HW 7 Evens

Chapter 6

(4) Suppose $\sqrt{6} = \frac{p}{q} \in \mathbb{Q}$, $q > 0$, and suppose p/q is fully reduced. Then,

$$\sqrt{6} = p/q \Longrightarrow 6q^2 = p^2$$

$\Longrightarrow$ p^2 is a multiple of 6 (& so even)

$\Longrightarrow$ p is even

pf: if $p = 2k+1$ is odd, then $p^2 = 2(2k^2+2k)+1$ is odd.

$\Longrightarrow$ $p = 2k$, $k \in \mathbb{Z}$

$\Longrightarrow$ $6q^2 = p^2 = (2k)^2 = 4k^2$

$\Longrightarrow$ $3q^2 = 2k^2$

$\Longrightarrow$ q^2 is even pf: $2 | 3q^2$

$\Longrightarrow 2|3$ or $2|q^2 \Longrightarrow 2|q^2$

$\Rightarrow q$ is even (as above)

$\Rightarrow q = 2l \quad (l \in \mathbb{Z})$

So $p = 2k,\ q = 2l$

contradicting our assumption that

$\frac{p}{q}$

be fully reduced.

Thus, $\sqrt{6} \notin \mathbb{Q}$.

(6) If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 2 \neq 0$.

pf: If $a^2 - 4b - 2 = 0$, then

$$a^2 = 2(2b+1)$$

$\Rightarrow a^2$ is even

$\Rightarrow a$ is even (as in # 4)

$\Rightarrow a = 2k,\ k \in \mathbb{Z}$

$\Rightarrow \cancel{2}(2b+1) = a^2 = \cancel{4}\,2k^2$

$$\Rightarrow 2b+1 = 2k^2$$

which is impossible, because then

$2b+1$ is both odd and even

a contradiction. Thus, $a^2-4b-2 \neq 0$

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

(8) Let $a, b, c \in \mathbb{Z}$ satisfy $a^2+b^2=c^2$, & let us show that either a or b must be even. Suppose, for the sake of contradiction, that neither a nor b is even, i.e. that

$$a = 2k+1$$
$$b = 2l+1$$

for some $k, l \in \mathbb{Z}$, are odd. Then

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

If $a^2+b^2=c^2$, this means c^2, and therefore c, must be even, so

$$c=2r \text{ for some } r\in\mathbb{Z}$$

$$\Rightarrow \cancel{2}\left(2(k^2+k+l^2+l)+1\right)$$

$$= a^2+b^2 = c^2 = \cancel{4}^{2} r^2$$

$$\Rightarrow \underbrace{2(k^2+k+l^2+l)+1}_{\text{odd}} = \underbrace{2r^2}_{\text{even}}$$

contradiction!

Therefore at least one of a or b is even.

(14) A, B - sets $\Rightarrow A\cap(B-A)=\emptyset$

pf: If not, if $\exists\, x\in A\cap(B-A)$, then $\underbrace{x\in A}$ and $\underbrace{x}\in B-A=\{b\in B \mid \underbrace{b\notin A}\}$

$x\notin A$

contradiction!

QED

pf 1: Direct proof using MVT

(16) $a, b \in \mathbb{R}^+ =$ pos. reals $\Longrightarrow a, b > 0$

$$\Longrightarrow 0 \le (a-b)^2 = a^2 - 2ab + b^2$$

+4ab +4ab

$$\Longrightarrow 4ab \le a^2 + 2ab + b^2 = (a+b)^2$$

$$\Longrightarrow \sqrt{4ab} \le \sqrt{(a+b)^2} = a+b$$

$$\Longrightarrow 2\sqrt{ab} \le a+b$$

pf1: by MVT, $\Longrightarrow$

$f(x) = \sqrt{x}$

$\Rightarrow f'(x) = \frac{1}{2\sqrt{x}} > 0$

on $(0, \infty)$

$\Rightarrow \sqrt{x}$ is incr.

pf2: $x_1 < x_2 \Longrightarrow$

$\sqrt{x_1} < \sqrt{x_2}$,

else if $\sqrt{x_1} \ge \sqrt{x_2}$

then $x_1 \ge x_2$

bec.

