ผลลัพธ์ และ อภิปราย

3. Results and Discussion

ทฤษฎีบทต่อไปนี้ กำหนดให้ p เป็นจำนวนเฉพาะ และ x, y, z เป็นจำนวนเต็มไม่ติดลบ

ทฤษฎีบท 3.1: สมการ $p^x + 5^y = z^2$ เมื่อ $p \equiv 1 \pmod 4$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ

พิสูจน์ สมมติให้ $p \equiv 1 \pmod 4$ จะได้ว่า $p^x \equiv 1 \pmod 4$

พิสูจน์ ให้ $p \equiv 1 \pmod 4$

จะได้ $p^x \equiv 1^x \pmod 4$

ดังนั้น $p^x \equiv 1 \pmod 4$

กรณีที่ 1: ให้ $x=0$ หรือ $y=0$

แบ่งเป็น 2 กรณี ดังนี้

กรณี 1.1: ให้ $x=0$

$x=0$ และ $y=0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1+1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x=0$ และ $y=1$: $p^x + 5^y = z^2$

$p^0 + 5^1 = z^2$

$1 + 5 = 6 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x=0$ และ $y>1$: $p^x + 5^y = z^2$

$p^0 + 5^y = z^2$

$1 + 5^y = z^2$

$z^2 - 5^y = 1$, เป็นไปไม่ได้

จากการคาดเดาของ Catalan

กรณี 1.2 : ให้ $y=0$

$y=0$ และ $x=0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1+1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$y=0$ และ $x=1$: $p^x + 5^y = z^2$

$p^1 + 5^0 = z^2$

$p+1 = z^2$, เป็นไปไม่ได้

จาก $p \equiv 1 \pmod 4$

$p+1 \equiv 2 \pmod 4$

ดังนั้น $z^2 \equiv 2 \pmod 4$

เป็นไปไม่ได้ เพราะ $z^2 \equiv 0 \pmod 4$.

$y=0$ และ $x > 1$: $p^x + 5^y = z^2$

$p^x + 5^0 = z^2$

$p^x + 1 = z^2$

$z^2 - p^x = 1$, เป็นไปไม่ได้ เพราะ $p > 3$ จากการคาดเดาของ Catalan

กรณีที่ 2 : ให้ $x \geq 1$ และ $y \geq 1$

พิสูจน์ ให้ $x \geq 1$ และ $y \geq 1$

จะได้ว่า p^x เป็นจำนวนเต็มคี่ และ

5^y เป็นจำนวนเต็มคี่

จากสมการ $p^x + 5^y = z^2$

จะได้ว่า จำนวนเต็มคี่ + จำนวนเต็มคี่ = จำนวนเต็มคู่

ดังนั้น z^2 เป็นจำนวนเต็มคู่. #

[จะแสดงว่า z เป็นจำนวนเต็มคู่]

ถ้า z^2 เป็นจำนวนเต็มคู่ แล้ว z เป็นจำนวนเต็มคู่ [ใช้การแย้งสลับที่]

พิสูจน์ ถ้า z เป็นจำนวนเต็มคี่ แล้ว z^2 เป็นจำนวนเต็มคี่

ให้ z เป็นจำนวนเต็มคี่

จะมีจำนวนเต็ม k ที่ทำให้ $z = 2k+1$

จะได้ว่า $z^2 = (2k+1)^2$

$= 4k^2+4k+1$

$= 2(2k^2+2k)+1$ เมื่อ $2k^2+2k$ เป็นจำนวนเต็ม.

นั่นคือ z^2 เป็นจำนวนเต็มคี่.

ดังนั้น z^2 เป็นจำนวนเต็มคู่ จะได้ว่า z เป็นจำนวนเต็มคู่. #

จาก z เป็นจำนวนเต็มคู่

จะได้ว่ามีจำนวนเต็ม k ที่ทำให้ $z = 2k$

จะได้ว่า $z^2 = (2k)^2$

$= 4k^2$

นั่นคือ $4 \mid z^2$

ดังนั้น $z^2 \equiv 0 \pmod 4$. #

จาก $5 \equiv 1 \pmod 4$ จะได้ว่า $5^y \equiv 1 \pmod 4$

จาก $5^y \equiv 1 \pmod 4$ และ $z^2 \equiv 0 \pmod 4$

จะได้ว่า $z^2 - 5^y \equiv -1 \pmod 4$

จากสมการ $p^x + 5^y = z^2$

จะได้ $z^2 - 5^y = p^x$

จะได้ว่า $p^x \equiv -1 \pmod 4$

ดังนั้น $p^x \equiv 3 \pmod 4$

เกิดข้อขัดแย้ง เพราะ $p \equiv 1 \pmod 4$ จะได้ว่า $p^x \equiv 1 \pmod 4$.

