Homework 3

1. (a) This is an equivalence relation because

1) Reflexivity: for any angle α, $\alpha-\alpha=0=0\cdot 2\pi$. Thus, $\alpha\sim\alpha$

2) Symmetricity: for any angles α,β, if $\alpha\sim\beta$, then $\alpha-\beta=2\pi k$ for some $k\in\mathbb{Z}$. Then, $\beta-\alpha=-2\pi k=2\pi\cdot(-k)$. Since $-k\in\mathbb{Z}$, $\beta\sim\alpha$

Thus, $\alpha\sim\beta \Rightarrow \beta\sim\alpha$.

3) Transitivity: for any angles α,β,γ, if $\alpha\sim\beta$ and $\beta\sim\gamma$, then $\alpha-\beta=2\pi m$, $m\in\mathbb{Z}$. $\beta-\gamma=2\pi n, n\in\mathbb{Z}$.

Then, $\alpha-\gamma=\alpha-\beta+\beta-\gamma=2\pi(m+n)$. Since $m+n\in\mathbb{Z}$, $\alpha\sim\gamma$.

Thus, $\alpha\sim\beta$ and $\beta\sim\gamma \Rightarrow \alpha\sim\gamma$.

Therefore, $\sim$ is an equivalence relation.

(b) $\alpha\sim\alpha'$, then $\alpha-\alpha'=2k\pi$ for some $k\in\mathbb{Z}$. Thus, $\sin\alpha=\sin(\alpha'+2k\pi)$ (By periodicity of sin) $=\sin\alpha'$

$$\Rightarrow \sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta$$
$$=\sin\alpha'\cos\beta+\cos(2k\pi+\alpha')\sin\beta$$
$$=\sin\alpha'\cos\beta+\cos\alpha'\sin\beta=\sin(\alpha'+\beta) \quad \forall\beta$$

$\beta\sim\beta'$, then $\beta-\beta'=2k_2\pi$ and $\beta=2k_2\pi+\beta'$, $k_2\in\mathbb{Z}$

$$\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta=\cos\alpha\cdot\cos(2k_2\pi+\beta')-\sin\alpha\sin(2k_2\pi+\beta')$$
$$=\cos\alpha\cos\beta'-\sin\alpha\sin\beta'=\cos(\alpha+\beta') \quad \forall\alpha$$

2.15 Last digit of 3^{5^7}

$3^0=1$ $\quad 3^1=3$ $\quad 3^2=9$ $\quad 3^3=27$ $\quad 3^4=\cdots 1$ $\quad 3^5=\cdots 3$

5^7 is ~~a~~ a number. ~~the last digit is 5.~~ ~~$5^7 \bmod 4 =$~~

~~Therefore, last digit of 3^{5^7} is 3~~

$5 \bmod 4 \equiv 1$ $\quad 5^2 \bmod 4 \equiv 1$ $\quad 5^3 \bmod 4 \equiv 1$. So $5^7 \bmod 4 \equiv 1$.

Therefore, last digit is 3.

7^{5^3}, $5^3=125$, ~~9~~, $7^1=7$, $7^2=49\equiv 9 \bmod 10$ $7^3 \equiv 3 \bmod 10$
$7^4 \equiv 1 \bmod 10$

~~Therefore, last digit of 7^{5^3} is~~ $125 \bmod 4 = 1$

Therefore, last digit of 7^{5^3} is 7

11^{10^6} $11 \bmod 10 = 1$, $11^2 \bmod 10 = 1$, $11^3 \bmod 10 = 1$ ... last digit is 1.

8^{5^4} $8 \bmod 10 = 8$, $8^2 \bmod 10 = 4$, $8^3 \bmod 10 = 2$ $8^4 \bmod 10 = 6$

$8^5 \bmod 10 = 8$ $5^4 = 25^2 = 625$, $625 \bmod 4 \equiv 1 \bmod 4$.

Therefore, last digit of 8^{5^4} is 8.

2.16 $2^{1000000} \bmod 17$ and $17^{77} \bmod 14$.

$2^1 \bmod 17 = 2$ $2^2 \bmod 17 = 4$ $2^3 \bmod 17 = 8$ $2^4 \bmod 17 = 16$

$2^5 \bmod 17 = 15$ $2^6 \bmod 17 = 64 \bmod 17 = 13$

$2^7 \bmod 17 = 128 \bmod 17 = 9$ $2^8 \bmod 17 = 1$ $2^9 \bmod 17 = 2$

period: 8 ... $1000000/8 = 125000$ so $1000000 \bmod 8 = 0$

Therefore, $2^{1000000} \bmod 17 = 1$.