$a < b \Longrightarrow$

$a^2 = a \cdot a$
$< a \cdot b$
$< b \cdot b = b^2$

pf 2: Contradiction

On the one hand, $(a-b)^2 \ge 0$, but on the other, if we suppose

$\cancel{2\sqrt{ab}}$

$$2\sqrt{ab} > a+b$$

then

$$4ab > (a+b)^2 = a^2 + 2ab + b^2$$

$$\Longrightarrow 0 > a^2 - 2ab + b^2 = (a-b)^2$$

Contradiction.

(16) $a, b \in \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\} \implies$

$$a, b > 0 \implies 0 \le (a-b)^2$$
$$= a^2 + b^2 - 2ab$$
$$+4ab \qquad +4ab$$
$$\implies$$
$$4ab \le a^2 + b^2 + 2ab$$
$$= (a+b)^2$$

$$\implies \sqrt{4ab} \le \sqrt{(a+b)^2}$$

Cdirectly $x_1 < x_2$

$\implies$

$\sqrt{x_1} = \dfrac{x_1}{\sqrt{x_1}} < \dfrac{x_2}{\sqrt{x_1}}$ | & $\sqrt{x_2} = \dfrac{x_2}{\sqrt{x_2}} > \dfrac{x_1}{\sqrt{x_2}}$

and $x_1 < x_2 \implies$

$$\frac{1}{x_2} < \frac{1}{x_1}$$

$\implies \dfrac{1}{\sqrt{x_2}} = \dfrac{\sqrt{x_2}}{x_2} < \dfrac{\sqrt{x_2}}{x_1}$

& $\dfrac{1}{\sqrt{x_1}} = \dfrac{\sqrt{x_1}}{x_1} > \dfrac{\sqrt{x_1}}{x_2}$

$$x_1 < x_2 \implies \sqrt{x_1} < \sqrt{x_2}$$

$$a+b < 2\sqrt{ab}$$

$$\implies a^2 + 2ab + b^2 < 4$$

(18) Let $a, b \in \mathbb{Z}$. If $4 \mid (a^2+b^2)$, then a and b are not both odd.

contrapositive

pf: Suppose $a = 2k+1$, $b = 2l+1$, $k, l \in \mathbb{Z}$, are both odd, & observe

$$a^2+b^2 = (2k+1)^2 + (2l+1)^2$$
$$= 4k^2+4k+4l^2+4l+2$$

which is not divisible by 4, unless we suppose 2 is divisible by 4, which it is not.

To make this into a proof by contradiction, adjust as follows: suppose $4 \mid (a^2+b^2)$ & $a = 2k+1$, $b = 2l+1$. The above calculation shows $4 \nmid (a^2+b^2)$, contradiction.

(20) $\underbrace{x^2+y^2-3}_{f(x,y)} = 0$ has no $\underbrace{\text{rational points}}_{(x,y)\in\mathbb{Q}^2 \text{ s.t. } f(x,y)=0}$.

pf: Suppose $A, B, C, D \in \mathbb{N}$ are all positive.

If

$$\frac{A}{B} + \frac{C}{D} = 3$$

then

$$\frac{AD+BC}{BD} = 3$$

which we may assume WOLOG fully reduced. Then,

$$BD = 1 \implies B = D = 1$$

$$\implies 3 = \frac{AD+BC}{BD} = A + C$$

Now, if we suppose $x = \frac{a}{b}$, $y = \frac{c}{d}$, let $A = a^2$, $B = c^2$, & observe that

$a^2+c^2=3$ & $a, c \in \mathbb{Z}$ is impossible,

$$\left\{ \begin{aligned} 3 = x^2+y^2 = \frac{a^2}{b^2} + \frac{c^2}{d^2} &= \frac{A}{B} + \frac{C}{D} \\ &= \frac{AD+BC}{BD} \\ &= A + C = a^2 + c^2 \end{aligned} \right.$$

