§3.4 Proof by cases

- If $n \in \mathbf{Z}$, then $n(n+1)/2$ is an integer.
- If $a, b \in \mathbf{Z}$ such that $a+b$ and ab are even, then a and b are even.

Assume $n \in \mathbb{Z}$

Case 1° If n is even. then $n = 2k$ $\therefore$ $n(n+1) = 2k(2k+1)$ is even

Case 2° If n is odd, then $n = 2k+1$ $\therefore$ $n(n+1) = (2k+1)(2k+2)$
$= 2(2k+1)(k+1)$ is even.

$\therefore$ $n(n+1)$ is even.

$\therefore$ $\frac{n(n+1)}{2} \in \mathbb{Z}$

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

Consider 4 cases

1° If $a = 2k$, $b = 2k$ then $a+b = 2(k+l)$, $ab = 4kl$ are even.

2° If $a = 2k$, $b = 2l+1$ then $a+b = 2(k+l)+1$ is odd
$ab = 2k(2l+1)$ is even

3° If $a = 2k+1$ $b = 2l$ then $a+b = 2(k+l)+1$ is odd
$ab = 2l(2k+1)$ is even

4° If $a = 2k+1$, $b = 2l+1$ then $a+b = 2(k+l+1)$ is even
$ab = (2k+1)(2l+1)$
$= 4kl + 2l + 2k + 1$
$= 2(2kl + l + k) + 1$ is odd

$\therefore$ If $a+b$, ab are even, case 1 is the only acceptable case
$\therefore$ a & b are even.

§4 & 5. More examples of proofs

Examples Prove or disprove the following.

(a) Let $x, y \in \mathbf{Z}$. If $3 \nmid xy$, then $3 \nmid x$ and $3 \nmid y$.

(b) If $n \in \mathbf{N}$ and $n \geq 7$, then $n = 2a + 3b$ for $a, b \in \mathbb{N}$.

Congruence of integers

Definition Let $n \in \mathbf{N}$. For $a, b \in \mathbf{Z}$, we say that a is congruent to b modulo n, denoted by $a \equiv b \pmod{n}$, if $a - b$ is divisible by n, i.e., a and b have the same remainder when they are divided by n.

$a - b \equiv 0 \pmod{n}$

Prove the following for $n \in \mathbf{N}, a, b \in \mathbf{Z}$.

(a) If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$ for any $k \in \mathbf{Z}$.

(b) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

(a) We prove the contrapositive: If $\sim(3 \nmid x \text{ and } 3 \nmid y)$, then $3 \mid xy$, i.e.

If $(3 \mid x \text{ or } 3 \mid y)$, then $3 \mid (xy)$.

Case 1 If $3 \mid x$, then $x = 3k$, $k \in \mathbb{Z}$. $\therefore xy = 3ky$ $\therefore xy = 3\boxed{ky}$

Case 2 If $3 \mid y$, then $y = 3l$, $l \in \mathbb{Z}$. $\therefore xy = 3lx = 3\tilde{m}$ with $\tilde{m} \in \mathbb{Z}$ $ky \in \mathbb{Z}$.

$\therefore 3 \mid xy$ in both Cases.

(b)

$n \neq 7$	(a, b)
7	$(a,b) = (2,1)$: $2 \cdot 2 + 3 \cdot 1 = 7$
8	$(a,b) = (1,2)$: $1 \cdot 2 + 3 \cdot 2 = 8$
9	$(3,1)$: $3 \cdot 2 + 3 \cdot 1 = 9$.
10	$(2,2)$: $3 \cdot 2 + 2 \cdot 2 = 10$
11	$(\star, 1)$: $4 \cdot 2 + 1 \cdot 3 = 11$

Consider 2 cases

Case 1° n is odd. $n \geq 7$

$n - 3 = 2k$ is even with $k > 0$

$\therefore n = 2 \cdot k + 3 \cdot 1$

a b

Case 2° n is even $n \geq 8$

Then $n - 3 \cdot 2 = 2k > 0$ with k positive

$\therefore n = 2 \cdot k + 3 \cdot 2$

a b

In both cases $n = 2 \cdot a + 3 \cdot b$ for suitable $a, b \in \mathbb{N}$.

