

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 $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$$\text{when } x=0 \Rightarrow 0 \equiv 0 \pmod{9}$$

$$\text{when } x=1 \Rightarrow 1 \equiv 1 \pmod{9}$$

$$\text{when } x=2 \Rightarrow 4 \equiv 4 \pmod{9}$$

$$\text{when } x=3 \Rightarrow 9 \equiv 0 \pmod{9}$$

$$\text{when } x=4 \Rightarrow 16 \equiv 7 \pmod{9}$$

$$\text{when } x=5 \Rightarrow 25 \equiv 7 \pmod{9}$$

$$\text{when } x=6 \Rightarrow 36 \equiv 0 \pmod{9}$$

$$\text{when } x=7 \Rightarrow 49 \equiv 4 \pmod{9}$$

$$\text{when } x=8 \Rightarrow 64 \equiv 1 \pmod{9}$$

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

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

$$x^2 + y^2 \equiv 996 \pmod{9} \quad 996 \div 9 = 110 \dots 6$$

↑ remainder.

$$\Rightarrow x^2 + y^2 \equiv 6 \pmod{9}$$

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

$$\textcircled{1} \quad 0^2 + 0^2 \not\equiv 6$$

$$\textcircled{2} \quad 0^2 + 1^2 \not\equiv 6$$

$$\textcircled{3} \quad 0^2 + 4^2 \not\equiv 6$$

$$\textcircled{4} \quad 0^2 + 7^2 \not\equiv 6$$

$$\textcircled{5} \quad 0^2 + 0^2 \not\equiv 6$$

$$\textcircled{6} \quad 1^2 + 0^2 \not\equiv 6$$

$$\textcircled{7} \quad 4^2 + 0^2 \not\equiv 6$$

$$\textcircled{8} \quad 7^2 + 0^2 \not\equiv 6$$

$$\textcircled{9} \quad 4^2 + 4^2 \not\equiv 6$$

$$\textcircled{10} \quad 1^2 + 1^2 \not\equiv 6$$

$$\textcircled{11} \quad 7^2 + 7^2 \not\equiv 6$$

$$\textcircled{12} \quad 7^2 + 1^2 \not\equiv 6$$

....

when $x=0$.

$$y = 0, 1, 4, 7$$

when $y=0$

$$x = 0, 1, 4, 7$$

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

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

$n = a_r(a_{r-1} \dots a_1 a_0) = a_r 10^{r-1} + a_{r-1} 10^{r-2} + \dots + a_1 10 + a_0$.
be a base ten expansion of n . prove that n divisible by 9 if
and only if sum of the digits $a_r + a_{r-1} \dots + a_0$ is divisible by 9.

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

hint $10 \equiv 1 \pmod{9} \Rightarrow 10^k \equiv 1^k \equiv 1 \pmod{9}, \forall k \in \mathbb{N}$
 $\Rightarrow 10^k \equiv 1 \pmod{9}, \forall k \in \mathbb{N}$.

use professor's note proof.

We Have $10^k \equiv 1 \pmod{9}, \forall k \in \mathbb{N}$.

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

$$\Rightarrow a_r \cdot 10^{r-1} \equiv a_r \pmod{9}, a_{r-1} \cdot 10^{r-2} \equiv a_{r-1} \pmod{9}, \dots, a_1 \cdot 10 \equiv a_1 \pmod{9}, a_0 \equiv a_0 \pmod{9}$$

$$\Rightarrow a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \dots + a_1 \cdot 10 + a_0 \equiv a_r + a_{r-1} + \dots + a_1 + a_0 \pmod{9}$$

$$\Rightarrow n \equiv a_r + a_{r-1} + \dots + a_0$$

Thus, $n \equiv 0 \pmod{9} \iff a_r + a_{r-1} + \dots + a_0 \equiv 0 \pmod{9}$
 $\iff 9 | a_r + a_{r-1} + \dots + a_0 \blacksquare$

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

$$(a) 14x \equiv 6 \pmod{22}$$

The General solution x for $ax \equiv b \pmod{n}$ are $x = x_0 + \frac{\text{lcm}(a,b)}{a} \cdot n, n \in \mathbb{Z}$

Step 1: check if it's solvable.

$$\gcd(a,m) \Rightarrow \gcd(14, 22) = 2 \quad 2|16. \text{ It's solvable.}$$

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

so. we have $14x - 6 = 22 \Rightarrow 14x = 28 \Rightarrow x_0 = 2$
 $\Rightarrow x_0 = 2$ is a solution for $14x \equiv 6 \pmod{22}$