จากกรณีที่ 1 และกรณีที่ 2 จะได้ว่า สมการ $p^x + 5^y = z^2$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ เมื่อ $p \equiv 1 \pmod 4$. #

ทฤษฎีบท 3.2 : สมการ $p^x + 5^y = z^2$ มีคำตอบจำนวนเต็มไม่ติดลบเพียง 2 คำตอบเท่านั้น เมื่อ (x, y, z) คือ $(3, 0, 3)$ และ $(2, 1, 3)$ เมื่อ $p \equiv 2 \pmod 4$

พิสูจน์ เนื่องจาก $p \equiv 2 \pmod 4$ ดังนั้น $p = 2$

จะได้ว่า $2^x + 5^y = z^2$

กรณีที่ 1 : ให้ $x = 0$ หรือ $y = 0$

แบ่งเป็น 2 กรณี ดังนี้

กรณี 1.1 : ให้ $x = 0$

$x = 0$ และ $y = 0$: $2^x + 5^y = z^2$

$2^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y = 1$: $2^x + 5^y = z^2$

$2^0 + 5^1 = z^2$

$1 + 5 = 6 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y > 1$: $2^x + 5^y = z^2$

$2^0 + 5^y = z^2$

$1 + 5^y = z^2$

$z^2 - 5^y = 1$, เป็นไปไม่ได้

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น

เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

กรณี 1.2 : ให้ $y = 0$

$y = 0$ และ $x = 0$: $2^x + 5^y = z^2$

$2^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$y = 0$ และ $x = 1$: $2^x + 5^y = z^2$

$2^1 + 5^0 = z^2$

$2 + 1 = 3 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$y = 0$ และ $x > 1$: $2^x + 5^y = z^2$

$2^x + 5^0 = z^2$

$2^x + 1 = z^2$

$z^2 - 2^x = 1$

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

ดังนั้น สมการ $z^2 - 2^x = 1$ มีคำตอบจำนวนเต็มไม่ติดลบ เมื่อ (x, y, z) คือ $(3, 0, 3)$. #

กรณีที่ 2 : ให้ $x \geq 1$ และ $y \geq 1$

พิสูจน์ ให้ $x \geq 1$ และ $y \geq 1$

จะได้ว่า 2^x เป็นจำนวนเต็มคู่ และ

5^y เป็นจำนวนเต็มคี่

จากสมการ $2^x + 5^y = z^2$

จะได้ว่า จำนวนเต็มคู่ + จำนวนเต็มคี่ = จำนวนเต็มคี่

ดังนั้น z^2 เป็นจำนวนเต็มคี่ . #

จากสมการ $2^x + 5^y = z^2$

จะได้ $2^x + 5^y \equiv z^2 \pmod 5$ $5^y \equiv 0 \pmod 5$

จะได้ว่า $2^x \equiv z^2 \pmod 5$

ดังนั้น $z^2 \not\equiv 0 \pmod 5$

นั่นคือ $5 \nmid z^2$

จาก $p \nmid a$ จะได้ว่า $(p, a) = 1$

ดังนั้น $(5, z^2) = 1$

จะได้ว่ามี $x, y \in I$ ที่ทำให้

$5x + z^2 y = 1$

$5x + z(zy) = 1$

ดังนั้น $(5, z) = 1$

นั่นคือ $5 \nmid z$. #

จาก $5 \nmid z$ และ z เป็นจำนวนเต็มคี่

จะได้ว่า $z \equiv 1, 2, 3, 4 \pmod 5$

จาก $z \equiv 1, 4 \equiv 1, -1 \pmod 5$

จะได้ว่า $z^2 \equiv 1 \pmod 5$

จาก $z \equiv 2, 3 \equiv 2, -2 \pmod 5$

จะได้ว่า $z^2 \equiv 4 \equiv -1 \pmod 5$.

