

1.7 Additional Examples of Proofs

Example: If $x+y$ is irrational then either x or y is irrational.

Idea: Implied universal quantifier

i.e. $(\forall x, y) [(x+y \text{ irrat}) \Rightarrow (x \text{ or } y \text{ irrat.})]$
real numbers

↳ Has the form $P \Rightarrow (Q \vee R)$

$$(P \wedge (\neg Q)) \Rightarrow R$$

$$(P \wedge (\neg R)) \Rightarrow Q$$

or $\neg(Q \vee R) \Rightarrow \neg P$

same as $(\neg Q \wedge \neg R) \Rightarrow \neg P$

$$\Rightarrow (x+y \text{ irrational})$$

$$(x \text{ and } y \text{ rational})$$

$$\wedge (x \text{ rational})$$

$$\Rightarrow (x+y \text{ rational})$$

$$\Rightarrow (y \text{ irrational})$$

↑

seems easier

Pf: Suppose that x and y are rational numbers.

This means $x = \frac{s}{t}$ and $y = \frac{p}{q}$ for $s, p, t, q \in \mathbb{Z}$

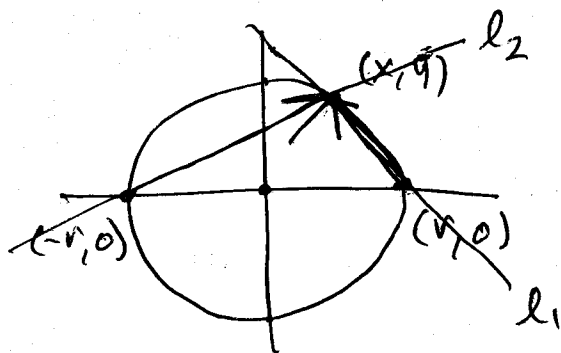
and $t, q \neq 0$. We must show that $x+y$ is

rational. But $x+y = \frac{s}{t} + \frac{p}{q} = \frac{sq+pt}{tq}$. Since

$sq+pt \in \mathbb{Z}$ and $tq \in \mathbb{Z}$ and non-zero, $x+y$ is

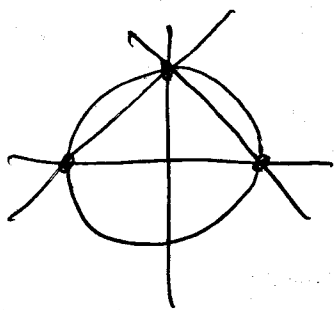
rational. \square

#4 (b)



show $l_1 \perp l_2$

Exceptions are
 $(-r, 0)$ and $(r, 0)$



How to show $l_1 \perp l_2$?

- 1) dot product of some vectors is zero or
- 2) product of slopes must be -1

Direction vector for l_1 : $\vec{a} = \langle x-r, y \rangle$

"

l_2 : $\vec{b} = \langle x+r, y \rangle$

$l_1 \perp l_2$ if and only if $\vec{a} \cdot \vec{b} = 0$ or

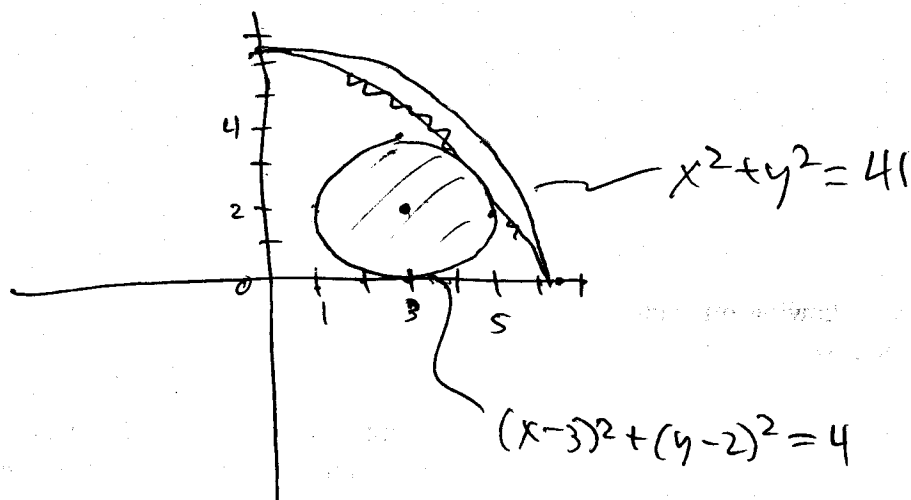
$$(x-r)(x+r) + y^2 = 0$$

$$x^2 - r^2 + y^2 = 0$$

true since (x, y) is on the circle.