But $a^2+c^2=3$ has no integer solutions:

a	c	$a^2+c^2=$
0	0	$0<3$
0	± 1	$1<3$
± 1	0	$1<3$
± 1	± 1	$2<3$
± 1	± 2	$5>3$
± 2	± 1	$5>3$
± 2	± 2	$8>3$
$\vdots$	$\vdots$	$\vdots$

only ones <3

all >3
(prove by induction on $|a|+|c| \geq 3$)

which contradicts our assumption that $a,c\in\mathbb{Z}$.

(i.e. $x,y\in\mathbb{Q}$ & $x^2+y^2=3 \Rightarrow a,c\in\mathbb{Z}$ & $a^2+c^2=3 \Rightarrow a,c\notin\mathbb{Z}$)

$\log_2 3 = \frac{a}{b}, \quad a, b \in \mathbb{Z}; \; b > 0$

$\Longrightarrow \quad 2^{a/b} = 3$

$\Longrightarrow \quad 2^a = 3^b$

$\Longrightarrow$ <u>case 1, $a = 0$</u> $\quad a = 0 \Longrightarrow 1 = 2^0 = 3^b$

$\Longrightarrow b = 0$

contradicting $b > 0$

<u>case 2 $a \neq 0$</u> $\quad$ first, $a > 0$

too bec. $\log_2 x < 0 \Longleftrightarrow 0 < x < 1$,

(but $x = 3 > 1$).

Next, 2^a is divisible by 2,

bec. $a > 0$, so 3^b is even

$\Longrightarrow 2 \mid 3^b = \underbrace{3 \cdots 3}_{b}$

$\Longrightarrow 2 \mid 3$, contradicting $2 \nmid 3$.

Chapter 7

(8) Let $a, b \in \mathbb{Z}$. Then,

$$a \equiv b \bmod 10 \iff \begin{array}{c} a \equiv b \bmod 2 \\ \& \\ a \equiv b \bmod 5 \end{array}$$

pf: $a \equiv b \bmod 10 \overset{def}{\iff} a - b = 10k,\ k \in \mathbb{Z}$

$$= 2(5k),\ 5k \in \mathbb{Z}$$
$$= 5(2k),\ 2k \in \mathbb{Z}$$

$$\implies \begin{array}{c} a \equiv b \bmod 2 \\ \& \\ a \equiv b \bmod 5 \end{array}$$

Conversely, $a \equiv b \bmod 5 \implies a - b = 5k$
&
$a \equiv b \bmod 2 \implies a - b = 2l$

$\implies 5k = 2l$

$\implies 2 | k \ \& \ 5 | l$

$\implies k = 2r,\ l = 5s, \quad r, s \in \mathbb{Z}$

$\implies a - b = 5k = 5 \cdot 2r = 10r \implies a \equiv b \bmod$

$= 2l = 2 \cdot 5s = 10s$

(10) $a \in \mathbb{Z} \implies a^3 \equiv a \bmod 3$

pf: $a^3 - a = a(a^2-1) = a(a-1)(a+1)$

Now, $a-1 < a < a+1$ are 3 consecutive integers, and since

$$\mathbb{Z}_3 = \{[0],[1],[2]\}$$

where

$$[0] = \{n \in \mathbb{Z} \mid n \equiv 0 \bmod 3\}$$
$$= \{n \in \mathbb{Z} \mid n = 3k\}$$
$$= \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$[1] = \{n \in \mathbb{Z} \mid n \equiv 1 \bmod 3\}$$
$$= \{n \in \mathbb{Z} \mid n - 1 = 3k\}$$
$$= \{n \in \mathbb{Z} \mid n = 3k+1\} = \{\ldots, -2, 1, 4, \ldots\}$$

$$[2] = \{n \in \mathbb{Z} \mid n \equiv 2 \bmod 3\}$$
$$= \{n \in \mathbb{Z} \mid n = 3k+2\}$$
$$= \{\ldots, -1, 2, 5, 8, \ldots\}$$

so

$$\mathbb{Z} = [0] \cup [1] \cup [2]$$
$$= \{\ldots, -3, 0, 3, \ldots\} \cup \{\ldots, -2, 1, 4, \ldots\} \cup \{\ldots, -1, 2, 5, \ldots\}$$

