Lecture 34: Revision

Consultation times are advertised on moodle as follows:

Fri 26 May: 12:30 - 1:30 at 9Rnf/418 (Daniel's office)

Mon 29 May: 12:00-1:00 at 9Rnf/418 (Daniel's office)

Wed 31 May: 1:00 - 2:00 at 9Rnf/448 (Ian's office)

Fri 2 June: 3:00 - 4:00 at 9Rnf/418 (Daniel's office)
Assignment 10's available for collection

Mon 5 June: 2:00 - 4:00 at 9Rnf/342
Assignment 10's available for collection

Wed 7 June: 2:00 - 4:00 at 9Rnf/442

What is wrong with this argument?

$P(k)$ is the proposition that in any set of k horses all the horses have the same colour.

We will prove, by induction, that $P(k)$ is true for all $k \geqslant 1$.

Base step: If I have only one horse, then clearly all my horses are the same colour. Hence $P(1)$ is true.

Inductive step: Suppose that $P(k)$ is true. We will use this to prove that $P(k+1)$ is true.

Consider $k+1$ horses. Since $P(k)$ is true, horses $1, 2, \ldots, k$ are the same colour. Similarly, horses $2, 3, \ldots, k, k+1$ are the same colour. Hence horse 1 is the same colour as horses $2, 3, \ldots, k$, which are the same colour as horse $k+1$. Thus all $k+1$ horses are the same colour.

QED.

Induction

Induction is used to prove a sequence $P(0)$, $P(1)$, $P(2), \ldots,$ of propositions.

If you can prove

- $P(0)$ is true, and
- $P(k) \to P(k+1)$ for $k \geqslant 0$.

Then it follows by induction that $P(k)$ is true for $k \geqslant 0$.

If you can prove

- $P(0)$ is true, and
- $\big(P(0) \wedge P(1) \wedge \cdots \wedge P(k)\big) \to P(k+1)$ for $k \geqslant 0$.

Then it follows by **strong induction** that $P(k)$ is true for $k \geqslant 0$.

Induction

You can start anywhere and work your way up:

If you can prove

- $P(1)$ is true, and
- $P(k) \to P(k+1)$ for $k \geqslant 1$.

Then it follows by induction that $P(k)$ is true for $k \geqslant 1$.

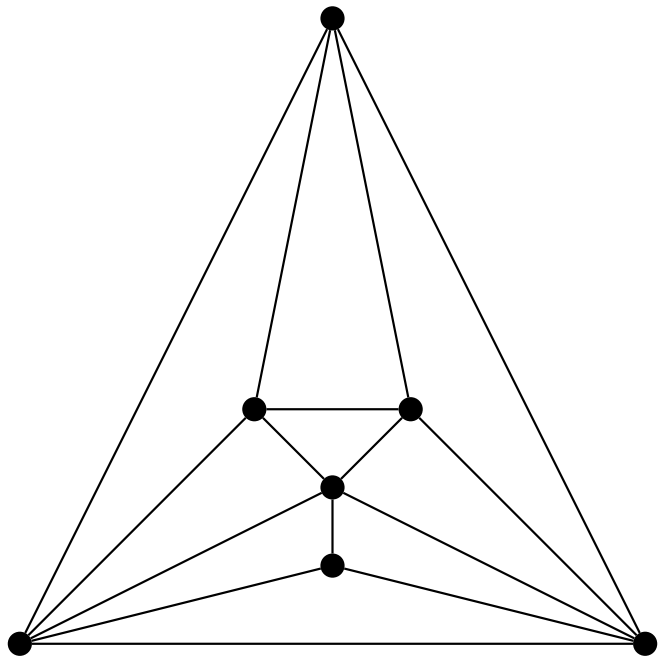
In the horses example

- $P(1)$ is true, and
- $P(k) \to P(k+1)$ for $k \geqslant 2$.

