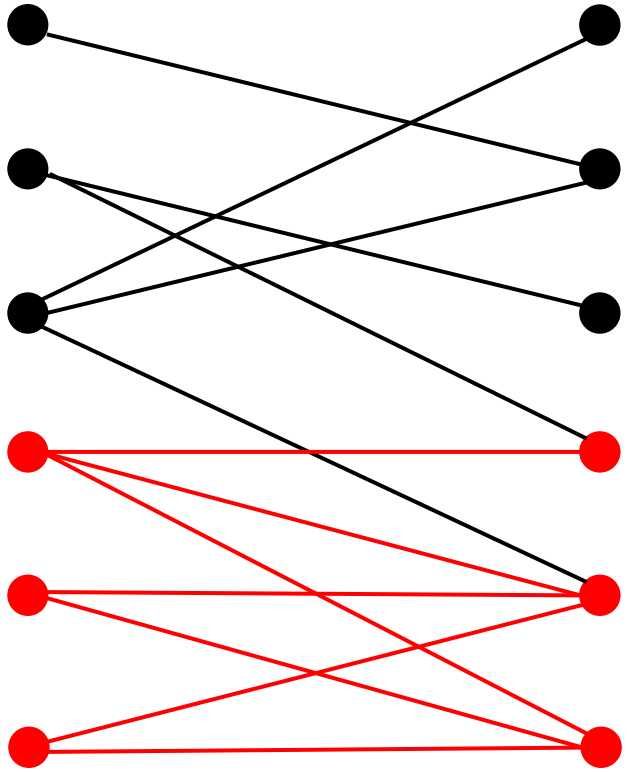
In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.



Hall's Marriage Theorem

In the village, there are *n* boys and *n* girls. It is known about every boy and girl whether they are friends or not. We know to form *n* married couples of them in such a way that every boy (girl) is married to his (her) friend.

If there are *k* boys such that the union of the sets of their girlfriends contains exactly k girls, then we say that this set of boys is **extremal.**

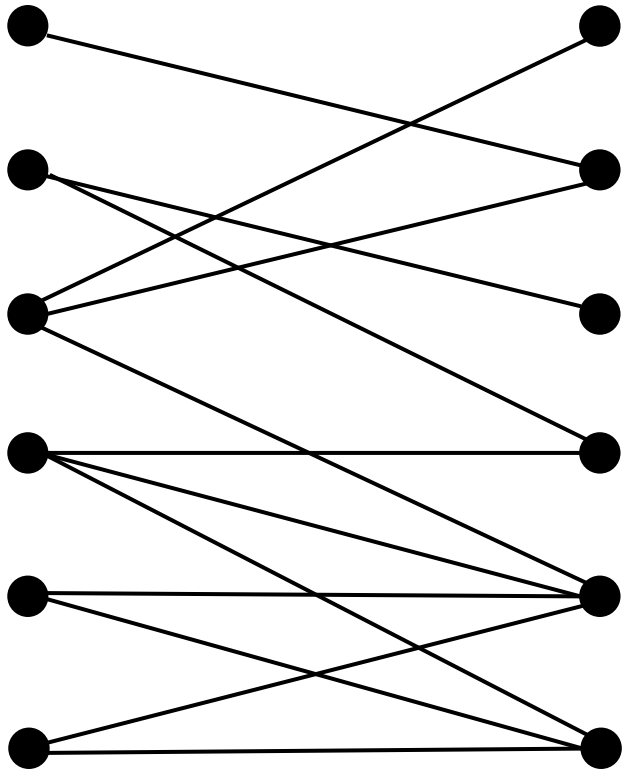


Hall's Marriage Theorem

We use the induction by the number n of boys (girls).

Base case. For $n = 1$ the statement is obvious.

Inductive step. Let the statement is proved for $n = k$. Let's try to prove it for $n = k + 1$.



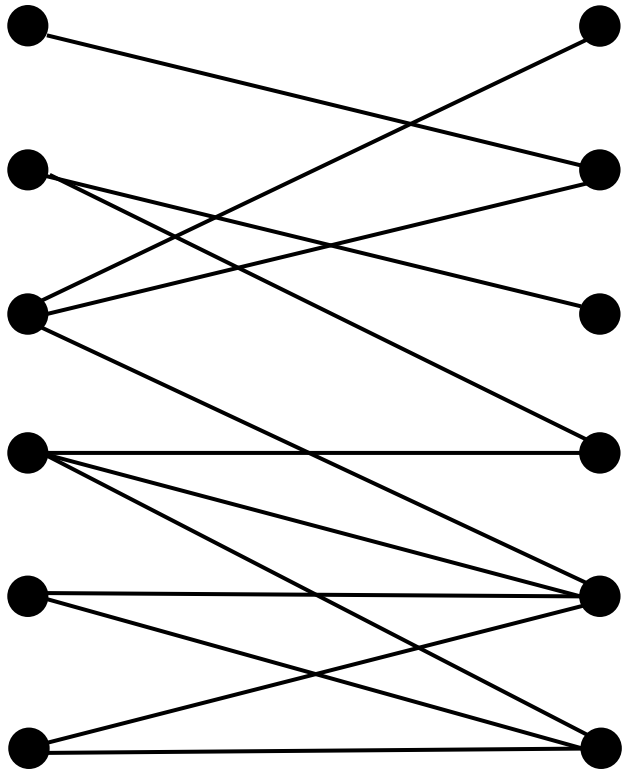
Hall's Marriage Theorem

We use the induction by the number n of boys (girls).

Base case. For $n = 1$ the statement is obvious.

Inductive step. Let the statement is proved for $n = k$. Let's try to prove it for $n = k + 1$.

Case 1. Suppose there are no extremal sets, so for any set of k boys there are at least $k + 1$ "suitable" girls.



