Ilana Sivan
205634272
Honors Course
Homework 4

Question 1

Compute $\gcd(210, 588)$ two different ways: by using Euclid's algorithm, and by finding the factorization of each number.

First we will compute with factorization:

- The factorization of 210 is:
  - $5 * 6 * 7$, where we can further break down 6,6 $= 2 * 3$, so we have $2 * 3 * 5 * 7$, but our greatest total here are $5 * 6 * 7$
- The factorization of 588 is:
  - $2 * 6 * 49$, where we can further break down 49,49 $= 7 * 7$ or 7^2, for $2 * 6 * 7 * 7$and we can again break down our 6,6 $= 2 * 3$ so we have $2 * 2 * 3 * 7 * 7$, but our greatest total here are $2 * 6 * 7^2$

So the greatest common divisors between 210 and 588 are 6 and 7, so we have $6 * 7 = 42$. So our greatest common divisor between the two is **42**.

Now we will compute with Euclid's algorithm:

In Euclid's algorithm, we divide the greatest value by the smallest value and find the remainder, then we use the remainder and the divisor of the division to find the greatest divisor.

- Divide the greatest value by the smallest:
  - $$\begin{array}{r|c} & 2 \\ \cline{2-2} 210 & 588 \\ & -\ 420 \\ \cline{2-2} & 168 \end{array}$$
- Divide the greatest value by the smallest:
  - $$\begin{array}{r|c} & 1 \\ \cline{2-2} 168 & 210 \\ & -\ 168 \\ \cline{2-2} & 42 \end{array}$$

- Divide the greatest value by the smallest:

$$
\begin{array}{r|l}
 & \quad 4 \\
\hline
42 & \ 168 \\
 & - 168 \\
\hline
 & \quad 0
\end{array}
$$

$\gcd(210, 588) = \gcd(210, 168) = \gcd(168, 42) = \gcd(42, 0) = 42$

Question 2

The Fibonacci numbers $\mathrm{F_0}, \mathrm{F_1}, \mathrm{F_2}, \ldots$ are defined by the rule:
$\mathrm{F_0} = 0$, $\mathrm{F_1} = 1$, $\mathrm{F_n} = \mathrm{F_{n-1}} + \mathrm{F_{n-2}}$
Prove that for all $n \geq 1$, $\gcd(\mathrm{F_{n-1}}, \mathrm{F_n}) = 1$

We will prove by induction.
Base case: $\mathrm{F_1} = 1$ and $\mathrm{F_2} = 1$, so clearly $\gcd(\mathrm{F_1}, \mathrm{F_2}) = 1$.

Induction hypothesis: Let $\gcd(\mathrm{F_{n-1}}, \mathrm{F_n}) = 1$.

Induction step: We will show that $\gcd(\mathrm{F_n}, \mathrm{F_{n+1}}) = 1$. We know from Euclid's

algorirthm that $\gcd(\mathrm{a}, \mathrm{a} + \mathrm{b}) = \gcd(\mathrm{a}, \mathrm{b})$. We also know that any number x that divides both a and b ($\mathrm{a} = \mathrm{ux}, \mathrm{b} = \mathrm{vx}$) must also divide $\mathrm{a} + \mathrm{b}$ ($\mathrm{a} + \mathrm{b} = (\mathrm{u} + \mathrm{v})\mathrm{x}$).

Similarly, any number xthat a, and $\mathrm{a} + \mathrm{b}$, where $\mathrm{a} = \mathrm{wx}$, and $\mathrm{a} + \mathrm{b} = \mathrm{tx}$, also divides b, where $\mathrm{b} = (\mathrm{t} - \mathrm{w})\mathrm{x}$.

Therefore, we can represent $\gcd(\mathrm{F_n}, \mathrm{F_{n+1}}) = \gcd(\mathrm{F_n}, \mathrm{F_n} + \mathrm{F_{n-1}}) = \gcd(\mathrm{F_n}, \mathrm{F_{n-1}}) = 1$, where the final step is our induction hypothesis, so our hypothesis holds.

Question 3

Answer the following questions:

a. If p is prime, how many elements of $\{0, 1, ..., \mathrm{p^n} - 1\}$ have an inverse modulo p^n?

