Remark: Multiplicative inverse of an integer x modulo n is an integer b so that $b \cdot x \equiv 1 \ (mod\ n)$. Just like 1c) and 1d). From 1d) we have that multiplicative inverse of 137 (mod 532) is 233.

1. Computations:

   (a) Find gcd(77,49).
   Solution: (For some of the problems I will not write details, but only the final answers.)
   Answer: $\boxed{gcd(77, 49) = 7}$

   (b) Express gcd(77,49) as $\alpha \cdot 77 + \beta \cdot 49$=gcd(77,49).
   Solution: (Some of the problems I will not write details, but only the final answers.)
   Answer: $\boxed{2 \cdot 77 + (-3)49 = 7}$

   (c) Find an integer b so that $b \cdot 7 \equiv 1(mod\ 10)$

   (d) Find an integer b so that $b \cdot 137 \equiv 1(mod\ 532)$
   Solution: Use Euclidean algorithm to find α and β so that $\alpha \cdot 532 + \beta \cdot 137 = 1$.

$$\begin{array}{rr|ll}
532 & 137 & & \\
\hline
1 & 0 & 532 & \\
0 & 1 & 137 & (3) \\
\hline
1 & -3 & 121 & (1) \\
-1 & 4 & 16 & (7) \\
8 & -31 & 9 & (1) \\
-9 & 35 & 7 & (1) \\
17 & -66 & 2 & (3) \\
-60 & 233 & \boxed{1} & \\
\hline
\end{array}$$

   Therefore $-60 \cdot 532 + 233 \cdot 137 = 1$.
   Now compute everithing modulo 532.
   $-60 \cdot 0 + 233 \cdot 137 \equiv 1 \ (mod\ 532)$
   $233 \cdot 137 \equiv 1 \ (mod\ 532)$
   $\therefore \boxed{b \equiv 233 \ (mod\ 532)}$ or $\boxed{b = 233}$

   Check: $233 \cdot 137 = 31,921 = 60 \cdot 532 + 1 \equiv 1 \ (mod\ 532)$.

   (e) Find an integer b so that $b \cdot 138 \equiv 1(mod\ 532)$
   Solution: Since $2|138$ and $2|532$ we know that $gcm(138, 532) \neq 1$. Then by Proposition done in class, it follows that there is no b such that $b \cdot 138 \equiv 1(mod\ 532)$.
   $\therefore$ $\boxed{\text{there is no solution for } b}$

   (f) Find d=gcd(177,48) and express d as $\alpha \cdot 177 + \beta \cdot 48 = $ d.

   (g) Express gcd(177,49) as $\alpha \cdot 177 + \beta \cdot 49 = $ gcd(177,49).

2. Computations (mod 15). Always express your answer in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$. Make sure that you show enough work.

   (a) $5 \cdot 2 \equiv$ ____ (mod 15)
   Solution: $\boxed{5 \cdot 2 \equiv 10\ (mod\ 15)}$

   (b) $5 \cdot 6 \equiv$ ____ (mod 15)
   Solution: $5 \cdot 6 \equiv 30\ (mod\ 15) \equiv 2 \cdot 15 + 0\ (mod\ 15) \equiv 0\ (mod\ 15)$
   $\therefore \boxed{5 \cdot 6 \equiv 0\ (mod\ 15)}$

   (c) $5 + 6 \equiv$ ____ (mod 15)
   Solution: $\boxed{5 + 6 \equiv 11\ (mod\ 15)}$

   (d) $9 \cdot 10 \equiv$ ____ (mod 15)
   Solution: $9 \cdot 10 \equiv 90\ (mod\ 15) \equiv 6 \cdot 15 + 0\ (mod\ 15) \equiv 0\ (mod\ 15)$
   $\therefore \boxed{9 \cdot 10 \equiv 0\ (mod\ 15)}$

   (e) $5^2 \equiv$ ____ (mod 15)
   Solution: $5^2 \equiv 25\ (mod\ 15) \equiv 15 + 10\ (mod\ 15) \equiv 10\ (mod\ 15)$
   $\therefore \boxed{5^2 \equiv 10\ (mod\ 15)}$

   (f) $5^3 \equiv$ ____ (mod 15)
   Solution: $5^3 \equiv 5^2 \cdot 5\ (mod\ 15) \equiv 10 \cdot 5\ (mod\ 15) \equiv 50\ (mod\ 15) \equiv$
   $\equiv 3 \cdot 15 + 5\ (mod\ 15) \equiv 5\ (mod\ 15)$
   $\therefore \boxed{5^3 \equiv 5\ (mod\ 15)}$

   (g) $5^4 \equiv$ ____ (mod 15)
   Solution: $5^4 \equiv 5^3 \cdot 5\ (mod\ 15) \equiv 5 \cdot 5\ (mod\ 15) \equiv 25\ (mod\ 15) \equiv$
   $\equiv 15 + 10\ (mod\ 15) \equiv 10\ (mod\ 15)$
   $\therefore \boxed{5^3 \equiv 10\ (mod\ 15)}$