จาก $2^x \equiv z^2 \pmod 5$ และ $x \geq 1$

ให้ x เป็นจำนวนเต็มคู่

จะได้ว่า $2^x = 2^{2k} = 4^k \equiv (-1)^k \pmod 5$

ให้ x เป็นจำนวนเต็มคี่

จะได้ว่า $2^x = 2^{2k+1} = 2 \cdot 4^k \equiv 2 \cdot (-1)^k \pmod 5$

เป็นไปไม่ได้ เพราะ $z^2 \equiv \pm 1 \pmod 5$.

ดังนั้น x เป็นจำนวนเต็มคู่. #

จาก x เป็นจำนวนเต็มคู่

จะมีจำนวนเต็ม k ที่ทำให้ $x = 2k$

จากสมการ $2^x + 5^y = z^2$

จะได้ $2^{2k} + 5^y = z^2$

$5^y = z^2 - 2^{2k}$

$= z^2 - (2^k)^2$

$= (z - 2^k)(z + 2^k)$

ให้ y และ n เป็นจำนวนเต็มที่ $y > 2n$ และ $n \geq 0$

จะได้ว่า $(5^{y-n})(5^n) = (z - 2^k)(z + 2^k)$

เนื่องจาก $z + 2^k > z - 2^k$

ทำให้ $(z + 2^k) = 5^{y-n}$ และ $(z - 2^k) = 5^n$.

จาก $(z + 2^k) = 5^{y-n}$ และ $(z - 2^k) = 5^n$

จะได้ $5^{y-n} - 5^n = \cancel{z} + 2^k - \cancel{z} + 2^k$

$5^n(5^{y-2n} - 1) = 2^{k+1}$

จาก $5^n(5^{y-2n} - 1) = 2^{k+1}$ ทำให้ได้ว่า n ต้องเท่ากับ 0

จะได้ $5^y - 1 = 2^{k+1}$

$5^y - 2^{k+1} = 1$

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

ทำให้ได้ว่า y ต้องเท่ากับ 1

จากสมการ $5^y - 2^{k+1} = 1$ และ $y=1$

จะได้ว่า $5 - 2^{k+1} = 1$

$2^{k+1} = 4$

$2^{k+1} = 2^2$

ทำให้ $k+1 = 2$

$k = 1$

นั่นคือ $x = 2k = 2$. #

จากสมการ $2^x + 5^y = z^2$, $y=1$ และ $x=2$

จะได้ว่า $2^2 + 5^1 = z^2$

$4+5 = 9 = z^2$

ดังนั้น $z = 3$.

ดังนั้น สมการ $2^x + 5^y = z^2$ มีคำตอบจำนวนเต็มไม่ติดลบ เมื่อ (x,y,z) คือ $(2,1,3)$. #

จากกรณีที่ 1 และกรณีที่ 2 จะได้ว่า สมการ $p^x + 5^y = z^2$ มีคำตอบจำนวนเต็มไม่ติดลบเพียง 2 คำตอบเท่านั้น เมื่อ (x,y,z) คือ $(3,0,3)$ และ $(2,1,3)$ เมื่อ $p \equiv 2 \pmod 4$. #

ทฤษฎีบท 3.3 : สมการ $p^x + 5^y = z^2$ เมื่อ $p \equiv 3 \pmod 4$ และ $p \equiv 2 \pmod 5$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ.

พิสูจน์ สมมติให้ $p \equiv 3 \pmod 4$ และ $p \equiv 2 \pmod 5$.

กรณีที่ 1 : ให้ $x = 0$ หรือ $y = 0$

แบ่งเป็น 2 กรณี ดังนี้

กรณี 1.1 : ให้ $x = 0$

$x = 0$ และ $y = 0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y = 1$: $p^x + 5^y = z^2$

$p^0 + 5^1 = z^2$

$1 + 5 = 6 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y > 1$: $p^x + 5^y = z^2$

$p^0 + 5^y = z^2$

$1 + 5^y = z^2$

$z^2 - 5^y = 1$, เป็นไปไม่ได้

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น

เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

กรณี 1.2 : ให้ $y = 0$

$y = 0$ และ $x = 0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$y = 0$ และ $x = 1$: $p^x + 5^y = z^2$

$p^1 + 5^0 = z^2$

$p + 1 = z^2$, เป็นไปไม่ได้

จาก $p \equiv 2 \pmod{5}$

$p+1 \equiv 3 \pmod{5}$

ดังนั้น $z^2 \equiv 3 \pmod{5}$

เป็นไปไม่ได้ เพราะ $z^2 \equiv 0 \pmod{5}$ หรือ $z^2 \equiv 1 \pmod{5}$ หรือ $z^2 \equiv 4 \pmod{5}$.