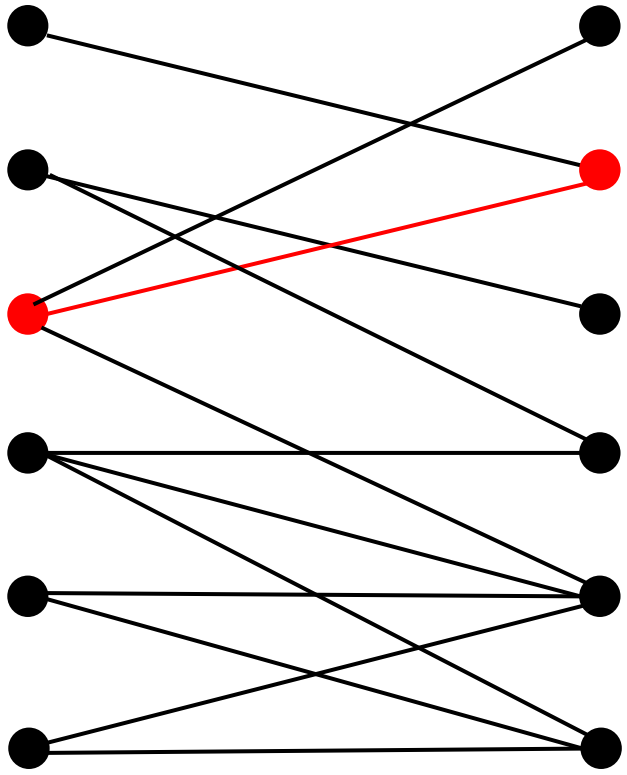
Hall's Marriage Theorem

Inductive step. Let the statement is proved for $n = k$. Let's try to prove it for $n = k + 1$.

Case 1. Suppose there are no extremal sets, so for any set of k boys there are at least $k + 1$ "suitable" girls.

Then we simply choose any boy and form a married couple from him and any of his "girlfriends".

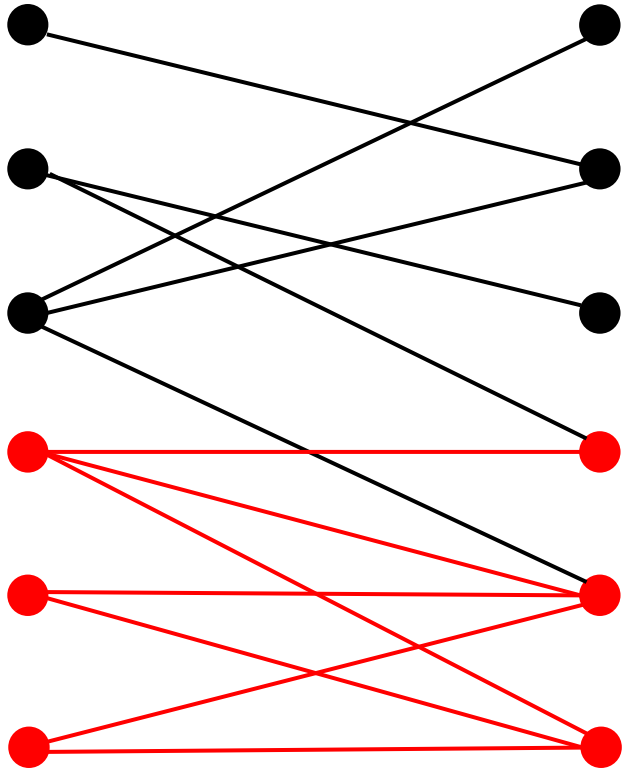
Any set of girls looses not more than one girl; so an extremal set may appear, but there are still at least $k + 1$ "suitable" girls for any set of k boys.



Hall's Marriage Theorem

Inductive step. Let the statement is proved for $n = k$. Let's try to prove it for $n = k + 1$.

Case 2. There is at least one extremal set.

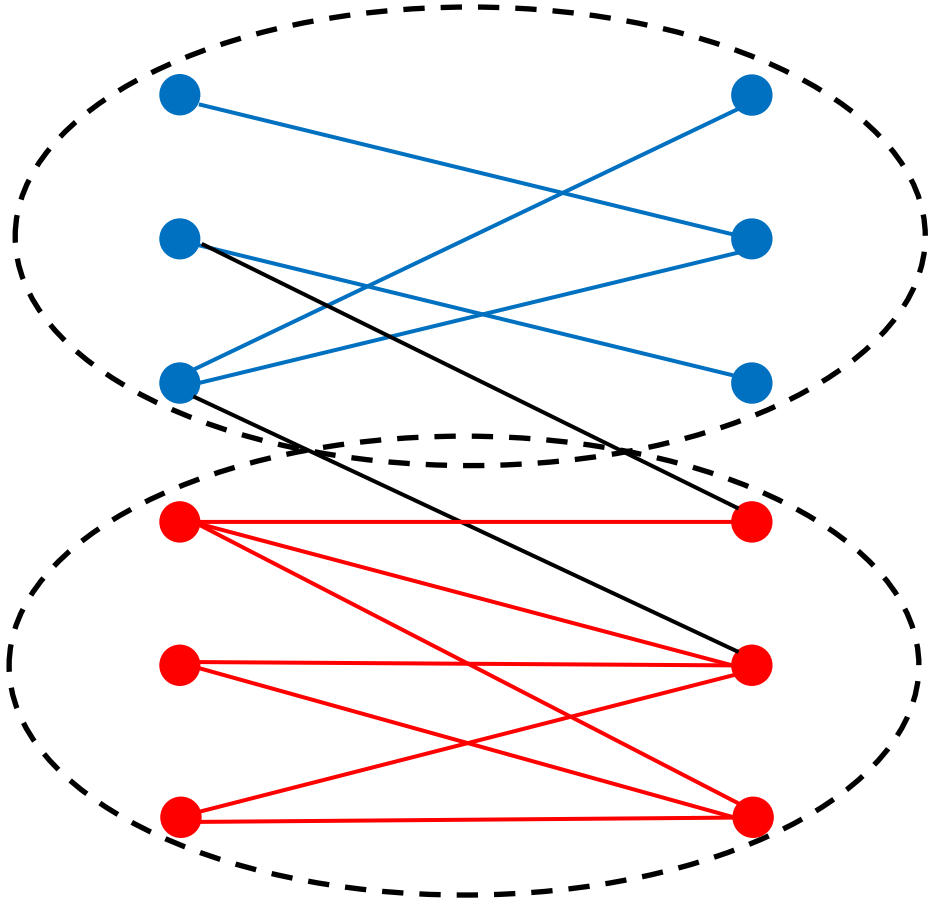


Hall's Marriage Theorem

Inductive step. Let the statement is proved for $n = k$. Let's try to prove it for $n = k + 1$.

Case 2. There is at least one extremal set.

According to the inductive supposition, we can form the pairs in the red set and in the blue set independently.