However, that one missing link is *vital*.
Of course $P(1)$ is true, but $P(2), P(3), P(4), P(5), \ldots$ are all false.
Remember that $F \to F$ is true!

What's wrong with this induction?

A triangulation is a graph that is drawn so that edges do not cross and every region is a triangle. For example:

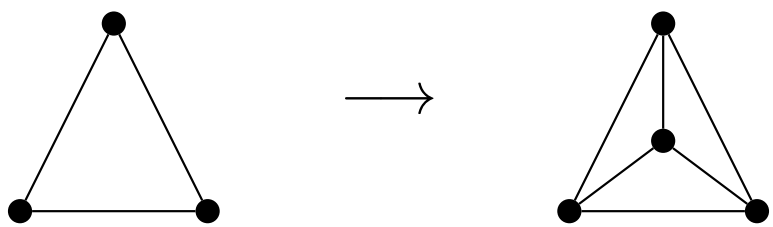


What's wrong with this induction?

If a triangulation has n vertices, it must have $3n - 6$ edges.

Proof by induction:
Base Case: It's true for a single triangle, since it has 3 vertices and $3 = 9 - 6$ edges.

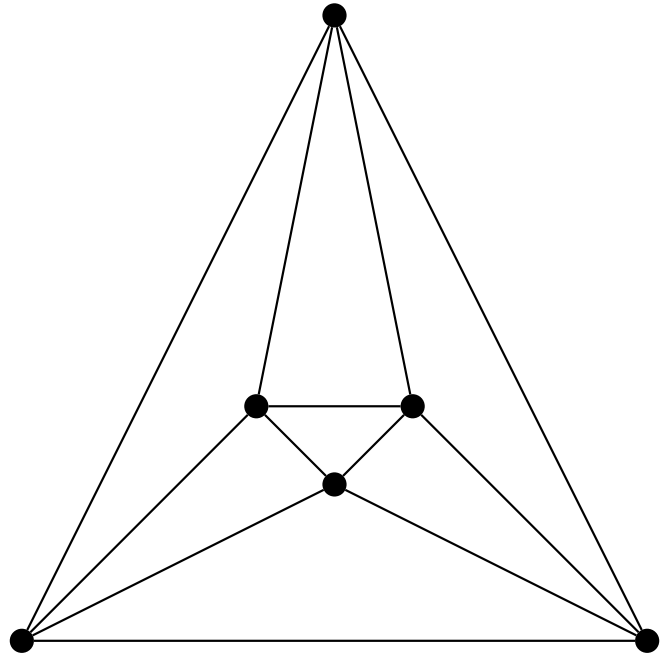
Inductive step: Suppose it's true when $n = k$. From a triangulation with k vertices we can build a triangulation with $k + 1$ vertices by choosing any triangle and subdividing it as follows:



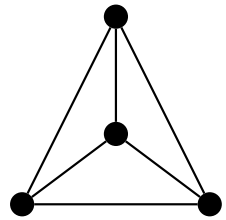
In doing so, we have increased the number of vertices by 1 and the number of edges by 3. So the number of edges now is $3 + (3n - 6) = 3(n + 1) - 6$, which proves the inductive step.

The flaw

The problem is that the argument doesn't cover all cases. There are triangulations which can't be built in the way described. For example:

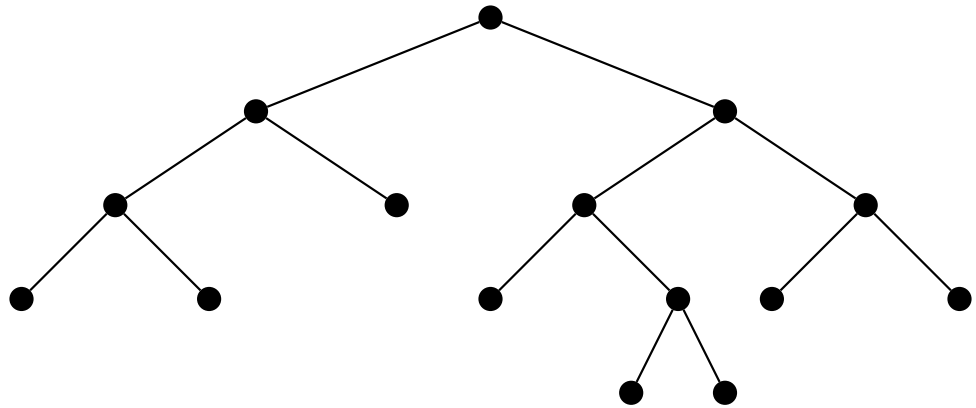


contains no subdivided triangle



Binary trees

A binary tree models a sequence of yes/no questions that lead to some decisions. At each vertex we either ask a question (leading to 2 further branches) or make a decision (no further branches).



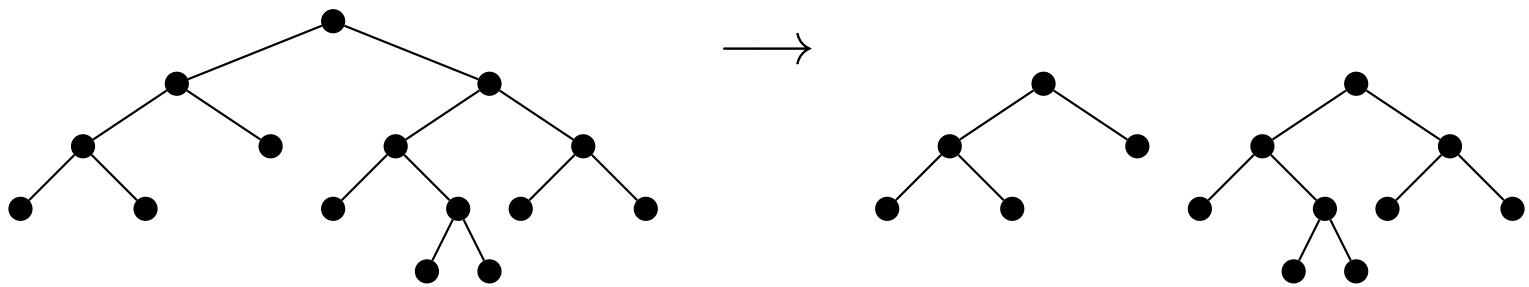
Suppose we classify vertices as either "question vertices" or "decision vertices".

How are the number of each type of vertex related?

Claim: If a binary tree has q question vertices then it has $q + 1$ decision vertices.

Base case: If a binary tree has 0 question vertices then it consists of a single (decision) vertex, which obeys the claimed rule.

Strong Induction: Assume that the statement is true for all $q \leqslant k$. Consider a binary tree with $q = k + 1$. What happens if we delete the first question vertex, and its two edges?



We get two smaller binary trees! By the inductive assumption, they both obey the claim. Suppose the trees have a, b question vertices (hence $a + 1, b + 1$ decision vertices). Then our original tree had $a + b + 1$ question vertices and $a + 1 + b + 1 = a + b + 2$ decision vertices, so the inductive step works.

Claim: If a binary tree has q question vertices then it has $q + 1$ decision vertices.

Challenge: Prove this directly, using the Handshaking lemma.

Proof by descent

In the chapter on induction it's proved that $n! > 2^n$ for $n \geqslant 4$.

Here's a proof of the same statement by "descent".

