Problem 1:

a) Find all possible natural residue of x^2 modulo 9.

> Def: r is called natural residue of a modulo m.
> The set $\{0, 1, 2 \dots m-1\}$ is called the set of natural residues modulo m.

In our case, we have x^2 modulo 9. which $a = x^2$, $m = 9$.
The set are $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

when $x=0 \Rightarrow 0 \equiv 0 \bmod(9)$
when $x=1 \Rightarrow 1 \equiv 1 \bmod(9)$
when $x=2 \Rightarrow 4 \equiv 4 \bmod(9)$
when $x=3 \Rightarrow 9 \equiv 0 \bmod(9)$
when $x=4 \Rightarrow 16 \equiv 7 \bmod(9)$
when $x=5 \Rightarrow 25 \equiv 7 \bmod(9)$
when $x=6 \Rightarrow 36 \equiv 0 \bmod(9)$
when $x=7 \Rightarrow 49 \equiv 4 \bmod(9)$
when $x=8 \Rightarrow 64 \equiv 1 \bmod(9)$

The number 0, 1, 4, 7 are natural residue.

b) Show that $x^2+y^2 = 996$ has no integer solution for x, y.

$x^2+y^2 \equiv 996 \bmod(9)$

$996 \div 9 = 110 \dots 6$ ← remainder.

$\Rightarrow x^2+y^2 \equiv 6 \bmod(9)$

Which mean $x^2, y^2 \in \{0, 1, 4, 7\}$.

① $0^2+0^2 \not\equiv 6$
② $0+1^2 \not\equiv 6$
③ $0+4^2 \not\equiv 6$
④ $0+7^2 \not\equiv 6$
⑤ $0^2+0^2 \not\equiv 0$
⑥ $1^2+0^2 \not\equiv 6$
⑦ $4^2+0^2 \not\equiv 6$
⑧ $7^2+0^2 \not\equiv 6$.
⑨ $4^2+4^2 \not\equiv 6$
⑩ $1^2+1^2 \not\equiv 6$
⑪ $7^2+7^2 \not\equiv 6$
⑫ $7^2+1^2 \not\equiv 6$.
....

when $x=0$.
$y = 0, 1, 4, 7$

when $y=0$
$x = 0, 1, 4, 7$.

..... So I check. no mater what number we try. there is no integer solution for x, y.

Problem 2: Let $n \in \mathbb{N}$. and let

$n = a_r(a_{r-1}) \ldots a_1 a_0 = a_r 10^{r-1} + a_{r-1} 10^{r-2} \ldots + a_1 10 + a_0$.

Be a base ten expansion of n. prove that n divisible by 9 if and only if sum of the digits $a_r + a_{r-1} \ldots + a_0$ is divisible by 9.

Pf: want to show $9 \mid n \iff 9 \mid (a_r + a_{r-1} \ldots + a_1 + a_0)$

hint $10 \equiv 1 \bmod(9) \implies 10^k \equiv 1^k \equiv 1 \bmod(9)\ \forall k \in \mathbb{N}$

$\implies 10^k \equiv 1 \bmod(9)\ \forall k \in \mathbb{N}$.

Use professor's note proof.

We Have $10^k \equiv 1 \bmod(9)\ \forall k \in \mathbb{N}$.

we know $n = a_r 10^{r-1} + a_{r-1} 10^{r-2} + \ldots + a_1 10 + a_0$.

$\implies a_r \cdot 10^{r-1} \equiv a_r \pmod 9$, $a_{r-1} \cdot 10^{r-2} \equiv a_{r-1} \pmod 9$

$\ldots\ a_1 \cdot 10 \equiv a_1 \pmod 9$, $a_0 \equiv a_0 \pmod 9$

$\implies a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \ldots + a_1 \cdot 10 + a_0 \equiv a_r + a_{r-1} + \ldots + a_1 + a_0 \bmod 9$

$\implies n \equiv a_r + a_{r-1} + \ldots + a_0$

Thus, $n \equiv 0 \bmod 9 \iff a_r + a_{r-1} + \ldots + a_0 \equiv 0 \bmod(9)$.

