M2200 Hw #8 Key (for Graded Problems)

3.7 # 2, 6, 15, 18, 36
4.1 # 4, 11, 16, 18, 35

3.7 #2) (a) 9, 11

① $11 = 1(9) + 2$
② $9 = 4(2) + 1$
$2 = 2(1) \Rightarrow \gcd(9, 11) = 1$

② $1 = 9 - 4(2)$
① $2 = 11 - 1(9)$
$\Rightarrow 1 = 9 - 4(11 - 1(9))$
$\boxed{1 = 5(9) - 4(11)}$

(b) 33, 44

$44 = 1(33) + 11$
$33 = 3(11) \Rightarrow \gcd(33, 44) = 11$

$\boxed{11 = 1(44) - 1(33)}$

(c) 35, 78

① $78 = 2(35) + 8$
② $35 = 4(8) + 3$
③ $8 = 2(3) + 2$
④ $3 = 1(2) + 1$
$2 = 2(1) \Rightarrow \gcd = 1$

④ $1 = 3 - 1(2)$
③ $2 = 8 - 2(3)$
$\Rightarrow 1 = 3 - 1(8 - 2(3))$
$1 = 3(3) - 1(8)$

② $3 = 35 - 4(8) \Rightarrow 1 = 3(35 - 4(8)) - 1(8)$
$1 = 3(35) - 13(8)$

① $8 = 78 - 2(35) \Rightarrow 1 = 3(35) - 13(78 - 2(35))$
$\boxed{1 = 29(35) - 13(78)}$

(d) 21, 55

① $55 = 2(21) + 13$
② $21 = 1(13) + 8$
③ $13 = 1(8) + 5$
④ $8 = 1(5) + 3$
⑤ $5 = 1(3) + 2$
⑥ $3 = 1(2) + 1$
$2 = 2(1) \Rightarrow \gcd = 1$

⑥ $1 = 3 - 1(2)$
⑤ $2 = 5 - 1(3)$
$\Rightarrow 1 = 3 - 1(5 - 1(3))$
$1 = 2(3) - 1(5)$

④ $3 = 8 - 1(5) \Rightarrow 1 = 2(8 - 1(5)) - 1(5)$
$1 = 2(8) - 3(5)$

③ $5 = 13 - 1(8) \Rightarrow 1 = 2(8) - 3(13 - 1(8))$
$1 = 5(8) - 3(13)$

② $8 = 21 - 1(13) \Rightarrow 1 = 5(21 - 1(13)) - 3(13)$
$1 = 5(21) - 8(13)$

① $13 = 55 - 2(21) \Rightarrow 1 = 5(21) - 8(55 - 2(21))$
$\boxed{1 = 21(21) - 8(55)}$

3.7 #2)

Continue in same manner

(e) $1 = -2(19) + 203$

(f) $1 = 43(323) - 112(124$

(g) $1 = 701(2339) - 819(2002)$

(h) $1 = 1256(3457) - 927(4669)$

(i) $1 = 1793(10001) - 1336(13422)$

#6) Find inverse of 2 modulo 17.

$17 = 8(2) + 1 \Rightarrow 1 = 17 - 8(2)$

$\gcd(2, 17) = 1$

$\Rightarrow$ inverse of $2 \equiv -8 \pmod{17}$
$\equiv 9 \pmod{17}$

#15) Show if p prime, the only solns of $x^2 \equiv 1 \pmod p$ are integers $x \ni x \equiv 1 \pmod p$ and $x \equiv -1 \pmod p$.

Pf If $x^2 \equiv 1 \pmod p$, then p divides $x^2 - 1$.

$\Leftrightarrow p \mid (x-1)(x+1) \Rightarrow p \mid (x-1)$ or $p \mid (x+1)$

(since p is prime)

$\Leftrightarrow \exists\ a \in \mathbb{Z} \ni ap = x - 1$ or $ap = x + 1$

+ we know $\gcd(p, x) = 1$ (since p is prime + it doesn't divide x)

$\Rightarrow 1 = x - ap$ or $1 = -x + ap$

$\Rightarrow x \equiv 1 \pmod p$ or $x \equiv -1 \pmod p$. //

3.7 #18 Find all solns to

$x \equiv 2 \pmod 3$ $\quad a_1 = 2 \quad m_1 = 3 \quad M_1 = 20$

$x \equiv 1 \pmod 4$ $\quad a_2 = 1 \quad m_2 = 4 \quad M_2 = 15$

$x \equiv 3 \pmod 5$ $\quad a_3 = 3 \quad m_3 = 5 \quad M_3 = 12$

$m = 60$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

y_1 = inverse of $M_1 \pmod{m_1}$ = inverse of $20 \pmod 3$

$20 \bmod 3 = 2 \bmod 3$ and $2(2) \equiv 4 \pmod 3$
$\equiv 1 \pmod 3$

$\Rightarrow \quad y_1 = 2$

y_2 = inverse of $15 \bmod 4$ = inverse of $3 \bmod 4$

$3(3) \equiv 9 \pmod 4 \equiv 1 \pmod 4 \quad \Rightarrow \quad y_2 = 3$

y_3 = inverse of $12 \bmod 5$ = inverse of $2 \bmod 5$

and $3(2) \equiv 6 \pmod 5 \equiv 1 \pmod 5$

$\Rightarrow \quad 3 = y_3$

$\Rightarrow \quad x = 2(20)2 + 1(15)(3) + 3(12)(3)$

$= 80 + 45 + 108 = 233 \bmod 60 \equiv \boxed{53 \bmod 60}$

3.7 #36 Find $a \in W$, $a < 28$ represented by each pair given as $(a \bmod 4, a \bmod 7)$

(a) 0

(b) 21

(c) 1

(d) 22

(e) 2

(f) 24

(g) 14

(h) 19

(i) 27

4.1 #4 $P(n) = 1^3+2^3+\dots+n^3 = \left(\frac{n(n+1)}{2}\right)^2 \quad \forall\ n \in \mathbb{Z}^+$

(a) $P(1): 1^3 = \left(\frac{1(1+1)}{2}\right)^2$

(b) $1^3 = 1$ and $\left(\frac{1(1+1)}{2}\right)^2 = \left(\frac{2}{2}\right)^2 = 1$ ✓

(c) Inductive hypothesis:

Assume $1^3+2^3+\dots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

(d) need to prove that $P(n) \to P(n+1)$.