PT: Let (x, y) be on the circle with $(x, y) \neq (r, 0)$ and $(x, y) \neq (-r, 0)$. The direction vector for the line joining (x, y) and $(r, 0)$ is $\langle x-r, y \rangle$ and that for the line joining (x, y) and $(-r, 0)$ is $\langle x+r, y \rangle$. The dot product of these vectors is $(x-r)(x+r) + y^2 = x^2 - r^2 + y^2 = 0$ since $x^2 + y^2 = r^2$. Hence the lines are perpendicular. \square

#7 (a)



Want to prove it.

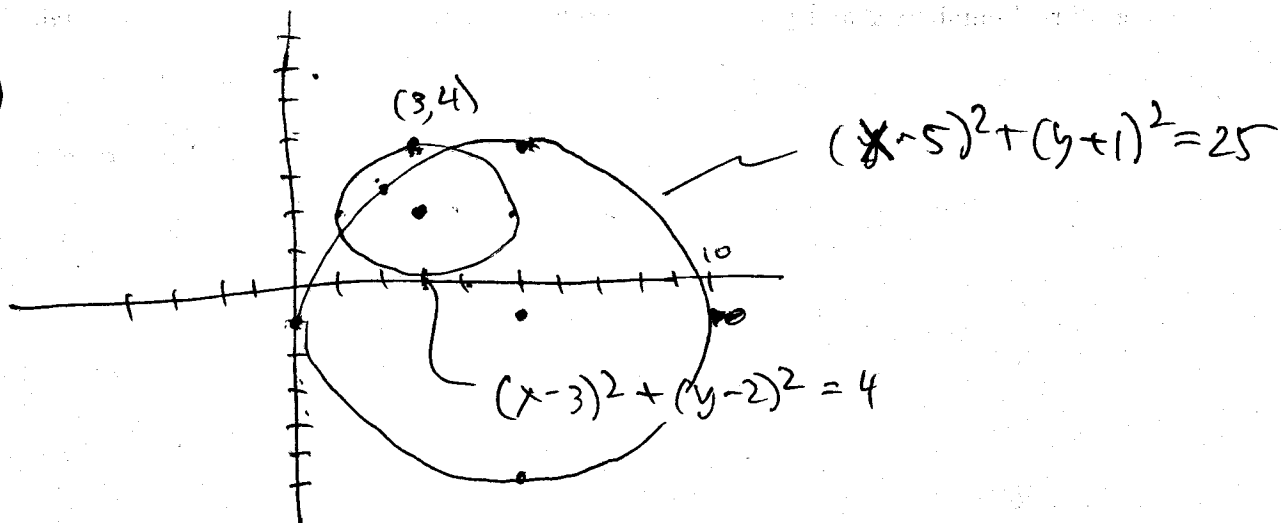
Let (x, y) satisfy $(x-3)^2 + (y-2)^2 \leq 4$.

Then $1 \leq x \leq 5$ and $0 \leq y \leq 4$. Therefore

$1 \leq x^2 \leq 25$ and $0 \leq y^2 \leq 16$. Hence

$$x^2 + y^2 \leq 25 + 16 = 41.$$

(c)



Disprove this. If $(x, y) = (2, 3)$ then
 $(x-5)^2 + (y+1)^2 = 9 + 16 = 25$ If $(x, y) = (3, 4)$
then $(x-3)^2 + (y-2)^2 = 0 + 4 = 4$ so (x, y) is
inside first circle. But $(x-5)^2 + (y+1)^2$
 $= 4 + 25 = 29$ so (x, y) not in other circle.

Euclid's Algorithm

~~84 28 14~~

~~Find GCD(84, 112)~~

~~84 28 14~~

$$a = 112 \quad b = 42$$

$$\text{GCD}(42, 112)$$

$$112 = 42(2) + 28$$

$$42 = 28(1) + \textcircled{14}$$

$$28 = 14(2) + 0$$

$$\therefore \text{GCD}(42, 112) = 14$$

① Well-ordering Principle

Every non-empty subset of \mathbb{N} has a least element.

② Archimedean Principle

Given $a, b \in \mathbb{N}$, there exists $s \in \mathbb{N}$ such that $a < sb$

PT: Just take $s = a + 1$. Then since $b \geq 1$

$$a < a + 1 \leq (a + 1)b$$

③ Division Algorithm

If $a, b \in \mathbb{N}$ with $b \leq a$ then there exists $q \in \mathbb{N}$ and $r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$

Pf: Define the set E to be the set of all natural numbers t such that $a < tb$.
By AP E is non-empty and by W.O.P. E contains a least element, call it t_0 .
Since $b \leq a$, $1 \notin E$ so $t_0 > 1$.

Let $q = t_0 - 1 \in \mathbb{N}$ and let $r = a - qb$.

Then $a = qb + r$, and

$$r = a - qb = a - t_0 b + b < b \text{ since } a - t_0 b < 0.$$

Also if $r < 0$ then $a < qb$. This means that $q \in E$ which means that t_0 is not the least element in E because $q < t_0$.