Suppose there is some $n \geqslant 4$ for which $n! \leqslant 2^n$.
Then

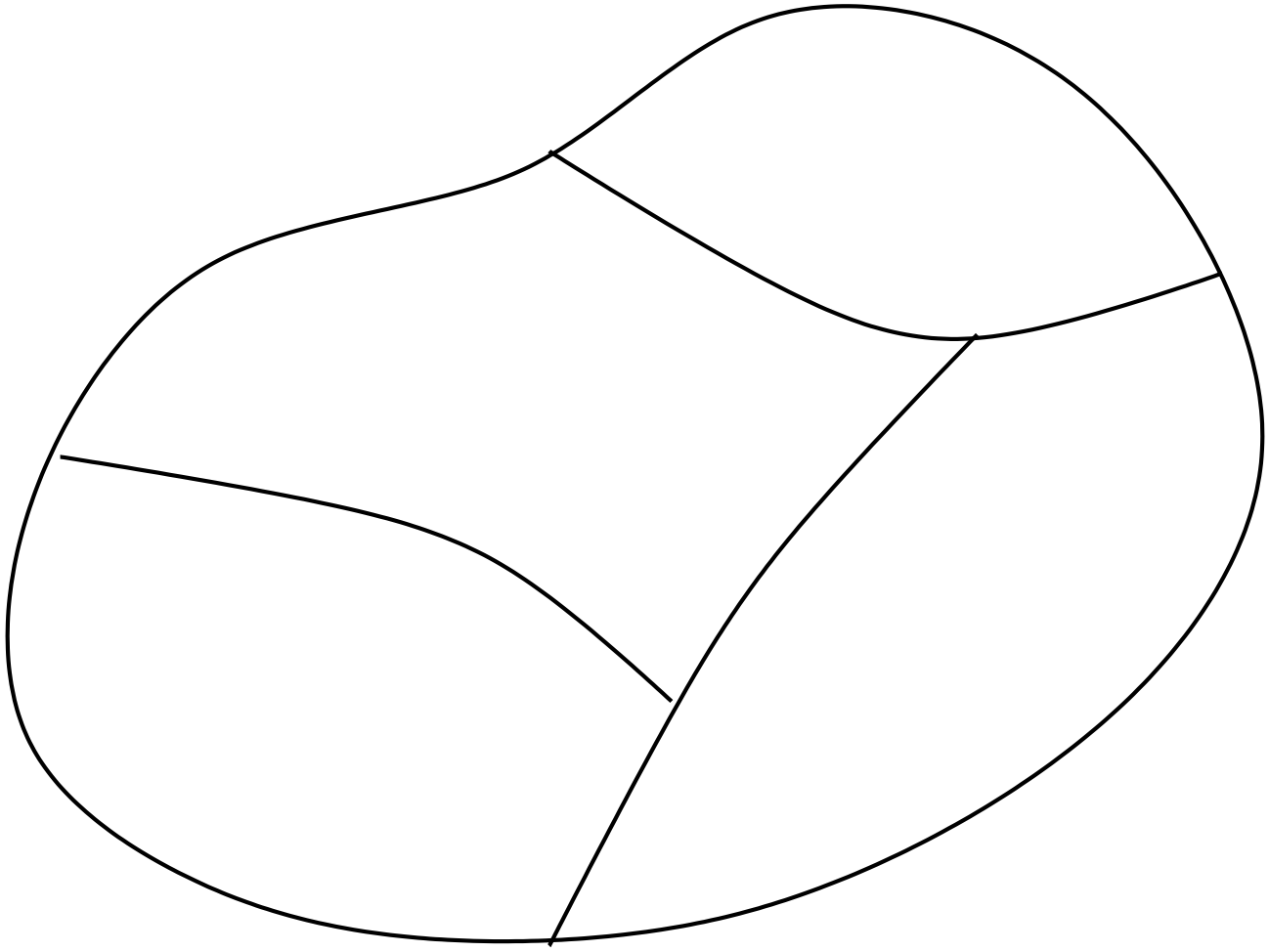
$$(n-1)! = \frac{n!}{n} \leqslant \frac{n!}{2} \leqslant \frac{2^n}{2} = 2^{n-1}$$

which is the same inequality, with n replaced by $n-1$.
By working backwards ("descent") we can get all the way to the base case, namely $n = 4$. But here we know that