$\iff 9 \mid a_r + a_{r-1} \ldots + a_0$ ▨

Problem 3: Determine if the following linear congruence equation are solvable. If they are solvable. find the general solution

(a) $14x \equiv 6 \bmod(22)$

The General solution x for $ax \equiv b \bmod(n)$ are $X = X_0 + \frac{\text{lcm}(a,b)}{a} \cdot n, n \in \mathbb{Z}$

Step 1: check if it's solvable.

$\gcd(a,m) \Rightarrow \gcd(14,22) = 2$ 216. it's solvable.

notice $m \mid a-b$. so $22 \mid 14x - 6$, we can see. $22 \mid 22$.

So we have $14x - 6 = 22 \Rightarrow 14x = 28 \Rightarrow x_0 = 2$.

$\Rightarrow x_0 = 2$ is a solution for $14x \equiv 6 \bmod(22)$

By Prop 2: the General Solution are

$$x = 2 + \frac{\text{lcm}(14,22)}{14} \cdot n \text{ for } n \in \mathbb{Z}$$

$$\Rightarrow x = 2 + \frac{154}{14} \cdot n \text{ for } n \in \mathbb{Z}$$

$$\Rightarrow x = 2 + 11(n) \text{ for } n \in \mathbb{Z}$$

$2 + 11(n)$ for $n \in \mathbb{Z}$ are the general solution.

$$\text{lcm}(14,22) = \frac{14 \cdot 22}{\gcd(14,22)} = \frac{14 \cdot 22}{2} = 7 \cdot 22 = 154$$

(b) $2021x \equiv 15 \bmod(47)$

Step 1: Check if it's solvable

$\gcd(a,m) = \gcd(2021,47) = 47$, $47 \nmid 15$, so no solution

Problem 4. Find a multiplicate inverse of 8, or prove that one does not exist, modulo 30, 31, 32, 33, 34.

① when $m=30$, $\gcd(8,30)=2$. 2+1, so no solution.

② when $m=31$, $\gcd(8,31)=1$ 111, 31 has solution.

③ when $m=32$, $\gcd(8,32)=8$ 8+1 so no solution.

④ when $m=33$, $\gcd(8,33)=1$ 111 . 33 has solution.

⑤ when $m=34$. $\gcd(8,34)=2$ 2+1. so no solution.

First part of answer.

we have 31, 33 has solution.

For 31.

Solve for x in $8x \equiv 1 \bmod(31)$. Find the solution: $8x+31y=1$

$31 = 3(8)+7$ $\quad 1 = 4(8)+31(-1)$

$8 = 1(7)+1$ $\quad 1 = 8-(31-3(8))$

$7 = 7(1)+0$ $\quad 1 = 8-7$

$x=4$ is a solution for $8x \equiv 1 \bmod(31)$.
4 is a multiplicate inverse of 8 mod(31).

Second Part of anwer.

For 33.

Solve for x $8x \equiv 1 \bmod(33)$. Find the solution. $8x+33y=1$

$33 = 4(8)+1$ $\quad 1 = 33+(-4)(8)$

$8 = 8(1)+0$. $\quad 1 = 33-4(8)$

$x=-4$ is a solution for $8x \equiv 1 \bmod(33)$
-4 is a multiplicate inverse of 8 mod(33).

third. Part of Answer.

By natural residues $-4+32=29$. 29 is also Answer.
So 29 is a multiplicate inverse of 8 mod(33)

Problem 5.: Let $\bar{a} \in \Phi(m)$ and $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$

a) Show that if $\bar{a} \cdot \bar{b} = \bar{1}$, then $\bar{b} \in \Phi(m)$.

$\bar{a} \cdot \bar{b} = \overline{ab} = \bar{1}$ Lecture 8. Prove it By professor.

so we have

$\Phi(m) = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a,m) = 1\}$, Since $\gcd(a,m) = 1$. By theorem

a is invertiable mod $m \iff \gcd(a,m) = 1$

So we have a is invertiable, which mean we can have $\exists b \in \mathbb{Z}$.

such that

$a \cdot b \equiv 1 \bmod(m)$. then By prop1 $= \overline{ab} = \bar{1}$ or $\bar{a} \cdot \bar{b} = \bar{1}$ in $\Phi(m)$.

That it, we can also prove $\bar{b}$ have $\gcd(b,m) = 1$.

For each $\bar{a} \in \Phi(m)$, $\exists\ \bar{b} \in \Phi(m)$ such that $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{b \cdot a} = \bar{1}$.

