AFRICAN INSTITUTE FOR MATHEMATICAL SCIENCES

(AIMS RWANDA, KIGALI)

Name: Darix SAMANI SIEWE Assignment Number: 1
Course: Algebra and Cryptography Date: March 1, 2025

Exercise 1

1. Prove that 13 divides $2^{70} + 3^{70}$.

   We are tasked with proving that 13 divides $2^{70} + 3^{70}$. In other words, we need to show:

   $2^{70} + 3^{70} \equiv 0 \pmod{13}$

   using the Fermat's little theorem :

   Fermat's Little Theorem tells us that if p is a prime and a is an integer not divisible by p, then:

   $a^{p-1} \equiv 1 \pmod{p}$

   For $p = 13$, Fermat's Little Theorem tells us that for any integer a not divisible by 13:

   $a^{12} \equiv 1 \pmod{13}$

   Thus, we can use this to simplify powers of 2 and 3 modulo 13.

   Simplify the exponents modulo 12

   Since $2^{12} \equiv 1 \pmod{13}$ and $3^{12} \equiv 1 \pmod{13}$, we can reduce the exponent 70 modulo 12:

   $70 \div 12 = 5$ remainder 10

   Thus:

   $2^{70} \equiv 2^{10} \pmod{13} \quad \text{and} \quad 3^{70}$

2. Compute $pgcd(2^a - 1, 2^b - 1)$ for any a and b natural numbers.

   we can find this using the proprieties that $pgcd(x, y) = pgcd(y, x \mod y)$ Specifically, we need to show that if $a = bq + r$, then $(2^a - 1)$ has a remainder related to $(2^r - 1)$ when divided by $(2^b - 1)$.

   Suppose $a = bq + r$, where $0 \leq r < b$. Then,

$$\begin{aligned} 2^a - 1 &= 2^{bq+r} - 1 \\ &= 2^{bq} \cdot 2^r - 1 \\ &= (2^{bq} - 1) \cdot 2^r + (2^r - 1) \end{aligned}$$

Since $2^b - 1$ divides $2^{bq} - 1$, we have that when $2^a - 1$ is divided by $2^b - 1$, the remainder is $2^r - 1$. This implies:

$$\text{pgcd}(2^a - 1, 2^b - 1) = \text{pgcd}(2^b - 1, 2^r - 1)$$

using the euclidean algorithm we have : Thus, we have

$$\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$$

We are tasked with finding the greatest common divisor (gcd) of $9n+4$ and $2n-1$ for any natural number n. We will use the Euclidean algorithm to compute$\gcd(9n+4, 2n-1)$.

3. Evaluate $gcd(9n + 4, 2n - 1)$ where n is a natural number.

   $\gcd(9n + 4, 2n - 1) = \gcd(2n - 1, (9n + 4) \mod (2n - 1))$

   Divide $9n + 4$ by $2n - 1$

   We divide $9n + 4$ by $2n - 1$: $\frac{9n+4}{2n-1}$

   First, divide the leading term of $9n$ by the leading term of $2n$:

   $\frac{9n}{2n} = \frac{9}{2}$

   Thus, the quotient is 4. Now, multiply 4 by $2n - 1$:

   $4 \times (2n - 1) = 8n - 4$

   Subtract this from $9n + 4$:

   $(9n + 4) - (8n - 4) = n + 8$

   Thus, we have the following.

   $9n + 4 = (2n - 1) \times 4 + (n + 8)$

   So:

   $9n + 4 \mod (2n - 1) = n + 8$

   Apply the Euclidean Algorithm again

   Now, we compute $\gcd(2n - 1, n + 8)$. We divide $2n - 1$ by $n + 8$: $\frac{2n-1}{n+8}$

   Divide the leading term of $2n$ by the leading term of n:

   $\frac{2n}{n} = 2$

   Multiply 2 by $n + 8$:

   $2 \times (n + 8) = 2n + 16$

   Subtract this from $2n - 1$:

   $(2n - 1) - (2n + 16) = -17$

So:

