

3 คำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$

เมื่อ μ เป็นจำนวนเฉพาะเกาส์

ในการหาคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ นี้ จำเป็นต้องรู้จักนิยามและคุณสมบัติบางอย่าง เพื่อนำไปสู่ทฤษฎีหลักที่สำคัญ และต่อไปจากนี้ จะกำหนด μ เป็นจำนวนเฉพาะเกาส์ที่เสมอเราทราบว่า (α, β, γ) เป็นคำตอบของ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ ก็ต่อเมื่อ $(p\alpha, p\beta, p\gamma)$ เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ เมื่อ p เป็นจำนวนเต็มเกาส์ใด ๆ ดังนั้น เราจึงสนใจเฉพาะคำตอบ (α, β, γ) ของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ ที่ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย)

เมื่อกำหนดให้ (α, β, γ) เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ ที่ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย) จะทำให้ได้ความสัมพันธ์ของคำตอบแต่ละคู่ดังต่อไปนี้

ทฤษฎีบท 3.1 ถ้า (α, β, γ) เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ ที่ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย) แล้วแต่ละคู่ของ α, β, γ จะเป็นจำนวนเฉพาะต่อกัน

พิสูจน์ ให้ (α, β, γ) เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $\mathbb{Z}[i]$ ที่ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย)

พิจารณา ห.ร.ม. ของ α และ β

สมมุติว่ามี p เป็นจำนวนเฉพาะที่เป็นตัวหารร่วมของ α และ β ดังนั้น $p \mid (\alpha^2 + \mu\beta^2)$ หรือ $p \mid \gamma^2$ จาก p เป็นจำนวนเฉพาะ จะได้ $p \mid \gamma$ นั่นคือ p เป็นตัวหารร่วมของ α, β และ γ แต่ α, β และ γ ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย) ดังนั้นเป็นไปไม่ได้ นั่นคือ α และ β เป็นจำนวนเฉพาะต่อกัน
พิจารณา ห.ร.ม. ของ β และ γ สามารถทำได้ทำนองเดียวกับ การพิจารณา ห.ร.ม. ของ α และ β

พิจารณา ห.ร.ม. ของ α และ γ

สมมุติว่ามี ρ เป็นจำนวนเฉพาะที่เป็นตัวหารร่วมของ α และ γ ดังนั้น $\rho^2 \mid (\gamma^2 - \alpha^2)$ หรือ $\rho^2 \mid \mu\beta^2$

จาก μ และ ρ เป็นจำนวนเฉพาะ จะได้ $\rho \mid \beta$ นั่นคือ ρ เป็นตัวหารร่วมของ α, β และ γ แต่ α, β และ γ ไม่มีตัวหารร่วมกัน (ยกเว้นสมาชิกหนึ่งหน่วย) ดังนั้นเป็นไปได้ นั่นคือ α และ γ เป็นจำนวนเฉพาะต่อกัน

□

ยิ่งไปกว่านั้น เรายังทราบว่ ถ้า (α, β, γ) เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ แล้ว $(\varepsilon_1 \alpha, \varepsilon_2 \beta, \varepsilon_3 \gamma)$ เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ เมื่อ $\varepsilon_1, \varepsilon_2, \varepsilon_3$ เป็นสมาชิกหนึ่งหน่วยและมีค่าดังตารางต่อไปนี้

ε_1	ε_2	ε_3	ε_1	ε_2	ε_3
1	1	1	i	i	i
1	1	-1	i	i	-i
1	-1	1	i	-i	i
1	-1	-1	-i	i	i
-1	1	1	i	-i	-i
-1	1	-1	-i	i	-i
-1	-1	1	-i	-i	i
-1	-1	-1	-i	-i	-i

ดังนั้นถ้าเรากำหนดความสัมพันธ์ระหว่างคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ ดังต่อไปนี้ ให้ (α, β, γ) และ $(\alpha_1, \beta_1, \gamma_1)$ เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ กำหนดความสัมพันธ์ ~ ดังนี้

