Transcendent Journal of Mathematics and Application
e-ISSN 2964-1845
Vol. 2, No. 2, Oct 2023, pp. 37-45

Kesiklikan Grup Unit dari Ring $\mathbb{Z}_n$

Dieny Ahda Damanik[1], Saiful Amri[1], Hafnani Hafnani[1,*]
[1]Mathematics Department, Faculty of Mathematics and Natural Sciences. Universitas Syiah Kuala, Banda Aceh, 23111, Indonesia.
*Corresponding email: hafnani@usk.ac.id

ARTICLE INFO
Article History
Received : 18-09-2023
Revised : 20-10-2023
Accepted : 22-10-2023

Keyword
unit group; cyclic group; generator; order.

ABSTRACT
The unit group of rings $\mathbb{Z}_n$ denoted by U_n is widely used in pure mathematics and applied mathematics. It makes the mathematics calculation in U_n more complicated as n gets bigger. However, when U_n is cyclic, the calculation is no longer matter. In previous research, it was shown that U_n is cyclic if and only if n = 2;4; p^k;$2p^k$ for any odd prim p and any positive integer k. This statement is known as Gauss' Theorem for primitive root. This paper aims to reprove The Gauss' Theorem using various tools like divisibility in $\mathbb{Z}$, group and ring, polynomials over integral domain and fields. It is stated by showing that U_{ab} is not cyclic where a,b > 2, (a,b) = 1. Thus, the necessity for U_n to be cyclic, n must be of the form 2^k; p^k or $2p^k$. Furthermore, we find U_{2^k} is cyclic if only if $k \in \{1,2\}$. And then, proved that U_p is cyclic and using induction on k, we find that U_{p^k} is cyclic. Finally, it is also found that U_{2p^k} is cyclic so that Gauss' Theorem is proven.

DOI: …

1. PENDAHULUAN

Diberikan aslian $n > 1$, himpunan cacahan yang lebih kecil dari n membentuk ring komutatif dengan satuan 1 terhadap tambah dan kali modulo n, disebut ring modulo n dan dinotasikan sebagai $\mathbb{Z}_n$. Grup unit dari ring $\mathbb{Z}_n$ (himpunan semua unit, yaitu unsur-unsur yang memiliki invers) dinotasikan sebagai U_n. Grup ini banyak digunakan dalam matematika murni maupun terapan seperti pemfaktoran utuhan yang digunakan dalam kriptografi RSA, uji prim, dan masih banyak lainnya.

Ini menjadikan perhitungan matematika di U_n semakin rumit seiring dengan semakin besarnya n. Akan tetapi, ketika $U_n = \langle a \rangle$ siklik, kendala tersebut dapat teratasi, dan akan lebih teratasi apabila pembangun a dipilih sekecil mungkin dari semua $\varphi(\varphi(n))$ pembangunnya. Ini suatu sebab mengapa jika U_n siklik orang tertarik untuk melihat apakah U_n dibangun oleh 2 atau tidak. Untuk lebih jelasnya, mari bandingkan antara grup siklik:

$$\begin{aligned} U_{13} = \langle 2 \rangle &= \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}\} \\ &= \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\} \end{aligned} \quad (1)$$

dengan grup tak-siklik $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Di U_{13}, untuk menghitung, katakanlah $x = 11^{100}5^{-1}3^{80}$, maka karena order dari 2 adalah sebanyak elemen U_{13} yaitu 12 dan 11 = 2^7,5 = 2^9,3 = 2^4, maka:

$$x = 2^{700}2^{-9}2^{320} = 2^4 2^3 2^8 = 2^3 = 8. \quad (2)$$

Perhatikan bahwa U_{13} memiliki $\varphi(\varphi(13)) = \varphi(12) = 4$ pembangun: 2,6,11,7; jika pembangun yang dipilih adalah 11, perhitungan untuk x di atas bisa juga dilakukan namun tidak semudah memilih 2 sebagai pembangunnya. Lain halnya dengan U_{15} yang tidak siklik, tidak semua unsurnya dapat ditulis sebagai pangkat suatu bilangan.

Tulisan ini bertujuan untuk melihat n yang bagaimana sehingga U_n siklik, tidak bertujuan untuk menentukan pembangunnya, apalagi mencari pembangun terkecil. Mencari pembangun dari U_n (jika siklik) masih *open problem* hingga saat ini.