Evaluate 17^{77}

$17 \bmod 14 = 3$ $17^2 \bmod 14 = 9$ $17^3 \bmod 14 = 13$

$17^4 \bmod 14 = 11$ $17^5 \bmod 14 = 5$ $17^6 \bmod 14 = 1$

period: 6 $77 \bmod 6 = 5$. Therefore, $17^{77} \bmod 14 = 5$.

2.19 Proof: ~~All possible~~ residues mod $8 = \{0,1,2,\ldots,7\}$

Let $k = a^2+b^2+c^2$, $a,b,c \in \mathbb{N}$. $a^2 \bmod 8 \in \{0,1,4\}$ $c^2 \bmod 8 \in \{0,1,4\}$
$b^2 \bmod 8 \in \{0,1,4\}$

Therefore, $(a^2+b^2+c^2) \bmod 3 \in \{0,1,2,3,4,5,6\}$ $(a^2+b^2+c^2) \bmod 3 \neq 7$

but there are infinitely many numbers that mod $3 = 7$

Therefore, there are infinitely many numbers that can't be written as sum of 3 squares.

2.17 Suppose that n has k digits and $n = n_1 n_2 \cdots n_{k-1} n_k$

Then, $n = n_k \cdot 1 + n_{k-1} \cdot 10 + n_{k-2} \cdot 10^2 + \dots + n_1 \cdot 10^{k-1}$

$m = n_1 + n_2 + \dots + n_k$

$[m] = (n_1 + \dots + n_k) \bmod 3$, $[n] = [n_k + n_{k-1} \cdot 10 + \dots + n_1 \cdot 10^{k-1}] \bmod 3$

Considering that $10^\alpha \bmod 3 = 1$ for $\alpha = 0, 1, 2, \dots,$ we have

$[n] = n_k \bmod 3 + (n_{k-1} \cdot 10) \bmod 3 + \dots + (n_1 \cdot 10^{k-1}) \bmod 3$

$= (n_1 + n_2 + \dots + n_k) \bmod 3 = [m]$

2.~~1~~9

Let $k = a^2 + b^2 + c^2$ ~~mod~~, where $a, b, c \in \mathbb{N}$.

then, $a^2 \bmod 8 \in \{0, 1, 4\}$, $b^2 \bmod 8 \in \{0, 1, 4\}$, $c^2 \bmod 8 \in \{0, 1, 4\}$

and $k \bmod 8 = (a^2 + b^2 + c^2) \bmod 8 \in \{0, 1, 2, 3, 4, 5, 6\}$

(choose 3 numbers from $\{0, 1, 4\}$ and sum them up and do mod 8)

It shows that $k \bmod 8 \neq 7$. However, there are infinitely many natural numbers which mod $8 = 7$. Thus, there are infinite number of natural numbers that cannot be written as the sum of 3 squares.

2.22

$\ulcorner 2 \urcorner = \{0, 1\}$

R is reflexive since $\forall f \in X$, $Dom(f) \subseteq Dom(f)$ and $f = f|_{Dom(f)}$.

Thus, fRf.

R is not symmetric. Let $Dom(f) = \{1, 2, 3\}$ and $Dom(g) = \{1, 2\}$

$f(x) = 0 \ \forall x \in Dom(f)$, $g(x) = 0 \ \forall x \in Dom(g)$. Then, fRg but g doesn't R f ($g \not R f$)

R is anti-symmetric if fRg and gRf, then $Dom(f) \subseteq Dom(g) \subseteq Dom(f)$

$\Rightarrow Dom(f) = Dom(g)$. Also, $g = f|_{Dom(g)} = f|_{Dom(f)} = f$. So $f = g$.

R is transitive. If fRg and gRh, then $Dom(h) \subseteq Dom(g) \subseteq Dom(f)$, $h = g|_{Dom(h)} = (f|_{Dom(g)})|_{Dom(h)}$

Ctd $= f|Dom(h)$. so fRh. It's transitive.