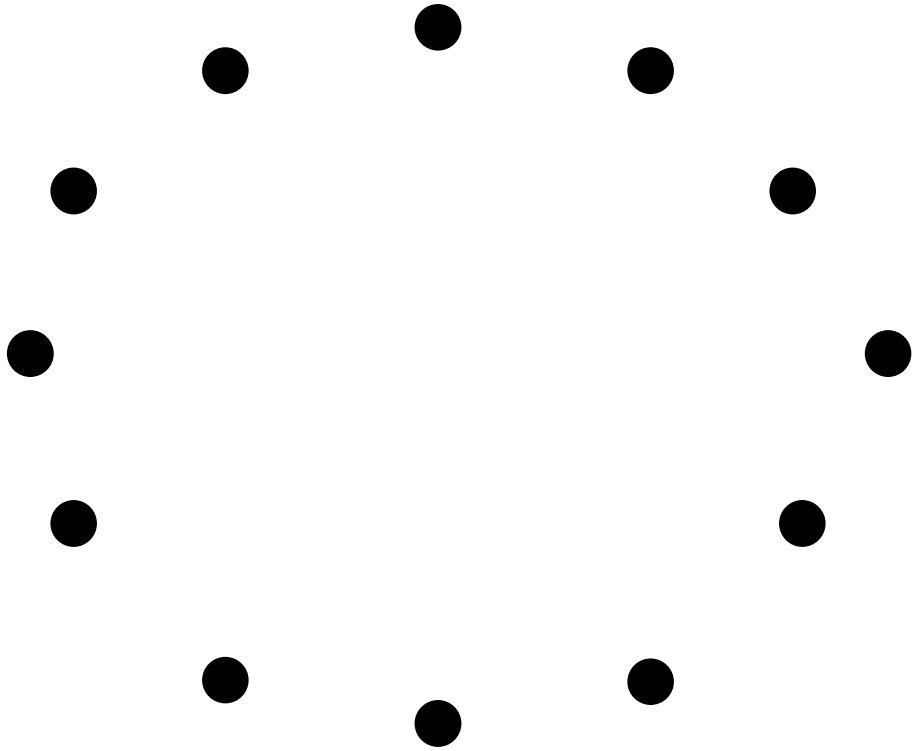


Ore’s Theorem

Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.

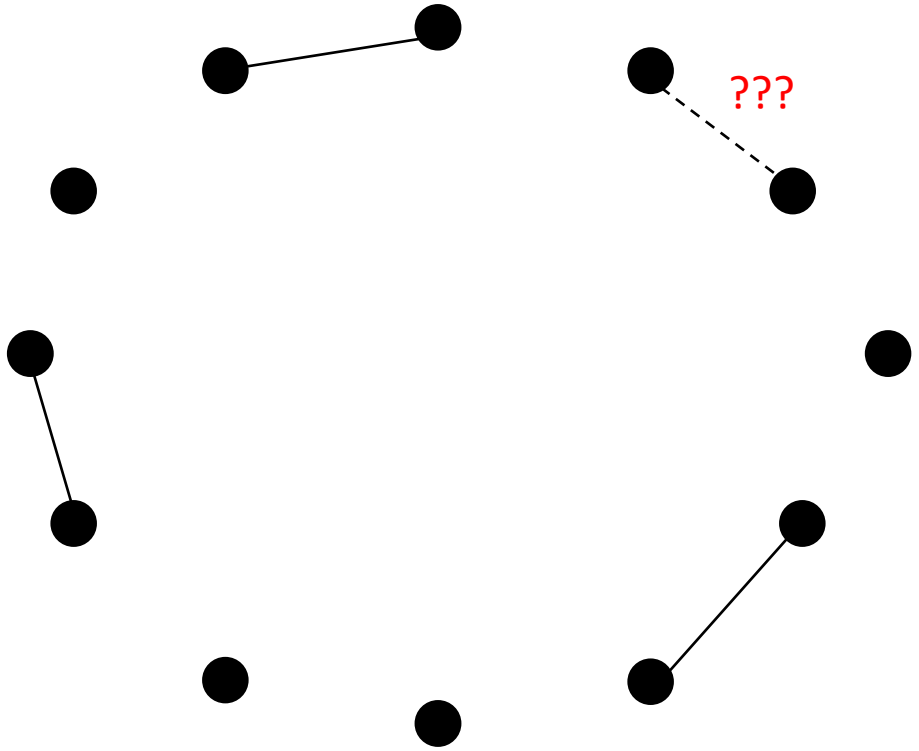
Ore’s Theorem

Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.



Ore's Theorem

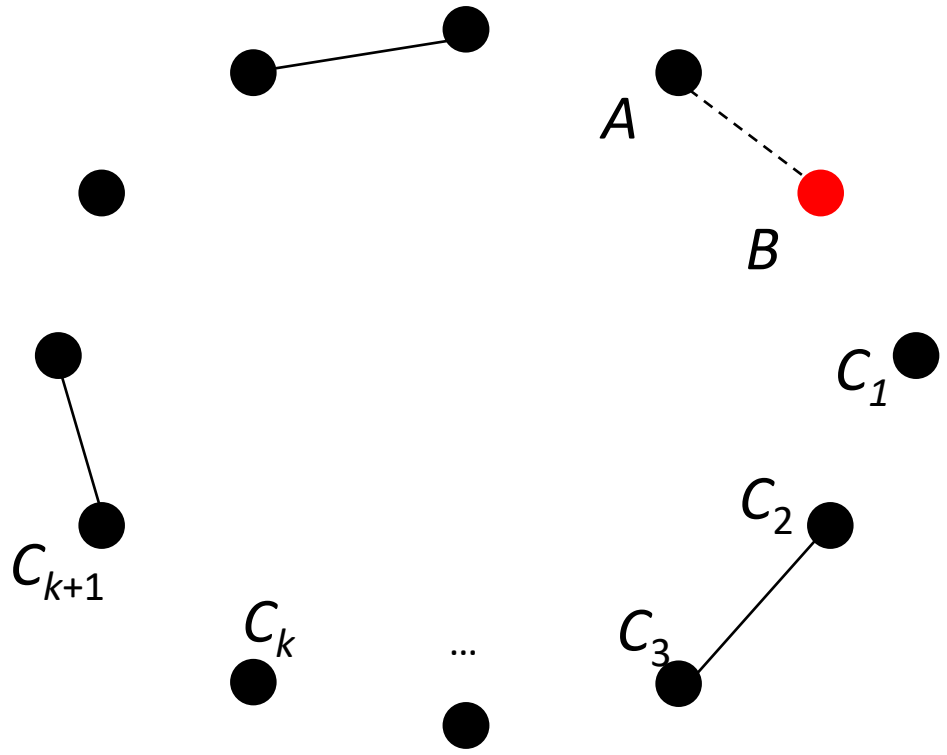
Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.



