TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH
Tập 22, Số 5 (2025): 814-823
Website: https://journal.hcmue.edu.vn
ISSN: 2734-9918

HO CHI MINH CITY UNIVERSITY OF EDUCATION
JOURNAL OF SCIENCE
Vol. 22, No. 5 (2025): 814-823
https://doi.org/10.54607/hcmue.js.22.5.4730(2025)

Bài báo nghiên cứu

CẤU TRÚC NHÓM NHÂN CỦA VÀNH CÁC LỚP THẶNG DƯ CỦA VÀNH EISENSTEIN

My Vinh Quang, Cao Phan Anh Dũng*

Trường Đại học Sư phạm Thành phố Hồ Chí Minh. Việt Nam

**Tác giả liên hệ: Cao Phan Anh Dũng – Email: 4801101010@student.hcmue.edu.vn*

Ngày nhận bài: 16-02-2025; ngày nhận bài sửa: 10-4-2025; ngày duyệt đăng: 17-4-2025

TÓM TẮT

Trong bài báo này, chúng tôi mô tả đầy đủ và chi tiết cấu trúc của nhóm nhân của vành các lớp thặng dư của vành Eisenstein theo modulo luỹ thừa của các phần tử nguyên tố. Từ đó, như là các hệ quả, chúng tôi mô tả được cấu trúc của nhóm nhân của vành các lớp thặng dư của vành Eisenstein theo modulo bất kì, cũng như xác định được tất cả các phần tử của vành Eisenstein có căn nguyên thuỷ.

Từ khoá: vành Eisenstein; nhóm nhân của vành; căn nguyên thuỷ

1. Mở đầu

Cho F là mở rộng đại số bậc n của trường số hữu tỉ $\mathbb{Q}$ ($[F:\mathbb{Q}]=n$). D là vành các số nguyên đại số của F. D được xem như là một mở rộng tự nhiên của vành các số nguyên $\mathbb{Z}$ ($D=\mathbb{Z}$ khi $n=1$). Với mỗi $m\in D$, kí hiệu $D/_{\langle m\rangle}$ là vành các lớp thặng dư modulo m, $\phi_D(m)=\left(D/_{\langle m\rangle}\right)^*$ là nhóm nhân của vành $D/_{\langle m\rangle}$, $\varphi_D(m)=|\phi_D(m)|$ là hàm Euler trên D. Phần tử $r\in D$ được gọi là căn nguyên thuỷ modulo m nếu $(r,m)=1$ và $o([r])$ trong $\phi_D(m)$ bằng $\varphi_D(m)$ (với kí hiệu $o(a)$ là cấp của a trong nhóm G tương ứng). Như vậy, $r\in D$ là căn nguyên thuỷ modulo m khi và chỉ khi $\phi_D(m)$ là nhóm cyclic và $[r]$ là phần tử sinh của $\phi_D(m)$.

Trong lí thuyết số, bài toán mô tả cấu trúc nhóm $\phi_{\mathbb{Z}}(m)$ và xác định các số tự nhiên m có căn nguyên thuỷ là bài toán thú vị và nổi tiếng, đến nay đã có lời giải trọn vẹn như sau. Xem (Bolker, 1970).

- $\phi_{\mathbb{Z}}(2)\cong\mathbb{Z}_1$; $\phi_{\mathbb{Z}}(4)\cong\mathbb{Z}_2$; $\phi_{\mathbb{Z}}(2^n)\cong\mathbb{Z}_2\times\mathbb{Z}_{2^{n-2}}$ nếu $n>2$;
- $\phi_{\mathbb{Z}}(p^n)\cong\mathbb{Z}_{p^n-p^{n-1}}$ nếu p là số nguyên tố lẻ;
- $\phi_{\mathbb{Z}}(kl)=\phi_{\mathbb{Z}}(k)\phi_{\mathbb{Z}}(l)$ nếu $(k,l)=1$;

trong đó $\mathbb{Z}_m$ là nhóm cộng của vành $\mathbb{Z}/_{\langle m\rangle}$, đây là nhóm cyclic cấp m.

Cite this article as: My, V. Q., & Cao, P. A. D. (2025). The structure of multiplicative groups of residue class rings of the Eisenstein integers. *Ho Chi Minh City University of Education Journal of Science, 22*(5), 814-823. https://doi.org/10.54607/hcmue.js.22.5.4730(2025)

Một vấn đề rất tự nhiên và thú vị là mở rộng các kết quả trên cho vành các số nguyên đại số D. Cross (1983), đã mở rộng thành công các kết quả trên cho vành số nguyên Gauss. Bài báo này sẽ mở rộng các kết quả trên cho vành các số nguyên Eisenstein. Lưu ý rằng vành các số nguyên Gauss và vành các số nguyên Eisenstein là vành các số nguyên đại số của trường $\mathbb{Q}(\sqrt{-1})$ và $\mathbb{Q}(\sqrt{-3})$. Đây là các vành quan trọng, có nhiều ứng dụng nhất trong các lớp vành số nguyên của mở rộng bậc 2 của trường $\mathbb{Q}$.

2. Kí hiệu và các kết quả mở đầu

Kí hiệu E là vành các số nguyên đại số của trường $\mathbb{Q}(\sqrt{-3})$. Khi đó

$E = \mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$, với $\omega = \frac{1+\sqrt{-3}}{2}$.

Vành E được gọi là vành các số nguyên Eisenstein. Với mỗi $m \in E$, vành $E/_{\langle m \rangle}$ được gọi là vành các lớp thặng dư modulo m, $\phi_E(m) = \left(E/_{\langle m \rangle}\right)^*$ là nhóm nhân của vành $E/_{\langle m \rangle}$.

