CSE 16 7-29-20

Ex. (ch. 5 p. 136 #17)

If $n \in \mathbb{Z}$ is odd, then $8 \mid (n^2-1)$.

Equivalently $n^2 \equiv 1 \pmod 8$.

Proof.

Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 4k(k+1)+1 \end{aligned}$$

Exactly one of k or $k+1$ is even.

Case 1 $k = 2l$ is even ($l \in \mathbb{Z}$).

$\therefore \quad n^2 = 4 \cdot 2l(k+1)+1 = 8l(k+1)+1$

$\therefore \quad n^2-1 = 8 \cdot l(k+1)$

$\therefore \quad 8 \mid (n^2-1)$ ✓

Case 2 $(k+1) = 2\ell$ is even $(\ell \in \mathbb{Z})$.

The Proof is similar in this case, exercise. ←

In either case $8 \mid (n^2-1)$. ∎

Ex. (ch 6. P. 144 #17)

For all $n \in \mathbb{Z}$: $4 \nmid (n^2+2)$. Equivalently

$$n^2 \not\equiv -2 \pmod 4$$

since $2 \equiv -2 \pmod 4$ $(2-(-2) = 4$ is div. by $4)$, this is equivalent to

$$n^2 \not\equiv 2 \pmod 4$$

Proof:

Assume $4 \mid (n^2+2)$. Then $n^2+2 = 4k$ for some $k \in \mathbb{Z}$.

$\therefore \quad n^2 = 4k-2$

$\therefore \quad n^2 = 2(2k-1)$

$\therefore \quad 2 \mid n^2$

$\therefore \quad 2 \mid n$ (P-ev. thm. 1

$\therefore \quad 4 \mid n^2$ (exercise: $a \mid b \Rightarrow a^2 \mid b^2$)

$\therefore \quad n^2 = 4l$ (some $l \in \mathbb{Z}$).

$\therefore \quad 4k-2 = 4l$

$\therefore \quad 2k-1 = 2l$

But LHS is odd while RHS is even.
This $\lightning$ shows our assumption was false, hence $4 \nmid (n^2+2)$. ∎

Alternate Proof:

The possible remainders on division by 4 are: 0, 1, 2, 3.

Thus n must satisfy exactly one of the following (for some $K \in \mathbb{Z}$).

$n = 4K \Rightarrow n^2 = 16K^2 = 4 \cdot (4K^2) \Rightarrow n^2 \equiv_4 0$

$n = 4K+1 \Rightarrow n^2 = 16K^2 + 8K + 1 = 4(\ ) + 1 \Rightarrow n^2 \equiv_4 1$

$n = 4K+2 \Rightarrow n^2 = 16K^2 + 16K + 4 = 4(\ ) \Rightarrow n^2 \equiv_4 0$

$n = 4K+3 \Rightarrow n^2 = 16K^2 + 24K + 9$

$= 16K^2 + 24K + 8 + 1 = 4(\ ) + 1 \Rightarrow n^2 \equiv_4 1$

Therefore every $n \in \mathbb{Z}$ satisfies either

$$n^2 \equiv 0 \pmod 4$$

or $$n^2 \equiv 1 \pmod 4$$

$\therefore$ $n^2 \equiv 2 \pmod 4$ is impossible, i.e.

for all $n \in \mathbb{Z}$: $n^2 \not\equiv 2 \pmod 4$. ∎

Chapter 7 : non-conditional statements.

Let $P(x)$ be a propositional function, with Universe U. A proof of

$$\exists x \in U : P(x)$$

is called an existence proof. There are 2 kinds of such proofs.

- constructive.
  find, construct or display a particular $a \in U$ such that $P(a)$ is true.
- non-constructive
  use some other method, often contradiction (not always.)

Ex.

There exist $x, y \in \mathbb{R} - \mathbb{Q}$ (irrational numbers) such that $x^y \in \mathbb{Q}$ (is rational.)

Proof.

Consider the real number $\sqrt{2}^{\sqrt{2}}$.

This number is either rational or it is not.