Ore's Theorem

Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.

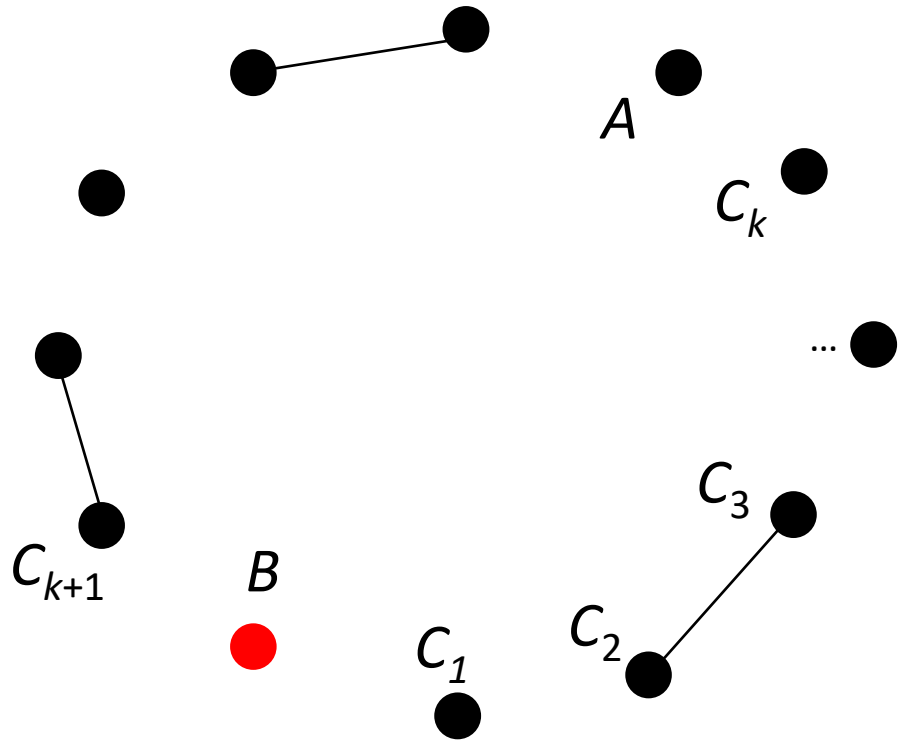
I'm choosing an arc $BC_1C_2\ldots C_k$ and I want to reverse it.



Ore's Theorem

Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.

I'm choosing an arc $BC_1C_2\ldots C_k$ and I want to reverse it.



Ore's Theorem

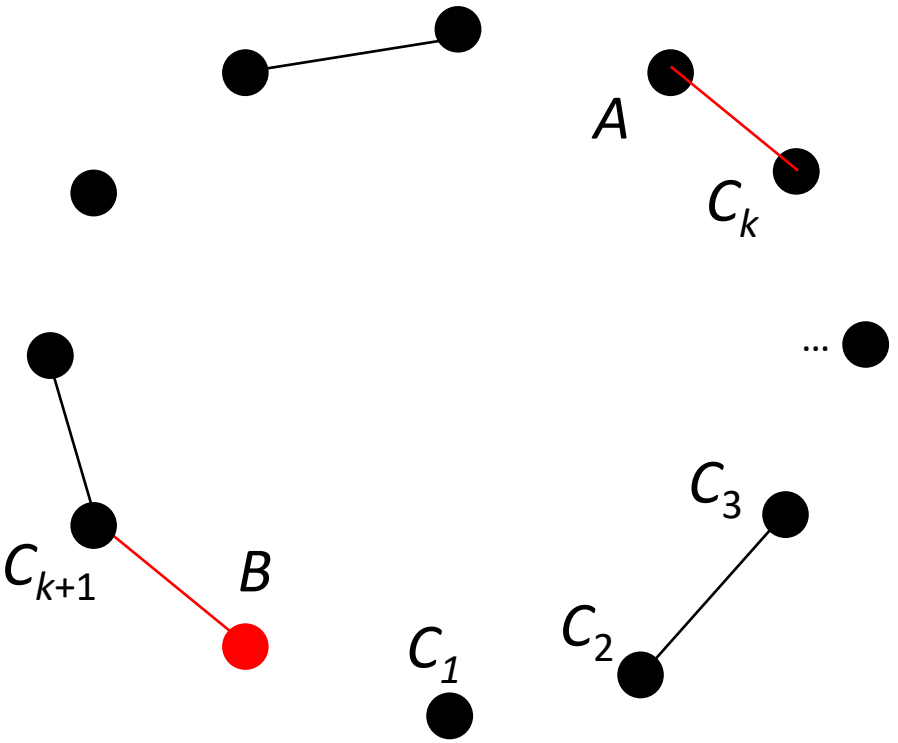
Let there is graph with 200 vertices, and the degree of each vertex is not less than 100. Then such a graph has a Hamiltonian cycle.

I'm choosing an arc $BC_1C_2\ldots C_k$ and I want to reverse it.

