Question 1. Compute the greatest Common divisor of the following steps.

a) 571 and -1127.

Based on A preperty of gcd: $\gcd(a,b) = \gcd(|a|,|b|)$

$\gcd(571, -1127) = \gcd(571, 1127)$. $a = 1127$, $b = 571$.

$$1127 = 1(571) + 556$$
$$571 = 1(556) + 15$$
$$556 = 37(15) + 1 \rightarrow \boxed{\gcd(571, -1127) = 1}$$
$$15 = 15(1) + 0$$

---

b) $\gcd(2112, 1024)$. , Let $a = 2112$, $b = 1024$

$$2112 = 2(1024) + 64 \rightarrow \boxed{\gcd(2112, 1024) = 64.}$$
$$1024 = 16(64) + 0$$

---

c) $\gcd(2^7 \times 3^5 \times 5^3 \times 7^2, 2^2 \times 3^3 \times 5^5 \times 7^7)$

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)}$$

Let $a = 2^7 \times 3^5 \times 5^3 \times 7^2$ $b = 2^2 \times 3^3 \times 5^5 \times 7^7$

$$\boxed{\begin{aligned} \gcd(a,b) &= 2^2 \times 3^3 \times 5^3 \times 7^2 \\ &= 4 \times 27 \times 125 \times 49 \\ &= 108 \times 125 \times 49 \\ &= 661{,}500 \end{aligned}}$$

Question 2: Let a, b and c be integer such that $c \mid ab$. If c is coprime with $\gcd(a,b)$, prove that c must divide $\text{lcm}[a,b]$.

pf: we have follow Given

$c \mid ab$ and $\gcd(c, \gcd(a,b)) = 1$.

set $c = x$, $\gcd(a,b) = y$ $\Rightarrow$ 假设(重写) $x = c$, $y = \gcd(a,b)$.

so we have $\gcd(x, y) = 1$.

we also know $\boxed{\text{Lcm}(a,b) = \frac{ab}{\gcd(a,b)}}$ → 公式，已成事实.

this $\Rightarrow$ $\gcd(a,b) \mid ab$

By def, 可行的

By the following, we have $x \mid ab$, $y \mid ab$.

By the Hw1 Question 8 proof.

$x \mid ab,\ y \mid ab \Rightarrow (x)(y) \mid ab$ → Hw1 Problem 8. proof it already. Lecture 3 Note.

Use the cancellation (e) from chapter 1. 可相除，相乘

If $d \mid n \Rightarrow ad \mid an$.

$(x)(y) \mid ab$

$\Rightarrow (x)(y)\left(\frac{1}{\gcd(a,b)}\right) \mid ab\left(\frac{1}{\gcd(a,b)}\right)$ But we know y is $\gcd(a,b)$.

$\Rightarrow (x)\left(\gcd(a,b) \cdot \frac{1}{\gcd(a,b)}\right) \mid ab \cdot \frac{1}{\gcd(a,b)}$

$\Rightarrow (x) \mid \frac{ab}{\gcd(a,b)}$

$\Rightarrow c \mid \text{lcm}(a,b)$ ▨

Question 3, Find General solution.

a). $571x - 1127y = 2$.

Step 1: Check if the equation have solution.
Base on Question 1 $\gcd(571, -1127)$, we know $1 | 2$, we have solution.

step 2: linear combination.

$1 = 556 - 37(15)$

$1 = 556 - 37(571 - 556)$

$1 = (1127 - 571) - 37(571 - 556)$

$1 = (1127 - 571) - 37(571 - (1127 - 571))$

$1 = (1127 - 571) - 37(2 \cdot (571) - 1127)$

$1 = (1127 - 571) - 74(571) + 37(1127)$

$1 = (1127 - 571)$

$1 = 38(1127) - 75(571)$

$2 = 76(1127) - 150(571)$

So $x_0 = -150$, $y_0 = -76$ is one solution.