$(\alpha, \beta, \gamma) \sim (\alpha_1, \beta_1, \gamma_1)$ ก็ต่อเมื่อ มีสมาชิกหนึ่งหน่วย $\varepsilon_1, \varepsilon_2, \varepsilon_3$ ที่ทำให้ $\alpha = \varepsilon_1 \alpha_1, \beta = \varepsilon_2 \beta_1, \gamma = \varepsilon_3 \gamma_1$ จะได้ว่า ~ เป็นความสัมพันธ์สมมูล ดังนั้นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ จะถูกแบ่งออกเป็นกลุ่มสมมูล และเขียน $[(\alpha, \beta, \gamma)]$ แทนกลุ่มสมมูลที่มี (α, β, γ) เป็นสมาชิก และจะถือว่า คำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ ที่อยู่ในกลุ่มสมมูลเดียวกันไม่แตกต่างกัน

นิยาม 3.1 อันดับสามชั้น (α, β, γ) เป็นคำตอบปฐมฐาน(Primitive root) ของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ ก็ต่อเมื่อ แต่ละคู่ของ α, β, γ เป็นจำนวนเฉพาะต่อกัน

นั่นคือ (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ ก็ต่อเมื่อ α, β, γ ไม่มีตัวหารร่วมกัน(ยกเว้นสมาชิกหนึ่งหน่วย)

นิยาม 3.2 ให้ α และ β เป็นจำนวนเต็มเกาส์ เราจะกล่าวว่า α กับ β มีภาวะเดียวกัน ถ้า α และ β จำนวนเต็มเกาส์คู่หรือ α และ β จำนวนเต็มเกาส์คี่ และจะกล่าวว่า α กับ β มีภาวะตรงกันข้าม ถ้า α และ β มีตัวใดตัวหนึ่งเป็นจำนวนเต็มเกาส์คู่และอีกจำนวนหนึ่งเป็นจำนวนเต็มเกาส์คี่

ข้อสังเกต ถ้า α กับ β มีภาวะเดียวกัน ก็ต่อเมื่อ $(1+i) \mid (\alpha \pm \beta)$
ถ้า α กับ β มีภาวะตรงกันข้าม ก็ต่อเมื่อ $(1+i) \nmid (\alpha \pm \beta)$

ทฤษฎีบทประกอบ 3.2 ถ้า (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ แล้ว จะได้ว่า

1. ถ้า β เป็นจำนวนเต็มเกาส์คู่ แล้ว α และ γ จะเป็นจำนวนเต็มเกาส์คี่
2. ถ้า β เป็นจำนวนเต็มเกาส์คี่ แล้ว α และ γ จะมีภาวะตรงกันข้าม

พิสูจน์ ให้ (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$

พิจารณา

กรณีที่ β เป็นจำนวนเต็มเกาส์คู่ จะได้ว่า $\mu\beta^2 = \gamma^2 - \alpha^2$ เป็นจำนวนเต็มเกาส์คู่

จาก (α, β, γ) เป็นคำตอบปฐมฐาน ดังนั้น α และ γ จะต้องเป็นจำนวนเต็มเกาส์คี่

กรณีที่ β เป็นจำนวนเต็มเกาส์คี่ จะได้ว่า $\mu\beta^2$ เป็นจำนวนเต็มเกาส์คี่ ดังนั้น $\gamma^2 - \alpha^2$ เป็นจำนวนเต็มเกาส์คี่ นั่นคือ α และ γ จะมีภาวะตรงกันข้าม □

ทฤษฎีบท 3.3 ถ้า (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ แล้ว จะได้ว่า

1. ถ้า β เป็นจำนวนเต็มเกาส์คู่ แล้ว ห.ร.ม. ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ จะหาร 2 ลงตัว
2. ถ้า β เป็นจำนวนเต็มเกาส์คี่ แล้ว $\gamma + \alpha$ และ $\gamma - \alpha$ จะเป็นจำนวนเฉพาะต่อกัน

พิสูจน์ พิจารณา กรณีที่ β เป็นจำนวนเต็มเกาส์คู่ จาก ทฤษฎีบทประกอบ 3.2 จะได้ว่า γ กับ α จะเป็นจำนวนเต็มเกาส์คี่ เพราะฉะนั้น $\gamma + \alpha$ กับ $\gamma - \alpha$ จะเป็นจำนวนเต็มเกาส์คู่