(a) Prove If $a \equiv b \pmod n$ then $ka \equiv kb \pmod n$ for any $k \in \mathbb{Z}$:

Proof: Assume $a \equiv b \pmod n$, i.e., $a - b = nl$, $l \in \mathbb{Z}$

Let $k \in \mathbb{Z}$. Then $ka - kb = k(a-b) = knl$
$= n(kl)$

$\therefore$ $ka - kb = lm$ with $m = \boxed{kl} \in \mathbb{Z}$

$\therefore$ $ka \equiv kb \pmod n$

(b) Assume $a \equiv b \pmod n$ & $c \equiv d \pmod n$.

$a - b = nk$ & $c - d = nl$, $k, l \in \mathbb{Z}$.

$\therefore$ $(a+c) - (b+d) = (a-b) + (c-d) = nk + nl = n(k+l) = np$ with $p = k+l$

$ac - bd = (b+nk)(nl+d) - bd$

$= n^2kl + nkd + nlb + bd - bd = n(nkl + kd + lb)$
$= nq$ with $q = nkl + kd + lb$

$\therefore$ $a + c \equiv b + d \pmod n$, i.e., $(a+c) - (b+d) = np$

& $ac \equiv bd \pmod n$, i.e., $ac - bd = nq$

Alternatively, $ac - bd = ac - ad + ad - bd$

$= a(c-d) + d(a-b) = a \cdot nl + d \cdot nk$

$= n(al + dk) = n\hat{q}$ with

$\hat{q} = al + dk$

§5.4 & 5.5 Proofs of statements involving quantifiers

(1) To prove a statement "P" is true (false) , prove that "$\sim P$" is false (true).

(2.a) To prove "$\exists x, P(x)$" is true, provide and example of $x \in S$, or show that there must be an $x \in S$, such that $P(x)$ holds.

(2.b) To prove that "$\exists x, P(x)$" is false, show that for every $x \in S$, $P(x)$ does not hold."

(3.a) To prove that "$\forall x, P(x)$" is true, show that for every $x \in S$ $P(x)$ holds.

(3.b) To prove that "$\forall x, P(x)$" is false, show that there is $x \in S$ such that $\sim P(x)$ hold.

Such an $x \in S$ is call a counter example for the statement "$\forall x, P(x)$".

Examples Prove or disprove the statements:

(a) There are no positive integers m and n such that $m^2 + m + 1 = n^2$.

(b) There are positive irrational numbers a and b such that a^b is rational.

(c) There exist odd integers a and b such that $4|(3a^2 + 7b^2)$.

(d) There is a real number x such that $x^6 + x^4 + 1 = 2x^2$.

$$\sim\left(\exists\, m,n \in \mathbb{N},\ m^2+m+1 = n^2\right) \equiv \forall\, m,n \in \mathbb{N},\ m^2+m+1 \neq n^2$$

Prove that $\exists$ positive irrational numbers a, b s.t. $a^b \in \mathbb{Q}$.

Consider $\sqrt{2}^{\sqrt{2}}$.

Case 1° If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$. Then we have $a = b = \sqrt{2}$ satisfy $a^b \in \mathbb{Q}$

Case 2° If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, then we can take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$

So that $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

The negation of the above is:

$$\sim\left[\left(\exists\, a,b \in \mathbb{R}-\mathbb{Q}\right)\left(a^b \in \mathbb{Q}\right)\right] \equiv \left(\forall\, a,b \in \mathbb{R}-\mathbb{Q}\right)\left(a^b \notin \mathbb{Q}\right).$$

(a) Clearly, Assume the contrary and that there $m, n \in \mathbb{N}$ s.t. $m^2+m+1 = n^2$.

Clearly, $n > m$.

~~Case 1° If $n = m+1$, then $n^2 = m^2+2m+1 > m^2+m+1$.~~

Case 2° If $n \geq m+1$, then $n^2 \geq (m+1)^2 > m^2+m+1$