Step 3: Consider the homogenous part $571x - 1127y = 0$

$$x = n \cdot \frac{\mathrm{Lcm}(571, -1127)}{571} = 1127 \cdot n \text{ for } \forall n \in \mathbb{Z}.$$

$$y = -n \cdot \frac{\mathrm{Lcm}(571, -1127)}{-1127} = n \cdot \frac{\mathrm{Lcm}(571, -1127)}{1127} = 571 \cdot n \text{ for } \forall n \in \mathbb{Z}.$$

$$\boxed{\begin{aligned} x &= -150 + 1127(n) \\ y &= -76 + 571(n), \end{aligned} \quad \forall n \in \mathbb{Z}.}$$

is the general solution of $571x - 1127y = 2$.

b) $2022x + 27y = 2019$.

Step 1: Check if the equation have solution.

Let $a = 2022$, $b = 27$. $3 \mid 2019$, so we have solution.

$$2022 = 74(27) + 24$$
$$27 = 1(24) + 3$$
$$24 = 8(3) + 0.$$

Step 2: linear Combination.

$$3 = 27 - 24$$
$$3 = 27 - (2022 - 74(27))$$
$$3 = -2022 + 75(27)$$
$$3 = (-1)(2022) + (75)(27)$$
$$2019 = (-673)(2022) + (50475)(27)$$

$$\boxed{\begin{aligned} &\mathrm{Lcm}(2022, 27) \\ &= \frac{2022 \cdot 27}{3} \\ &= 18198 \end{aligned}}$$

is one solution.

so $x_0 = -673$, $y_0 = 50475$ is one solution.

Step 3: Consider the homogenous part. $2022x + 27y = 0$.

$$x = n \cdot \frac{\mathrm{Lcm}(2022, 27)}{2022} = n \cdot \frac{18198}{2022} = 9n \quad \forall n \in \mathbb{Z}.$$

$$y = -n \cdot \frac{\mathrm{Lcm}(2022, 27)}{27} = -n \frac{18198}{27} = -674n \quad \forall n \in \mathbb{Z}.$$

$$\boxed{\begin{aligned} x &= -673 + 9n \quad \forall n \in \mathbb{Z}. \\ y &= 50475 - 674n \end{aligned}}$$

is the general solution of $2022x + 27y = 2019$

Question 4.

a) a and b are coprime if and only if they have no common prime factors.

By Lecture 5 Fact 3. two integers are coprime if and only if both of them have no common prime factors.

if part.

"$\Rightarrow$"

we know $a, b \in \mathbb{Z}$ and $\gcd(a,b)=1$.

suppose p is prime and $p|a, p|b$. By def of gcd,

$p | \gcd(a,b) = 1$. This is a Contraduction.

so a and b have no common prime divisors. $\blacksquare$

only if part

"$\Leftarrow$"

suppose $\gcd(a,b) = d > 1$, then by FTA,

$\exists$ prime p such that $p|d$, But $d|a$ and $d|b \Rightarrow p|a, p|b$.

we see p is common prime factor. This is a Contraduction.

so $\gcd(a,b) = 1$, we see a and b are coprime. $\blacksquare$

b) If a and b are coprime, then a^n and b^m are also coprime.

Pf: If a and b are coprime, then by def. $\gcd(a,b)=1$.

we want to show: $\gcd(a^n, b^m) = 1$.

First, Let us Assume $d = \gcd(a^n, b^m)$ instead of 1.

By lecture 3, Coro 3, we rewrite $d = \gcd(a^n, b^m)$

$$a^n = d \cdot a_1 \qquad b^m = d \cdot b_1 \text{ where } a_1, b_1 \in \mathbb{Z}$$

but this also show that $d | a^n$, $d | b^m$.

$\Rightarrow d | a^n$ and $d | b^m$ $\longrightarrow$ Example: $316^2 = 3136$

Let $n=2$. $= 316$

$\Rightarrow d | a$ and $d | b$ $\longrightarrow$

we got d is the common divisor of a and b,

we also know that a and b are coprime, $\gcd(a,b)=1$.