We conclude that $a-1$, a, and $a+1$ must fall into a different equivalence class each, so one of them is in $[0]$, i.e. $\equiv 0 \bmod 3$, i.e. divisible by 3, the others in $[1]$ & $[2]$, respectively.

<u>ex.</u> 14, 15, 16 — 15 $\equiv 0 \bmod 3$

<u>ex.</u> 47, 48, 49 — 48 $\equiv 0 \bmod 3$

<u>ex.</u> 19, 20, 21 $\equiv 0 \bmod 3$

<u>pf 2</u>: $a^3 - a = a(a^2-1)$. If $3 \mid a$, then $3 \mid a(a^2-1) = a^3 - a$ & $a^3 \equiv a \bmod 3$.

If $3 \nmid a$, then $3 \mid a^2-1$, since if $3 \nmid a$, $\{[a], [2a]\} = \{[1], [2]\}$, for $a \not\equiv 2a \bmod 3$ bec. $a \not\equiv 0 \bmod 3$ ($a - 2a = -a \neq 3k \iff a \neq 3k$). and we already know $a \not\equiv 0 \bmod 3$, so

$a \in [1]$ or $a \in [2]$, & in that case $2a$ is in the other one (Certainly $2a \not\equiv 0 \mod 3$ bec. $3 \nmid 2$ & $3 \nmid a$).

(12) $\exists x \in \mathbb{R}$, $x > 0$, s.t. $x^2 < \sqrt{x}$

pf: $x = \frac{1}{2} \Rightarrow x^2 = \frac{1}{4}$ & we claim

$$\frac{1}{4} < \sqrt{\frac{1}{2}} = \frac{1}{\sqrt{2}}$$

since $\frac{1}{16} < \frac{1}{2}$ & the square root function is increasing (see #16, p. 6)

$$\Rightarrow x^2 = \frac{1}{4} < \frac{1}{\sqrt{2}} = \sqrt{x}.$$

(14) Let $a \in \mathbb{Z}$. Then $a^2 | a \iff a \in \{0, \pm 1\}$.

pf: If $a^2 | a$, then $a = a^2 k$, so either $a = 0$, or if $a \neq 0$,

$$a = a^2 k \Rightarrow 1 = ak$$
$$\Rightarrow a = k = \pm 1$$

bec. $a \in \mathbb{Z}$
$k \in \mathbb{Z}$

Conversely, if $a = 0$, then certainly $\underbrace{0 = 0^2 \cdot k}$ for any $k \in \mathbb{Z}$, while if $a = \pm 1$, then

$\Downarrow$
$a = a^2 k$
$\Downarrow$
$a^2 | a$

$$a = \pm 1 = (\pm 1)^2 \cdot (\pm 1)$$
$$= a^2 k$$

$$\Rightarrow a^2 | a$$

(16) If ab is odd, then both a & b are odd (else, if say $a=2k$, then $ab=2kb$ is even), so $a=2k+1$, $b=2l+1$ for some $k,l\in\mathbb{Z}$, &

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

is even.

(20) $\exists n\in\mathbb{N}$ for which $11 \mid 2^n-1$.

pf: From $2^{11}\equiv 2 \bmod 11$ & the fact that $11\nmid 2$, we know $2^{11-1}\equiv 1 \bmod 11$, i.e.

$$2^{10}\equiv 1 \bmod 11$$

see #5 on exam 2

or $11 \mid 2^{10}-1$, so $\boxed{n=10}$.