Carl Frederick Gauss dalam bukunya Disquisitiones Arithmeticae, menunjukkan bahwa U_n siklik jika dan hanya jika $n = 2,4,p^k,2p^k$ untuk sebarang prim ganjil p dan aslian k. Pernyataan ini dikenal dengan sebutan Dalil Gauss untuk akar primitif sebab Gauss memiliki banyak dalil dan dalil ini membicarakan pembangun grup siklik dari U_n yang pada masa itu disebut akar primitif dimana teori grup belum dikenal (Gauss, 1966). Disini Dalil Gauss akan dibuktikan ulang dengan menggunakan berbagai landasan teori seperti keterbagian pada $\mathbb{Z}$, teori grup, ring, polinom atas daerah integral, lapangan dan lain sebagainya. Pembaca dari tulisan ini diharapkan telah memahami teori-teori dasar mengenai grup dan ring sehingga pada tinjauan kepustakaan, semua istilah dari grup dan ring tidak disinggung lagi dan hanya membahas beberapa saja yang terkait erat dengan tulisan ini.

2. METODE

Pada tulisan ini, semua istilah dan teori dasar mengenai grup dan ring tidak disinggung lagi dan hanya membahas beberapa yang terkait erat dengan tulisan ini. Mulai sekarang dan seterusnya, himpunan semua utuhan ditulis dengan $\mathbb{Z}$ dan himpunan semua utuhan tak-negatif ditulis dengan $\mathbb{N}$. Setiap variabel atau quantitas selalu diasumsikan di $\mathbb{Z}$, kecuali ada keterangan khusus. Semua istilah pada metode mengacu pada Burton (2010), Amri (2020) dan Gallian (2012).

2.1. Keterbagian

Well Ordering Principle (WOP). Jika $S \subset N$ dengan $S \neq \emptyset$, maka S memiliki unsur terkecil.

Dalil 1 (Algoritma Pembagian). Diberikan a dan $b > 0$, ada q dan r yang tunggal sehingga $a = qb + r$ dengan $0 \leq r < b$.

Definisi 1. Utuhan $a \neq 0$ dikatakan pembagi dari b (atau b kelipatan dari a) bila ada x sehingga $b = ax$. Ini dinotasikan dengan $a|b$ dan negasinya dengan $a \nmid b$.

Jelas bahwa | transitif dan jika $c \mid a \wedge c \mid b$ maka $c \mid ax + by, \forall x, y$.

Definisi 2. Diberikan a dan b, utuhan c disebut pembagi sekutu dari a dan b bila $c|a$ dan $c|b$; jika a dan b tidak keduanya nol, faktor persekutuan terbesar dari a dan b, dinotasikan dengan $gcd(a,b)$ atau (a,b), adalah utuhan d yang bersifat $d|a \wedge d|b$ dan jika $c|a \wedge c|b$, maka $c \leq d$. Bila $(a,b) = 1$, maka a dan b dikatakan saling prim, atau yang satu koprim dengan yang lainnya.

Jelas bahwa $(b,a) = (|a|,|b|), (a,0) = |a|$ dan jika $e|a$, maka $(e,a) = |e|$. Jika (a,b) ada dan $a = bq + r$, maka $(a,b) = (b,r)$.

Dalil 2 (Dalil Bezout). Diberikan a dan b yang tidak keduanya nol, maka ada x dan y yang memenuhi $(a,b) = ax + by$.

Dalil 3. $(a,b) = 1$ jika dan hanya jika $\exists x, y \in \mathbb{Z} \ni 1 = ax + by$.

Dalil 4 (Lemma Euclid). Jika $a|bc$ dan $(a,b) = 1$, maka $a|c$.

Dalil 5. Jika $a|m$ dan $b|m$ dengan $(a,b) = 1$, maka $ab|m$.

Dalil 6. Jika $(a,n) = 1$ dan $(b,n) = 1$ dengan $(a,b) = 1$, maka $(ab,n) = 1$.

Dalil 7. Jika $d = (a, b)$ dan c sebarang pembagi sekutu dari a dan b, maka $c|d$ dan $(a/c, b/c) = d/c$; akibatnya $(a/d, b/d) = 1$.

2.2. Bilangan Prim

Definisi 3. Utuhan $p > 1$ disebut prim bila pembagi positifnya hanya 1 dan p. Utuhan yang lebih besar dari satu dan tidak prim disebut komposit.

Jelas p prim, maka $(p, a) = 1$ bila $p \nmid a$, selainnya $(p, a) = p$.