$y = 0$ และ $x > 1$: $p^x + 5^y = z^2$

$p^x + 5^0 = z^2$

$p^x + 1 = z^2$

$z^2 - p^x = 1$, เป็นไปไม่ได้ เพราะ $p > 3$

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

กรณีที่ 2 : ให้ $x \geq 1$ และ $y \geq 1$

พิสูจน์ ให้ $x \geq 1$ และ $y \geq 1$

จะได้ว่า p^x เป็นจำนวนเต็มคี่ และ

5^y เป็นจำนวนเต็มคี่

จากสมการ $p^x + 5^y = z^2$

จะได้ว่า จำนวนเต็มคี่ + จำนวนเต็มคี่ = จำนวนเต็มคู่

ดังนั้น z^2 เป็นจำนวนเต็มคู่. #

[จะแสดงว่า z เป็นจำนวนเต็มคู่]

ถ้า z^2 เป็นจำนวนเต็มคู่ แล้ว z เป็นจำนวนเต็มคู่ [ใช้การแย้งสลับที่]

พิสูจน์ ถ้า z เป็นจำนวนเต็มคี่ แล้ว z^2 เป็นจำนวนเต็มคี่

ให้ z เป็นจำนวนเต็มคี่

จะมีจำนวนเต็ม k ที่ทำให้ $z = 2k+1$

จะได้ว่า $z^2 = (2k+1)^2$

$= 4k^2+4k+1$

$= 2(2k^2+2k)+1$ เมื่อ $2k^2+2k$ เป็นจำนวนเต็ม.

นั่นคือ z^2 เป็นจำนวนเต็มคี่.

ดังนั้น z^2 เป็นจำนวนเต็มคู่ จะได้ว่า z เป็นจำนวนเต็มคู่. #

จาก z เป็นจำนวนเต็มคู่

จะได้ว่ามีจำนวนเต็ม k ที่ทำให้ $z = 2k$

จะได้ว่า $z^2 = (2k)^2$

$= 4k^2$

นั่นคือ $4 \mid z^2$

ดังนั้น $z^2 \equiv 0 \pmod 4$. #

จาก z เป็นจำนวนเต็มคู่

จะได้ว่า $z \equiv 0, 1, 2, 3, 4 \pmod 5$

จะได้ว่า $z^2 \equiv 0, 1, 4, 9, 16 \pmod 5$

นั่นคือ $z^2 \equiv 0, 1, 4, 4, 1 \pmod 5$

ดังนั้น $z^2 \equiv 0, 1, 4 \pmod 5$. #

จาก $5 \equiv 1 \pmod 4$ จะได้ว่า $5^y \equiv 1 \pmod 4$

จาก $5^y \equiv 1 \pmod 4$ และ $z^2 \equiv 0 \pmod 4$

จะได้ว่า $z^2 - 5^y \equiv -1 \pmod 4$

จากสมการ $p^x + 5^y = z^2$

จะได้ $p^x = z^2 - 5^y$

จะได้ว่า $p^x \equiv -1 \pmod 4$

ดังนั้น $p^x \equiv 3 \pmod 4$. #

ถ้า $p^x \equiv 3 \pmod 4$ แล้ว x เป็นจำนวนเต็มคี่ [ใช้การแย้งสลับที่]

พิสูจน์ ให้ x เป็นจำนวนเต็มคู่

จะมีจำนวนเต็ม k ที่ทำให้ $x = 2k$

จาก $p \equiv 3 \pmod 4$

จะได้ว่า $p \equiv -1 \pmod 4$

$p^{2k} \equiv 1 \pmod 4$

แต่ $1 \not\equiv 3 \pmod 4$

ดังนั้น $p^x \not\equiv 3 \pmod 4$. เมื่อ $x = 2k$

ถ้า x เป็นจำนวนเต็มคี่ แล้ว $p^x \equiv 2 \pmod 5$ หรือ $p^x \equiv 3 \pmod 5$.