ดังนั้น ห.ร.ม. ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ จะไม่ใช่สมาชิกหนึ่งหน่วย ให้ p เป็น ห.ร.ม. ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ จะได้ว่า $p \mid (\gamma - \alpha)$ และ $p \mid (\gamma + \alpha)$ หรือ $p \mid 2\gamma$ และ $p \mid 2\alpha$ จาก γ กับ α เป็นจำนวนเฉพาะต่อกัน จะได้ $p \mid 2$

พิจารณา กรณีที่ β เป็นจำนวนเต็มเกาส์คี่ จาก ทฤษฎีบทประกอบ 3.2 จะได้ว่า γ กับ α จะมีภาวะตรงกันข้าม ดังนั้น $\gamma + \alpha$ กับ $\gamma - \alpha$ จะเป็นจำนวนเต็มเกาส์คี่

กำหนดให้ p เป็น ห.ร.ม. ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ สมมติว่า p ไม่เป็นสมาชิกหนึ่งหน่วย จะมี λ เป็นจำนวนเฉพาะที่ $\lambda \mid p$ นั่นคือ $\lambda \mid (\gamma - \alpha)$ และ $\lambda \mid (\gamma + \alpha)$ หรือ $\lambda \mid 2\gamma$ และ $\lambda \mid 2\alpha$ จาก γ กับ α เป็นจำนวนเฉพาะต่อกัน จะได้ $\lambda \mid 2$ ดังนั้น λ เป็นจำนวนเฉพาะคู่ ซึ่งขัดแย้งกับ $\gamma + \alpha$ กับ $\gamma - \alpha$ จะเป็นจำนวนเต็มเกาส์คี่ ดังนั้น ห.ร.ม. ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ ต้องเป็นสมาชิกหนึ่งหน่วย $\square$

พิจารณา ให้ σ เป็นหรม ของ $\gamma + \alpha$ กับ $\gamma - \alpha$ จากทฤษฎีบท 3.3 จะได้ว่า σ เป็นสมาชิกหนึ่งหน่วยหรือเป็นจำนวนเต็มเกาส์คู่

$$\text{จาก } \mu\beta^2 = \gamma^2 - \alpha^2 = (\gamma + \alpha)(\gamma - \alpha)$$

$$\text{จะได้ } \frac{\mu\beta^2}{\sigma^2} = \frac{(\gamma + \alpha)}{\sigma} \frac{(\gamma - \alpha)}{\sigma}$$

ถ้า σ เป็นสมาชิกหนึ่งหน่วย จะได้ $\sigma \mid \beta$

ถ้า σ เป็นจำนวนเต็มเกาส์คู่ จาก μ เป็นจำนวนเฉพาะคี่ จะได้ σ หาร μ ไม่ลงตัว นั่นคือ $\sigma^2 \mid \beta^2$

ดังนั้น สรุปได้ว่า $\sigma \mid \beta$ เพราะฉะนั้น จะได้

$$\mu \left(\frac{\beta^2}{\sigma^2} \right) = \frac{(\gamma + \alpha)}{\sigma} \frac{(\gamma - \alpha)}{\sigma}$$

เนื่องจาก $\frac{(\gamma + \alpha)}{\sigma}$ และ $\frac{(\gamma - \alpha)}{\sigma}$ เป็นจำนวนเฉพาะต่อกัน

จะได้ว่า $\mu \mid \frac{(\gamma + \alpha)}{\sigma}$ หรือ $\mu \mid \frac{(\gamma - \alpha)}{\sigma}$ อย่างใดอย่างหนึ่ง(*)

พิจารณา กรณีที่ $\mu \mid \frac{(\gamma + \alpha)}{\sigma}$

$$\text{จะได้ } \left(\frac{\beta^2}{\sigma^2} \right) = \frac{(\gamma + \alpha)}{\mu\sigma} \frac{(\gamma - \alpha)}{\sigma}$$