Vành E là vành Euclide với ánh xạ:

$N: E\backslash\{0\} \to \mathbb{N}, \alpha \longmapsto N(\alpha) = |\alpha|^2$.

Tập hợp các phần tử khả nghịch trong vành là $\{\pm 1, \pm\omega, \pm\overline{\omega}\} = \langle\omega\rangle$.

Các phần tử nguyên tố trong E được mô tả thông qua định lí sau.

Định lí 2.1. Trong vành E có bốn loại phần tử nguyên tố:

1) 2 là phần tử nguyên tố.
2) $\alpha = \sqrt{-3}$ là phần tử nguyên tố.
3) Nếu p là số nguyên tố dạng $6k + 5$ thì p là phần tử nguyên tố trong E.
4) Nếu q là số nguyên tố dạng $6k + 1$ thì q có phân tích duy nhất trong E dưới dạng $q = \pi_q\overline{\pi_q}$, trong đó $\pi_q, \overline{\pi_q}$ là các phần tử nguyên tố không liên kết trong E.

Ngoài ra, bất kì một phần tử nguyên tố nào của E cũng liên kết với một trong bốn loại phần tử nguyên tố nói trên.

Chứng minh định lí này có thể tìm thấy trong (Alaca & Williams, 2004). Kể từ đây, ta quy ước p là số nguyên tố dạng $6k + 5$, q là số nguyên tố dạng $6k + 1$, $\pi_q, \overline{\pi_q}$ là các phần tử nguyên tố thỏa mãn $q = \pi_q\overline{\pi_q}$.

Hai định lí dưới đây mô tả các phần tử và phần tử khả nghịch trong vành các lớp thặng dư theo modulo lũy thừa các phần tử nguyên tố.

Định lí 2.2. Ta có:

1) $E/_{\langle 2^n \rangle} = \{[a + b\omega]: 0 \le a, b \le 2^n - 1\}$.
2) $E/_{\langle \pi_q^n \rangle} = \{[a]: 0 \le a \le q^n - 1\}$.
3) $E/_{\langle p^n \rangle} = \{[a + b\omega]: 0 \le a, b \le p^n - 1\}$.
4) $E/_{\langle \alpha^{2m} \rangle} = \{[a + b\omega]: 0 \le a, b \le 3^m - 1\}$

$E/_{\langle \alpha^{2m+1} \rangle} = \{[a + b\omega]: 0 \le a \le 3^m - 1, 0 \le b \le 3^{m+1} - 1\}$.

Chứng minh: Ta cần chỉ ra các lớp tương đương ở vế phải từng mục (1) – (4) là không lặp và đầy đủ.

- Không lặp: Dưới đây ta quy ước các phần tử được lấy đều là đại diện các lớp tương đương nêu ra ở vế phải. Ta cũng kí hiệu $|_R$ và $\nmid_R$ để chỉ tính chia hết và không chia hết trong vành R.

1) Giả sử $a + b\omega \equiv c + d\omega \pmod{2^n}$, khi đó $2^n|_E[(a-c) + (b-d)\omega]$.

Suy ra $2^n|_{\mathbb{Z}}\ (a-c)$ và $2^n|_{\mathbb{Z}}\ (b-d)$, hay $a = c, b = d$.

2) Giả sử $a \equiv b \pmod{\pi_q^n}$, khi đó $\pi_q^n|_{\mathbb{Z}}\ (a-b)$. Suy ra $\overline{\pi_q}^n = \overline{\pi_q^n}\ |_E\ \overline{(a-b)} = a - b$.

Hơn nữa, do $\pi_q, \overline{\pi_q}$ nguyên tố cùng nhau trong E nên $\pi_q^n\overline{\pi_q^n}\ |_E\ (a-b)$, hay $q^n\ |_E\ (a-b)$, suy ra $q^n\ |_{\mathbb{Z}}\ (a-b)$, do đó $a = b$.

3) Chứng minh tương tự (1).

4) Đối với $E/_{\langle\alpha^{2m}\rangle}$, do $\alpha^{2m} \sim 3^m$ trong E nên chứng minh được tiến hành tương tự như (1)

Đối với $E/_{\langle\alpha^{2m+1}\rangle}$, lưu ý rằng $\alpha^{2m+1} \sim 3^m\alpha$. Bây giờ, giả sử

$a + b\omega \equiv c + d\omega \pmod{\alpha^{2m+1}}$;

khi đó $3^m\alpha\ |_E\ [(a-c) + (b-d)\omega]$. Nói riêng, ta có $3^m\ |_E\ [(a-c) + (b-d)\omega]$, do đó $3^m\ |_{\mathbb{Z}}\ (a-c)$, hay $a = c$. Ta suy ra $3^m\alpha\ |_E\ (b-d)\omega$, do đó $N(3^m\alpha)\ |_{\mathbb{Z}}\ N\big((b-d)\omega\big)$, tức $3^{2m+1}\ |_{\mathbb{Z}}\ (b-d)^2$. Như vậy $3^{m+1}\ |_{\mathbb{Z}}\ (b-d)$, hay $b = d$.

- Đầy đủ: Lấy $\beta = x + y\omega \in E$ tùy ý $(x, y \in \mathbb{Z})$, ta cần chứng minh β thuộc một trong các lớp tương đương được liệt kê trong các phát biểu (1) – (4). Trong phần còn lại của chứng minh, với $a, m \in \mathbb{N}$, ta gọi việc tìm $a' \in \mathbb{N}$ thỏa $0 \le a' \le m-1$ và $a \equiv a' \pmod{m}$ là việc rút a theo modulo m.

1) Rút x, y theo modulo 2^n cho ta lớp tương đương cần tìm.

2) Trước hết ta chỉ ra rằng ω thuộc một trong các lớp tương đương liệt kê ở vế phải của (2).