   (h) $32 \cdot 6 \equiv$ ____ (mod 15)
   Solution: First notice that $32 \equiv 2 \cdot 15 + 2 (mod\ 15) \equiv 2\ (mod\ 15)$. Now use this:
   $32 \cdot 6 \equiv 2 \cdot 6\ (mod\ 15) \equiv 12\ (mod\ 15)$
   $\therefore \boxed{32 \cdot 6 \equiv 12\ (mod\ 15)}$

   (i) $32^3 \equiv$ ____ (mod 15)
   Solution: First notice that $32 \equiv 2 \cdot 15 + 2 (mod\ 15) \equiv 2\ (mod\ 15)$. Now use this:
   $32^3 \equiv 2^3\ (mod\ 15) \equiv 8\ (mod\ 15)$

$\therefore \boxed{32^3 \equiv 8\ (mod\ 15)}$

(j) $151^7 \equiv$ ____ $(mod\ 15)$
Solution: $151^7 \equiv (10 \cdot 15 + 1)^7\ (mod\ 15) \equiv 1^7\ (mod\ 15) \equiv 1\ (mod\ 15)$
$\therefore \boxed{151^7 \equiv 1\ (mod\ 15)}$

(k) $149^7 \equiv$ ____ $(mod\ 15)$
Solution: $149^7 \equiv (10 \cdot 15 - 1)^7\ (mod\ 15) \equiv (-1)^7\ (mod\ 15) \equiv (-1)\ (mod\ 15) \equiv$
$\equiv (15 - 1)\ (mod\ 15) \equiv 14\ (mod\ 15)$
$\therefore \boxed{149^7 \equiv 14\ (mod\ 15)}$

(l) $1/7 \equiv$ ____ $(mod\ 15)$
Solution: First notice that $1/7$ is the number b such that $b \cdot 7 \equiv 1\ (mod 15)$.
So this is the same type of problem as 1c) or 1d).

One way -
guess: $b = 13$ and
check $13 \cdot 7 \equiv 91\ (mod\ 15) \equiv 6 \cdot 15 + 1\ (mod\ 15) \equiv 1\ (mod\ 15)$
$\therefore \boxed{1/7 \equiv 13\ (mod\ 15)}$

Second way - use Euclidean algorithm to find α and β so that $\alpha \cdot 15 + \beta \cdot 7 = 1$

(m) $4/7 \equiv$ ____ $(mod\ 15)$
Solution: First notice that $1/7 \equiv 13\ (mod\ 15)$ from the previous part.
$4/7 = 4 \cdot (1/7) \equiv 4 \cdot 13\ (mod\ 15) \equiv 52\ (mod\ 15) \equiv 3 \cdot 15 + 7\ (mod\ 15) \equiv 7\ (mod\ 15)$.
$\therefore \boxed{4/7 \equiv 7\ (mod\ 15)}$

3. Solve the following congruences:

(a) $5x \equiv 6(mod\ 7)$

(b) $5x \equiv 6(mod\ 35)$

(c) $5x \equiv 10(mod\ 35)$

(d) $15x \equiv 6(mod\ 35)$

(e) $15x \equiv 10(mod\ 35)$

(f) $153x \equiv 10(mod\ 35)$
Solution:
Step 1: $153 = 4 \cdot 35 + 13 \equiv 13\ (mod\ 35)$

Step 2: Solve $13x \equiv 10\ (mod\ 35)$

Step 3: Find multiplicative inverse of 13 (mod 35), i.e. find b such that $b{\cdot}13 \equiv 1\ (mod\ 35)$.
Use Euclidean algorithm to find α and β so that $\alpha \cdot 35 + \beta \cdot 13 = 1$.

35	13		
1	0	35	
0	1	13	(2)
1	−2	9	(1)
−1	3	4	(2)
3	−8	$\boxed{1}$	(1)

Therefore $3 \cdot 35 + (-8) \cdot 13 = 1$.
Now compute everithing modulo 35.
$3 \cdot 0 + (-8) \cdot 13 \equiv 1\ (mod\ 35)$
$(-8) \cdot 13 \equiv 1\ (mod\ 35)$
$(-8) \equiv (35 - 8)\ (mod\ 35) \equiv 27\ (mod\ 35)$
$\therefore \boxed{b \equiv 27\ (mod\ 35)}$ or $\boxed{b = 27}$

<u>Check:</u> $27 \cdot 13 = 351 = 10 \cdot 35 + 1 \equiv 1\ (mod\ 35)$.