$$4! = 24 > 16 = 2^4.$$

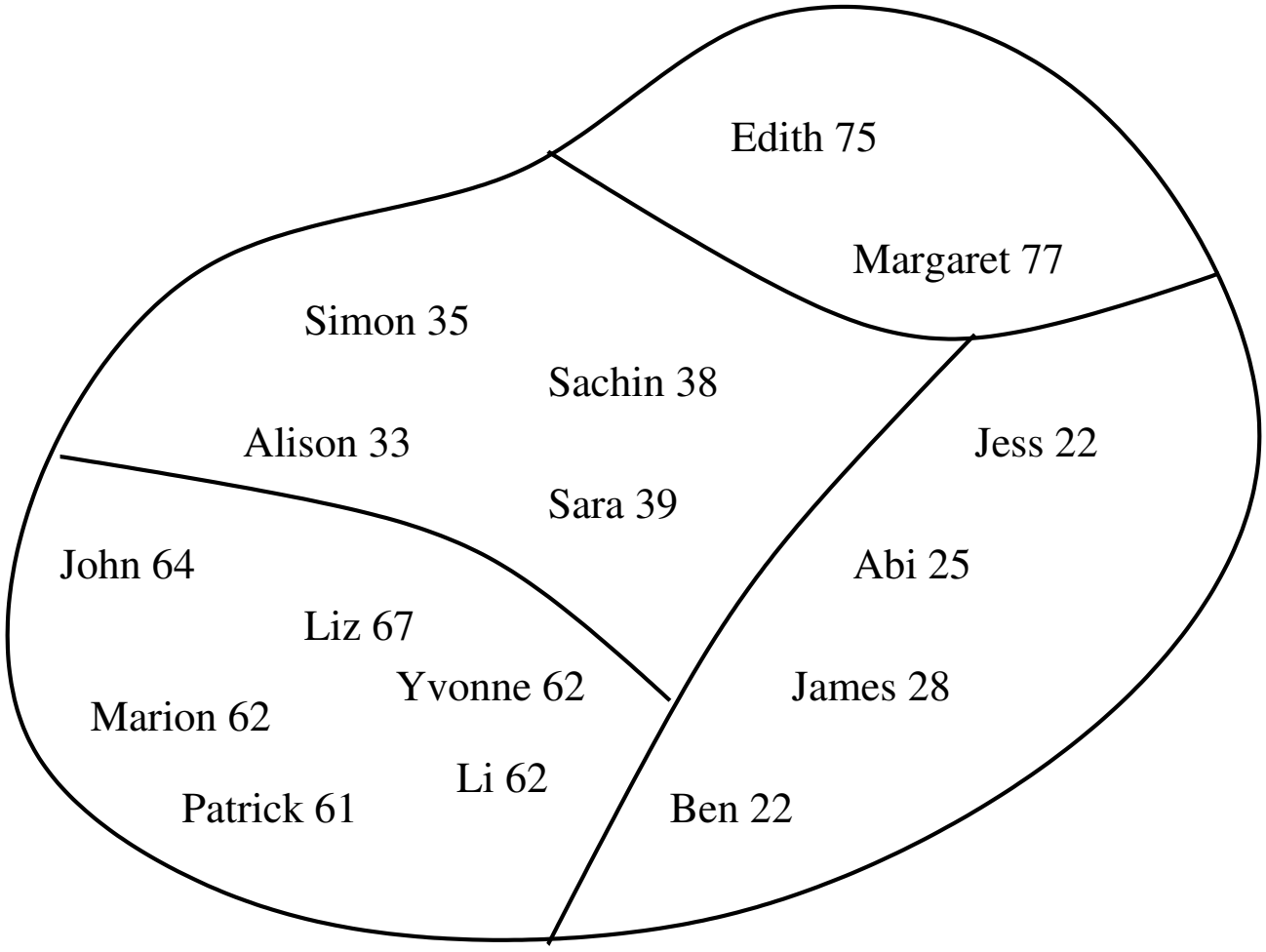
This contradiction shows that our original supposition is false.