Đặt $\pi_q^n = a - b\omega$ với $a, b \in \mathbb{Z}$, khi đó $b\omega \equiv a \pmod{\pi_q^n}$. Lưu ý rằng q và b nguyên tố cùng nhau trong $\mathbb{Z}$, vì nếu $q\ |_{\mathbb{Z}}\ b$ thì $\pi_q\overline{\pi_q}\ |_E\ b$, do đó $\pi_q\ |_E\ a$, tức $q\ |_{\mathbb{Z}}\ a$. Ta suy ra $q\ |_E\ \pi_q^n$, vô lí.

Như vậy, phương trình đồng dư $bt \equiv 1\ (mod\ q^n)$ có nghiệm $t_0 \in \mathbb{Z}$, do đó

$\omega \equiv (bt_0)\omega \equiv at_0 \pmod{\pi_q^n}$;

và bằng việc rút at_0 theo modulo q^n, ta suy ra ω thuộc một trong các lớp tương đương cần tìm. Như vậy, vì cả x, y, ω đều thuộc lớp tương đương nào đó trong vế phải của (2) nên $\beta = x + y\omega$ cũng vậy.

3) Rút x, y theo modulo p^n cho ta lớp tương đương cần tìm.

4) Đối với $E/_{\langle\alpha^{2m}\rangle}$, rút x, y theo modulo 3^m cho ta lớp tương đương cần tìm.

Đối với $E/_{\langle\alpha^{2m+1}\rangle}$, trước hết ta rút x, y theo modulo 3^{m+1} để có

$x + y\omega \equiv x' + y'\omega \pmod{\alpha^{2m+1}}$, $0 \le x', y' \le 3^{m+1} - 1$.

Lúc này, có 3 trường hợp có thể xảy ra:

- Nếu $x' \le 3^m - 1$ thì $\beta \in [x' + y'\omega]$ là một lớp tương đương ở vế phải của (4).

- Nếu $3^m \le x' \le 2.3^m - 1$, khi đó do $\alpha = -1 + 2\omega$ nên:

$$x' + y'\omega \equiv (x' - 3^m) + (y' + 2.3^m)\omega + 3^m(1 - 2\omega)$$
$$\equiv (x' - 3^m) + (y' + 2.3^m)\omega \ (mod\ \alpha^{2m+1}).$$

Đến đây, bằng cách rút $y' + 2.3^m$ theo modulo 3^{m+1}, ta suy ra β thuộc một lớp tương đương ở vế phải của (4).

- Nếu $2.3^m \le x' \le 3^{m+1} - 1$, khi đó:

$$x' + y'\omega \equiv (x' - 2.3^m) + (y' + 4.3^m)\omega + 3^m(2 - 4\omega)$$
$$\equiv (x' - 2.3^m) + (y' + 4.3^m)\omega \ (mod\ \alpha^{2m+1}).$$

Rút $y' + 4.3^m$ theo modulo 3^{m+1} cho ta kết luận tương tự trường hợp 2.

Chứng minh hoàn tất. ■

Định lí 2.3. Với $a, b \in \mathbb{Z}$, ta có:

1) $[a + b\omega]$ khả nghịch trong $E/_{\langle 2^n \rangle}$ ($E/_{\langle p^n \rangle}$) khi và chỉ khi $2 \nmid_{\mathbb{Z}} a$ hoặc $2 \nmid_{\mathbb{Z}} b$ (tương ứng $p \nmid_{\mathbb{Z}} a$ hoặc $p \nmid_{\mathbb{Z}} b$).

2) $[a]$ khả nghịch trong $E/_{\langle \pi_q^n \rangle}$ khi và chỉ khi $q \nmid_{\mathbb{Z}} a$.

3) $[a + b\omega]$ khả nghịch trong $E/_{\langle \alpha^n \rangle}$ khi và chỉ khi $a \not\equiv b\ (mod\ 3)$ trong $\mathbb{Z}$.

Chứng minh. Lấy β và γ trong E, khi đó $[\beta]$ khả nghịch trong $E/_{\langle \gamma \rangle}$ khi và chỉ khi tồn tại $\delta \in E$ sao cho $[\beta][\delta] = [1]$. Điều này xảy ra khi và chỉ khi có $\delta \in E$ sao cho $\beta\delta \equiv 1\ (mod\ \gamma)$ trong E, hay β và γ nguyên tố cùng nhau trong E.

Như vậy, với $a, b \in \mathbb{Z}$:

1) $[a + b\omega]$ khả nghịch trong $E/_{\langle 2^n \rangle}$ khi và chỉ khi $2 \nmid_E (a + b\omega)$, hay $2 \nmid_{\mathbb{Z}} a$ hoặc $2 \nmid_{\mathbb{Z}} b$. Chứng minh được tiến hành tương tự với $E/_{\langle p^n \rangle}$.

2) $[a]$ khả nghịch trong $E/_{\langle \pi_q^n \rangle}$ khi và chỉ khi $\pi_q \nmid_E a$. Lưu ý rằng:

$$\pi_q \nmid_E a \Rightarrow q = \pi_q\overline{\pi_q} \nmid_E a \Rightarrow q \nmid_{\mathbb{Z}} a;$$

và

$$\pi_q \mid_E a \Rightarrow \overline{\pi_q} \mid_E \overline{a} = a \Rightarrow q = \pi_q\overline{\pi_q} \mid_E a \Rightarrow q \mid_{\mathbb{Z}} a.$$

Do đó $\pi_q \nmid_E a$ khi và chỉ khi $q \nmid_{\mathbb{Z}} a$.