B) If $\bar{a} \cdot \bar{b} = \bar{1}$. and $\bar{a} \cdot \bar{b_1} = \bar{1}$, show that $\bar{b} = \bar{b_1}$.

for prop 5. Elements in Φm satisty the 'cacelation rule'.

In this Question: $\bar{a} \in \Phi(m)$ and if $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{b_1}$ for $\bar{b}, \bar{b_1} \in \mathbb{Z}/m\mathbb{Z}$, then $\bar{b} = \bar{b_1}$

Pf: we have $\gcd(a,m) = 1$, so

$\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{b_1} \Longrightarrow ab \equiv ab_1 \pmod{m} \Longrightarrow m \mid ab - ab_1$

Because $m \mid a(b - b_1)$ and $\gcd(a,m) = 1$ By Euclid's Lemma

$m \mid b - b_1$ i.e $b \equiv b_1 \bmod(m) \Longrightarrow \bar{b} = \overline{b_1}$ □

Class lecture & notes, proof by professor.

Problem 6.

(a) $5^{2022} \bmod (24)$

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1024$

$2022 = 1024 + 512 + 256 + 128 + 64 + 32 + 4 + 2$.

$5^{2022} = (5^{1024} \cdot 5^{512} \cdot 5^{256} \cdot 5^{128} \cdot 5^{64} \cdot 5^{32} \cdot 5^4 \cdot 5^2)$

$5^{2022} \bmod (24) = [5^{1024} \bmod (24) \cdot 5^{512} \bmod (24) \cdot 5^{256} \bmod (24) \cdot 5^{128} \bmod (24) \cdot 5^{64} \bmod (24) \cdot 5^{32} \bmod (24) \cdot 5^4 \bmod (24) \cdot 5^2 \bmod (24)]$

$5^2 \bmod (24) = 1$
$5^4 \bmod (24) = 1$
$5^8 \bmod (24) = 1$
$5^{16} \bmod (24) = 1$
$5^{32} \bmod (24) = 1$
$5^{64} \bmod (24) = 1$
$5^{128} \bmod (24) = 1$
$5^{256} \bmod (24) = 1$
$5^{512} \bmod (24) = 1$
$5^{1024} \bmod (24) = 1$

So $5^{2022} \bmod (24) = [1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1] \bmod (24)$.

$= 1^8 \bmod 24$

$\boxed{5^{2022} \bmod (24) \equiv 1 \bmod 24}$

(b) $3^{2022} \pmod{24}$

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1024$

$2022 = 1024 + 512 + 256 + 128 + 64 + 32 + 4 + 2$

$3^{2022} = (3^{1024} \cdot 3^{512} \cdot 3^{256} \cdot 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^4 \cdot 3^2)$

$3^{2022} \bmod (24) = [3^{1024} \bmod (24) \cdot 3^{512} \bmod (24) \cdot 3^{256} \bmod (24) \cdot 3^{128} \bmod (24) \cdot 3^{64} \bmod (24) \cdot 3^{32} \bmod (24) \cdot 3^4 \bmod (24) \cdot 3^2 \bmod (24)$.

$3^2 \bmod (24) = 9$
$3^4 \bmod (24) = 9$
$3^8 \bmod (24) = 9$
$3^{16} \bmod (24) = 9$
$3^{32} \bmod (24) = 9$
$3^{64} \bmod (24) = 9$
$3^{128} \bmod (24) = 9$
$3^{256} \bmod (24) = 9$
$3^{512} \bmod (24) = 9$
$3^{1024} \bmod (24) = 9$

$3^{2022} \bmod (24) = [9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9] \bmod 24$

$= [3^{16}] \bmod (24)$

$= 9 \bmod (24)$

$\boxed{3^{2022} \bmod (24) \equiv 9 \bmod (24)}$

c) $4^{99} \bmod (6)$

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$

$99 = 64 + 32 + 2 + 1$

$4^{99} = [\,4^{64} \cdot 4^{32} \cdot 4^{1} \cdot 4^{0}]$

$4^{99} \bmod (6) = [4^{64} \bmod (6) \cdot 4^{32} \bmod (6) \cdot 4^{1} \bmod (6) \cdot 4^{0} \bmod (6)$

$4^{0} \bmod 6 = 1$ $\quad 4^{4} \bmod (6) = 4$ $\quad 4^{32} \bmod (6) = 4$

$4^{1} \bmod 6 = 4$ $\quad 4^{8} \bmod (6) = 4$ $\quad 4^{64} \bmod (6) = 4$

$4^{2} \bmod 6 = 4$ $\quad 4^{16} \bmod (6) = 4$

$4^{99} \bmod 6 \equiv [4 \cdot 4 \cdot 4 \cdot 1] \bmod (6)$

$\equiv [64] \bmod (6)$

$4^{99} \bmod 6 \equiv \boxed{4 \bmod (6)}$

---

d) $101^{100^{99}} \bmod (7)$.