(e) $1^3+2^3+\dots+n^3 = \left(\frac{n(n+1)}{2}\right)^2$

$$\Leftrightarrow 1^3+2^3+\dots+n^3+(n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$$

$$= (n+1)^2\left[\frac{n^2}{2^2} + n+1\right]$$

$$= (n+1)^2\left[\frac{n^2+4n+4}{4}\right]$$

$$= \frac{(n+1)^2(n+2)^2}{4} = \left[\frac{(n+1)(n+2)}{2}\right]^2 \ //$$

(f) If it's true for $n=1$ and we know $P(n) \to P(n+1)$, then it's true for all $n = 1, 2, 3, \dots$.

4.1 # 11 (a) Find formula for $\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\dots+\frac{1}{2^n}$.

n	sum
1	$1/2$
2	$1/2+1/4 = 3/4$
3	$7/8$
4	$15/16$
5	$31/32$
⋮	⋮
n	$\frac{2^n-1}{2^n}$

$$\Rightarrow \frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\dots+\frac{1}{2^n} = \frac{2^n-1}{2^n}$$

4.1 #11 (cont)

(b) Prove it.

claim $\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}=\frac{2^n-1}{2^n}$

Pf ① If $n=1$, $\frac{1}{2}=\frac{2^1-1}{2}=\frac{1}{2}$ ✓ true

② Assume it's true for n, i.e. $\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}=\frac{2^n-1}{2^n}$

check $n+1$ case. $\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}=\frac{2^n-1}{2^n}+\frac{1}{2^{n+1}}$

$$=\frac{2^{n+1}-2}{2^{n+1}}+\frac{1}{2^{n+1}}=\frac{2^{n+1}-1}{2^{n+1}} \quad //$$

4.1 #16 Prove $\forall n\in\mathbb{Z}^+$, $1\cdot2\cdot3+2\cdot3\cdot4+\cdots+n(n+1)(n+2)$
$=\frac{n(n+1)(n+2)(n+3)}{4}$.

Pf ① check $n=1$ case.

$$1\cdot2\cdot3=\frac{1(2)(3)(4)}{4} \quad ✓ \quad \text{true}$$

② Assume true for n case.

$$\Leftrightarrow \quad 1\cdot2\cdot3+2\cdot3\cdot4+\cdots+n(n+1)(n+2)=\frac{n(n+1)(n+2)(n+3)}{4}$$

$$1\cdot2\cdot3+2\cdot3\cdot4+\cdots+n(n+1)(n+2)+(n+1)(n+2)(n+3)$$

$$=\frac{n(n+1)(n+2)(n+3)}{4}+(n+1)(n+2)(n+3)\left(\frac{4}{4}\right)$$

$$=\frac{n(n+1)(n+2)(n+3)+4(n+1)(n+2)(n+3)}{4}$$

$$=\frac{(n+1)(n+2)(n+3)(n+4)}{4} \quad //$$

4.1 #18 Let $P(n)$ be statement $n! < n^n$, $n \in \mathbb{Z}^+$

$n > 1$.

(a) $P(2) = ?$ $P(2)$ is $2! < 2^2$.

(b) $2! = 2$ and $2^2 = 4$ $\Rightarrow$ $2! < 2^2$ is true.

(c) Assume $P(n)$ is true, i.e. $n! < n^n$.

(d) Need to show $P(n) \to P(n+1)$.

(e) $n! < n^n$

$\Leftrightarrow$ $(n+1)n! < n^n(n+1)$

$\Leftrightarrow$ $(n+1)! < (n+1)n^n$ we know $n^n < (n+1)^n$

(since $n < n+1$)

$\Leftrightarrow$ $(n+1)n^n < (n+1)^{n+1}$

$\Rightarrow$ $(n+1)! < (n+1)n^n < (n+1)^{n+1}$ //

4.1 #35 Prove n^2-1 is divisible by 8 whenever n is an odd positive integer.

If n is an odd +ve integer, then $\exists\, k \in \mathbb{Z}^+ \ni$

$n = 2k+1$.

So our claim reduces to

$(2k+1)^2 - 1$ is divisible by 8 $\forall\, k = 1, 2, 3, \ldots$

Pf ① check $k=1$ case $(2(1)+1)^2 - 1 = 9 - 1 = 8$ is divisible by 8.

② Assume $(2k+1)^2 - 1$ is divisible by 8.

Check $k+1$ case.

$$(2(k+1)+1)^2 - 1 = ((2k+1)+2)^2 - 1$$
$$= (2k+1)^2 + 4(2k+1) + 4 - 1$$

4.1
#35 (cont)

$(2(k+1)+1)^2-1 = (2k+1)^2 + 8k + 4 + 4 - 1$

$\star \quad = \left[(2k+1)^2 - 1\right] + (8k+8)$

we know $(2k+1)^2-1$ is divisible by 8

i.e. $\exists\, a \in \mathbb{Z}^+ \ni (2k+1)^2 - 1 = 8a$

$\Rightarrow \star$ becomes $8a + 8k + 8 = 8(a+k+1)$

which is also divisible by 8 //