By Prop 1: the General solution are

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

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

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

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

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

$$b) 2021x \equiv 15 \pmod{47}$$

Step 1: Check if it's solvable

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

Problem 4. Find a multiplicative 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 $m=31$, $\gcd(8, 31) = 1$ | $1 1$ | 31 has solution. |
| ③ When $m=32$, $\gcd(8, 32) = 8$ | $8+1$ | so no solution. |
| ④ When $m=33$, $\gcd(8, 33) = 1$ | $1 1$ | 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 $8x \equiv 1 \pmod{31}$. Find the solution: $8x + 31y = 1$

$$\begin{aligned} 31 &= 3(8) + 7 & 1 &= 4(8) + 31(-1) \\ 8 &= 1(7) + 1 & 1 &= 8 - (31 - 3(8)) \\ 7 &= 7(1) + 0 & 1 &= 8 - 7 \end{aligned}$$

Second
part of answer.

$x=4$ is a solution for $8x \equiv 1 \pmod{31}$.
 4 is a multiplicative inverse of $8 \pmod{31}$.

For 33.

Solve for x $8x \equiv 1 \pmod{33}$. Find the solution. $8x + 33y = 1$

$$\begin{aligned} 33 &= 4(8) + 1 & 1 &= 33 + (-4)(8) \\ 8 &= 8(1) + 0. & 1 &= 33 - 4(8) \end{aligned}$$

Third.
part of Answer.

$x=-4$ is a solution for $8x \equiv 1 \pmod{33}$.

-4 is a multiplicative inverse of $8 \pmod{33}$.

By natural residues. $-4+32=29$. 29 is also Answer.

So 29 is a multiplicative inverse of $8 \pmod{33}$.

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 $\bar{b} \in \Phi(m)$.

$$\bar{a} \cdot \bar{b} = \bar{ab} = \bar{1}$$

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

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

$a \cdot b \equiv 1 \pmod{m}$. then by prop 1 $= \bar{ab} = \bar{1}$ or $\bar{a} \cdot \bar{b} = \bar{1}$ in $\Phi(m)$.

That is, 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 $\bar{a} \cdot \bar{b} = \bar{ab} = \bar{b} \cdot \bar{a} = \bar{1}$.

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 $\Phi(m)$ satisfy the 'cancelation 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

$$\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{b}_1 \Rightarrow ab \equiv ab_1 \pmod{m} \Rightarrow m \mid ab - ab_1$$

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

$$m \mid b - b_1 \text{ i.e. } b \equiv b_1 \pmod{m} \Rightarrow \bar{b} = \bar{b}_1 \quad \square$$

Class lecture & notes, proof by professor.

Problem 6.

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

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1024$$

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

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

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

$$5^2 \pmod{24} = 1 \quad 5^{32} \pmod{24} = 1 \quad 5^{512} \pmod{24} = 1$$

$$5^4 \pmod{24} = 1 \quad 5^{64} \pmod{24} = 1 \quad 5^{1024} \pmod{24} = 1$$

$$5^8 \pmod{24} = 1 \quad 5^{128} \pmod{24} = 1$$

$$5^{16} \pmod{24} = 1 \quad 5^{256} \pmod{24} = 1$$

$$\text{So } 5^{2022} \pmod{24} = [1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1] \pmod{24}.$$