3) $[a + b\omega]$ khả nghịch trong $E/_{\langle \alpha^n \rangle}$ khi và chỉ khi $\alpha \nmid_E (a + b\omega)$. Hơn nữa, do

$$\frac{a+b\omega}{\alpha} = \frac{2b+a}{3} + \frac{2a+b}{-3}\omega;$$

nên $\alpha \nmid_E (a + b\omega)$ khi và chỉ khi thương trên không thuộc E, hay $a \not\equiv b\ (mod\ 3)$ trong $\mathbb{Z}$.

Chứng minh hoàn tất. ■

Hệ quả 2.4. Giá trị φ −hàm Euler cho các luỹ thừa phần tử nguyên tố trong E với $n \ge 1$ là:

1) $\varphi_E(2^n) = 3.2^{2n-2}$.

2) $\varphi_E(\pi_q^n) = q^{n-1}(q - 1)$.

3) $\varphi_E(p^n) = p^{2n-2}(p^2 - 1)$.

4) $\varphi_E(\alpha^n) = 2.3^{n-1}$.

3. Các kết quả chính

3.1. Một số bổ đề

Bổ đề 3.1. Lấy $\beta \in E$, r là số nguyên tố trong $\mathbb{Z}$, k là số nguyên dương. Khi đó ta có

$$(1+\beta r)^{r^k} = 1+\beta r^{k+1} + \frac{\beta^2}{2}(r^k-1)r^{k+2} + \gamma r^{k+2},\ \ \gamma \in E;$$

hay

$$(1+\beta r)^{r^k} = 1+\beta r^{k+1} + \frac{\beta^2}{2}(r^k-1)r^{k+2} \pmod{r^{k+2}}.$$

Chứng minh. Sử dụng khai triển Newton, ta thu được:

$$(1+\beta r)^{r^k} = \sum_{i=0}^{r^k} C_{r^k}^i(\beta r)^i = \left[1+\beta r^{k+1} + \frac{\beta^2}{2}(r^k-1)r^{k+2}\right] + \sum_{i=3}^{r^k} C_{r^k}^i(\beta r)^i.$$

Như vậy, ta cần chứng minh $r^{k+2} \mid C_{r^k}^i r^i$ trong $\mathbb{Z}$ với $i \geq 3$. Gọi số mũ đúng của số nguyên tố r trong phân tích tiêu chuẩn của số nguyên t là $\nu_r(t)$, ta cần chứng minh $k+2 \leq \nu_r\left(C_{r^k}^i r^i\right)$.

Theo Định lí Kummer (Titu et al., 2017), ta có $\nu_r\left(C_{r^k}^i\right) = k - \nu_r(i)$, do đó $\nu_r\left(C_{r^k}^i r^i\right) = k - \nu_r(i) + i$.

Nếu $\nu_r(i) \leq 1$ thì ta có ngay điều phải chứng minh. Nếu $\nu_r(i) \geq 2$ thì $\nu_r\left(C_{r^k}^i r^i\right) \geq k + r^{\nu_r(i)} - \nu_r(i)$ và ta quy về chứng minh $r^{\nu_r(i)} \geq \nu_r(i) + 2$, đúng do chứng minh bằng quy nạp theo $\nu_r(i)$.

Chứng minh hoàn tất. ■

Bổ đề 3.1 cho ta hệ quả sau, được sử dụng để chứng minh Bổ đề 3.3.

Hệ quả 3.2. Với k là số nguyên dương, ta có:

1) $(1+p\omega)^{p^k} \equiv 1 + p^{k+1}\omega \pmod{p^{k+2}}$.

2) $(1+2\omega)^{2^k} \equiv 1 + 2^{k+1} \pmod{2^{k+2}}$; $(1+4\omega)^{2^k} \equiv 1 + 2^{k+2}\omega \pmod{2^{k+3}}$.

Bổ đề 3.3. Với $n \geq 1$, ta có:

1) $[1+p\omega]$ có cấp p^{n-1} trong $\phi_E(p^n)$.

2) $[1+2\omega]$ có cấp 2^{n-1} trong $\phi_E(2^n)$; $[1+4\omega]$ có cấp 2^{n-2} trong $\phi_E(2^n)$ với $n \geq 2$.

3) $[1+3\omega]$ có cấp 3^{m-1} trong $\phi_E(\alpha^{2m})$ và có cấp 3^m trong $\phi_E(\alpha^{2m+1})$.

Chứng minh.

1) Theo Hệ quả 3.2, ta có:

$$(1+p\omega)^{p^{n-1}} \equiv 1 + p^n\omega \pmod{p^{n+1}};$$

và do đó $(1+p\omega)^{p^{n-1}} \equiv 1\ (mod\ p^n)$.

Vẫn theo Hệ quả 3.2:

$$(1+p\omega)^{p^{n-2}} \equiv 1 + p^{n-1}\omega \not\equiv 1 \pmod{p^n};$$

do đó cấp của $[1+p\omega]$ trong $\phi_E(p^n)$ là p^{n-1}.

2) Theo Hệ quả 3.2, ta có:

- $(1+2\omega)^{2^{n-1}} \equiv 1 + 2^n \pmod{2^{n+1}}$, do đó $(1+2\omega)^{2^{n-1}} \equiv 1 \pmod{2^n}$.
- $(1+2\omega)^{2^{n-2}} \equiv 1 + 2^{n-1} \not\equiv 1 \pmod{2^n}$.

và do đó cấp của $[1+2\omega]$ trong $\phi_E(2^n)$ là 2^{n-1}.

Ta cũng có từ hệ quả 3.2:

- $(1+4\omega)^{2^{n-2}} \equiv 1+2^n\omega \pmod{2^{n+1}}$, do đó $(1+4\omega)^{2^{n-2}} \equiv 1 \pmod{2^n}$.
- $(1+4\omega)^{2^{n-3}} \equiv 1+2^{n-1}\omega \not\equiv 1 \pmod{2^n}$.

và do đó cấp của $[1+4\omega]$ trong $\phi_E(2^n)$ là 2^{n-2}.