พิสูจน์ ให้ x เป็นจำนวนเต็มคี่

จะมีจำนวนเต็ม k ที่ทำให้ $x = 2k+1$

จาก $p \equiv 2 \pmod 5$

$$p^x \equiv 2^x \pmod 5$$

$$p^{2k+1} \equiv 2^{2k+1} \pmod 5$$

$$p^{2k+1} \equiv 2\cdot 4^k \equiv 2\cdot(-1)^k \pmod 5$$

นั่นคือ $p^{2k+1} \equiv -2, 2 \equiv 3, 2 \pmod 5$

ดังนั้น $p^x \equiv 2 \pmod 5$ หรือ $p^x \equiv 3 \pmod 5$. #

จาก $5^y \equiv 0 \pmod 5$ และ $p^x \equiv 2 \pmod 5$ หรือ $p^x \equiv 3 \pmod 5$

จากสมการ $p^x + 5^y = z^2$

จะได้ว่า $z^2 \equiv 2 \pmod 5$ หรือ

$z^2 \equiv 3 \pmod 5$

เกิดข้อขัดแย้ง เพราะ $z^2 \equiv 0 \pmod 5$ หรือ $z^2 \equiv 1 \pmod 5$ หรือ $z^2 \equiv 4 \pmod 5$.

จากกรณีที่ 1 และกรณีที่ 2 จะได้ว่า สมการ $p^x+5^y=z^2$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ
เมื่อ $p \equiv 3 \pmod 4$ และ $p \equiv 2 \pmod 5$. #

ทฤษฎีบท 3.4 : สมการ $p^x + 5^y = z^2$ เมื่อ $p \equiv 3 \pmod{4}$ และ $p \equiv 3 \pmod{5}$ มีคำตอบที่เป็นจำนวนเต็มไม่เป็นลบ เมื่อ (x, y, z) คือ $(1, 0, 2)$

พิสูจน์ สมมติให้ $p \equiv 3 \pmod{4}$ และ $p \equiv 3 \pmod{5}$.

กรณีที่ 1 : ให้ $x = 0$ หรือ $y = 0$

แบ่งเป็น 2 กรณี ดังนี้

กรณี 1.1 : ให้ $x = 0$

$x = 0$ และ $y = 0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y = 1$: $p^x + 5^y = z^2$

$p^0 + 5^1 = z^2$

$1 + 5 = 6 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$x = 0$ และ $y > 1$: $p^x + 5^y = z^2$

$p^0 + 5^y = z^2$

$1 + 5^y = z^2$

$z^2 - 5^y = 1$, เป็นไปไม่ได้

จากการคาดเดาของ Catalan ; สมการ $a^x - b^y = 1$ จะมีคำตอบเพียงคำตอบเดียวเท่านั้น เมื่อแทน (a, b, x, y) ซึ่งเป็นจำนวนเต็มบวกที่มากกว่า 1 ด้วย $(3, 2, 2, 3)$.

กรณี 1.2 : ให้ $y = 0$

$y = 0$ และ $x = 0$: $p^x + 5^y = z^2$

$p^0 + 5^0 = z^2$

$1 + 1 = 2 = z^2$, เป็นไปไม่ได้ เพราะ z เป็นจำนวนเต็ม.

$y=0$ และ $x=1$: $p^x+5^y=z^2$

$p+1=z^2$

มีคำตอบเมื่อ $p=3$ และ $z=2$

$y=0$ และ $x>1$: $p^x+5^y=z^2$

$p^x+5^0=z^2$

$p^x+1=z^2$, เป็นไปไม่ได้ เมื่อ $p>3$

จาก Lemma 2.2 : สมการ $p^x+1=z^2$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ เมื่อ p เป็นจำนวนเฉพาะที่มากกว่า 3.

กรณีที่ 2 : ให้ $x \geq 1$ และ $y \geq 1$

พิสูจน์ ให้ $x \geq 1$ และ $y \geq 1$

จะได้ว่า p^x เป็นจำนวนเต็มคี่ และ

5^y เป็นจำนวนเต็มคี่

จากสมการ $p^x+5^y=z^2$

จะได้ว่า จำนวนเต็มคี่ + จำนวนเต็มคี่ = จำนวนเต็มคู่

ดังนั้น z^2 เป็นจำนวนเต็มคู่. #

[จะแสดงว่า z เป็นจำนวนเต็มคู่]

ถ้า z^2 เป็นจำนวนเต็มคู่ แล้ว z เป็นจำนวนเต็มคู่ [ใช้การแย้งสลับที่]

พิสูจน์ ถ้า z เป็นจำนวนเต็มคี่ แล้ว z^2 เป็นจำนวนเต็มคี่

ให้ z เป็นจำนวนเต็มคี่

จะมีจำนวนเต็ม k ที่ทำให้ $z=2k+1$

จะได้ว่า $z^2=(2k+1)^2$

$=4k^2+4k+1$

$=2(2k^2+2k)+1$ เมื่อ $2k^2+2k$ เป็นจำนวนเต็ม.