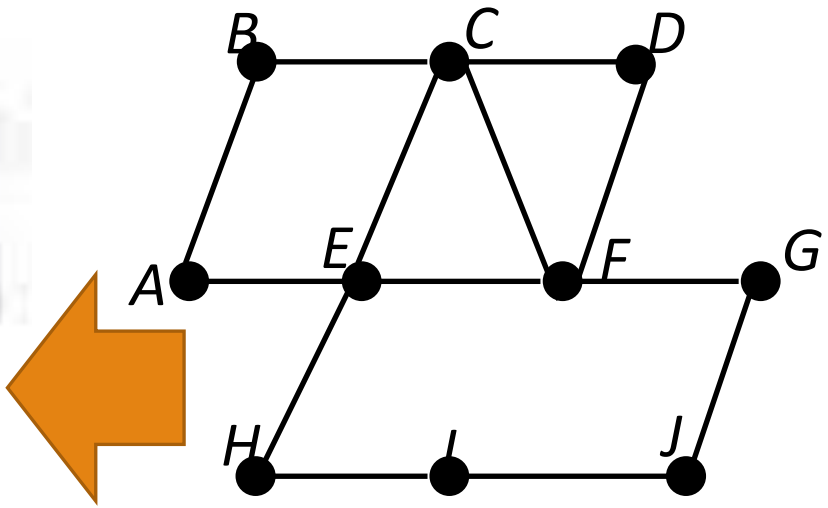
I need to choose such an arc that:

1) B and C_{k+1} need to be connected by an edge;

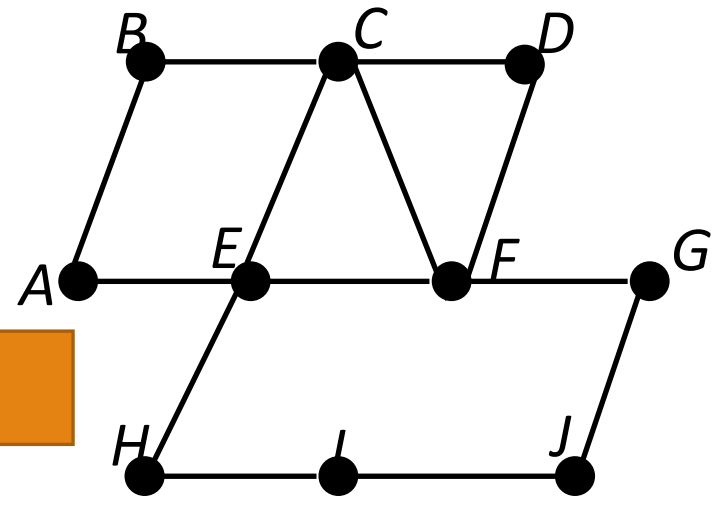
2) A and C_k need to be connected by an edge.



One Nice Trick For Saving Your Privacy

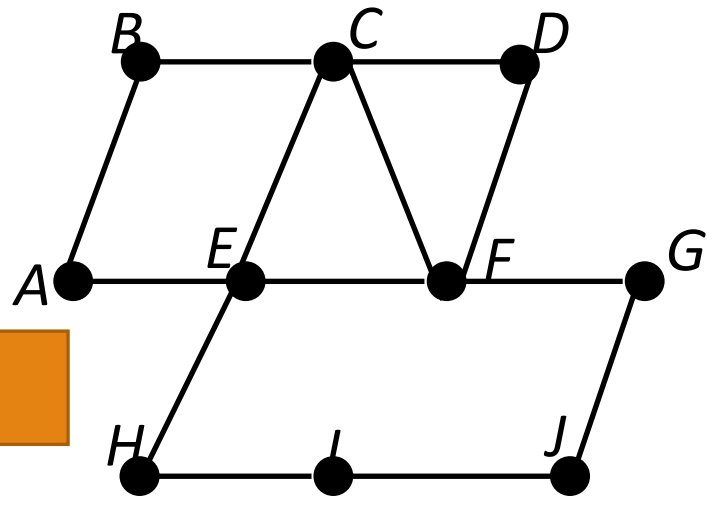


One Nice Trick For Saving Your Privacy

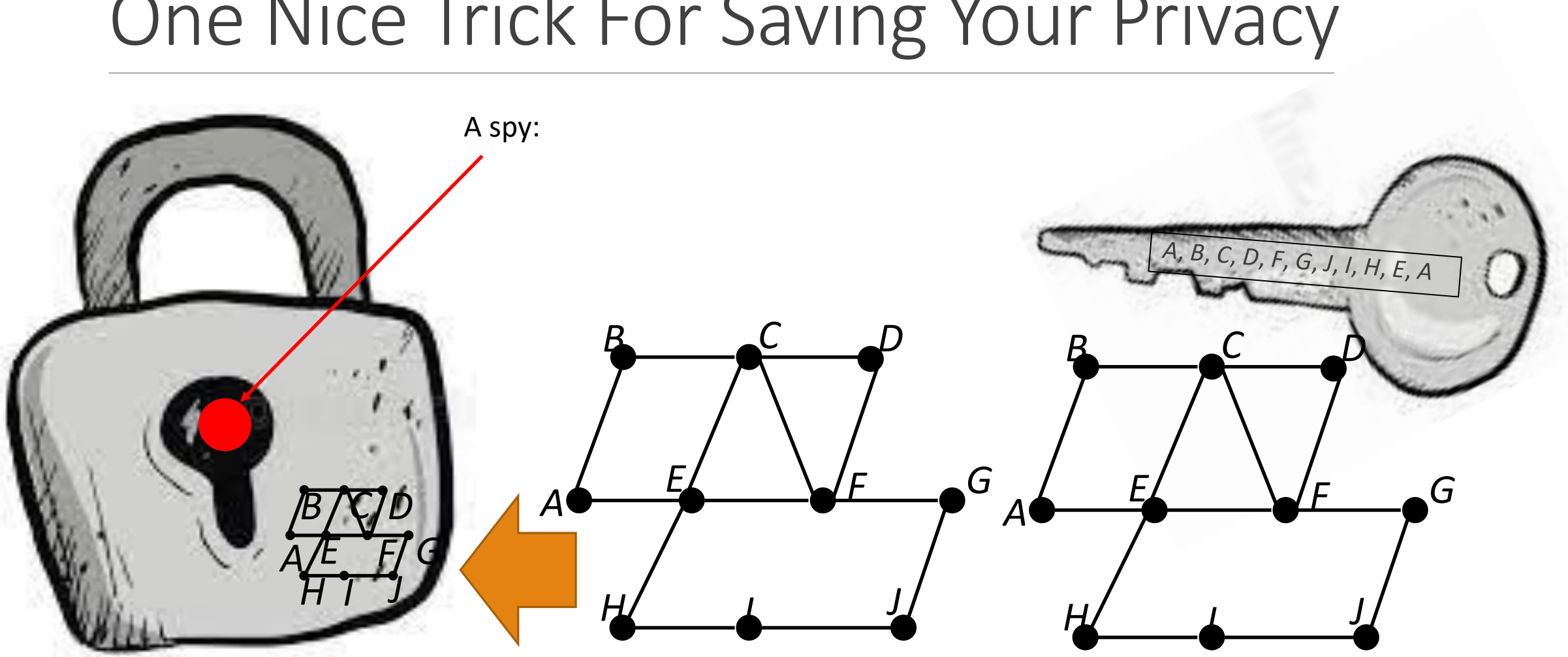


One Nice Trick For Saving Your Privacy

A spy: (*A*, *B*, *C*, *D*, *F*, *G*, *J*, *I*, *H*, *E*, *A*)



