**Problem 1.** (10pts) Does the following Diophantine equation

$$20x + 10y = 65.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

**Theorem 4.10**

The Diophantine equation

$$c = ax + by$$

has integer solutions if and only if $\gcd(a,b)|c$.
If $\gcd(a,b)|c$, then one *particular* solution $(x_0, y_0)$ is given by Euclid's extended algorithm. Let $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$. Then *all* integer solutions to the equation are

$$(x_0 + nb', y_0 - na'), \ n \in \mathbb{Z}.$$

First we calculate the greatest common divisor using the Euclidean algorithm:

**Definition 4.6** (Euclidean algorithm)

Let $a, b \in \mathbb{Z}$.

- Let $r = a - qb$ be the remainder of $a$ modulo $b$.
- Then $\gcd(a,b) = \gcd(r,b) = \gcd(b,r)$.
- $\gcd(b,0) = b$ for all integers $b \neq 0$.

This gives an *algorithm* for computing the greatest common divisor

$$\gcd(a,b)$$

of two numbers $a \geq b$ in $O(\log a)$ steps.

The Diophantine equation: 20x + 10y = 65
20 = 1 x 10 + 10
10 = 10 x 1 + 0
The greatest common divisor is the last non-zero remainder: gcd(20, 10) = 10
Since 65 is not divisble by gcd(20,10) = 10
**=> The Diophantine equation 20x + 10y = 65 does not have any solutions x, y ∈ N. (answer)**

**Problem 2.** (10pts) Does the following Diophantine equation

$$20x + 16y = 500.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

The Diophantine equation: 20x + 16y = 500
20 = 1 x 16 + 4
16 = 4 x 4 + 0
The greatest common divisor is the last non-zero remainder: gcd(20, 16) = 4
Since 500 is divisble by gcd(20,16) = 4
**=> The Diophantine equation 20x + 16y = 500 has solutions x, y ∈ N. (answer)**
All of the solutions of this Diophantine equation are:

### 4.2.3 Linear Diophantine equations in two variables

An equation where the variables are integer valued is called a *Diophantine* equation. The extended Euclidean algorithm gives a solution $(x_B, y_B)$ to the Diophantine equation

$$\gcd(a, b) = ax + by.$$

The integers $(x_B, y_B)$ are the *Bézout coefficients* of $a$ and $b$:

$$\gcd(a, b) = ax_B + by_B.$$

If $\gcd(a, b)|c$, then the pair

$$(x_0, y_0) = \frac{c}{\gcd(a, b)}(x_B, y_B)$$

**Theorem 4.10**

The Diophantine equation

$$c = ax + by$$

has integer solutions if and only if $\gcd(a, b)|c$.
If $\gcd(a, b)|c$, then one *particular* solution $(x_0, y_0)$ is given by Euclid's extended algorithm. Let $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$. Then *all* integer solutions to the equation are

$$(x_0 + nb', y_0 - na'), \ n \in \mathbb{Z}.$$

The Bezout coefficients of a and b are:
gcd(20, 16) = 20 x (1) + 16 x (-1) = 4 => $(x_B, y_B)$ = (1, -1)
The particular solution $(x_0, y_0)$ = c/gcd(a,b) * $(x_B, y_B)$ = 500/4 * (1, -1) = (125, -125)
We have: a' = a/gcd(a,b) = 20/gcd(20, 16) = 20/4 = 5
b' = b/gcd(a,b) = 16/gcd(20, 16) = 16/4 = 4
All integer solutions to the equation are therefore:
$(x_o$ + nb', $y_0$-na') = (125 + 4n, -125 - 5n), n ∈ Z
Since the solutions are strictly natural numbers, we have to ensure that:
125 + 4n >= 0 => 4n >= -125 => n >= -31.25
-125 - 5n >= 0 => 5n <= -125 => n <= -25
With the condition n ∈ Z, all possible values of n are therefore
n = [-25, -26, -27, -28, -29, -30, -31]