จาก $\frac{(\gamma + \alpha)}{\mu\sigma}$ และ $\frac{(\gamma - \alpha)}{\sigma}$ เป็นจำนวนเฉพาะต่อกัน และ $Z[i]$ มีคุณสมบัติเป็นโดเมนเชิงจำนวนเต็ม

ที่มีการแยกตัวประกอบ ออกเป็นจำนวนเฉพาะได้แบบเดียว(Unique Factorization Domain) จะได้ว่า

มีสมาชิกหนึ่งหน่วย $\varepsilon_1, \varepsilon_2$ และจำนวนเต็มเกาส์ p, λ ที่

$$\frac{(\gamma + \alpha)}{\mu\sigma} = \varepsilon_1 p^2 \quad \text{และ} \quad \frac{(\gamma - \alpha)}{\sigma} = \varepsilon_2 \lambda^2$$

ทฤษฎีบทประกอบต่อไปนี้จะเป็นการแสดงว่า $\varepsilon_1, \varepsilon_2$ สามารถเลือกเป็น 1 ได้

ทฤษฎีบทประกอบ 3.4 ถ้า (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน

$Z[i]$ ที่มี $\mu \mid \frac{(\gamma + \alpha)}{\sigma}$ แล้วจะมี $(\alpha_1, \beta_1, \gamma_1)$ ใน $[(\alpha, \beta, \gamma)]$ และจำนวนเต็มเกาส์ ρ, λ ที่

$$\frac{\gamma_1 + \alpha_1}{\mu\sigma} = \rho^2 \text{ และ } \frac{\gamma_1 - \alpha_1}{\sigma} = \lambda^2$$

พิสูจน์ จาก $\frac{\gamma + \alpha}{\mu\sigma} = \varepsilon_1 \rho^2$ และ $\frac{\gamma - \alpha}{\sigma} = \varepsilon_2 \lambda^2$

จะได้ว่า $\varepsilon_1 \varepsilon_2 \rho^2 \lambda^2 = \left(\frac{\gamma + \alpha}{\mu\sigma}\right) \left(\frac{\gamma - \alpha}{\sigma}\right) = \left(\frac{\beta}{\sigma}\right)^2$

นั่นคือ $\varepsilon_1 \varepsilon_2 = \left(\frac{\beta}{\sigma\rho\lambda}\right)^2$

ดังนั้น สรุปได้ว่า $\varepsilon_1 \varepsilon_2$ เป็นสมาชิกหนึ่งหน่วย ที่สามารถเขียนอยู่ในรูปของกำลังสอง ดังนั้น $\varepsilon_1 \varepsilon_2 = \pm 1$

พิจารณา กรณีที่ $\varepsilon_1 \varepsilon_2 = 1$ จะสามารถแบ่งได้เป็น 4 กรณี คือ

กรณีที่ 1 เมื่อ $\varepsilon_1 = \varepsilon_2 = 1$ จะได้ $\frac{\gamma + \alpha}{\sigma\mu} = \rho^2$ และ $\frac{\gamma - \alpha}{\sigma} = \lambda^2$

กรณีที่ 2 เมื่อ $\varepsilon_1 = \varepsilon_2 = -1$ จะได้ $\frac{\gamma + \alpha}{\sigma\mu} = -\rho^2$ และ $\frac{\gamma - \alpha}{\sigma} = -\lambda^2$

$$\frac{\gamma + \alpha}{\sigma\mu} = (i\rho)^2 \text{ และ } \frac{\gamma - \alpha}{\sigma} = (i\lambda)^2$$

กรณีที่ 3 เมื่อ $\varepsilon_1 = i$ และ $\varepsilon_2 = -i$ จะได้ $\frac{\gamma + \alpha}{\sigma\mu} = i\rho^2$ และ $\frac{\gamma - \alpha}{\sigma} = -i\lambda^2$

$$\frac{\gamma i + \alpha i}{\sigma\mu} = (i\rho)^2 \text{ และ } \frac{\gamma i - \alpha i}{\sigma} = \lambda^2$$

