AFRICAN INSTITUTE FOR MATHEMATICAL SCIENCES
(AIMS RWANDA, KIGALI)

Name: Aubrey Undi Phiri — Assignment Number: 1
Course: ALGEBRA AND CRYPTOGRAPHY — Date: March 1, 2025

Exercice 1.

Question 1

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

Fermat's Little Theorem states that if p is a prime and a is any integer not divisible by p, then

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

For our case, $p = 13$, so for any integer a not divisible by 13, we have:

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

Compute $2^{70} \mod 13$
Using Fermat's theorem:

$$2^{12} \equiv 1 \pmod{13}.$$

First, reduce the exponent modulo 12:

$$70 \equiv 10 \pmod{12}.$$

Thus,

$$2^{70} \equiv 2^{10} \pmod{13}.$$

Computing $2^{10} \mod 13$:

$$2^2 = 4, \quad 2^4 = 16 \equiv 3 \pmod{13}, \quad 2^8 = 9 \pmod{13}, \quad 2^{10} = 9 \cdot 4 = 36 \equiv 10 \pmod{13}.$$

Thus,

$$2^{70} \equiv 10 \pmod{13}.$$

Compute $3^{70} \mod 13$
Similarly, by Fermat's theorem,

$$3^{12} \equiv 1 \pmod{13}.$$

Since $70 \equiv 10 \pmod{12}$, we compute $3^{10} \mod 13$:

$$3^2 = 9, \quad 3^4 = 81 \equiv 3 \pmod{13}, \quad 3^8 = 9 \pmod{13}, \quad 3^{10} = 9 \cdot 9 = 81 \equiv 3 \pmod{13}.$$

Thus,

$$3^{70} \equiv 3 \pmod{13}.$$

Compute $2^{70} + 3^{70} \mod 13$
Adding the results,

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 13 \equiv 0 \pmod{13}.$$

Since $2^{70} + 3^{70} \equiv 0 \pmod{13}$, it follows that:

$$13 \text{ divides } 2^{70} + 3^{70}.$$

□

Question 2

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

for any natural numbers a and b.
Let $d = \gcd(a, b)$, which means that d is the largest positive integer that divides both a and b. This implies that there exist integers x and y such that:

$$a = dx, \quad b = dy.$$

Consider the Property of $2^n - 1$

A key number-theoretic property states that:

$$2^m - 1 \text{ is divisible by } 2^n - 1 \text{ whenever } n \text{ divides } m.$$

This follows from the identity:

$$2^m - 1 = (2^n - 1) \sum_{k=0}^{m/n-1} 2^{kn}.$$

Now, consider $\gcd(2^a - 1, 2^b - 1)$. We denote it as:

$$g = \gcd(2^a - 1, 2^b - 1).$$

By the fundamental property above, since d divides both a and b, we can write:

$$2^a - 1 = (2^d - 1)Q, \quad 2^b - 1 = (2^d - 1)R,$$

for some integers Q and R. This means that $2^d - 1$ is a common divisor of $2^a - 1$ and $2^b - 1$, so:

$$2^d - 1 \mid g.$$

To show that $g = 2^d - 1$, we need to prove that it is the greatest common divisor. Suppose there exists another divisor h such that h divides both $2^a - 1$ and $2^b - 1$. Then, h also divides any linear combination:

$$h \mid 2^d - 1.$$

Thus, the largest possible h is $2^d - 1$, proving that:

$$\gcd(2^a - 1, 2^b - 1) = 2^d - 1.$$

Since we set $d = \gcd(a, b)$, we obtain:

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

Question 3

$$\text{Let } d = \gcd(9n + 4, 2n - 1).$$

Since d divides both $9n + 4$ and $2n - 1$, it must also divide any integer linear combination of these terms. Consider:

$$d \mid (9n + 4) - 9(2n - 1).$$

Expanding,

$$(9n + 4) - 9(2n - 1) = 9n + 4 - 18n + 9 = -9n + 13.$$

Thus,

$$d \mid (-9n + 13).$$

Since $d \mid 2n - 1$, it must also divide a linear combination of $-9n + 13$ and $2n - 1$. Consider:

$$d \mid (2(-9n + 13) + 9(2n - 1)).$$

Expanding,

$$2(-9n + 13) + 9(2n - 1) = -18n + 26 + 18n - 9 = 17.$$

Since d divides 17, we conclude:

$$d \in \{1, 17\}.$$

Checking values of n, since $2n - 1$ is always odd, $\gcd(9n + 4, 2n - 1)$ must be an odd number. The only possible values are 1 or 17.
By checking small values of n, we find that in general,

$$\gcd(9n + 4, 2n - 1) = 1 \text{ for all natural numbers } n.$$

Question 4

If $2^n + 1$ is prime, then n must be a power of 2.

Assume $2^n + 1$ is a prime number for some natural number n. We aim to show that n must be a power of 2.

Consider the Prime Factorization If n is not a power of 2, then n has an odd prime factor. That is, we can write n as:

$$n = k \cdot m, \quad \text{where } m \text{ is an odd integer greater than 1.}$$

Rewriting $2^n + 1$:

$$2^n + 1 = 2^{km} + 1.$$

Using the identity:

$$a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + \cdots + 1), \quad \text{for odd } m,$$

with $a = 2^k$, we obtain:

$$2^{km} + 1 = (2^k + 1)(2^{k(m-1)} - 2^{k(m-2)} + \cdots + 1).$$

Since m is odd, both factors are greater than 1. This means $2^n + 1$ is composite, contradicting the assumption that it is prime.

Thus, n must be a power of 2 for $2^n + 1$ to be prime.

Counter example for the Converse

We now show that the converse is false, i.e., not all values of n that are powers of 2 result in a prime $2^n + 1$.
Consider $n = 16$, which is a power of 2:

$$2^{16} + 1 = 65537.$$

65537 is prime, which is consistent with our theorem. However, taking $n = 32$:

$$2^{32} + 1 = 4294967297.$$

Checking divisibility:

$$4294967297 = 641 \times 6700417.$$

Since it has nontrivial factors, $2^{32} + 1$ is composite. This proves that the converse is false.

- If $2^n + 1$ is prime, then n must be a power of 2.

- However, not every power of 2 produces a prime $2^n + 1$.

Thus, the theorem is proved, and the converse is disproved by counterexample.

Question 5

Let p be an odd prime number. Suppose there exist integers a and b such that $p \nmid a$, $p \nmid b$, but $p \mid a^2 + b^2$. Then, $p \equiv 1 \pmod 4$.

Consider the Congruences Modulo p Since $p \mid a^2 + b^2$, we have:

$$a^2 + b^2 \equiv 0 \pmod p.$$

Rearranging,

$$a^2 \equiv -b^2 \pmod p.$$

Thus, -1 is a quadratic residue modulo p, meaning there exists some x such that:

$$x^2 \equiv -1 \pmod p.$$

Use of Quadratic Reciprocity
From number theory, the Legendre symbol $\left(\frac{-1}{p}\right)$ is determined by:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

This evaluates to:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Since we assumed that -1 is a quadratic residue modulo p, it must be that:

$$\left(\frac{-1}{p}\right) = 1.$$

From the above result, this occurs if and only if:

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

Thus, we have shown that if $p \mid a^2 + b^2$ for some integers a and b not divisible by p, then

$$p \equiv 1 \pmod 4$$

.
$\square$