Equivalence relations



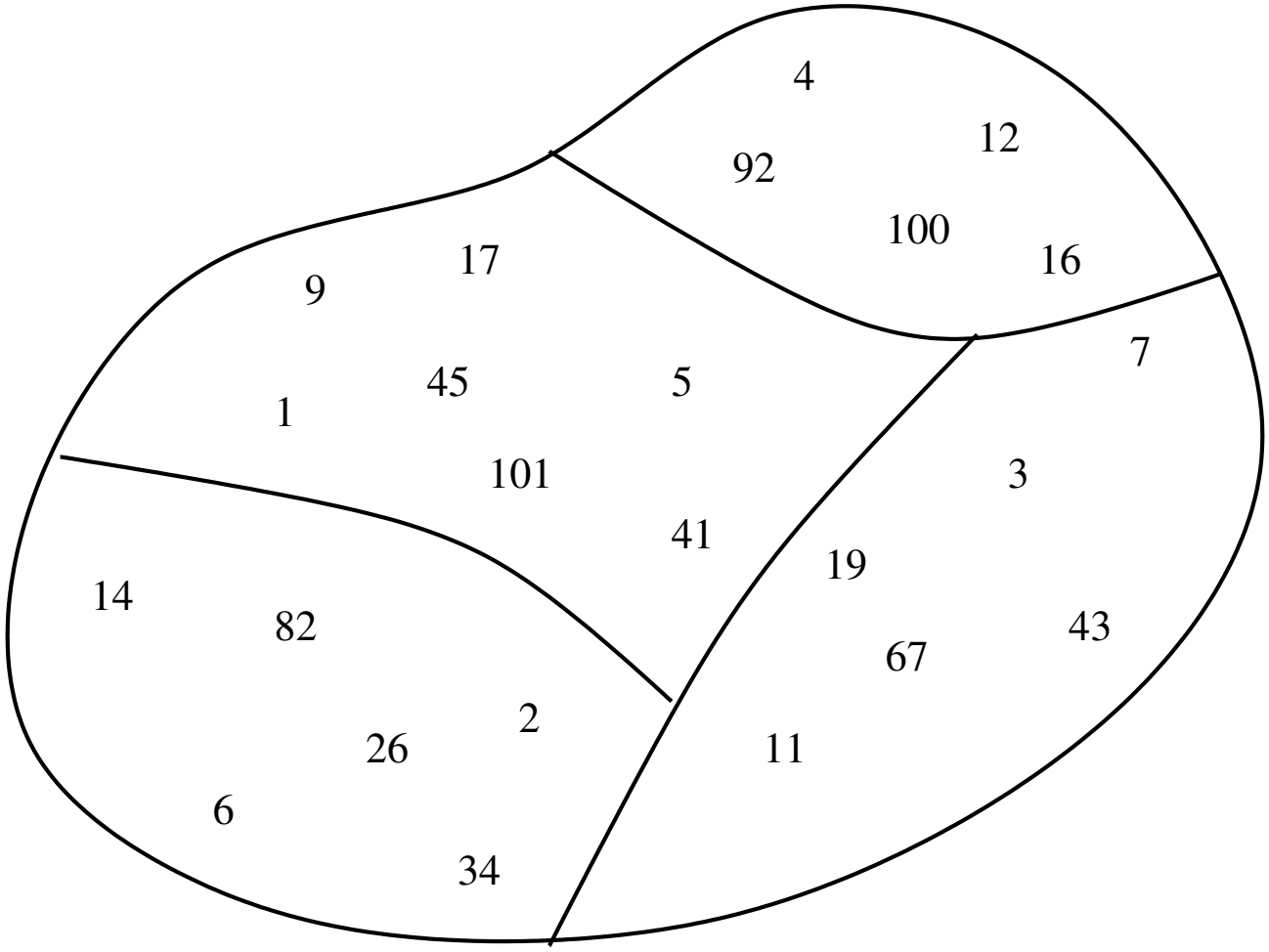
An equivalence relation partitions a set into equivalence classes.
An equivalence class is a SET of equivalent things.