Dalil 8. Jika p prim dan $p|ab$, maka $p|a$ atau $p|b$.

Dalil 9. (Dalil Dasar Aritmatika). Setiap utuhan $n > 1$ adalah prim atau perkalian dari sejumlah prim secara tunggal (tanpa memerhatikan urutan faktor-faktornya).

Akibat 1. Setiap utuhan $n > 1$ dapat ditulis sebagai (disebut bentuk kanonik)

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \tag{3}$$

dimana setiap $k_i \geq 1$ dan setiap p_i prim dengan $p_1 < \cdots < p_r$.

Dalam bentuk kanonik di atas jelas bahwa $(p_i^{k_i}, p_j^{k_j}) = 1$ jika dan hanya jika $i \neq j$.

2.3. Kongruensi

Definisi 4. Misal m sebarang aslian. Utuhan a dan b dikatakan kongruen modulo m, dinotasikan dengan $a \equiv b(mod\ m)$, bila $m|a - b$; negasinya ditulis dengan $a \not\equiv b(mod\ m)$. Utuhan m didalam kedua notasi itu disebut modulus. Bila modulusnya jelas dari topik pembicaraan, notasi $a \equiv b(mod\ m)$ cukup disingkat sebagai $a \equiv b$. Jika $a \in \mathbb{Z}$, maka didalam modulo n notasi $[a]_n$ menyatakan sisa tak-negatif terkecil dari pembagian a dengan n; bila n jelas dari apa yang dibicarakan, maka $[a]_n$ ditulis dengan $\bar{a}$ atau $\underline{a}$ atau cukup a saja.

Dalam modulo m jelas $a \equiv a$, jika $a \equiv b$ maka $b \equiv a$, dan jika $a \equiv b \wedge b \equiv c$ maka $a \equiv c$.

Dalil 10. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$, maka $a + c \equiv b + d(mod\ m)$ dan $ac \equiv bd(mod\ m)$.

Akibat 2. Jika $a \equiv b(mod\ m)$ maka $ak \equiv bk(mod\ m)$ untuk setiap $k \in \mathbb{N}$.

Dalil 11. Jika $ca \equiv cb(mod\ n)$, maka $a \equiv b(mod \frac{n}{c,n})$.

2.4. Fungsi Phi Euler

Definisi 5. Diberikan aslian n, banyaknya aslian $\leq n$ yang saling prim dengan n ditulis sebagai $\varphi(n)$ dan disebut dengan fungsi phi Euler.

Dalil 12 (Gauss). Untuk sebarang aslian n berlaku $\sum_{d|n} \varphi(d) = n$.

Dalil 13 (Euler). Jika n aslian dan $(a, n) = 1$, maka $a\varphi(n) \equiv 1(mod\ n)$.

Akibat 3 (Dalil Kecil). Jika p prim dan $p \nmid a$, maka $ap - 1 \equiv 1(mod\ p)$.

Dalil 14. $\varphi(1) = 1$ dan untuk $n > 1$ berlaku $\varphi(n) = \prod_{\text{prim } p|n} (\text{p} - 1)\text{p}^{\text{k}-1}$.

Akibat 4. Jika $m, n \geq 1$ dan $(m, n) = 1$, maka $\varphi(mn) = \varphi(m)\varphi(n)$.

2.5. Order Element Grup

Misal G grup (selalu diasumsikan multiplikatif, kecuali ada keterangan lain) dan $a \in G$. Aslian terkecil k (jika ada) disebut order dari a bila $ak = 1$, dinotasikan sebagai $k = o(a)$; bila k tidak ada, maka a disebut tidak memiliki order.

Dalil 15. Jika G grup hingga maka setiap unsurnya memiliki order.
Bukti: Jika $a \in G$ maka a_1, a_2 ,... semuanya di G dan karena G hingga, tidak mungkin a_1, a_2,... saling berbeda, jadi ada $1 \leq i < j$ sehingga $a^j = a^i$, akibatnya $a^{j-i} = 1$, yaitu ada suatu aslian k sehingga $ak = 1$. WOP mengatakan, ada aslian terkecil k_0 yang bersifat $a^{k_0} = 1$, yaitu $k_0 = o(a)$.