กรณีที่ 4 เมื่อ $\varepsilon_1 = -i$ และ $\varepsilon_2 = i$ จะได้ $\frac{\gamma + \alpha}{\sigma\mu} = -i\rho^2$ และ $\frac{\gamma - \alpha}{\sigma} = i\lambda^2$

$$\frac{\gamma i + \alpha i}{\sigma\mu} = \rho^2 \text{ และ } \frac{\gamma i - \alpha i}{\sigma} = (i\lambda)^2$$

ในการพิจารณา กรณีที่ $\varepsilon_1 \varepsilon_2 = -1$ จะทำได้คล้ายกับ กรณี $\varepsilon_1 \varepsilon_2 = 1$

นั่นคือ เราสามารถหา $(\alpha_1, \beta_1, \gamma_1)$ ใน $[(\alpha, \beta, \gamma)]$ และจำนวนเต็มเกาส์ ρ, λ ที่

$$\frac{\gamma_1 + \alpha_1}{\sigma\mu} = \rho^2 \text{ และ } \frac{\gamma_1 - \alpha_1}{\sigma} = \lambda^2$$

□

จาก (α, β, γ) เป็นกลุ่มสมมูลที่เป็นคำตอบพื้นฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$

ที่มี $\mu \mid \frac{(\gamma+\alpha)}{\sigma}$ จะได้ว่า

$$\frac{\gamma+\alpha}{\mu\sigma} = \rho^2 \quad \text{และ} \quad \frac{\gamma-\alpha}{\sigma} = \lambda^2$$

$$\gamma+\alpha = \sigma\mu\rho^2 \quad \text{และ} \quad \gamma-\alpha = \sigma\lambda^2$$

$$2\gamma = \sigma\mu\rho^2 + \sigma\lambda^2 \quad \text{และ} \quad 2\alpha = \sigma\mu\rho^2 - \sigma\lambda^2$$

ดังนั้น

$$\gamma = \frac{\sigma\mu\rho^2 + \sigma\lambda^2}{2} \quad \text{และ} \quad \alpha = \frac{\sigma\mu\rho^2 - \sigma\lambda^2}{2}$$

จาก $\alpha^2 + \mu\beta^2 = \gamma^2$ จะได้ $\mu\beta^2 = (\gamma + \alpha)(\gamma - \alpha)$

$$\frac{\beta^2}{\sigma^2} = \left(\frac{\gamma+\alpha}{\sigma\mu}\right)\left(\frac{\gamma-\alpha}{\sigma}\right) = \rho^2\lambda^2$$

$$\beta^2 = (\sigma\rho\lambda)^2$$

ดังนั้น จะได้ $\beta = \sigma\rho\lambda$ หรือ $\beta = -\sigma\rho\lambda$

นั่นคือจะได้ $\beta = \pm\sigma\rho\lambda$

เพราะฉะนั้น เราสรุปได้ว่า $\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2}$, $\beta = \pm\sigma\rho\lambda$, $\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2}$

จาก(*) เราได้ว่า $\mu \mid \frac{(\gamma+\alpha)}{\sigma}$ หรือ $\mu \mid \frac{(\gamma - \alpha)}{\sigma}$ อย่างใดอย่างหนึ่ง

ในกรณีที่ $\mu \mid \frac{(\gamma+\alpha)}{\sigma}$ เราสรุปได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} \quad \beta = \pm\sigma\rho\lambda, \quad \gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2}$$

เมื่อ σ, ρ, λ เป็นจำนวนเต็มเกาส์ที่ $N(\sigma) \leq 2$ และ ρ, λ เป็นจำนวนเฉพาะต่อกัน

ในกรณีที่ $\mu \mid \frac{(\gamma - \alpha)}{\sigma}$ โดยการกระทำแบบเดียวกันกับแบบ $\mu \mid \frac{(\gamma+\alpha)}{\sigma}$ เราจะได้ว่า

$$\alpha = -\frac{\sigma(\mu\rho^2 - \lambda^2)}{2} \quad \beta = \pm\sigma\rho\lambda, \quad \gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2}$$

เมื่อ σ, ρ, λ เป็นจำนวนเต็มเกาส์ที่ $N(\sigma) \leq 2$ และ ρ, λ เป็นจำนวนเฉพาะต่อกัน