We know from the definition of our set$\{0, 1, ..., \mathrm{p^n} - 1\}$ that we exclude all the numbers which are multiples of p. In fact, since p is a prime, all elements in the range that are not a multiple of p have an inverse of $\mathrm{modp^n}$. As $\mathrm{gcd(xp, p^n)}$ for an xwhich is $0 \le \mathrm{x} \le \mathrm{p} - 1$. We can see that $0 \le \mathrm{x} \le \mathrm{p} - 1 \ne 1$, since pis the common divisor. Similarly, for $\mathrm{x, i} \in \mathbb{Z}$, if we have $\mathrm{xp + i}$, we have $\mathrm{gcd(xp + i, p^n) = 1}$, as p is not a divisor of $\mathrm{xp + i}$, but it is the only prime divisor of $\mathrm{p^n}$, the numbers in the set which are multiples of p are $\mathrm{p^{n-1}}$,and numbers which have an inverse are of the form $\mathrm{p^n - p^{n-1}}$.

b. Find the inverse of: 20 mod 79, 3 mod 62, 21 mod 91, 5 mod 23.

A modular multiplicative inverse of an integer a is an integer x such that $\mathrm{a * x}$ is congruent to 1 modular some modulus m. To write it in a formal way: we want to find an integer x so that $\mathrm{a * x \equiv 1mod}m$. We will also denote x simply with $\mathrm{a^{-1}}$. If a modular inverse exists then it is unique.

$20\mathrm{mod}79$:

Our equation here is $20 * \mathrm{x} = 1(\mathrm{mod}79)$, as the value of $1\mathrm{mod}79 = 80$, we need to find the x that solves for $20 * x = 80$.
$\frac{80}{20} = 4$, and indeed we get:
$4 \equiv 20^{-1}(\mathrm{mod}79)$
$4 * 20 \equiv 1(\mathrm{mod}79)$

$3\mathrm{mod}62$:

Our equation here is $3 * \mathrm{x} = 1(\mathrm{mod}62)$, as the value of $1\mathrm{mod}62 = 63$, we need to find the x that solves for $3 * x = 63$.
$\frac{63}{3} = 21$, and indeed we get:
$21 \equiv 3^{-1}(\mathrm{mod}62)$
$21 * 3 \equiv 1(\mathrm{mod}62)$

$21\mathrm{mod}91$:

This equation has no solution because 21 and 91 aren't coprime.
$\mathrm{gcd}(21, 91) = 7$

5mod23 :

Our equation here is $5 * \mathrm{x} = 1(\mathrm{mod}23)$, as the value of $1\mathrm{mod}23 = 24$, we need to find the x that solves for this.

$\mathrm{x} = 14$
$14 \equiv 5^{-1}(\mathrm{mod}23)$
$14 * 5 \equiv 1(\mathrm{mod}23)$

Question 4

Determine necessary and sufficient conditions on x, N so that the following holds: for any a, b, if $\mathrm{ax} \equiv \mathrm{bxmodN}$, then $\mathrm{a} \equiv \mathrm{bmodN}$.

Necessity and sufficiency are terms used to describe a conditional or implicational relationship between two statements.

$\mathrm{ax} \equiv \mathrm{bx}(\mathrm{modN}) \Rightarrow \mathrm{N}|(\mathrm{a}-\mathrm{b})\mathrm{x}$: N divides $(\mathrm{a}-\mathrm{b})\mathrm{x}$
$\mathrm{a} \equiv \mathrm{b}(\mathrm{modN}) \Rightarrow \mathrm{N}|(\mathrm{a}-\mathrm{b})$: N divides $(\mathrm{a}-\mathrm{b})$

Here, N must divide $(\mathrm{a}-\mathrm{b})\mathrm{x}$ and $(\mathrm{a}-\mathrm{b})$, therefore, we need an x st. $\gcd(\mathrm{N}, \mathrm{x}) = 1$. With $\gcd(\mathrm{N}, \mathrm{x}) = 1$, we have $(\mathrm{a}-\mathrm{b})\mathrm{x}$ which is divisible by N, so $(\mathrm{a}-\mathrm{b})$ must be as well.

Question 5

Choose your favorite programming language and implement in it:

a. Euclid's algorithm for input $n \in N$ of arbitrary length

b. Euclid's extended algorithm for input $n \in N$ of arbitrary length

I have provided the answers in separate files. Thank you.