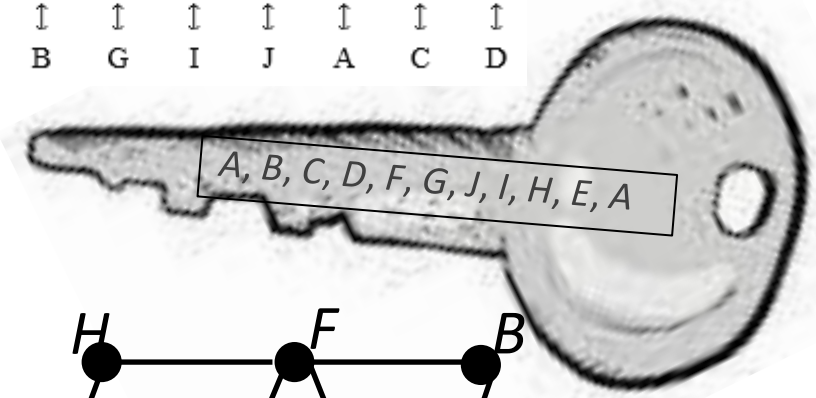
One Nice Trick For Saving Your Privacy

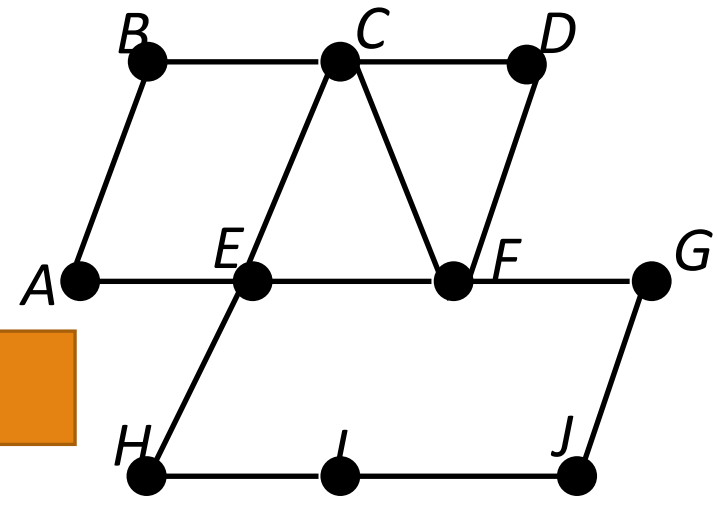


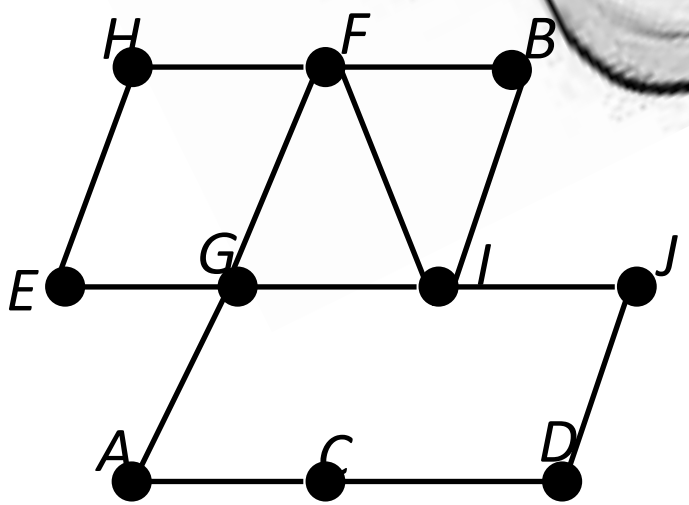
One Nice Trick For Saving Your Privacy

A spy:

A	B	C	D	E	F	G	H	I	J
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	H	F	B	G	I	J	A	C	D







One Nice Trick For Saving Your Privacy

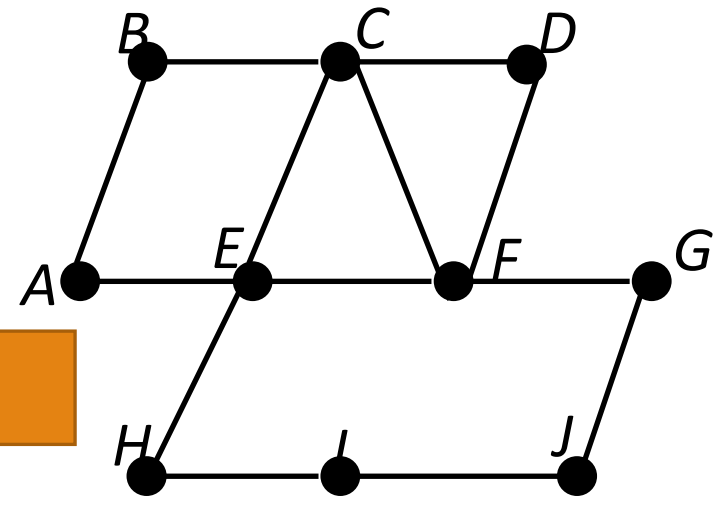
A spy:

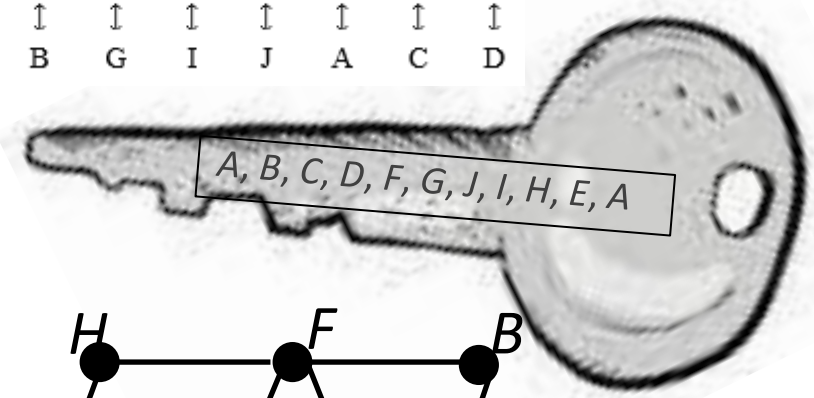
A	B	C	D	E	F	G	H	I	J
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	H	F	B	G	I	J	A	C	D