3) Đối với $\phi_E(\alpha^{2m})$, chứng minh được tiến hành tương tự như 1.

Đối với $\phi_E(\alpha^{2m+1})$, trước hết theo Hệ quả 3.2 ta có:

$$(1+3\omega)^{3^m} \equiv 1+3^{m+1}\omega \pmod{3^{m+2}};$$

và do $\alpha^{2m+1} \sim 3^m\alpha \mid_E 3^{m+1}$ nên:

$$(1+3\omega)^{3^m} \equiv 1 \pmod{\alpha^{2m+1}}.$$

Cũng theo Hệ quả 3.2 ta có:

$$(1+3\omega)^{3^{m-1}} \equiv 1+3^m\omega \pmod{3^{m+1}};$$

và do $\alpha^{2m+1} \mid_E 3^{m+1}$ nên

$$(1+3\omega)^{3^{m-1}} \equiv 1+3^m\omega \pmod{\alpha^{2m+1}}.$$

Do $\alpha^{2m+1} \nmid_E 3^m\omega$ nên $(1+3\omega)^{3^{m-1}} \not\equiv 1 \ (mod\ \alpha^{2m+1})$, và do đó cấp của $[1+3\omega]$ trong $\phi_E(\alpha^{2m+1})$ là 3^m.

Chứng minh hoàn tất. ■

Bổ đề 3.4. Với $m,n \geq 1$, ngoại trừ $[1]$, không phần tử nào của nhóm con $\langle[1+p\omega]\rangle$ của $\phi_E(p^n)$ có đại diện là $c, c\omega, c\overline{\omega}$ với $c \in \mathbb{R}$. Phát biểu vẫn đúng cho nhóm con $\langle[1+3\omega]\rangle$ của $\phi_E(\alpha^{2m})$ và $\phi_E(\alpha^{2m+1})$.

Chứng minh. Ta thực hiện chứng minh cho p. Chứng minh cho α được tiến hành tương tự.

Gọi một số phức c là *đặc biệt* nếu c có dạng $c_1, c_1\omega, c_1\overline{\omega}$ với $c_1 \in \mathbb{Z}$. Giả sử $(1+p\omega)^b$ đồng dư trong E với một số đặc biệt theo modulo p^n, với b nguyên dương thoả $0 < b < p^{n-1}$. Gọi B là tập hợp tất cả các số b như vậy. Trước hết, ta chứng minh p^{n-2} không thuộc B. Thật vậy, theo Hệ quả 3.2 ta có:

$$(1+p\omega)^{p^{n-2}} \equiv 1+p^{n-1}\omega \ (mod\ p^n).$$

Giả sử $(1+p\omega)^{p^{n-2}}$ đồng dư với số đặc biệt s theo modulo p^n, khi đó

$$1+p^{n-1}\omega - s \equiv 0 \ (mod\ p^n).$$

Với $s_1 \in \mathbb{Z}$, nếu $s = s_1$ thì p^n chia hết p^{n-1}, nếu $s = s_1\omega$ thì p^n chia hết 1, nếu $s = s_1\overline{\omega} = s_1 - s_1\omega$ thì p^n chia hết $1-s_1$ và $p^{n-1}+s_1$. Cả ba đều dẫn đến vô lí. Như vậy $p^{n-2} \notin B$. Tiếp theo, lấy L là phần tử nhỏ nhất của B và viết $p^{n-1} = Ld + r$ với $0 \leq r < L$. Nếu $r = 0$ thì $L = p^t$ với $0 < t < p^{n-2}$ (do $p^{n-2} \notin B$), khi đó

$$(1+p\omega)^{p^{n-2}} \equiv [(1+p\omega)^L]^{p^{n-2-t}};$$

cũng đồng dư với số đặc biệt. Điều này mâu thuẫn với kết luận $p^{n-2} \notin B$ ở trên. Nếu $r > 0$ thì trong $\phi_E(p^n)$ ta có

$$[1] = [1+p\omega]^{p^{n-1}} = [1+p\omega]^{Ld+r} = [1+p\omega]^{Ld}[1+p\omega]^r.$$

Do $(1+p\omega)^L$ đồng dư số đặc biệt nên $(1+p\omega)^{Ld}$ cũng vậy, giả sử là với s. Viết $s = s_1$ hoặc $s = s_1\omega$ hoặc $s = s_1\overline{\omega}$ với $s_1 \in \mathbb{Z}$. Vì s nằm trong nhóm nhân khả nghịch ứng với p^n nên s_1 nguyên tố cùng nhau với p. Như vậy, tồn tại $s_2 \in \mathbb{Z}$ sao cho $s_1 s_2 \equiv 1\ (mod\ p^n)$ trong $\mathbb{Z}$. Ta suy ra $s_1 s_2 \equiv 1\ (mod\ p^n)$ trong E, do đó $[s_1][s_2] = [1]$ trong $\phi_E(p^n)$. Như vậy

$$[s_2] = [ss_2][(1+p\omega)^r].$$

Nếu $s = s_1$ thì $[(1+p\omega)^r] = [s_2]$, nếu $s = s_1\omega$ thì $[(1+p\omega)^r] = [s_2\overline{\omega}]$, nếu $s = s_1\overline{\omega}$ thì $[(1+p\omega)^r] = [s_2\omega]$. Trong cả ba trường hợp, ta đều thấy $(1+p\omega)^r$ đều đồng dư số đặc biệt, điều này mâu thuẫn với cách chọn L.