$2n - 1 = (n + 8) \times 2 + (-17)$

Thus:

$2n - 1 \mod (n + 8) = -17$

Now, we compute $\gcd(n + 8, -17)$. Since the gcd of a number and its negative is the same, we have:

$\gcd(n + 8, 17)$

Since 17 is prime, the gcd depends on whether $n + 8$ is divisible by 17. Therefore:

$\gcd(n + 8, 17) = \begin{cases} 1 & \text{if } n + 8 \text{ is not divisible by } 17 \\ 17 & \text{if } n + 8 \text{ is divisible by } 17 \end{cases}$

Thus, the gcd of $9n + 4$ and $2n - 1$ is:

$\gcd(9n + 4, 2n - 1) = \begin{cases} 1 & \text{if } n + 8 \text{ is not divisible by } 17 \\ 17 & \text{if } n + 8 \text{ is divisible by } 17 \end{cases}$

4. Let n be a natural number. Show that if $2^n + 1$ is a prime number, the integer n must be a power of 2. Prove by a counterexample that the converse is false.

   - Part 1: Let n be a natural number. Show that if $2^n + 1$ is a prime number, the integer n must be a power of 2.
     let's proof by Contraposition:
     We are tasked with proving the statement:

     $$\text{If } 2^n + 1 \text{ is a prime number, then } n \text{ must be a power of 2.}$$

     The contrapositive of this statement is:

     $$\text{If } n \text{ is not a power of 2, then } 2^n + 1 \text{ is not a prime number.}$$

     We will prove this contrapositive.
     Let n be a natural number, and assume that n is **not** a power of 2. We aim to show that $2^n + 1$ is not a prime number in this case.
     Since n is not a power of 2, we can express n as:

     $$n = 2^k \cdot m \quad \text{where} \quad k \geq 1 \quad \text{and} \quad m \geq 2 \quad \text{is an odd integer.}$$

     In other words, n is a product of a power of 2 and an odd integer $m \geq 2$.
     Now, we aim to show that for n not a power of 2, $2^n + 1$ can be factored. When n is not a power of 2, and more specifically when $n = 2^k \cdot m$ for some odd integer $m \geq 2$, the number $2^n + 1$ can often be factored.
     For example, when $n = 6$, we have:

     $$2^6 + 1 = 64 + 1 = 65 = 5 \times 13,$$

     which is not a prime number. Similar factorizations can be shown for other values of n where n is not a power of 2.

Thus, when n is not a power of 2, $2^n + 1$ is typically not prime because it can be factored into smaller integers.

Since we have shown that if n is not a power of 2, then $2^n + 1$ is not prime, the contrapositive of the original statement is true. Therefore, the original statement holds: if $2^n + 1$ is prime, then n must be a power of 2. $\square$

- Part 2: The converse is false

  The converse would state that if n is a power of 2, then $2^n + 1$ must be prime. We will provide a counterexample to show that this is not true.

  Let $n = 4$, which is a power of 2. Then:

  $$2^4 + 1 = 16 + 1 = 17$$

  17 is indeed prime. But, let's consider $n = 6$, which is also a power of 2. Then:

  $$2^6 + 1 = 64 + 1 = 65$$

  65 is not a prime number because it factors as $65 = 5 \times 13$.

  Thus, we have found that $2^6 + 1 = 65$ is not prime, even though 6 is a power of 2. Therefore, the converse is false.

5. Let p be an odd prime number. Consider two integer a and b such that p does not divide a nor b, but divides $a^2 + b^2$. Show that $p \equiv 1 \pmod 4$.

   $p/(a^2 + b^2)$ can be written as $a^2 + b^2 \equiv 0 \pmod p \implies a^2 \equiv -b^2 \pmod p$

   It is a well-known result in number theory that an odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$. This result is based on Fermat's theorem on sums of two squares, which states that an odd prime p can be expressed as:

   $$p = x^2 + y^2 \quad \text{for some integers } x \text{ and } y,$$

   if and only if:

   $$p \equiv 1 \pmod 4.$$