Dalil 16. Jika G grup hingga dan abelian maka untuk setiap $a \in G$: $o(a)$ membagi $|G|$.
Bukti: Untuk sembarang grup G (tidak harus abelian atau hingga) dan $a \in G$, pemetaan $aG \longrightarrow G$, $ag \longmapsto g$, jelas bijektif; akibatnya, karena $aG \subseteq G$, maka $aG = G$. Jika $G = \{a_1, \ldots, a_n\}$ hingga, perkalian dari semua unsur di G dapat dilakukan, dan karena $\{a_1, \ldots, a_n\} = \{aa_1, \ldots, aa_n\}$ plus G abelian maka:

$$a_1 \cdots a_n = aa_1 \cdots aa_n = a^n a_1 \cdots a_n, \qquad (4)$$

jadi $a^n = 1$. Tinggal dibuktikan n kelipatan $k = o(a)$ (keberadaan k jelas dari dalil sebelumnya). Karena $k > 0$ maka n bisa dibagi dengan k untuk mendapatkan $n = qk + r, 0 \leq r < k$, dan diharapkan sisa $r = 0$. Harapan ini pasti terjadi, sebab jika $r \neq 0$, maka r aslian yang $< k$ namun $a^r = a^n(a^k)^{-q} = ee^{-q} = 1$, padahal tadinya k aslian terkecil yang bersifat $a^k = 1$.

Dalil 17. Misal G grup dan $a \in G$ memiliki order k. Maka:
(a) $a^m = 1$ jika dan hanya jika $k|m$.
(b) $a^s = a^t$ jika dan hanya jika $s \equiv t(mod\ k)$.
(c) Untuk $n \in \mathbb{Z}^+$, $o(a^n) = \frac{k}{(k,n)}$.

Bukti:
(a) Syarat perlu sudah dibuktikan pada bukti dari dalil sebelumnya. Bukti untuk konversnya trivial.
(b) $a^s = a^t \Leftrightarrow a^{s-t} = 1 \Leftrightarrow k|s - t$ (menurut (a)) $\Leftrightarrow s \equiv t(mod\ k)$.
(c) Tulis $d = (k, n)$. Maka $s = k/d$ dan $t = n/d$ saling prim. Targetnya adalah $k/d = s$ adalah order dari a^n. Pertama, $(a^n)s = a^{dts} = (a^k)^t = 1^t = 1$. Berikutnya, jika l sebarang utuhan yang memenuhi $(a^n)^l = 1$, maka dari (a) didapat $o(a) = k = ds$ membagi $nl = dtu$ dan karena $d \neq 0$ tentu $s|tl$. Tetapi $(s, t) = 1$, Lemma Euclid berkata $s|l$. Ini menyimpulkan s order dari a^n.

2.6. Grup Siklik

Misal G grup dan $a \in G$. Subgrup terkecil dari G yang memuat a ditulis dengan $\langle a \rangle$ dan mudah diperiksa bahwa $\langle a \rangle = \{ak: k \in \mathbb{Z}\}$. Jika $k = o(a)$ ada, maka $\langle a \rangle = \{a^0, \ldots, a^{k-1}\}$. Sekedar mengulang, grup G disebut siklik bila ada $g \in G$ (disebut pembangun) sehingga $\langle g \rangle = G$.

Dalil 18. Misal grup **G=⟨a⟩** siklik. Maka:
(a) Jika G tak-hingga maka G memiliki pas dua pembangun (a dan a^{-1}) dan $G \approx \mathbb{Z}$.
(b) Jika $|G| = n$ maka G memiliki $\varphi(n)$ pembangun dan $G \approx \mathbb{Z}_n$.

Bukti:
(a) Jika G tak hingga maka $a^i \neq a^j$ jika dan hanya jika $i \neq j$ (jika ini tidak benar, maka a memiliki order, akibatnya $|G| = |\langle a \rangle| = o(a)$ berhingga). Maka pemetaan $G \rightarrow Z, a^m \mapsto m$, adalah bijektif dan keawetan operasinya terjaga (jika $x = a^s$ dan $y = a^t$ di G, maka $x \mapsto x$, $y \mapsto t$, sehingga $xy = a^s a^t = a^{s+t} \mapsto s + t$.
(b) Jika $|G| = n$ maka $o(a) = n$, akibatnya pemetaan $G \rightarrow \mathbb{Z}_n$, $a^m \mapsto m \cdot 1$ bijektif dan keawetan operasinya terjaga.

Akibat 5. Jika U_n siklik maka ia memiliki tepat $\varphi(\varphi(n))$ pembangun.