Therefore, R is a partial ordering but not an equivalence relation

2.26 $\forall y \in Y$, ~~$\exists y \in G$~~ define $f^{-1}(y)$ in the following way:

$f^{-1}(y) = \{x \mid f(x) = y,\ x \in X\}$. Then, $X/f = \{f^{-1}(f(x)) \mid x \in X\}$

If f is an injection, then, ~~$f(y)$~~ $f^{-1}(f(x))$ contains only one element.

and thus X/f is composed of singletons.

If X/f is composed of singletons, then $f^{-1}(f(x))\ \forall x \in X$ contains only one element. Then, if $f(x_1) = f(x_2)$, $x_1 \in f^{-1}(f(x_1))$ so $x_1 \in f^{-1}(f(x_2))\ \exists x_2$

Since $f^{-1}(f(x_1)) = f^{-1}(f(x_2))$ contains only 1 element, $x_1 = x_2$.

f is injective.

To conclude, X/f is composed of singletons iff f is an injection.

3.1 (i) $[\neg(P \wedge Q)] \equiv [(\neg P) \vee (\neg Q)]$

Table

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Thus, $[\neg(P \wedge Q)]$

$\equiv [(\neg P) \vee (\neg Q)]$

3.2 1) if $P \Leftrightarrow Q$, we have if P then Q (*) and if Q then P (**)

~~If $P=1$, then $T(P)=1$~~

Therefore, if $T(P)=1$, then $T(Q)=1$. Also, if $T(Q)=0$, then $T(P)=0$ by (*)

if $T(Q)=1$, then $T(P)=1$. Also, if $T(P)=0$, then $T(Q)=0$ by (**)

$T(P) = T(Q)$ for any assignment of truth value, and thus ~~the~~ $P \equiv Q$.

2) If $P \equiv Q$, then $T(P) = T(Q)$ ~~for~~ If P is true, then $T(P) = 1 = T(Q)$ Q is true

If Q is true, the $T(Q) = 1 = T(P) \Rightarrow P$ is true

so $P \Leftrightarrow Q$

3.3 Let P be the statement that $3 > 2^3$, let Q be the statement that $3 > 5$.
For $P \Rightarrow Q$, P is the antecedent and Q is the consequence.
P is ~~true~~ false and Q is false. Since P is false, $T(P \Rightarrow Q) = 1 - T(P) + T(P) \cdot T(Q)$

$$= 1 - 0 + 0 = 1$$

$P \Rightarrow Q$ is thus true.

34 a) $P \wedge \neg P \Rightarrow Q$ is true because $T(P \wedge \neg P) = 0$ and thus

$$T(P \wedge \neg P \Rightarrow Q) = 1 - T(P \wedge \neg P) + T(P \wedge \neg P) \cdot T(Q) = 1$$

b) $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q) \wedge (Q \Rightarrow R)$	$P \Rightarrow R$	$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

c) $[P \Rightarrow (Q \wedge \neg Q)] \Rightarrow \neg P$

When $T(P) = 0$, $T[P \Rightarrow (Q \wedge \neg Q)] = 1$, $T(\neg P) = 1$.
and $T([P \Rightarrow (Q \wedge \neg Q)] \Rightarrow \neg P) = 1$

When $T(P) = 1$, $T[P \Rightarrow (Q \wedge \neg Q)] = 0$ and thus $T([P \Rightarrow (Q \wedge \neg Q)] \Rightarrow \neg P) = 1$

Thus, $[P \Rightarrow (Q \wedge \neg Q)] \Rightarrow \neg P$

d) $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$

When $T(P) = 0$, $T(P \Rightarrow Q) = 1$. Thus $T[P \wedge (P \Rightarrow Q)] = 0$
and $T([P \wedge (P \Rightarrow Q)] \Rightarrow Q) = 1$.

When $T(P) = 1$,
- if $T(Q) = 0$, then $T[P \wedge (P \Rightarrow Q)] = 0$ and thus $T([P \wedge (P \Rightarrow Q)] \Rightarrow Q) = 1$
- if $T(Q) = 1$, then $T[P \wedge (P \Rightarrow Q)] = 1$ thus $T([P \wedge (P \Rightarrow Q)] \Rightarrow Q) = 1$

So $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$.

e) $T(Q \vee \neg Q) = 1$, then $T[P \Rightarrow (Q \vee \neg Q)] = 1$ nomatter $T(P) = 1$ or $T(P) = 0$
so $P \Rightarrow (Q \vee \neg Q)$.