Math 417
HW 1
Due 1/25/19

1. $g = \gcd(40,65)$

$65 = 1\cdot 40 + 25$
$40 = 1\cdot 25 + 15$
$25 = 1\cdot 15 + 10$
$15 = 1\cdot 10 + 5$
$10 = 2(5) + 0$

So $5 = \gcd(40,65)$

And: $5 = 15 - 10 = 15 - (25-15)$
$= 2\cdot 15 - 1\cdot 25 = 2(40-25) - 25$
$= 2\cdot 40 - 3\cdot 25 = 2\cdot 40 - 3(65-40)$
$5 = 5\cdot 40 - 3\cdot 65 = 5\cdot 40 + (-3)\cdot 65$

2a. If $\gcd(a,14)=1$, then $2+a$ and $7+a$, which rules out $0,2,4,6,8,10,12 \bmod 14$ and $0, 7 \bmod 14$.
This leaves $1,3,5,9,11,13 \bmod 14$.

2b.

	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

2c. The powers of the elements, from the table, are:
1; $1, 3, 3^2=9, 3^3=13, 3^4=11, 3^5=5, 3^6=1$; $1, 5, 5^2=11, 5^3=13, 5^4=9, 5^5=3, 5^6=1$; $1, 9, 9^2=11, 9^3=1$; $1, 11, 11^2=9, 11^3=1$; $1, 13, 13^2=1$

So the elements with the desired property are $a=3,5$, or $[3]_{14}, [5]_{14}$. These will be called the "generators" of this "cyclic" group.

---

3. This is my preferred method:

$x \equiv 2 \bmod 5 \Rightarrow x = 2+5u,\ u \in \mathbb{Z}$
$x \equiv 6 \bmod 7 \Rightarrow 2+5u \equiv 6 \bmod 7$
$\Rightarrow 5u \equiv 6-2 \equiv 4 \bmod 7$
We need to find a so that $a\cdot 5 \equiv 1 \bmod 7$
For small numbers, we can do this by hand $3\cdot 5 = 15 \equiv 1 \bmod 7$, so

$5u \equiv 4 \bmod 7$
$\Rightarrow 3(5u) \equiv 3\cdot 4 \bmod 7$
$15u \equiv 12 \bmod 7$
$15 \equiv 1 \bmod 7$, $12 \equiv 5 \bmod 7$, so
$u \equiv 5 \bmod 7$.

That is, $u = 5+7v$, $v \in \mathbb{Z}$.
Thus, $x = 2+5u = 2+5(5+7v)$
$= 2+25+35v = 27+35v$
or $\boxed{x \equiv 27 \bmod 35}$

---

4. With correction to $\frac{1}{407}$

$11 \mid 10^2-1 \Rightarrow 10^2 \equiv 1 \bmod 11 \Rightarrow$
$10^2\cdot 10^2\cdot 10^2 = 10^6 \equiv 1 \bmod 11 \Rightarrow$
$11 \mid 10^6-1$.
$37 \mid 10^3-1 \Rightarrow 10^3 \equiv 1 \bmod 37 \Rightarrow$
$10^3\cdot 10^3 = 10^6 \equiv 1 \bmod 37 \Rightarrow$
$37 \mid 10^6-1$

so $10^6 - 1 = 11 \cdot u$

$37 \mid 10^6 - 1 = 11u$ and $\gcd(11, 37) = 1$

$\Rightarrow 37 \mid u \Rightarrow u = 37v$

$\Rightarrow 10^6 - 1 = 11(37v) = 407v$

Thus $\frac{1}{407} = \frac{v}{407v} = \frac{v}{10^6 - 1}$

If you do the arithmetic,

$v = 2457$, and

$\frac{1}{407} = .002457002457\ldots$

(This is what I had in mind.)

---

5 G:

	u	v	w	x
u	v	x	u	w
v	x	w	v	u
w	u	v	w	x
x	w	u	x	v

5a.

Since $w \cdot u = u$, $w \cdot v = v$, $w \cdot w = w$ and $w \cdot x = x$, w is the identity element

5b.

Since $u \cdot x = w = x \cdot u$, x is the inverse of u and u is the inverse of x.

Since $v \cdot v = w \cdot w = w$, v is the inverse of v and w is the inverse of w.

6. This is almost more a "logic" problem than a "math" problem

6a. $4 \mid a$ and $4 \mid b$, $6 \mid a$ and $6 \mid c$

So $2 \mid b$ and $2 \mid c$ Does $4 \mid c$?

If $4 \mid c$, then $4 \mid a \Rightarrow 4 \mid a, c \Rightarrow 4 \mid 6$, which isn't true.

Thus, the highest power of 2 that divides g is 2^1.

6b. $6 \mid a$ and $6 \mid c$, so $3 \mid a$ and $3 \mid c$.

if $3 \mid b$, then $3 \mid \gcd(a, b) = 4$, which isn't true.

Thus, $3 \nmid b$

6c. We can't say anything about the power of 5 that divides g!

For example, let

$a = 12$

$b = 4 \cdot 5^m$

$c = 6 \cdot 5^m$

Then $\gcd(a, b) = 4$

$\gcd(a, c) = 6$

and $\gcd(b, c) = 2 \cdot 5^m$

for any m!

Advice: I like this problem, but two 417 classes don't. The people have spoken!