Step 4: Multiply congruence $13x \equiv 10\ (mod\ 35)$ by 27.
$27 \cdot 13x \equiv 27 \cdot 10\ (mod\ 35)$
Use the fact that $27 \cdot 13 \equiv 1\ (mod\ 35)$ and get
$x \equiv 27 \cdot 10\ (mod\ 35) \equiv 270\ (mod\ 35) \equiv 7 \cdot 35 + 25\ (mod\ 35) \equiv 25\ (mod\ 35)$
$\therefore \boxed{x \equiv 25\ (mod\ 35)}$ or $\boxed{x = 25}$

<u>Check:</u> $153 \cdot 25 = 3825 = 109 \cdot 35 + 10 \equiv 10\ (mod\ 35)$.

4. Find the greatest common divisors gcd and least common multiples lcm for the following pairs of numbers:

   (a) $gcd(5, 7) =$ ________ $lcm(5, 7) =$ ________
   (b) $gcd(1, 27) =$ ________ $lcm(1, 27) =$ ________
   (c) $gcd(5^3{\cdot}7^2, 7{\cdot}11{\cdot}13^4) =$ ________________ $lcm(5^3{\cdot}7^2, 7{\cdot}11{\cdot}13^4) =$ ________________
   (d) $gcd(5^{123}{\cdot}7^2, 5^2{\cdot}7^{11}{\cdot}13^4) =$ ________________ $lcm(5^{123}{\cdot}7^2, 5^2{\cdot}7^{11}{\cdot}13^4) =$ ________________
   (e) $gcd(p^5, p^7) =$ ________ $lcm(p^5, p^7) =$ ________ (here p is a prime).
   (f) $gcd(10^5, 10^7) =$ ________ $lcm(10^5, 10^7) =$ ________
   (g) $gcd(56, 77) =$ ________, $lcm(56, 77) =$ ________

5. Find all the divisors of 15.
6. Find all the divisors of 27.
7. Find the prime factorization of 15.
8. Find the prime factorization of 27.
9. Find the prime factorization of 360.
10. True -False - Sometimes

    $\boxed{T}$ F S - 5 has multiplicative inverse $(mod\ 11)$

    $\boxed{T}$ F S - 6 has multiplicative inverse $(mod\ 11)$

    T F $\boxed{S}$ - Let $a \in \mathbb{Z}_{>0}$. Then a has multiplicative inverse $(mod\ 11)$

    T $\boxed{F}$ S - 5 has multiplicative inverse $(mod\ 10)$

    T $\boxed{F}$ S - 6 has multiplicative inverse $(mod\ 10)$

    $\boxed{T}$ F S - 7 has multiplicative inverse $(mod\ 10)$

    T F $\boxed{S}$ - Let $a \in \mathbb{Z}_{>0}$. Then a has multiplicative inverse $(mod\ 10)$

    $\boxed{T}$ F S - Let $10x \equiv 23(mod\ 41)$. There is a unique solution mod 41 for x.

    T $\boxed{F}$ S - Let $10x \equiv 20(mod\ 40)$. There is a unique solution mod 40 for x.

    $\boxed{T}$ F S - Let $10x \equiv 20(mod\ 40)$. There are 10 distinct solutions mod 40 for x.

    $\boxed{T}$ F S - Let $10x \equiv c(mod\ 41)$. There is a unique solution mod 41 for x.

    T $\boxed{F}$ S - Let $10x \equiv c(mod\ 40)$. There is a unique solution mod 40 for x.

    T F $\boxed{S}$ - Let $10x \equiv c(mod\ 40)$. There are 10 distinct solutions mod 40 for x.

    T F $\boxed{S}$ - Let $10x \equiv c(mod\ 40)$. There are no solutions mod 40 for x.

11. Make the table for the addition of equivalence classes (mod 8) which are given as

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}.$$

12. Make the table for the multiplication of equivalence classes (mod 8) which are given as

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}.$$

13. Make the table for the addition of equivalence classes (mod 3)

14. Make the table for the multiplication of equivalence classes (mod 3)

15. Examples - You should justify your answers.

    (a) Give an example of a prime number.

    (b) Give an example of a number which is not prime number.

    (c) Give an example of two integers which are relatively prime.

    (d) Give an example of two integers which are not relatively prime.

    (e) Give an example of two integers a, b such that $gcd(a, b) = 12$.

    (f) Give an example of two integers a, b such that $lcm(a, b) = 12$.

    (g) Give an example of two integers a, b such that $lcm(a, b) = 12$.

    (h) Give an example of two integers a, b such that $lcm(a, b) = 5$.

    (i) Give an example of two integers a, b such that $gcd(a, b) = 5$.

    (j) Give an example of two integers a, b such that $gcd(a, b) = lcm(a, b)$.

    (k) Give an example of two integers a, b such that $[a]_7 + [b]_7 = [0]_7$.

    (l) Give an example of two integers $a, b \neq 0$ such that $[a]_6[b]_6 = [0]_6$.

HAVE FUN!