นั่นคือ z^2 เป็นจำนวนเต็มคี่.

ดังนั้น z^2 เป็นจำนวนเต็มคู่ จะได้ว่า z เป็นจำนวนเต็มคู่. #

จาก z เป็นจำนวนเต็มคู่

จะได้ว่ามีจำนวนเต็ม k ที่ทำให้ $z = 2k$

จะได้ว่า $z^2 = (2k)^2$

$= 4k^2$

นั่นคือ $4 \mid z^2$

ดังนั้น $z^2 \equiv 0 \pmod{4}$. #

จาก z เป็นจำนวนเต็มคู่

จะได้ว่า $z \equiv 0, 1, 2, 3, 4 \pmod{5}$

จะได้ว่า $z^2 \equiv 0, 1, 4, 9, 16 \pmod{5}$

นั่นคือ $z^2 \equiv 0, 1, 4, 4, 1 \pmod{5}$

ดังนั้น $z^2 \equiv 0, 1, 4 \pmod{5}$. #

จาก $5 \equiv 1 \pmod{4}$ จะได้ว่า $5^y \equiv 1 \pmod{4}$

จาก $5^y \equiv 1 \pmod{4}$ และ $z^2 \equiv 0 \pmod{4}$

จะได้ว่า $z^2 - 5^y \equiv -1 \pmod{4}$

จากสมการ $p^x + 5^y = z^2$

จะได้ $p^x = z^2 - 5^y$

จะได้ว่า $p^x \equiv -1 \pmod{4}$

ดังนั้น $p^x \equiv 3 \pmod{4}$. #

ถ้า $p^x \equiv 3 \pmod{4}$ แล้ว x เป็นจำนวนเต็มคี่ [ใช้การแย้งสลับที่]

พิสูจน์ ให้ x เป็นจำนวนเต็มคู่

จะมีจำนวนเต็ม k ที่ทำให้ $x = 2k$

จาก $p \equiv 3 \pmod{4}$

จะได้ว่า $p \equiv -1 \pmod{4}$

$p^{2k} \equiv 1 \pmod{4}$

แต่ $1 \not\equiv 3 \pmod{4}$

ดังนั้น $p^x \not\equiv 3 \pmod{4}$ เมื่อ $x = 2k$

ถ้า x เป็นจำนวนเต็มคี่ แล้ว $p^x \equiv 2 \pmod{5}$ หรือ $p^x \equiv 3 \pmod{5}$.

พิสูจน์ ให้ x เป็นจำนวนเต็มคี่

จะมีจำนวนเต็ม k ที่ทำให้ $x = 2k+1$

จาก $p \equiv 3 \pmod{5}$

$p^x \equiv 3^x \pmod{5}$

$p^{2k+1} \equiv 3^{2k+1} \pmod{5}$

$p^{2k+1} \equiv 3 \cdot 9^k \equiv 3 \cdot (-1)^k \pmod{5}$

นั่นคือ $p^{2k+1} \equiv -3, 3 \equiv 2, 3 \pmod{5}$

ดังนั้น $p^x \equiv 2 \pmod{5}$ หรือ $p^x \equiv 3 \pmod{5}$. #

จาก $5^y \equiv 0 \pmod{5}$ และ $p^x \equiv 2 \pmod{5}$ หรือ $p^x \equiv 3 \pmod{5}$

จากสมการ $p^x + 5^y = z^2$

จะได้ว่า $z^2 \equiv 2 \pmod{5}$ หรือ

$z^2 \equiv 3 \pmod{5}$

เกิดข้อขัดแย้ง เพราะ $z^2 \equiv 0 \pmod{5}$ หรือ $z^2 \equiv 1 \pmod{5}$ หรือ $z^2 \equiv 4 \pmod{5}$.

จากกรณีที่ 1 และกรณีที่ 2 จะได้ว่า สมการ $p^x + 5^y = z^2$ ไม่มีคำตอบจำนวนเต็มไม่ติดลบ

เมื่อ $p \equiv 3 \pmod{4}$ และ $p \equiv 3 \pmod{5}$. #