Since t_0 is the least element in E , $r \geq 0$.

Lemma^(1.5): Let a, b, c be integers. If $c|a$ and $c|b$ then for all $m, n \in \mathbb{Z}$, $c|(an + bm)$

Pf: You do it.

Def: Let $a, b, c \in \mathbb{Z}$. We say c is a common divisor of a and b if $c|a$ and $c|b$.

We say that $d \in \mathbb{Z}$ is the greatest common divisor of a and b , denoted $d = \text{GCD}(a, b)$ if (1) d is a common divisor of a and b and (2) if c is any common divisor of a and b , $c \leq d$.

Thm: (Euclid's Algorithm)

Let $a, b \in \mathbb{N}$ with $b \leq a$ and let $d = \text{GCD}(a, b)$

Then

(1) There ~~are numbers~~ is a number $k \in \mathbb{N}$ and numbers $q_1, \dots, q_{k+1} \in \mathbb{N}$ (the quotients) and numbers $b > r_1 > r_2 > r_3 > \dots > r_k > r_{k+1} = 0 \in \mathbb{N}$ (the remainders) such that

$$a = b q_1 + r_1 \quad \begin{cases} 0 \leq r_1 < b \\ 0 \leq r_2 < \underline{r_1} \end{cases}$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$r_2 = r_3 q_4 + r_4$$

⋮

$$r_j = r_{j+1} q_{j+2} + r_{j+2} \quad j = 1, 2, 3, \dots, k-1$$

$$r_{k-1} = r_k q_{k+1} + \cancel{r_{k+1}}^0$$

and $d = r_k$

(2) $d = \text{GCD}(a, b)$ can be written as
 $d = ax + by$ for some $x, y \in \mathbb{Z}$.

PR (1) Since $b \leq a$ the Division Algorithm says that there exist $q_1 \in \mathbb{N}$ and $0 \leq r_1 < b$ such that $a = bq_1 + r_1$. If $r_1 = 0$ we are done but if not there is a $q_2 \in \mathbb{N}$ and $0 \leq r_2 < r_1$ such that $b = r_1q_2 + r_2$. Again if $r_2 = 0$ we are done but if not there is a $q_3 \in \mathbb{N}$ and $0 \leq r_3 < r_2$ such that $r_1 = r_2q_3 + r_3$. Continuing in this way we have numbers $r_1 > r_2 > r_3 > r_4 > \dots$ all in \mathbb{N} . Therefore we must eventually arrive at $r_{j+2} = 0$ some $j \in \mathbb{N}$. Let $k = j+1$, so that $r_{k+1} = 0$. We must show that $r_k = \text{GCD}(a, b)$. To do this we make two claims.

claim 1: $r_k | a$ and $r_k | b$

To see this note that

$$r_{k-1} = r_k q_{k+1} + r_{k+1} = r_k q_{k+1}$$

so $r_k | r_{k-1}$. But $r_{k-2} = r_{k-1} q_k + r_k$

so by Lemma, $r_k | r_{k-2}$. Once more,

$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$ and since $r_k | r_{k-1}$
and $r_k | r_{k-2}$, Lemma says $r_k | r_{k-3}$.

Continuing we arrive at $r_k | b$ and $r_k | a$.

Claim 2: If $c | a$ and $c | b$ then $c \leq r_k$.

To see this suppose $c | a$ and $c | b$. Since

$r_1 = a - bq_1$, the Lemma says that $c | r_1$.

Since $r_2 = b - r_1q_2$, the Lemma says that

$c | r_2$. Since $r_3 = r_1 - r_2q_3$, the Lemma

says that $c | r_3$. Continuing we arrive at

$c | r_k$. Hence $c \leq r_k$.

Therefore $r_k = \text{GCD}(a, b)$.

(2) To show that there exist $x, y \in \mathbb{Z}$ such
that $d = ax + by$ note that

$r_1 = a - bq_1$ so that there exist $x_1, y_1 \in \mathbb{Z}$
such that $r_1 = ax_1 + by_1$. Since $r_2 = b - r_1q_2$

$= b - (ax_1 + by_1)q_2$, there exist $x_2, y_2 \in \mathbb{Z}$

such that $r_2 = ax_2 + by_2$. Continuing we

arrive at the existence of x_k and $y_k \in \mathbb{Z}$

such that $r_k = ax_k + by_k$. \square

e.g.

$$a = 112 \quad b = 42$$

$$\text{GCD}(42, 112) = 14$$

$$112 = 42(2) + 28$$

$$42 = 28(1) + 14 \leftarrow d = 14$$

$$28 = 14(2) + 0$$

$$28 = 112 - 42(2)$$

$$\begin{aligned} 14 &= 42 - 28 = 42 - (112 - 42(2)) \\ &= 112(-1) + 42(3) \end{aligned}$$