Chứng minh hoàn tất. ■

3.2. Cấu trúc của nhóm $\phi_E(\pi_q^n)$

Định lí 3.5. Với $n \in \mathbb{N}, n \geq 1$, ta có

$$\phi_{\mathrm{E}}\left(\pi_{\mathrm{q}}^{\mathrm{n}}\right) \cong \mathbb{Z}_{q^n - q^{n-1}}.$$

Chứng minh. Theo Định lí 2.3:

$$\phi_E\left(\pi_q^n\right) = \{[a]: 1 \leq a < q^n, \gcd(q,a) = 1\}.$$

Lúc này, ánh xạ

$$\phi_{\mathbb{Z}}(q^n) \to \phi_E\left(\pi_q^n\right), [a] \mapsto [a];$$

là một đồng cấu, hơn nữa ta cũng thấy nếu $[a] = [b]$ trong $\phi_{\mathbb{Z}}\left(\pi_q^n\right)$ thì $q^n \mid_{\mathbb{Z}} (a-b)$, do đó $\pi_q^n \mid_E q^n \mid_E (a-b)$, hay $[a] = [b]$ trong $\phi_E\left(\pi_q^n\right)$, do đó ánh xạ trên là một đơn cấu.

Vì $\left|\phi_E\left(\pi_q^n\right)\right| = q^n - q^{n-1} = |\phi_{\mathbb{Z}}(q^n)|$ nên ta có đẳng cấu giữa hai nhóm, do đó

$$\phi_E\left(\pi_q^n\right) \cong \phi_{\mathbb{Z}}(q^n) \cong \mathbb{Z}_{q^n - q^{n-1}}.$$

Chứng minh hoàn tất. ■

3.3. Cấu trúc của nhóm $\phi_E(p^n)$

Định lí 3.6. Với $n \in \mathbb{N}, n \geq 1$, ta có:

$$\phi_E(p^n) \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Đặc biệt, với $n = 1$ thì $\phi_E(p)$ là nhóm cyclic cấp $p^2 - 1$.

Chứng minh. Trước hết, từ Bổ đề 3.3 ta có cấp của $[1+p\omega]$ trong $\phi_E(p^n)$ là p^{n-1}, hay $H = \langle[1+p\omega]\rangle$ có cấp là p^{n-1}.

Tiếp theo, ta có ánh xạ

$$\phi_{\mathbb{Z}}(p^n) \to \phi_E(p^n), [a] \mapsto [a];$$

là một đơn cấu. Lưu ý rằng $\phi_{\mathbb{Z}}(p^n)$ là nhóm cyclic và có cấp là $\varphi_{\mathbb{Z}}(p^n) = p^{n-1}(p-1)$, do đó tồn tại $[a]$ trong nhóm $\phi_{\mathbb{Z}}(p^n)$ có cấp p^{n-1}. Đặt $K = \langle[a]\rangle$ trong $\phi_E(p^n)$, khi đó cấp của K là p^{n-1}. Theo Bổ đề 3.4, không có phần tử nào của H có đại diện là số nguyên, như vậy $H \cap K = \{[1]\}$ và HK có cấp p^{2n-2}. Vì p nguyên tố trong E nên $E/_{\langle p\rangle}$ là trường hữu hạn, do đó $\phi_E(p)$ là nhóm cyclic và có cấp $p^2 - 1$ (do Hệ quả 2.4). Lấy $[\beta]$ là phần tử sinh $\phi_E(p)$, khi đó $\beta^{p^2-1} \equiv 1\ (mod\ p)$ hay $\beta^{p^2-1} = 1 + \gamma p$ với $\gamma \in E$. Theo Bổ đề 3.1:

$$\left(\beta^{p^2-1}\right)^{p^{n-1}} \equiv 1\ (\mathrm{mod}\ p^n);$$

hay

$$\left(\beta^{p^{n-1}}\right)^{p^2-1} \equiv 1 \pmod{p^n}.$$

Suy ra $\left[\beta^{p^{n-1}}\right]$ có cấp $t \mid (p^2-1)$. Ta suy ra $\beta^{tp^{n-1}} \equiv 1 \pmod{p}$, do đó $(p^2-1) \mid tp^{n-1}$, hay $(p^2-1) \mid t$. Do đó $t = p^2-1$ và $\left[\beta^{p^{n-1}}\right]$ có cấp là p^2-1 trong $\phi_E(p^n)$. Lấy $R = \langle\left[\beta^{p^{n-1}}\right]\rangle$. Vì mỗi phần tử trong HK đều có cấp là luỹ thừa của p nên $(HK) \cap R = \{[1]\}$ và cấp của nhóm HKR là $p^{2n-2}(p^2-1) = \varphi_E(p^n)$. Ta kết luận

$$\phi_E(p^n) = HKR \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Bổ đề 3.4. Với $m, n \geq 1$, ngoại trừ [1], không phần tử nào của nhóm con $\langle[1+p\omega]\rangle$ của $\phi_E(p^n)$ có đại diện là $c, c\omega, c\overline{\omega}$ với $c \in \mathbb{R}$. Phát biểu vẫn đúng cho nhóm con $\langle[1+3\omega]\rangle$ của $\phi_E(\alpha^{2m})$ và $\phi_E(\alpha^{2m+1})$.