$\gcd(a,b) = 1 \Longrightarrow d = 1$.

we get

$\gcd(a^n, b^m) = 1$, this show a^n and b^m are coprime

Question 5.

5a). In the set of natural residues module 2022. how many element are coprime with 2022?

$n = 2022. = 2^1 \cdot 3^1 \cdot 337^1$

Use product formula: $\phi(n) = n \cdot (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$

$$\phi(2022) = 2022(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{337})$$

$$= 2022 (\frac{1}{2})(\frac{2}{3})(\frac{336}{337})$$

$$= 2022 \cdot \frac{112}{337}$$

$$= 6 \cdot 112$$

$$= 672$$

5b). How many positive divisor does 2016 have? and what is the sum of them?

$$\boxed{\begin{aligned}2016 &= 2^5 \cdot 63 \\ &= 2^5 \cdot 3^2 \cdot 7^1\end{aligned}}$$

positive divisor.

$\sigma_0(n) = (e_1+1)(e_2+1)(e_3+1) \ldots (e_r+1)$

$= (5+1)(2+1)(1+1)$

$= 6 \cdot 3 \cdot 2$

$= 18 \cdot 2$

$\boxed{= 36}$ ← positive divisor

$p_1 = 2, \ e_1 = 5$

$p_2 = 3, \ e_2 = 2$

$p_3 = 7, \ e_3 = 1$

Sum of them.

$\sigma_1(n) = \dfrac{p^{e+1} - 1}{p - 1}$

$= \sigma_1(2^5) \cdot \sigma_1(3^2) \cdot \sigma_1(7^1)$

$= \left(\dfrac{2^6-1}{2-1}\right) \cdot \left(\dfrac{3^3-1}{3-1}\right) \cdot \left(\dfrac{7^2-1}{7-1}\right)$

$= 63 \cdot 13 \cdot 8$

$\boxed{= 6552}$ ← sum of them.

Question 6a.

Let n and d be two natural number.

Let p be a prime number that does not divide n.

pf: we already know p be a prime number and doesn't divide n.

so. also mean $\gcd(P, n) = 1$.

if part "$\Longrightarrow$"

we have n and d are coprime, $\gcd(n, d) = 1$.

we also have $\gcd(p, n) = 1$.

so Assume by controdiction that $\gcd(p, nd) = X$ and $d \neq 1$.

since $X | p$ and $X | nd$, so $d | p(x) + nd(y)$

Base on Corol.

$\gcd(d, n) = d(x_0) + n(y_0) = 1$ for some $x_0, y_0 \in \mathbb{Z}$

$\gcd(p, n) = P(x_1) + n(y_1) = 1$ for some $x_1, y_1 \in \mathbb{Z}$

multiply second $\gcd(p, n)$ by d, so $d = P(d)(x_1) + n(d)(y_1)$

plug into the first equation.

$\Longrightarrow P(d)(x_1)(x_0) + (n)(d)(x_1)(x_0) + n(y_0) = 1$

$\Longrightarrow (pd)(x_1 x_0) + (n)(d x_1 x_0 + y_0) = 1$

By Bezout Lemma. if $X | pd$ and $X | n$, then $X | 1$

we have $\gcd(n, pd) = 1$

Next if only part.

if only "$\Longrightarrow$"

We have $\gcd(n, pd) = 1$ and $\gcd(p, n) = 1$

so Assume by controdiction that $\gcd(n, d) = D$ and $D \neq 1$.

since $D \mid n$ $D \mid d$, so $D \mid n(x) + d(y)$.