$$= 1^8 \pmod{24}$$

$$\boxed{5^{2022} \pmod{24} = 1 \pmod{24}}$$

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

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1024$$

$$2^{11} = 2048$$

$$2^{12} = 4096$$

$$2^{13} = 8192$$

$$2^{14} = 16384$$

$$2^{15} = 32768$$

$$2^{16} = 65536$$

$$2^{17} = 131072$$

$$2^{18} = 262144$$

$$2^{19} = 524288$$

$$2^{20} = 1048576$$

$$2^{21} = 2097152$$

$$2^{22} = 4194304$$

$$2^{23} = 8388608$$

$$2^{24} = 16777216$$

$$2^{25} = 33554432$$

$$2^{26} = 67108864$$

$$2^{27} = 134217728$$

$$2^{28} = 268435456$$

$$2^{29} = 536870912$$

$$2^{30} = 1073741824$$

$$2^{31} = 2147483648$$

$$2^{32} = 4294967296$$

$$2^{33} = 8589934592$$

$$2^{34} = 17179869184$$

$$2^{35} = 34359738368$$

$$2^{36} = 68719476736$$

$$2^{37} = 137438953472$$

$$2^{38} = 274877906944$$

$$2^{39} = 549755813888$$

$$2^{40} = 1099511627776$$

$$2^{41} = 219902325552$$

$$2^{42} = 439804651104$$

$$2^{43} = 879609302208$$

$$2^{44} = 1759218604416$$

$$2^{45} = 3518437208832$$

$$2^{46} = 7036874417664$$

$$2^{47} = 14073748835328$$

$$2^{48} = 28147497670656$$

$$2^{49} = 56294995341312$$

$$2^{50} = 112589990682624$$

$$2^{51} = 225179981365248$$

$$2^{52} = 450359962730496$$

$$2^{53} = 900719925460992$$

$$2^{54} = 1801439850921984$$

$$2^{55} = 3602879701843968$$

$$2^{56} = 7205759403687936$$

$$2^{57} = 14411518807375872$$

$$2^{58} = 28823037614751744$$

$$2^{59} = 57646075229503488$$

$$2^{60} = 115292150459006976$$

$$2^{61} = 230584300918013952$$

$$2^{62} = 461168601836027904$$

$$2^{63} = 922337203672055808$$

$$2^{64} = 1844674407344111616$$

$$2^{65} = 3689348814688223232$$

$$2^{66} = 7378697629376446464$$

$$2^{67} = 14757395258752892928$$

$$2^{68} = 29514790517505785856$$

$$2^{69} = 59029581035011571712$$

$$2^{70} = 118059162070023143424$$

$$2^{71} = 236118324140046286848$$

$$2^{72} = 472236648280092573696$$

$$2^{73} = 944473296560185147392$$

$$2^{74} = 1888946593120370294784$$

$$2^{75} = 3777893186240740589568$$

$$2^{76} = 7555786372481481179136$$

$$2^{77} = 15111572744962962358272$$

$$2^{78} = 30223145489925924716544$$

$$2^{79} = 60446290979851849432088$$

$$2^{80} = 120892581959703698864176$$

$$2^{81} = 241785163919407397728352$$

$$2^{82} = 483570327838814795456704$$

$$2^{83} = 967140655677629590913408$$

$$2^{84} = 1934281311355259181826816$$

$$2^{85} = 3868562622710518363653632$$

$$2^{86} = 7737125245421036727307264$$

$$2^{87} = 15474250490842073454614528$$

$$2^{88} = 30948500981684146909229056$$

$$2^{89} = 61897001963368293818458112$$

$$2^{90} = 12379400392673658763691624$$

$$2^{91} = 24758800785347317527383248$$

$$2^{92} = 49517601570694635054766496$$

$$2^{93} = 99035203141389270109532992$$

$$2^{94} = 198070406282778540219065984$$

$$2^{95} = 396140812565557080438131968$$

$$2^{96} = 792281625131114160876263936$$

$$2^{97} = 1584563252262228321752527872$$

$$2^{98} = 3169126504524456643505055744$$

$$2^{99} = 6338253009048913287010111488$$

$$2^{100} = 12676506018097826574020222976$$

$$2^{101} = 25353012036195653148040445952$$

$$2^{102} = 50706024072391306296080891904$$

$$2^{103} = 101412048144782612592161783808$$

$$2^{104} = 202824096289565225184323567616$$

$$2^{105} = 405648192579130450368647135232$$

$$2^{106} = 811296385158260900737294270464$$

$$2^{107} = 1622592770316521801474588540928$$

$$2^{108} = 3245185540633043602949177081856$$

$$2^{109} = 6490371081266087205898354163712$$

$$2^{110} = 12980742162532174411796708327424$$

$$2^{111} = 25961484325064348823593416654848$$

$$2^{112} = 51922968650128697647186833309696$$

$$2^{113} = 103845937300257395294373666619392$$

$$2^{114} = 207691874600514790588747333238784$$

$$2^{115} = 415383749201029581177494666477568$$

$$2^{116} = 830767498402059162354989332955136$$

$$2^{117} = 1661534996804118324709898665910272$$

$$2^{118} = 3323069993608236649419797331820544$$

$$2^{119} = 6646139987216473298839594663641088$$

$$2^{120} = 1329227997443294659767918932728216$$

$$2^{121} = 2658455994886589319535837865456432$$

$$2^{122} = 5316911989773178639071675730912864$$

$$2^{123} = 10633823979546357278143351461825728$$