Chứng minh. Ta thực hiện chứng minh cho p. Chứng minh cho α được tiến hành tương tự. Gọi một số phức c là *đặc biệt* nếu c có dạng $c_1, c_1\omega, c_1\overline{\omega}$ với $c_1 \in \mathbb{Z}$. Giả sử $(1+p\omega)^b$ đồng dư trong E với một số đặc biệt theo modulo p^n, với b nguyên dương thoả $0 < b < p^{n-1}$. Gọi B là tập hợp tất cả các số b như vậy. Trước hết, ta chứng minh p^{n-2} không thuộc B. Thật vậy, theo Hệ quả 3.2 ta có:

$$(1+p\omega)^{p^{n-2}} \equiv 1 + p^{n-1}\omega \ (mod\ p^n).$$

Giả sử $(1+p\omega)^{p^{n-2}}$ đồng dư với số đặc biệt s theo modulo p^n, khi đó

$$1 + p^{n-1}\omega - s \equiv 0 \ (mod\ p^n).$$

Với $s_1 \in \mathbb{Z}$, nếu $s = s_1$ thì p^n chia hết p^{n-1}, nếu $s = s_1\omega$ thì p^n chia hết 1, nếu $s = s_1\overline{\omega} = s_1 - s_1\omega$ thì p^n chia hết $1 - s_1$ và $p^{n-1} + s_1$. Cả ba đều dẫn đến vô lí. Như vậy $p^{n-2} \notin B$. Tiếp theo, lấy L là phần tử nhỏ nhất của B và viết $p^{n-1} = Ld + r$ với $0 \leq r < L$. Nếu $r = 0$ thì $L = p^t$ với $0 < t < p^{n-2}$ (do $p^{n-2} \notin B$), khi đó

$$(1+p\omega)^{p^{n-2}} \equiv [(1+p\omega)^L]^{p^{n-2-t}};$$

cũng đồng dư với số đặc biệt. Điều này mâu thuẫn với kết luận $p^{n-2} \notin B$ ở trên. Nếu $r > 0$ thì trong $\phi_E(p^n)$ ta có

$$[1] = [1+p\omega]^{p^{n-1}} = [1+p\omega]^{Ld+r} = [1+p\omega]^{Ld}[1+p\omega]^r.$$

Do $(1+p\omega)^L$ đồng dư số đặc biệt nên $(1+p\omega)^{Ld}$ cũng vậy, giả sử là với s. Viết $s = s_1$ hoặc $s = s_1\omega$ hoặc $s = s_1\overline{\omega}$ với $s_1 \in \mathbb{Z}$. Vì s nằm trong nhóm nhân khả nghịch ứng với p^n nên s_1 nguyên tố cùng nhau với p. Như vậy, tồn tại $s_2 \in \mathbb{Z}$ sao cho $s_1 s_2 \equiv 1 \ (mod\ p^n)$ trong $\mathbb{Z}$. Ta suy ra $s_1 s_2 \equiv 1 \ (mod\ p^n)$ trong E, do đó $[s_1][s_2] = [1]$ trong $\phi_E(p^n)$. Như vậy

$$[s_2] = [ss_2][(1+p\omega)^r].$$

Nếu $s = s_1$ thì $[(1+p\omega)^r] = [s_2]$, nếu $s = s_1\omega$ thì $[(1+p\omega)^r] = [s_2\overline{\omega}]$, nếu $s = s_1\overline{\omega}$ thì $[(1+p\omega)^r] = [s_2\omega]$. Trong cả ba trường hợp, ta đều thấy $(1+p\omega)^r$ đều đồng dư số đặc biệt, điều này mâu thuẫn với cách chọn L.

Chứng minh hoàn tất. ■

3.2. Cấu trúc của nhóm $\phi_E(\pi_q^n)$

Định lí 3.5. Với $n \in \mathbb{N}, n \geq 1$, ta có

$\phi_{\mathrm{E}}(\pi_{\mathrm{q}}^{\mathrm{n}}) \cong \mathbb{Z}_{q^n - q^{n-1}}$.

Chứng minh. Theo Định lí 2.3:

$\phi_E(\pi_q^n) = \{[a]: 1 \le a < q^n, \gcd(q,a) = 1\}$.

Lúc này, ánh xạ

$\phi_{\mathbb{Z}}(q^n) \to \phi_E(\pi_q^n), [a] \mapsto [a]$;

là một đồng cấu, hơn nữa ta cũng thấy nếu $[a] = [b]$ trong $\phi_{\mathbb{Z}}(\pi_q^n)$ thì $q^n \mid_{\mathbb{Z}} (a-b)$, do đó $\pi_q^n \mid_E q^n \mid_E (a-b)$, hay $[a] = [b]$ trong $\phi_E(\pi_q^n)$, do đó ánh xạ trên là một đơn cấu.

Vì $|\phi_E(\pi_q^n)| = q^n - q^{n-1} = |\phi_{\mathbb{Z}}(q^n)|$ nên ta có đẳng cấu giữa hai nhóm, do đó

$\phi_E(\pi_q^n) \cong \phi_{\mathbb{Z}}(q^n) \cong \mathbb{Z}_{q^n - q^{n-1}}$.

Chứng minh hoàn tất. ■

3.3. Cấu trúc của nhóm $\phi_E(p^n)$

Định lí 3.6. Với $n \in \mathbb{N}, n \ge 1$, ta có:

$\phi_E(p^n) \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}$.

Đặc biệt, với $n = 1$ thì $\phi_E(p)$ là nhóm cyclic cấp $p^2 - 1$.

Chứng minh. Trước hết, từ Bổ đề 3.3 ta có cấp của $[1 + p\omega]$ trong $\phi_E(p^n)$ là p^{n-1}, hay $H = \langle [1 + p\omega] \rangle$ có cấp là p^{n-1}.