2.7. Ring

Ring yang memiliki unsur netral terhadap perkalian disebut unital. Dalam tulisan ini, jika A ring unital, selalu diasumsikan $1 \neq 0$, jadi A sedikitnya memiliki dua unsur.

Misal A ring unital. Himpunan semua unsur tak nol dari A ditulis dengan $A^\times$ dan himpunan semua unit dari A ditulis dengan $U(A)$ atau A^*. Khusus untuk ring $\mathbb{Z}_n$, grup unitnya ditulis dengan U_n. Misal A ring unital dan komutatif: (1) A disebut daerah integral atau domain bila untuk $ab = 0$ berlaku $a = 0 \vee b = 0$, (2) A disebut lapangan bila $A^* = A^\times$.

Diberikan ring komutatif A, dapat ditulis:

$$P = \{(c_0, \ldots, c_n) : c_i \in A,\ n \in N\}. \tag{5}$$

Misal diberikan $\alpha = (a_0, \ldots, a_h)$ dan $\beta = (b_0, \ldots, b_k)$ di P, sebutlah $h \geq k$. Definisikan $\alpha = \beta$ bila $a_i = b_i$ untuk $i = 1, \ldots, k$ dan $a_i = 0$ untuk $i > k$. Jika pada P operasi tambah dan kali ditetapkan sebagai sebagai:

$$\alpha + \beta = (a_0 + b_0, \ldots, a_h + b_h),\ b_i = 0,\ i > k, \tag{6}$$

dan

$$\alpha\beta = (\gamma_0, \ldots, \gamma_{h+k}),\ \gamma_i = \textstyle\sum_{j=0}^{i} a_{i-j} b_j\,, \tag{7}$$

maka P membentuk ring. Tambah dan kali dari dua unsur di P persis seperti tambah dan kali dua polinom: α dan β masing-masing dipandang sebagai polinom $f(x) = a_0 + a_1 x + \cdots + a_h x_h$, dan $g(x) = b_0 + b_1 x + \cdots + a_k x_k$. Untuk alasan ini, ring P disebut sebagai ring polinom dengan koefisien di A, ditulis dengan $A[x]$. Polinom konstan $(a, 0, \ldots, 0) \in A[x]$ ditulis sebagai $\hat{a}$ untuk membedakan dengan $a \in A$. Unsur $\hat{a}$ di $A[x]$ disebut polinom nol bila $a = 0$.

Setiap polinom tak-nol f dari $A[x]$ dapat ditulis sebagai

$$f(x) = a_0 + \cdots + a_n x_n,\ a_n \neq 0, \tag{8}$$

dan f dikatakan berderajat n (ditulis $n = \deg f$) dengan koefisien utama a_n. Maka polinom konstan berderajat nol, tetapi polinom nol tidak memiliki derajat. Unsur $a \in A$ disebut nol (atau akar) dari f bila $f(a) = 0$.

Dalil 19. Jika D domain, maka $D[x]$ juga domain.

Dalil 20. Misal ring A unital dan komutatif. Jika $f, g \in A[x]$ dimana $g \neq \hat{0}$ dan koefisien utama dari f berupa unit, maka ada $q, r \in A[x]$ yang tunggal sehingga $f = qg + r$ dimana $r = \hat{0}$ atau $\deg r < \deg g$.

Akibat 6. Jika D domain, $a \in D$, $f \in D[x]$, maka sisa pembagian $f(x)$ dengan $x - a$ adalah $f(a)$. Akibatnya, a akar dari f jika dan hanya jika $(x - a) | f(x)$.

Dalil 21 (Lagrange). Jika D domain dan f di $D[x]$ dengan $n = \deg f > 0$, maka persamaan $f(x) = 0$ memiliki paling banyak n buah akar.

3. HASIL DAN PEMBAHASAN

Langkah pengerjaan yang dilakukan yaitu pertama memastikan jika $a, b > 2$ saling prim maka U_{ab} tidak siklik. Akibatnya jika U_n siklik, maka n tidak mungkin memiliki dua pembagi prim ganjil atau lebih, jadi n harus berbentuk 2^k atau p^k atau $2p^k$ untuk suatu prim ganjil p dan aslian k. Langkah selanjutnya adalah meninjau bentuk $n = 2^k$ dan memastikan bahwa untuk kasus ini, hanya U_2 dan U_4 yang siklik. Kemudian akan ditinjau kasus $n = pk$ dengan cara membuktikan dahulu bahwa U_p siklik untuk sembarang prim ganjil p lalu melakukan induksi pada k untuk membuktikan U_{p^k} siklik; uniknya, basis induksi tidak mudah dibuktikan namun langkah induksinya lebih mudah, kebalikan dari kasus-kasus induksi pada umumnya. Terakhir yaitu membuktikan U_{2p^k} siklik dengan memanfaatkan hasil-hasil yang telah didapat sebelumnya.