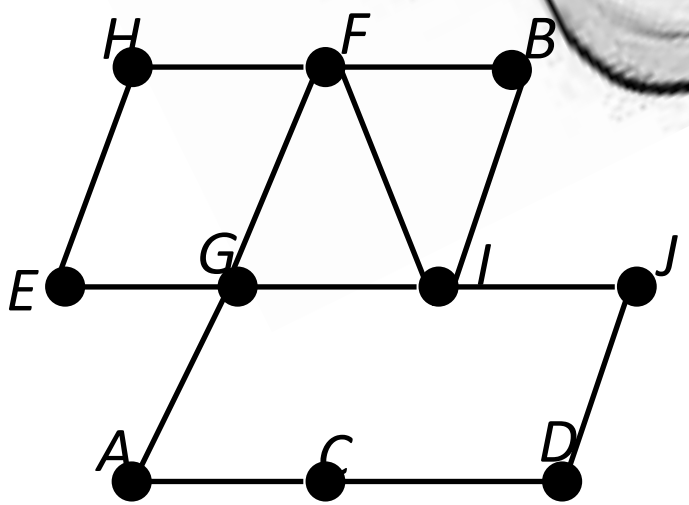
The lock asks me to:

a) show the isomorphism **or**

b) to show the Hamiltonian cycle.







One Nice Trick For Saving Your Privacy

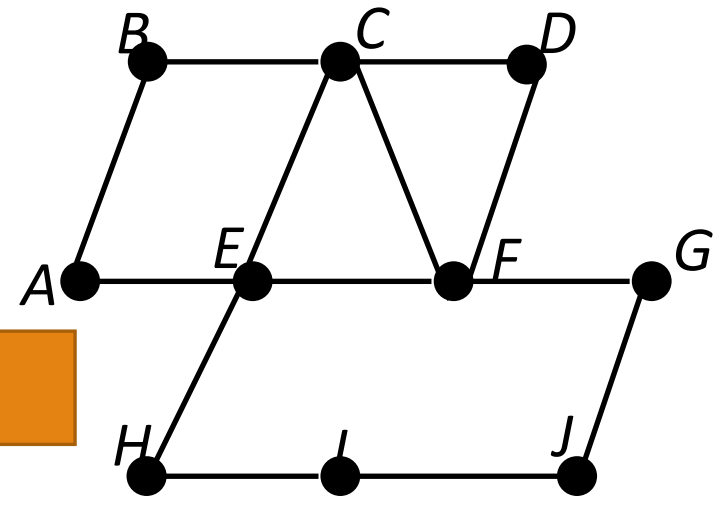
A spy: ($B \to H$, $C \to F$, …, $J \to D$)

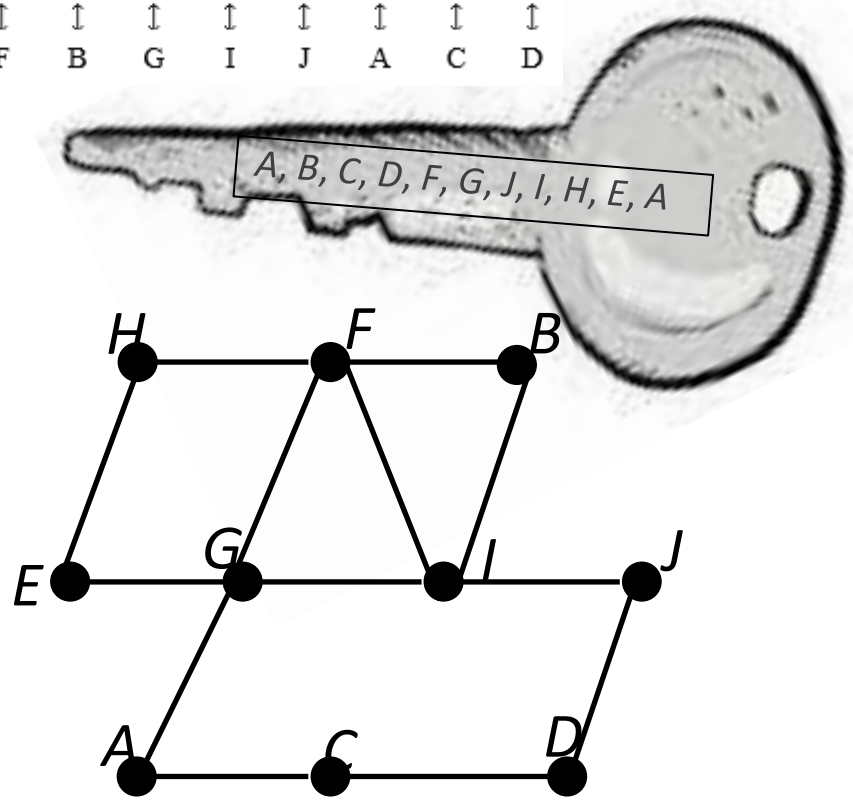
A	B	C	D	E	F	G	H	I	J
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	H	F	B	G	I	J	A	C	D

The lock asks me to:

a) **show the isomorphism or**

b) to show the Hamiltonian cycle.