Case 1: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$

Let $x = y = \sqrt{2}$. Then $x, y \in \mathbb{R} - \mathbb{Q}$ and

$$x^y = \sqrt{2}^{\sqrt{2}} \in \mathbb{Q}.$$

Case 2: $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} - \mathbb{Q}$

Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then $x, y \in \mathbb{R} - \mathbb{Q}$, and

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}.$$

In either case there exist $x, y \in \mathbb{R} - \mathbb{Q}$ such that $x^y \in \mathbb{Q}$. ∎

Remark

This was not a constructive existence proof, since we don't know which case holds.

Instead, we relied on the fact

$$R \vee \neg R$$

is a tautology. (called law of excluded middle.)

Fact: $\sqrt{2}^{\sqrt{2}}$ is actually irrational.

Book: Irrational numbers by Ivan Niven.

Ex.
There exist $x, y \in \mathbb{R} - \mathbb{Q}$ with $x^y \in \mathbb{Q}$.

Lemma: $\log_2(9)$ is irrational.

Defn $\log_b(a)$ is the exponent on b that gives a:

$$b^{\log_b(a)} = a$$

i.e. $2^{\log_2(9)} = 9$.

Proof.
Assume $\log_2(9) \in \mathbb{Q}$, which means

$$\log_2(9) = \frac{a}{b}$$

for some $a, b \in \mathbb{Z}$. Then

$$2^{\log_2(9)} = 2^{a/b}$$

$$\therefore \quad 9 = 2^{a/b}$$

$$\therefore \quad 9^b = \left(2^{a/b}\right)^b = 2^{\frac{a}{b}\cdot b} = 2^a$$

$$\therefore \quad \left(3^2\right)^b = 2^a$$

$$\therefore \quad 3^{2b} = 2^a$$

This contradicts the uniqueness of prime factorization. Also LHS is odd and RHS is even. These contradictions show our assumption was false, hence $\log_2(9)$ is irrational. ∎

Constructive Proof of $x, y \in \mathbb{R} - \mathbb{Q}$ with $x^y \in \mathbb{Q}$.

Proof.

Let $x = \sqrt{2}$ and $y = \log_2(9)$. We've shown both $x, y \in \mathbb{R} - \mathbb{Q}$. However,

$$\begin{aligned} x^y &= \sqrt{2}^{\log_2(9)} \\ &= \sqrt{2}^{\log_2(3^2)} \\ &= \sqrt{2}^{2 \cdot \log_2(3)} \\ &= \left(\sqrt{2}^2\right)^{\log_2(3)} \\ &= 2^{\log_2(3)} \\ &= 3 \quad \in \mathbb{Q} \end{aligned}$$

■

Exercise:

- try $x = \sqrt{5}$, $y = \log_5(25)$
- try $x = \sqrt[3]{2}$, $y = \log_2(27)$

Theorem

Let $a, b \in \mathbb{N}$. Then there exist $n, m \in \mathbb{Z}$ for which

$$\gcd(a,b) = an + bm$$

Proof.

Let

$$S = \{ ax + by \mid x, y \in \mathbb{Z} \}.$$

some integers in S are positive, some negative, one is zero.

However $S \cap \mathbb{N}$ contains only positive integers, and is non-empty.

Let d least positive integer in S (which exists by the W.O.P. of $\mathbb{N}$)

By the definition of S, there exist $n, m \in \mathbb{Z}$ such that

$$d = an + bm$$

we must show that $d = \gcd(a,b)$.

Then

$$\gcd(a,b) = d = an + bm$$

as required. we must show that both

(i) $d \mid a$ and $d \mid b$

and

(ii) if $e \mid a$ and $e \mid b$, then $e \leq d$.

Proof of (ii)

to show $d \mid a$, use division algorithm:

$$a = qd + r \quad \text{and} \quad 0 \leq r < d$$

$\therefore \quad r = a - qd$

$= a - q(an + bm)$

$= a(1 - qn) + b(-qm)$

$\therefore$ r has form $ax + by$, > 0

$r \in S$.

But $0 \leq r < d$. if $0 < r < d$,

this would contradict defn of d

as least positive int. in S.

$\therefore \quad r = 0$

$\therefore \quad a = qd$

$\therefore \quad d \mid a$.

Exercise: show $d \mid b$.

Proof of (ii) next time. (or exercise).