3.1. Syarat perlu bagi n agar U_n siklik

Lemma 1. Untuk sebarang aslian $k > 2$, maka $\varphi(k)$ genap.

Bukti: Jika $k > 2$ maka $-1 \not\equiv 1(mod\ k)$ dan $-1 \equiv k - 1 \in Uk$. Karena $(-1)^2 \equiv 1$ yang berarti $o(-1) = 2$, maka berdasarkan Dalil 16, 2 adalah pembagi dari $|U_k| = \varphi(k)$ sehingga terbukti untuk $k > 2$, $\varphi(k)$ kelipatan 2.

Bukti lainnya (kombinatorik): $a \in U_k$ jika dan hanya jika $k - a \in U_k$ dan $a \not\equiv k - a$, tentu U_k dapat dipartisi kedalam pasangan $\{a, k - a\}$ dimana $a \in U_k$, $1 \leq a < \frac{k}{2}$.

Lemma 2. Untuk $a > 0$ dan $b > 0$, maka kelipatan sekutu terkecil dari a dan b adalah $\frac{ab}{(a,b)}$.

Bukti: Tulis $d = (a, b)$, maka tentu a dan b kelipatan dari d atau bisa ditulis $a = ds, b = dt$ untuk suatu utuhan s, t dan berdasarkan Dalil 2, d dapat ditulis sebagai kombinasi linier dari a dan b yaitu $d = ax + by$ untuk suatu utuhan x, y. Misal $l = \frac{ab}{d}$, maka $l = \left(\frac{a}{d}\right) b = sb$ dan juga $l = a\left(\frac{b}{d}\right) = at$ sehingga l adalah kelipatan a dan juga kelipatan b. Jika $h > 0$ sembarang kelipatan sekutu dari a dan b, sebut $h = au = bv$ untuk suatu utuhan u, v, maka

$$\frac{h}{l} = \frac{hd}{ab} = \frac{hax + hby}{ab} = \frac{bvax + auby}{ab} = vx + uy \qquad (9)$$

merupakan suatu utuhan sehingga jelas $h \geq l$. Maka terbukti kelipatan sekutu terkecil dari a dan b adalah $l = \frac{ab}{d}$.

Dalil 22. Jika a dan b saling prim dan keduanya lebih besar dari 2, maka U_{ab} tidak siklik.

Bukti: Jika $r \in U_{ab}$, yaitu $(r, ab) = 1$, maka $(r, a) = 1$ dan $(r, b) = 1$ sehingga berdasarkan Dalil 13, $r\varphi(a) \equiv 1(mod\ a)$ dan $r\varphi(b) \equiv 1(mod\ b)$. Misal $d = \big(\varphi(a), \varphi(b)\big)$ dan l kelipatan sekutu terkecil dari $\varphi(a)$ dan $\varphi(b)$. Karena $rl \equiv 1(mod\ a)$ dan $rl \equiv 1(mod\ b)$, maka kondisi $(a, b) = 1$ berakibat $rl \equiv 1(mod\ ab)$.

Kedua lemma di atas mengatakan $d \geq 2$ dan $l = \frac{\varphi(a)\varphi(b)}{d} = \frac{\varphi(ab)}{d} \leq \frac{\varphi(ab)}{2} < \varphi(ab)$. Ini menyimpulkan bahwa order dari setiap unsur r di U_{ab} adalah kurang dari $\varphi(ab)$, jadi U_{ab} tidak memiliki pembangun sehingga U_{ab} tidak siklik.

Akibat dari dalil ini adalah U_n pasti tidak siklik bila n memiliki lebih dari satu pembagi prim ganjil atau n berbentuk $2^t p^k$ dimana p prim ganjil, $t > 2$ atau dapat diperjelas seperti pada Akibat 7 berikut.