ดังนั้น เมื่อรวมทั้งสองกรณีเข้าด้วยกัน จะได้

$$\alpha = \pm \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} \quad \beta = \pm\sigma\rho\lambda, \quad \gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2}$$

จาก (α, β, γ) เป็นคำตอบปฐมฐานของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ ซึ่งเมื่อเลือกเครื่องหมายแล้ว จะได้หลายคำตอบ แต่อย่างไรก็ตาม คำตอบทั้งหมดนี้ ถือว่าไม่แตกต่างกัน นั่นคือคำตอบทั้งหมดจะอยู่ในกลุ่มสมมูลเดียวกัน ซึ่งจะแทนได้ด้วย

$$\left[\left(\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}, \sigma\rho\lambda, \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} \right) \right]$$

ต่อไปจะแสดงว่า จำนวนเต็มเกาส์ใด ๆ ก็ตามที่อยู่ในรูปแบบ $\left(\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}, \sigma\rho\lambda, \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} \right)$

เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ เสมอ

ทฤษฎีบท 3.5 กำหนดให้ σ, ρ, λ และ μ เป็นจำนวนเต็มเกาส์ใด ๆ

ถ้า $\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}$ เป็นจำนวนเต็มเกาส์ แล้ว $\left(\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}, \sigma\rho\lambda, \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} \right)$ เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$

พิสูจน์ กำหนดให้ $\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}$ เป็นจำนวนเต็มเกาส์ จะได้ว่า $\sigma\rho\lambda$ เป็นจำนวนเต็มเกาส์ และจาก $\frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} + \sigma\lambda^2$ จะได้ $\frac{\sigma(\mu\rho^2 + \lambda^2)}{2}$ เป็นจำนวนเต็มเกาส์ ดังนั้น ให้ $(\alpha, \beta, \gamma) = \left(\frac{\sigma(\mu\rho^2 - \lambda^2)}{2}, \sigma\rho\lambda, \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} \right)$ จะได้ว่า

$$\alpha^2 + \mu\beta^2 = \left(\frac{\sigma(\mu\rho^2 - \lambda^2)}{2} \right)^2 + \mu(\sigma\rho\lambda)^2 = \left(\frac{\sigma(\mu\rho^2 + \lambda^2)}{2} \right)^2 = \gamma^2$$

นั่นคือ (α, β, γ) เป็นคำตอบของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$ □

ต่อไปจะเป็นตัวอย่าง การหารากของสมการ $x^2 + \mu y^2 = z^2$ ใน $Z[i]$

ตัวอย่าง 3.1 กำหนดให้ $\mu = 3, \sigma = 1, \rho = 1$ และ $\lambda = 1$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1)(3(1)^2 - 1^2)}{2} = 1$$

$$\beta = \sigma\rho\lambda = (1)(1)(1) = 1$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1)(3(1)^2 + 1^2)}{2} = 2$$

ดังนั้น $(1, 1, 2)$ เป็นรากชุดหนึ่งของสมการ $x^2 + 3y^2 = z^2$ ใน $Z[i]$ □

ตัวอย่าง 3.2 กำหนดให้ $\mu = 3$, $\sigma = 2$, $\rho = 2+i$ และ $\lambda = 1+i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(2)(3(2+i)^2 - (1+i)^2)}{2} = 9+10i$$

$$\beta = \sigma\rho\lambda = (2)(2+i)(1+i) = 2+6i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(2)(3(2+i)^2 + (1+i)^2)}{2} = 9+14i$$

ดังนั้น $(9+10i, 2+6i, 9+14i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + 3y^2 = z^2$ ใน $Z[i]$ $\square$

ตัวอย่าง 3.3 กำหนดให้ $\mu = 3$, $\sigma = 1+i$, $\rho = 2+i$ และ $\lambda = 1$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1+i)(3(2+i)^2 - (1)^2)}{2} = -2+10i$$

$$\beta = \sigma\rho\lambda = (1+i)(2+i)(1) = 1+3i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1+i)(3(2+i)^2 + (1)^2)}{2} = -1+11i$$

