Mon Feb 23

Reminders
- HW 7 due Wed
- What is at the end of Ch 5?
- Today: Finish prob from Fri sheet
- Midterm 2 ≈ 2 weeks
  Fri 6 Mar.
- Ch 4, 5, 6, 7, 8

From Fri

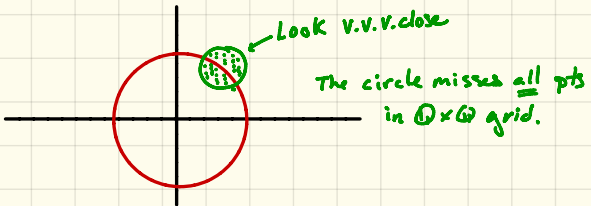
A $\forall x, y \in \mathbb{Q}, \exists a, b, n \in \mathbb{Z}$, $x = \frac{a}{n}$, $y = \frac{b}{n}$, and $\gcd(a,b,n) = 1$.

B $\forall n \in \mathbb{Z}$, ① n^2 is congruent to 0 or 1 mod 3 and
② $n^2 \equiv 0 \bmod 3 \iff n \equiv 0 \bmod 3$.

C $\forall a, b \in \mathbb{Z}$, if $a + b \equiv 0 \bmod 3$, then

$$a \equiv b \equiv 0 \mod 3$$
OR
$$a \equiv 1 \mod 3 \text{ and } b \equiv 2 \mod 3 \text{ (WOLG)}$$

- Goal: Show $x^2 + y^2 - 3 = 0$ has no solutions in $\mathbb{Q} \times \mathbb{Q}$.



Pf (by contradiction)

Suppose $x^2+y^2-3=0$ has a soln in $\mathbb{Q}\times\mathbb{Q}$.

By [A], $\exists\ a,b,n$ s.t. $x=\frac{a}{n}$, $y=\frac{b}{n}$ $\wedge$ $\gcd(a,b,n)=1$.

Plug in: $\frac{a^2}{n^2}+\frac{b^2}{n^2}-3=0$ or $a^2+b^2=3n^2$.

Thus, $a^2+b^2\equiv 0 \bmod 3$.

By [C], $a^2+b^2\equiv 0 \bmod 3$ implies that either

(i) $a^2\equiv b^2\equiv 0 \bmod 3$ or

(ii) $a^2\equiv 1 \bmod 3$ and $b^2\equiv 2 \bmod 3$.

But [B] implies option (ii) is impossible since

$b^2\not\equiv 2 \bmod 3$ for any integer b.

So $a^2\equiv b^2\equiv 0 \bmod 3$. Thus, also from [B] we know

$a=3k$ and $b=3\ell$.

Plug in: $9k^2+9\ell^2=3n^2$. Divide by 3: $3(k^2+\ell^2)=n^2$.

So $n^2\equiv 0 \bmod 3$. Apply [B] again to conclude

$n=3m$, $m\in\mathbb{Z}$. Now $\gcd(a,b,n)\geq 3$,

which contradicts $\gcd(a,b,c)=1$.

Ch7 Other types of propositions

Prop: $P \iff Q$

Pf ① $P \Rightarrow Q$
② $Q \Rightarrow P$

$a = 4 \Rightarrow a^2 = 16$
$\not\Leftarrow$

$a = b \Rightarrow ac = bc$
$\not\Leftarrow$
↳ Need $c \neq 0$.
Need not be in mod. arithmetic

$a = b \Rightarrow f(a) = f(b)$
$\not\Leftarrow$

Existence.

Prop ∃ circles C in the xy-plane such that

$$C \cap \mathbb{Q} \times \mathbb{Q} = \emptyset.$$

Pf: Find one. (Gs first problem)

//

Generally **Prop**: $\exists x, P(x)$

Pf: Pick $x = x_0$. Show $P(x_0) = T$.

Prop 7.1 If $a, b \in \mathbb{Z}$, then there are integers k, ℓ so that $\gcd(a,b) = ka + \ell b$.

[logical structure: $\forall a,b \in \mathbb{Z}, \exists k,\ell \in \mathbb{Z}$, $\gcd(a,b) = ka + \ell b$]

[Bad: $\gcd(12,9)=3$ and $12-9=3$]

Parallel Example

$a=12$, $b=9$

$A = \{1\cdot 12 + 0\cdot 9 = 12,\ 0\cdot 12 + 0\cdot 9 = 0,\ -1\cdot 12 + 0\cdot 9 = -12,\ 9, -9,\ 1\cdot 12 + 1\cdot 9 = 21, \ldots\}$

Pf: Let $a, b \in \mathbb{Z}$.

Define $A = \{ak + b\ell : k, \ell \in \mathbb{Z}\}$

Let d be the smallest positive element in A. Let $d' = \gcd(a,b)$.

Strategy: ① Show $d \mid a \wedge d \mid b$. ② Show $d \geq d'$. $\Rightarrow d = d'$

(a) $d \in A \Rightarrow d = ak + b\ell$ for some $k, \ell \in \mathbb{Z}$.

(b) Apply DA to get $a = qd + r$, $0 \leq r < d$., $q \in \mathbb{Z}$

(b) $\Rightarrow r = a - qd = a - q(ak + b\ell) = a(1 - qk) + b\ell \Rightarrow r \in A$

But $0 \leq r < d$ and d is smallest pos. element in $A \Rightarrow r = 0$.

$\Longrightarrow$ DA actually gives $a = qd \Rightarrow d \mid a$.

(Cut-n-paste "b" for "a" to conclude $d \mid b$.) So d is a common divisor of a and b. (So ① holds)

Recall $d' = \gcd(a,b)$. By def gcd, $\exists m, n \in \mathbb{Z}$ s.t $d' \cdot m = a \wedge d' n = b$.

So $d = ak + b\ell = d'mk + d'nb = d'(mk + nb)$, $mk + nb \in \mathbb{Z}$.

So $d' \mid d$. So $d' \leq d$.

↑ Since $d' > 0 \wedge d > 0$