Akibat 7. Syarat perlu agar U_n siklik adalah n berbentuk 2^k atau p^k atau $2p^k$ untuk suatu prim ganjil p dan aslian k. Kesiklikan U_{2^k} , U_{p^k} dan U_{2p^k} akan dibahas secara berurutan dalam setiap subbab berikut.

3.2. Kesiklikan U_{2^k}

Dalil 23. U_{2^k} siklik untuk $k \in \{1,2\}$ dan tidak siklik untuk $k > 2$.

Bukti: Jelas $U_2 = \langle 1 \rangle$ dan $U_4 = \langle 3 \rangle$ siklik, jadi asumsikan $k > 2$. Jelas $\bar{r} \in U_{2^k}$ jika dan hanya jika r ganjil. Jika untuk setiap r ganjil berhasil dibuktikan $r^{2^{k-2}} \equiv 1 (mod\ 2^k)$, maka order dari setiap unsur di U_{2^k} pasti lebih kecil atau sama dengan $2^{k-2} < 2^{k-1} = \varphi(2^k) = |U_{2^k}|$, ini membuktikan U_{2^k} tidak siklik. Untuk sembarang ganjil r, akan dilakukan induksi pada k.

Untuk basis induksi, akan diperlihatkan untuk $k = 3$, jelas $r^2 \equiv 1 (mod\ 8)$ sehingga pernyataan benar. Untuk hipotesis induksi diasumsikan untuk $k - 1 > 3$, $r^{2^{k-3}} \equiv 1 (mod\ 2^{k-1})$, jadi ada s sehingga $r^{2^{k-2}} = 1 + s2^{k-1}$. Maka untuk k:

$$r^{2^{k-2}} = \left(r^{2^{k-3}}\right)^2 = (1 + s2^{k-1})^2 = 1 + s2^k + s^2 2^{2k-2} \equiv 1 (mod\ 2^k), \quad (10)$$

sebab jika $k > 3$ maka $2k - 2 - k = k - 2 > 0$ sehingga $2k - 2 > k$ dan $2^k | 2^{2k-2}$. Akibatnya pernyataan terbukti dan jelas U_{2^k} tidak siklik.

Sebagai contoh, untuk $k = 6$, yaitu pada $U_{2^6} = U_{64}$ yang beranggotakan seluruh bilangan ganjil positif yang lebih kecil dari 64 berlaku $\forall r \in U_{64}, r^{\varphi(25)} = r^{16} \equiv 1 (mod\ 64)$. Akibatnya, tidak ada anggota U_{64} yang memiliki order $|U_{64}| = \varphi(64) = 32$ sehingga U_{64} tidak siklik.

3.3. Kesiklikan U_p

Pada dalil berikut tidak hanya akan ditunjukkan bahwa U_p memiliki pembangun melainkan juga berapa banyak pembangun dari U_p sehingga langsung berakibat bahwa U_p siklik untuk setiap prim p, genap atau ganjil.

Dalil 24. Jika F lapangan dan G subgrup hingga dari F^*, maka G siklik.

Bukti: Misal $\psi(d)$ adalah banyaknya unsur di G yang berorder d. Karena order dari setiap unsur di G adalah pembagi dari $n = |G|$, maka d cukup dibatasi pada semua pembagi positif dari n saja dan ini juga berakibat $\sum_{(d|n)} \psi(d) = n$. Jika terbuktikan:

$$\psi(d) \leq \varphi(d), \ \forall 0 < d | n, \quad (11)$$

maka $\psi(d) = \varphi(d)$; sebab jika (11) tidak benar maka dari Identitas Gauss diperoleh $n = \sum_{(d|n)} \varphi(d) > \sum_{(d|n)} \psi(d) = n$. Akibatnya, dengan memilih $d = n$ (hal ini boleh sebab tentu $n|n$), diperoleh bahwa G memiliki $\psi(n) = \varphi(n) > 0$ pembangun, jadi G siklik.

Jadi tinggal dibuktikan (11) bisa terjadi bahwa meskipun $d|n$ namun G tidak memiliki unsur berorder d, dalam hal ini $\psi(d) = 0$ dan ini jelas memenuhi (11). Jika $\psi(d) \neq 0$, maka ada subgrup siklik $\langle a \rangle = \{1, a, \ldots, a^{d-1}\}$ berorder d dari G yang memiliki $\varphi(d)$ pembangun (yaitu unsur berorder d), jadi $\psi(d) \geq \varphi(d)$. Untuk menjamin (11) terpenuhi, harus dipastikan bahwa $G \backslash \langle a \rangle$ tidak memuat unsur b yang berorder d. Jaminan itu pasti sebab jika b ada maka ia akar dari polinom $p(x) = x^d - 1$. Tetapi kesemua d unsur di $\langle a \rangle$ memenuhi $p(x) = 0$, keberadaan b bertentangan dengan Dalil 21 bahwa p memiliki lebih dari $\deg p = d$ akar.