Tiếp theo, ta có ánh xạ

$\phi_{\mathbb{Z}}(p^n) \to \phi_E(p^n), [a] \mapsto [a]$;

là một đơn cấu. Lưu ý rằng $\phi_{\mathbb{Z}}(p^n)$ là nhóm cyclic và có cấp là $\varphi_{\mathbb{Z}}(p^n) = p^{n-1}(p-1)$, do đó tồn tại $[a]$ trong nhóm $\phi_{\mathbb{Z}}(p^n)$ có cấp p^{n-1}. Đặt $K = \langle [a] \rangle$ trong $\phi_E(p^n)$, khi đó cấp của K là p^{n-1}. Theo Bổ đề 3.4, không có phần tử nào của H có đại diện là số nguyên, như vậy $H \cap K = \{[1]\}$ và HK có cấp p^{2n-2}. Vì p nguyên tố trong E nên $E/_{\langle p \rangle}$ là trường hữu hạn, do đó $\phi_E(p)$ là nhóm cyclic và có cấp $p^2 - 1$ (do Hệ quả 2.4). Lấy $[\beta]$ là phần tử sinh $\phi_E(p)$, khi đó $\beta^{p^2-1} \equiv 1 \ (mod\ p)$ hay $\beta^{p^2-1} = 1 + \gamma p$ với $\gamma \in E$. Theo Bổ đề 3.1:

$\left(\beta^{p^2-1}\right)^{p^{n-1}} \equiv 1 \pmod{p^n}$;

hay

$\left(\beta^{p^{n-1}}\right)^{p^2-1} \equiv 1 \pmod{p^n}$.

Suy ra $\left[\beta^{p^{n-1}}\right]$ có cấp $t \mid (p^2-1)$. Ta suy ra $\beta^{tp^{n-1}} \equiv 1 \pmod{p}$, do đó $(p^2-1) \mid tp^{n-1}$, hay $(p^2-1) \mid t$. Do đó $t = p^2 - 1$ và $\left[\beta^{p^{n-1}}\right]$ có cấp là $p^2 - 1$ trong $\phi_E(p^n)$. Lấy $R = \langle \left[\beta^{p^{n-1}}\right] \rangle$. Vì mỗi phần tử trong HK đều có cấp là luỹ thừa của p nên $(HK) \cap R = \{[1]\}$ và cấp của nhóm HKR là $p^{2n-2}(p^2-1) = \varphi_E(p^n)$. Ta kết luận

$\phi_E(p^n) = HKR \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}$.

3.6. Cấu trúc nhóm nhân của vành các lớp thặng dư tổng quát của E

Do E là vành Euclide nên mỗi phần tử $m \in E$, khác không và không khả nghịch đều phân tích được duy nhất dưới dạng $m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, trong đó với mỗi $i \in \{1,2,\dots,k\}$, p_i

là các phần tử nguyên tố trong vành E như đã mô tả ở Định lí 2.3, n_i là số nguyên dương. Khi đó theo Định lí thặng dư Trung Hoa cho vành chính E, ta có đẳng cấu vành sau:

$E/_{\langle m\rangle} \cong E/_{\langle p_1^{n_1}\rangle} \times E/_{\langle p_2^{n_2}\rangle} \times \cdots \times E/_{\langle p_k^{n_k}\rangle}$.

Đẳng cấu này cảm sinh ra đẳng cấu nhóm được phát biểu trong định lí sau.

Định lí 3.9. Nếu $m \in E$ có phân tích tiêu chuẩn $m = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ thì

$\phi_E(m) \cong \phi_E(p_1^{n_1}) \times \phi_E(p_2^{n_2}) \times \ldots \times \phi_E(p_k^{n_k})$;

do đó: $\varphi_E(m) = \varphi_E(p_1^{n_1})\varphi_E(p_2^{n_2}) \ldots \varphi_E(p_k^{n_k})$.

Chú ý rằng Định lí 3.9 cho phép mô tả cấu trúc của nhóm $\phi_E(m)$ vì cấu trúc của các nhóm $\phi_E(p_i^{k_i})$ đã được mô tả trong các Định lí 3.5 – 3.8.

Áp dụng Định lí 3.9 cùng các Định lí 3.5 – 3.8 ta có hệ quả sau.

Hệ quả 3.10. Phần tử $m \in E$ có căn nguyên thuỷ khi và chỉ khi m liên kết với một trong các phần tử sau: $2, p, \alpha, \alpha^2, \pi_q^n, 2\alpha$; trong đó $n \geq 1$.

- ***Tuyên bố về quyền lợi:*** *Các tác giả xác nhận hoàn toàn không có xung đột về quyền lợi.*
- ***Lời cảm ơn:*** *Nghiên cứu này được tài trợ bởi Nguồn ngân sách khoa học và công nghệ Trường Đại học Sư phạm Thành phố Hồ Chí Minh trong đề tài nghiên cứu khoa học của sinh viên năm học 2024-2025.*

TÀI LIỆU THAM KHẢO

Alaca, S., & Williams, K. S. (2004). *Introductory Algebraic Number Theory*. Cambridge University Press.

Bolker, E. D. (1970). *Elementary Number Theory*. W. A. Benjamin.

Cross, J. T. (1983). The Euler φ-function in the Gauss integers**.** *American Mathematical Monthly, 90*(8), 518-528.

Titu, A., Andreescu, T., & Mushkarov, O. (2017). *Number Theory: Concepts and Problems*. XYZ Press.

THE STRUCTURE OF MULTIPLICATIVE GROUPS OF RESIDUE CLASS RINGS OF THE EISENSTEIN INTEGERS

My Vinh Quang, Cao Phan Anh Dung*

Ho Chi Minh City University of Education, Vietnam

**Corresponding Author: Nguyen Phuc Duyet – Email: npduyet.spv@gmail.com*

Received: February 16, 2025; Revised: April 10, 2025; Accepted: April 17, 2025

ABSTRACT

This paper presents a comprehensive analysis of residue class ring of the Eisenstein integer ring modulo powers of prime elements. As a consequence, we also characterize the structure of the multiplicative group modulo arbitrary (composite) Eisenstein integers. Additionally, we determine all Eisenstein integers that admit primitive roots.

Keywords: Eisenstein integers; multiplicative groups; primitive roots