The "age group" relation



In this case $\{Abi, Ben, James, Jess\}$ is an equivalence class.
We might write this as $[Abi]$ (or as $[Jess]$ etc.)

The mod 4 relation



Numbers are equivalent ("congruent") mod 4 if they leave the same remainder when divided by 4.

Solving congruences

When working with congruences mod n you can replace any number by any other number that it is congruent to, mod n.

A particularly useful case of this is that you can replace any multiple of n by 0.

To solve a congruence $ax \equiv b \pmod{n}$ you want to write $b = ax + ny$ for some integers x, y. Then by the above principle, you can throw the ny term away, and you have your solution.

For given a, b, n you can find the x, y you need using the extended Euclidean algorithm. (Or in trying to find them you may find that they don't exist. This happens if $\gcd(a, n)$ doesn't divide b.)

Use Euclid's algorithm to find g, where $g = \gcd(21, 36)$ and then to find integers x, y such that $g = 21x + 36y$.

ANS: Euclid's algorithm gives

$$\begin{aligned} 36 &= 1 \times 21 + 15 \\ 21 &= 1 \times 15 + 6 \\ 15 &= 2 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

So $g = 3$, the last non-zero remainder. Back substituting we find

$$\begin{aligned} 3 &= 15 - 2 \times 6 \\ &= 15 - 2 \times (21 - 15) \\ &= 3 \times 15 - 2 \times 21 \\ &= 3 \times (36 - 21) - 2 \times 21 \\ &= 3 \times 36 - 5 \times 21 \end{aligned}$$

so $x = -5$, $y = 3$ is a solution.

If you were asked to find a solution to $21x \equiv 12 \pmod{36}$ your first step might be to find that:

$$3 = 3 \times 36 - 5 \times 21.$$

Multiplying by 4 we get,

$$12 = 12 \times 36 - 20 \times 21.$$

Which means that

$$12 \equiv -20 \times 21 \pmod{36}.$$

It follows that $x = -20$ is a solution. As is $x = 36 - 20 = 16$.

If you were asked to find a solution to $21x \equiv 14 \pmod{36}$ your answer would be that there are no solutions, since 14 isn't divisible by $\gcd(21, 36) = 3$.

Find integers x, y such that $1 = 21x + 37y$.

ANS: Euclid's algorithm gives

$$\begin{aligned} 37 &= 1 \times 21 + 16 \\ 21 &= 1 \times 16 + 5 \\ 16 &= 3 \times 5 + 1 \\ 5 &= 5 \times 1 + 0 \end{aligned}$$

So $\gcd(37, 21) = 1$. Back substituting we find

$$\begin{aligned} 1 &= 16 - 3 \times 5 \\ &= 16 - 3 \times (21 - 16) \\ &= 4 \times 16 - 3 \times 21 \\ &= 4 \times (37 - 21) - 3 \times 21 \\ &= 4 \times 37 - 7 \times 21 \end{aligned}$$

Hence $x = -7$ and $y = 4$ is a solution.

What is the modular inverse of 21 mod 37?

ANS: We just saw that

$$1 = 4 \times 37 - 7 \times 21.$$

Hence $1 \equiv 21 \times (-7) \equiv 21 \times 30 \pmod{37}$.
So 30 is the modular inverse for 21 mod 37.

Solve $21x \equiv 3 \pmod{37}$.

ANS: To solve $21x \equiv 3 \pmod{37}$ we multiply both sides by the modular inverse of 21 to get $30 \times 21x \equiv 30 \times 3 \pmod{37}$ and hence $x \equiv 90 \pmod{37}$. As $90 \equiv 16 \pmod{37}$ we find that 16 is a solution (as is any integer that is congruent to 16 mod 37).