Base on corol.

$$\gcd(n, pd) = n(x_0) + pd(y_0) = 1 \text{ for some } x_0, y_0 \in \mathbb{Z}$$

$$\gcd(n, p) = n(x_1) + p(y_1) = 1 \text{ for some } x_1\ y_1 \in \mathbb{Z}.$$

multiply second $\gcd(n,p)$ by d, $\Rightarrow d = nd(x_1) + pd(y_1)$

plug into the first equation.

$$n(x_0) + pd(y_0) = 1$$

$$\Rightarrow n(x_0) + p(nd(x_1) + pd(y_1))(y_0) = 1$$

$$\Rightarrow n(x_0) + d(pn(x_1)(y_0) + p^2(y_1)(y_0)) = 1$$

By Bezout lemma. If $D \mid n$, $D \mid d$, then $D \mid 1$.

we have $\gcd(n, d) = 1$

Finish Both if and only if.

6b). Among the sequence of integer
3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51
54, 57, 60, How manyof them are coprime with 20?

Coprime: $\gcd(a,b) = 1$, we have $b = 20$., $\gcd(a, 20) = 1$. coprime.

$$\left.\begin{array}{l} \gcd(3,20)=1 \\ \gcd(9,20)=1 \\ \gcd(21,20)=1 \\ \gcd(27,20)=1 \\ \gcd(33,20)=1 \\ \gcd(39,20)=1 \\ \gcd(51,20)=1 \\ \gcd(57,20)=1 \end{array}\right\}$$

we have 8 number that are coprime with 20.

Question 7

a) $f(x) = \sin(x)$, $x \in \mathbb{R}$ is an arithmetical function.

$\boxed{\text{x shoud } x \in \mathbb{N}}$

False, Because no matter what you do, x shoud $x \in \mathbb{N}$

By the def of arithmetical function

A function $f: \mathbb{N} \to \mathbb{R}$ or $\mathbb{C}$. So in this case

$x \in \mathbb{R}$, which is not correct, x shoud $x \in \mathbb{N}$.

b) $f(n) = (-3)^n$ is multiplicate arithmetal function.

False, use An example in class lecture.

$m = 2$, $n = 5$. $\gcd(2,5) = 1$, but

$f(m \cdot n) = f(10) = (-3)^{10} = 59049$

$f(m) \cdot f(n) = (-3)^2 \cdot (-3)^5 = 9 \cdot -243 = -2187$

$f(m \cdot n) \neq f(m) \cdot f(n)$, so it's not multiplicate

c) The Euler's toient function ϕ is a multiplicate arithmetical function

Yes, it's true, Based on Lecture 5 prop 6.

Question 8.

a) $2019^{10} \pmod{2022}$

$2019 \equiv -3 \pmod{2022}$

$(2019)^{10} \equiv (-3)^{10} \pmod{2022}$

$(-3)^{10} \Rightarrow (-1)^{10}(3)^{10} = 59049$

$59049 \equiv 411 \bmod (2022)$

By transitivy. $\boxed{2019^{10} \equiv 411 \bmod (2022) \quad \text{the answer is } 411}$

b) $3^{1000} \pmod 7$

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

$1000 = 512 + 256 + 128 + 64 + 32 + 8$

$3^{1000} = (3^{512} \cdot 3^{256} \cdot 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^{8})$

$3^{1000} \bmod 7 = [(3^{512} \bmod 7) \cdot (3^{256} \bmod 7)(3^{128} \bmod 7)(3^{64} \bmod 7)$
$(3^{32} \bmod 7) \cdot (3^{8} \bmod 7)] \bmod 7$

$(3^4 \bmod 7 \cdot 3^4 \bmod 7) \bmod 7 = 2$

$3^2 \bmod 7 = 2$
$3^4 \bmod 7 = 4$
$3^8 \bmod 7 = 2$
$3^{16} \bmod 7 = 4$
$3^{32} \bmod 7 = 2$
$3^{64} \bmod 7 = 4$
$3^{128} \bmod 7 = 2$
$3^{256} \bmod 7 = 4$
$3^{512} \bmod 7 = 2$

$3^{1000} \bmod 7 = [2 \cdot 4 \cdot 2 \cdot 4 \cdot 2 \cdot 2] \bmod 7$
$= 4^4 \bmod 7$
$= 256 \bmod 7$
$= 4$

$\boxed{3^{1000} \bmod 7 \equiv 4 \bmod 7}$