(in fact $2^{10}-1 = 1024-1 = 1023 = 11\cdot 93$)

(26) The product of n consecutive integers is divisible by $n!$

ex. $\frac{14\cdot 15\cdot 16}{3!} = \frac{\overset{7}{\cancel{14}}\cdot \overset{5}{\cancel{15}}\cdot 16}{\cancel{3}\cdot\cancel{2}\cdot 1} = 35\cdot 16 = 560$

ex. $\frac{13\cdot 14\cdot 15\cdot 16}{4!} = \frac{13\cdot \overset{7}{\cancel{14}}\cdot \overset{5}{\cancel{15}}\cdot \overset{4}{\cancel{16}}}{\cancel{4}\cdot\cancel{3}\cdot\cancel{2}\cdot 1} = 9100$

pf: Clearly $a = 1\cdot a$ for any $a \in \mathbb{Z}$

$a\cdot(a+1) = 2k$, $k \in \mathbb{Z}$, bec. either a or $a+1$ is even

$a(a+1)(a+2) = 3k$, $k \in \mathbb{Z}$

bec. any 3 consecutive integers must have one divisible by 3

The reason is $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$

$[0] = \{r \in \mathbb{Z} \mid \underbrace{r - 0 = nk}_{\text{i.e. } n \mid r}\}$

Since $\equiv \bmod n$ is an equivalence relation on $\mathbb{Z}$ which is cyclical, i.e. $r \in [0] \Rightarrow n + r \in [0]$
$\Rightarrow 2n + r \in [0]$ etc.

if we take n consecutive integers

$$a, a+1, \ldots, a+n-1 \in \mathbb{Z}$$

and write them à la division algorithm,

$$\left.\begin{aligned} a &= nq_1 + r_1 \\ a+1 &= nq_2 + r_2 \\ &\vdots \\ a+n-1 &= nq_n + r_n \end{aligned}\right\} \text{ where } 0 \leq r_k < n$$

then exactly one of the r_k equals 0, exactly one equals 1, ..., exactly one $r_k = n-1$, since

$$a = nq_1 + r_1 \implies a+k = (nq_1 + r_1) + k$$
$$= nq_1 + (r_1 + k).$$

and

$$\underbrace{r_1 + k = nq' + r'}, \quad 0 \leq r' < n$$

$$\implies a+k = nq_1 + (r_1 + k)$$
$$= nq_1 + nq' + r'$$
$$= n(q_1 + q') + r'$$

$$\implies \boxed{\begin{array}{l} a+k \equiv r' \bmod n \\ \text{for unique } r' \in \{0, \ldots, n-1\} \end{array}}$$

For example, say $a=2$, $n=5$, then $a+1=3$, &

$2+1 = 3 = 0\cdot 5+3$, $k=1, r=3$

$2+2 = 4 = 0\cdot 5+4$, $k=2, r=4$

$2+3 = 5 = 1\cdot 5+0$ $k=3, r=0$

$2+4 = 6 = 1\cdot 5+1$ $k=4, r=1$

$7 = 1\cdot 5+2$ $k=5, r=2$

$2+5 =$

$\Rightarrow$ since $a=2 \equiv 2 \bmod 5$,

$a+1 = 2+1 \equiv 3 \bmod 5$

$\vdots$

$a+5 \equiv 2 \bmod 5$

if $\boxed{a \equiv r \bmod n}$, then $\boxed{a+k \equiv (r+k) \bmod n}$ for $k=1,\dots,n$, & the only thing to consider is when $r+k \equiv r' \bmod n$

There is thus a bijective map $\boxed{f: \{1,\dots,n\} \to \{1,\dots,n\} \quad f(k)=r}$

and we conclude that f descends to the quotient,

$$f : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$f([k]) = [r]$$

and is bijective. We conclude that

$$\prod_{k=1}^{n} (a+k) \equiv \prod_{r=1}^{n} r \mod n$$
$$= n! \mod n$$
$$= 0 \mod n$$

$$\Rightarrow \prod_{k=1}^{n} (a+k) \text{ is divisible by } n!$$