By Fermat's little theorem $a^{p-1} \equiv 1 \bmod (p)$.

we see $\gcd(101, 7) = 1$. notice $101^{6} \equiv 1 \bmod (7)$

Consider $100^{99} \pmod 6$, say we have $100^{99} \equiv n \pmod 6$

$100^{99} \equiv n \pmod 6$.

$\Rightarrow 100^{99} = n + 6K$

$\Rightarrow 101^{100^{99}} = 101^{n+6K} = 101^{n} \cdot 101^{6K}$

$\Rightarrow 101^{100^{99}} \equiv 101^{n} \cdot (1 \bmod (7))$

$101^{6K} \equiv 1^{K} \bmod (7)$

$\Rightarrow \equiv 1 \bmod (7)$

$\boxed{101^{100^{99}} \equiv 101^{n} \bmod (7) \Longrightarrow 101^{101^{99}} \equiv 101^{4} \bmod 7 \equiv 4 \bmod 7}$

$100^{99} \equiv n \pmod 6$ $\quad$ n answer between 0-5. so n=4

$100^{99} \bmod (6) \Rightarrow 4^{4} \bmod (6)$

$99 = 64 + 32 + 2 + 1$ $\quad 256 \bmod (6)$

$= 4 \bmod (6)$

$100 \bmod (6) = 4$

$100^{2} \bmod (6) = 4$

$100^{4} \bmod (6) = 4$

WTS: $\binom{p}{k} \equiv 0 \bmod(p)$. Question 7a)

given: $1 \leq k \leq p-1$.

Statement(hint) $p|n$, $r|n$, $p \nmid r$, then $pr|n$.

Pf: Let $n = p \cdot a$, $a \in \mathbb{Z}$ $n = r \cdot b$, $b \in \mathbb{Z}$

WTS $n = pr \cdot c$, $c \in \mathbb{Z}$.

$p|n = p \cdot a = r \cdot b$

$\Rightarrow p | r \cdot b$. P is a prime., then last function $p \nmid r$.

$\Rightarrow p | b$. I only have $p|b$ left.

So $b = p \cdot d$ for some $\in \mathbb{Z}$.

$n = r \cdot (p \cdot d)$

$n = pr \cdot d$, $d \in \mathbb{Z}$.

$\Rightarrow pr|n$. ▨

Fact: If $p|n$, $r|n$ and $p \nmid r$. then $pr|n$., Now Let $n = p!$ $r = k!(p-k)!$

$p|n = p!$, $k!(p-k)! | p!$ so $pr|n \Rightarrow p(k!(p-k)!) | p!$ from fact 2.

$p! = p(k!(p-k)!) \cdot c$, $c \in \mathbb{Z}$ $\Rightarrow \frac{p!}{k!(p-k)!} = p \cdot c$.

$\binom{p}{k} = p \cdot c$, $c \in \mathbb{Z}$ $\binom{p}{k} \equiv 0 \bmod(p)$.

b) Prove that for all integers x, y, $(x+y)^p \equiv x^p + y^p \bmod(p)$.

As Professor go over this question on lecture.
we need A binamial coefficients formula.

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \dots \binom{p}{p-1}xy^{p-1} + y^p$$

So

this term congrient .. 0 mod(p)

So $(x+y)^p = x^p + 0 + y^p \bmod p$

$\equiv x^p + y^p \bmod p$

c) Prove that for all integers x, $x^p \equiv x \bmod(p)$. By Professor proof

$x^p = (x-1+1)^p$

$x^p \equiv (x-1)^p + 1^p \bmod(p)$

Then By induction for hypotheis

$x^p \equiv (x-1) + 1 \bmod(p)$

$x \equiv x \bmod(p)$ □