One Nice Trick For Saving Your Privacy

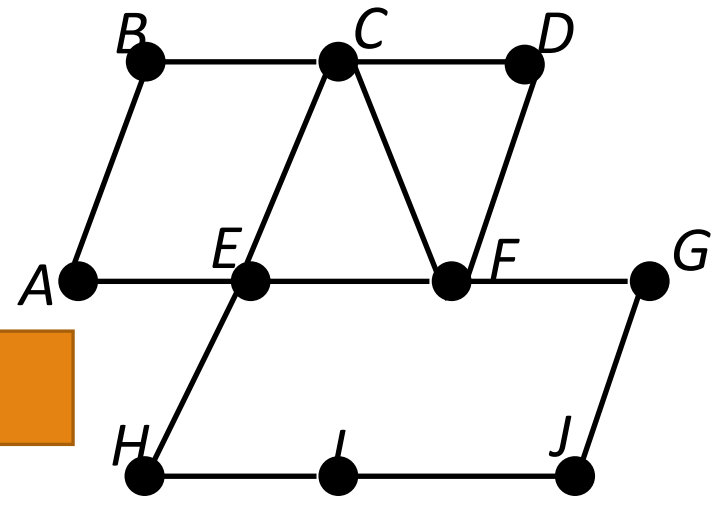
A spy: (*E*, *H*, *F*, *B*, *I*, *J*, *D*, *C*, *A*, *G*, *E*)

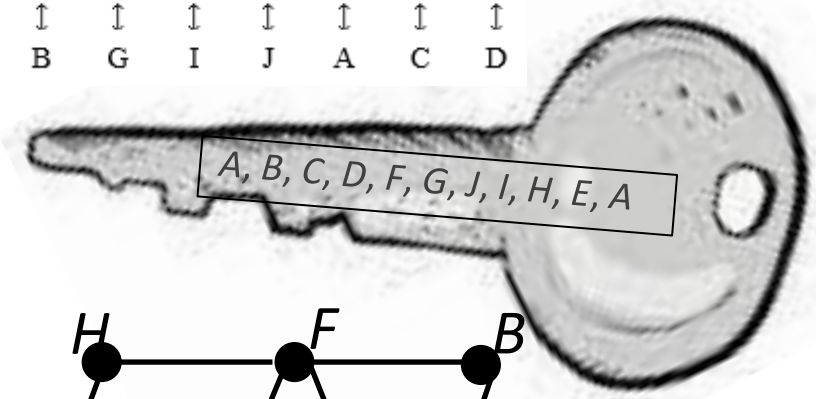
A	B	C	D	E	F	G	H	I	J
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	H	F	B	G	I	J	A	C	D

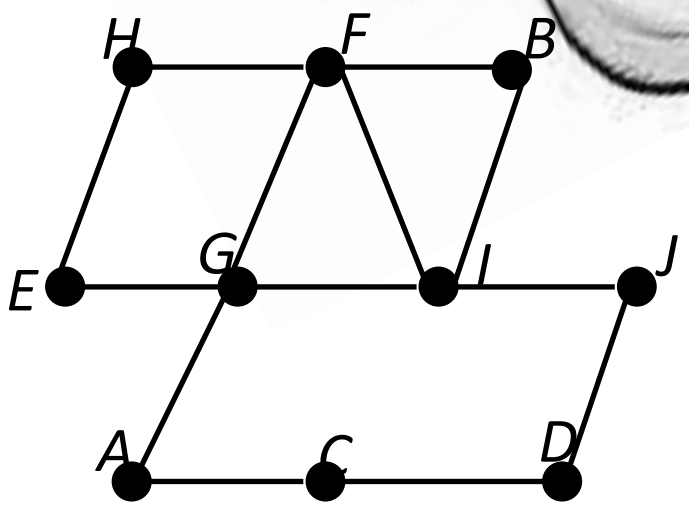
The lock asks me to:

a) show the isomorphism **or**

b) to show the Hamiltonian cycle.







Fermat primality test

Suppose Bob has a big number n and he wants to check if it is prime.

He can do the following:

take a number a which is not divisible by n;

check if it is true that

$$a^{n-1} \equiv 1 \pmod{n}.$$

If it is not so then n is not a prime.

If it is so you can repeat the test several times.

Carmichael numbers

A Carmichael number is such a composite number n that for any a which is coprime to n

$$a^{n-1} \equiv 1 \pmod{n}.$$

Such a number cannot be proved to be composite using the Fermat primality test.

For example, take $n = 561 = 3 \times 11 \times 17$:

$$a^{560} \equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3};$$

$$a^{560} \equiv (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11};$$

$$a^{560} \equiv (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}.$$

So $a^{560} - 1$ is divisible by 3, 11 and 17; thus, it is also divisible by 561 and

$$a^{560} \equiv 1 \pmod{561}.$$

Fermat's Method

Let n be an odd composite number, $n = ab$, $a \geq b > 1$.

Then also

$$\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = \frac{a^2+2ab+b^2}{4} - \frac{a^2-2ab+b^2}{4} = ab = n$$

And thus

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

Fermat's Method

Let n be an odd composite number, $n = ab$, $a \geq b > 1$.

Then also

$$\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = \frac{a^2+2ab+b^2}{4} - \frac{a^2-2ab+b^2}{4} = ab = n$$

And thus

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

If we will find two numbers, t and s, such that $n = t^2 - s^2$, then we will factorize n.

Fermat's Method

Let n be an odd composite number, $n = ab$, $a \geq b > 1$.

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

If we will find two numbers, t and s, such that $n = t^2 - s^2$, then we will factorize n.

We start with $t = \left[\sqrt{n}\right] + 1$ and increase t by 1, while the number $n - t^2$ is a square.

Fermat's Method

Let n be an odd composite number, $n = ab$, $a \geq b > 1$.

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

If we will find two numbers, t and s, such that $n = t^2 - s^2$, then we will factorize n.

We start with $t = \left[\sqrt{n}\right] + 1$ and increase t by 1, while the number $n - t^2$ is a square.

Example. Let $n = 200819$.

Then $\left[\sqrt{n}\right] + 1 = 449$. We take $t = 449$. $n - t^2 = 782$ is not a square, but if $t = 450$ then $n - t^2 = 1681$ which is 41^2. Thus $t = 450$, $s = 41$, $n = 450^2 - 41^2 = 491 \times 409$.

Fermat's Method

Let n be an odd composite number, $n = ab$, $a \geq b > 1$.

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

If we will find two numbers, t and s, such that $n = t^2 - s^2$, then we will factorize n.

We start with $t = \left[\sqrt{n}\right] + 1$ and increase t by 1, while the number $n - t^2$ is a square.

Example. Let $n = 200819$.

Then $\left[\sqrt{n}\right] + 1 = 449$. We take $t = 449$. $n - t^2 = 782$ is not a square, but if $t = 450$ then $n - t^2 = 1681$ which is 41^2. Thus $t = 450$, $s = 41$, $n = 450^2 - 41^2 = 491 \times 409$.

So, for RSA-cryptosystem it is better to choose $n = pq$ such that the difference between p and q is not too small.