Plugging n into ($x_o$ + nb', $y_0$-na') = (125 + 4n,  -125 - 5n), we have all possible natural number solutions as:
n = -25, (x, y) = (25, 0)
n = -26, (x, y) = (21, 5)
n = -27, (x, y) = (17, 10)
n = -28, (x, y) = (13, 15)
n = -29, (x, y) = (9, 20)
n = -30, (x, y) = (5, 25)
n=  -31, (x, y) = (1, 30)
**(answer)**
**----------------------------------------------------------------------------------------------------------**

**Problem 3.** (10pts) How many integers less than 22220 are relatively prime to 22220?

If $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$. (Proof omitted.) Thus,

$$\varphi(p_1^{k_1} \cdots p_r^{k_r}) = (p_1 - 1) \cdots (p_r - r) \cdot p_1^{k_1 - 1} \cdots p_r^{k_r - 1}$$

First we need to calculate the prime factorization of 22220
22220 = 2 x 11110 = 2 x 2 x 5555 = 2 x 2 x 5 x 1111 = $2^2$ x 5 x 11 x 101
The totient of 22220, thus, would be
$\varphi(22220) = (2 - 1)2^1 \text{ x } (5 - 1) \text{ x } (11 - 1) \text{ x } (101 - 1) = 8000$
The totient of the natural number n is the number of coprimes with regards to n and less than n
**=> There are 8000 integers less than 22220 that are relatively prime to 22220 (answer)**
**----------------------------------------------------------------------------------------------------------**

**Problem 4.** (10pts) Compute the last two digits of $2022^{2022}$.

The last two digits can be found by modulo 100. Therefore, we need to compute:
$2022^{2022}$ mod 100
The modular exponentiation property is:

**A^B mod C = ( (A mod C)^B ) mod C**

=> $2022^{2022}$ mod 100 = ((2022 mod 100)$^{2022}$) mod 100
=> $2022^{2022}$ mod 100 = $22^{2022}$ mod 100
The modular multiplication property is:

(A * B) mod C = (A mod C * B mod C) mod C

=> $2022^{2022}$ mod 100 = ($11^{2022}$ x $2^{2022}$) mod 100
= ($11^{2022}$ mod 100 x $2^{2022}$ mod 100) mod 100 (*)

**Theorem 4.33** (Euler's theorem)

Let $n \in \mathbb{N}$, and $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \mod n$.

Since gcd(11,100) = 1 => $11^{\varphi(100)} \equiv 1$ mod 100 => $11^{40}$ = 1 mod 100 or $11^{40}$ mod 100 = 1

- First, $11^{2022}$ mod 100 = $((11^{40})^{50} \times 11^{22})$ mod 100
= $((11^{40})^{50}$ mod 100 x $(11^{2})^{11}$ mod 100) mod 100 (modular multiplication)
= $((11^{40}$ mod $100)^{50}$ mod 100 x $(11^{2}$ mod $100)^{11}$ mod 100) mod 100
(modular exponentiation)
= $((1^{50})$ mod 100 x $(21)^{11}$ mod 100) mod 100
= (1 x $((21^{2}$ mod $100)^{5}$ x (21 mod 100))) mod 100
= ((441 mod $100)^{5}$ x 21) mod 100 = (1 x 21) mod 100 = 21

- Secondly, we know that exponentiation is cyclic. For 2, the cycle is 2 x 10^n when it cycles in the last (n -1) digits. In other words:

$2^{2k + n} \equiv 2^{n}$ mod 10
$2^{20k + n} \equiv 2^{n}$ mod 100
$2^{200k + n} \equiv 2^{n}$ mod 1000
and so on. Now, we compute $2^{2022}$ mod 100
$2^{2022}$ mod 100 = $2^{20 \times 101 + 2}$ mod 100 = $2^{2}$ mod 100 = 4

- Finally, from (*) we have:

$2022^{2022}$ mod 100 = ($11^{2022}$ mod 100 x $2^{2022}$ mod 100) mod 100 = (4 x 21) mod 100
= 84 mod 100 = 84

**Answer: The last two digits of $2022^{2022}$ is 84**