ดังนั้น $(-2+10i, 1+3i, -1+11i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + 3y^2 = z^2$ ใน $Z[i]$ $\square$

ตัวอย่าง 3.4 กำหนดให้ $\mu = 2+i$, $\sigma = 2$, $\rho = 1$ และ $\lambda = 2$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(2)((2+i)(1)^2 - (2)^2)}{2} = -2+i$$

$$\beta = \sigma\rho\lambda = (2)(2)(1) = 4$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(2)((2+i)(1)^2 + (2)^2)}{2} = 6+i$$

ดังนั้น $(-2+i, 4, 6+i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + (2+i)y^2 = z^2$ ใน $Z[i]$ $\square$

ตัวอย่าง 3.5 กำหนดให้ $\mu = 3+2i$, $\sigma = 1$, $\rho = 3$ และ $\lambda = 2+i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1)((3+2i)(3)^2 - (2+i)^2)}{2} = 12+7i$$

$$\beta = \sigma\rho\lambda = (1)(3)(2+i) = 6+3i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1)((3+2i)(3)^2 + (2+i)^2)}{2} = 15+11i$$

ดังนั้น $(12+7i, 6+3i, 15+11i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + (3+2i)y^2 = z^2$ ใน $Z[i]$ $\square$

ตัวอย่าง 3.6 กำหนดให้ $\mu = 7$, $\sigma = 1$, $\rho = 4$ และ $\lambda = 1+i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1)((7)(4)^2 - (1+i)^2)}{2} = 56-i$$

$$\beta = \sigma\rho\lambda = (1)(4)(1+i) = 4+4i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1)((7)(4)^2 + (1+i)^2)}{2} = 56+i$$

ดังนั้น $(56+i, 4+4i, 56+i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + 7y^2 = z^2$ ใน $\mathbb{Z}[i]$ $\square$

ตัวอย่าง 3.7 กำหนดให้ $\mu = 3i$, $\sigma = 1+i$, $\rho = 2+3i$ และ $\lambda = 4+5i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1+i)((3i)(2+3i)^2 - (4+5i)^2)}{2} = 14-41i$$

$$\beta = \sigma\rho\lambda = (1+i)(2+3i)(4+5i) = -29+15i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1+i)((3i)(2+3i)^2 + (4+5i)^2)}{2} = -35-10i$$

ดังนั้น $(14-41i, -29+15i, -35-10i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + 3iy^2 = z^2$ ใน $\mathbb{Z}[i]$ $\square$

ตัวอย่าง 3.8 กำหนดให้ $\mu = 2+5i$, $\sigma = 1$, $\rho = 1+i$ และ $\lambda = 1-i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1)((2+5i)(1+i)^2 - (1-i)^2)}{2} = -5+3i$$

$$\beta = \sigma\rho\lambda = (1)(1+i)(1-i) = 2$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1)((2+5i)(1+i)^2 + (1-i)^2)}{2} = -5+i$$

ดังนั้น $(-5+3i, 2, -5+i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + (2+5i)y^2 = z^2$ ใน $\mathbb{Z}[i]$ $\square$

ตัวอย่าง 3.9 กำหนดให้ $\mu = 4+5i$, $\sigma = 1+i$, $\rho = 2+i$ และ $\lambda = 2-i$ จะได้ว่า

$$\alpha = \frac{\sigma(\mu\rho^2 - \lambda^2)}{2} = \frac{(1+i)((4+5i)(2+i)^2 - (2-i)^2)}{2} = -23+12i$$

$$\beta = \sigma\rho\lambda = (1+i)(2+i)(2-i) = 5+5i$$

$$\gamma = \frac{\sigma(\mu\rho^2 + \lambda^2)}{2} = \frac{(1+i)((4+5i)(2+i)^2 + (2-i)^2)}{2} = -16+11i$$

ดังนั้น $(-23+12i, 5+5i, -16+11i)$ เป็นรากชุดหนึ่งของสมการ $x^2 + (4+5i)y^2 = z^2$ ใน $\mathbb{Z}[i]$ $\square$