$$2^{124} = 21267647959092714556286702923651456$$

$$2^{125} = 42535295918185429112573405847302912$$

$$2^{126} = 85070591836370858225146811694605824$$

$$2^{127} = 17014118367274171645029362338921168$$

$$2^{128} = 34028236734548343290058724677842336$$

$$2^{129} = 68056473469096686580117449355684672$$

$$2^{130} = 13611294693819337316023489871136944$$

$$2^{131} = 27222589387638674632046979742273888$$

$$2^{132} = 54445178775277349264093959484547776$$

$$2^{133} = 10889035755055469852818791896909552$$

$$2^{134} = 21778071510110939705637583793819104$$

$$2^{135} = 43556143020221879411275167587638208$$

$$2^{136} = 87112286040443758822550335175276416$$

$$2^{137} = 174224572080887517645100670350552832$$

$$2^{138} = 348449144161775035290201340701105664$$

$$2^{139} = 696898288323550070580402681402211328$$

$$2^{140} = 1393796576647100141160805362804422656$$

$$2^{141} = 2787593153294200282321610725608845312$$

$$2^{142} = 5575186306588400564643221451217690624$$

$$2^{143} = 1115037261317680112928644290243538128$$

C) $4^{99} \text{ mod } 6$.

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$99 = 64 + 32 + 2 + 1$$

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

$$4^{\text{mod}(6)} = [4^{64 \text{ mod}(6)} \cdot 4^{32 \text{ mod}(6)} \cdot 4^1 \text{ mod}(6) \cdot 4^0 \text{ mod}(6)]$$

$$4^0 \text{ mod } 6 = 1$$

$$4^4 \text{ mod } 6 = 4$$

$$4^8 \text{ mod } 6 = 4$$

$$4^{16} \text{ mod } 6 = 4$$

$$4^{32} \text{ mod } 6 = 4$$

$$4^{64} \text{ mod } 6 = 4$$

$$4^{96} \text{ mod } 6 = 4$$

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

$$\equiv [64] \text{ mod}(6)$$

$$4^{99} \text{ mod } 6 \equiv \boxed{4 \text{ mod } 6}$$

d) $101^{100^{99}} \text{ mod } 7$.

By Fermat's little theorem
we see $\gcd(101, 7) = 1$. notice $101^6 \equiv 1 \text{ mod } 7$ $a^{p-1} \equiv 1 \text{ mod } (p)$.

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

$$100^{99} \equiv n \text{ mod } 6.$$

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

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

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

$$\boxed{101^{100^{99}} \equiv 101^n \text{ mod } 7} \Rightarrow 101^{100^{99}} \equiv 101^4 \text{ mod } 7 \equiv 4 \text{ mod } 7$$

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

$$100^{99} \text{ mod } 6 \Rightarrow 4^4 \text{ mod } 6$$

$$99 = 64 + 32 + 2 + 1 \equiv 2 \text{ mod } 6$$

$$100 \text{ mod } 6 = 4$$

$$100^2 \text{ mod } 6 = 4$$

$$100^4 \text{ mod } 6 = 4$$

WTS: $\binom{P}{k} \equiv 0 \pmod{P}$.

Question 7a).

Given: $1 \leq k \leq P-1$.

Statement(hint) $P \mid n, r \mid n, p \mid r$, then $p \mid n$.

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

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

$$P \mid n = P \cdot a = r \cdot b$$

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

$\Rightarrow P \mid b$. I only have $P \mid b$ left.

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

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

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

$\Rightarrow p \mid n$. \blacksquare

Fact: If $P \mid n, r \mid n$ and $p \mid r$. then $p \mid n$. Now let $n = P!$ $r = k!(P-k)!$

$P \mid n = P!, k!(P-k)! \mid P!$ so $p \mid n \Rightarrow P(k!(P-k)!) \mid P!$ from fact

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

$$(P) = P \cdot c, c \in \mathbb{Z}. \quad (P) \equiv 0 \pmod{P}$$

b) Prove that for all integers x, y , $(x+y)^P \equiv x^P + y^P \pmod{P}$.

As professor go over this question on lecture.

We need A binomial coefficients formula.

$$(x+y)^P = x^P + \underbrace{\binom{P}{1} x^{P-1} y + \binom{P}{2} x^{P-2} y^2 + \dots}_{\text{This term congruent } 0 \pmod{P}} + \dots + y^P$$

So $(x+y)^P \equiv x^P + 0 + y^P \pmod{P}$.

$$\begin{aligned} \text{So } (x+y)^P &= x^P + 0 + y^P \pmod{P} \\ &= x^P + y^P \pmod{P} \end{aligned}$$

c) Prove that for all integers x , $x^P \equiv x \pmod{P}$. By Professor proof.

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

$$x^P \equiv (x-1)^P + 1^P \pmod{P}$$

Then by induction for hypothesis

$$x^P \equiv (x-1) + 1 \pmod{P}$$

$$x \equiv x \pmod{P} \quad \square$$