Jika p prim, maka $\mathbb{Z}_p$ lapangan hingga, dan $\mathbb{Z}_p^* = \{1,2,\dots,p-1\} = U_p$. Akibatnya, dengan memilih $F = \mathbb{Z}_p$ dan $G = \mathbb{Z}_p^*$ terbukti bahwa U_p siklik. Atau lebih jelasnya pada Akibat 8 berikut:

Akibat 8. Untuk setiap prim p, U_p siklik dan memiliki $\varphi(|U_p|)$ buah pembangun.

3.4. Kesiklikan U_{p^k}

Dengan mengetahui U_p, akan dibuktikan U_{p^k} juga siklik dengan melakukan induksi pada k. Buktinya memerlukan Lemma 3 berikut:

Lemma 3. Jika p prim ganjil dan $k > 1$, maka ada pembangun $\underline{r}$ dari U_p sehingga:

$$r^{\varphi(p^{k-1})} \not\equiv 1(mod\ p^k). \tag{12}$$

Bukti: Telah dilihat bahwa U_p siklik, sebutlah dibangun oleh r. Maka akan dilakukan induksi pada k.

Untuk basis induksi, tinjau kasus $k = 2$, sehingga (12) menjadi

$$r^{\varphi(p)} = r^{p-1} \not\equiv 1(mod\ p\text{^}2). \tag{13}$$

Bila r memenuhi (13) maka tugas selesai, bila $r^{p-1} \equiv 1(mod\ p^2)$ maka pilih utuhan $s = r + p$ (yang juga wakil dari r) dan s inilah sekarang yang memenuhi (13):

$$\begin{aligned} s^{p-1} = (r+p)^{p-1} &\equiv r^{p-1} + (p-1)r^{p-2}p(mod\ p^2) \\ &\equiv 1 - pr^{p-2}(mod\ p^2) \\ &\not\equiv 1(mod\ p^2) \end{aligned} \tag{14}$$

sebab $p \nmid r^{p-2}$ (andaikan $p|r^{p-2}$, maka $p|r$, bertentangan dengan $\underline{r} \in U_p$). Jadi lemma berlaku untuk $k = 2$.

Untuk hipotesis induksi, diasumsikan lemma berlaku untuk suatu $k > 2$. Karena $(r, p^{k-1}) = (r, p) = 1$, dari Dalil 13

$$r^{p-1}p^{k-2} = r^{\varphi(p^{k-1})} \equiv 1(mod\ p^{k-1}), \tag{15}$$

jadi $r^{(p-1)p^{k-2}} = 1 + ap^{k-1}$ untuk suatu a, maka untuk k:

$$r^{\varphi(p^k)} = r^{(p-1)p^{k-1}} = (1 + ap^{k-1})^p \equiv 1 + pap^{k-1}(mod\ p^{k+1}). \tag{16}$$

Dari hipotesis induksi, $p \nmid a$ (andaikan $p|a$, maka bertentangan dengan (12)), tentu $p^{k+1} \nmid pap^{k-1}$. Maka $r^{\varphi(p^k)} \not\equiv 1(mod\ p^{k+1})$ dan Lemma 3 terbukti.

Dalil 25. Jika p prim ganjil, maka U_{p^k} siklik untuk setiap aslian k.

Bukti: Akan dibuktikan dengan melakukan induksi terhadap k. Untuk basis induksi, telah dibuktikan bahwa U_{p^k} siklik untuk $k = 1$ dan misal $\underline{r}$ sembarang pembangun dari U_p. Untuk hipotesis induksi, asumsikan $k > 1$ dan misal n adalah order dari $r \in U_{p^k}$. Kondisi $r^n \equiv 1(mod\ p^k)$ berakibat $r^n \equiv 1(mod\ p)$, dan karena $\langle \underline{r} \rangle = U_p$ maka Dalil 17-a mengatakan $n = (p-1)a$ untuk suatu a. Kemudian Dalil 16 mengatakan $n|\varphi(p^k) = (p-1)p^{k-1}$, sehingga tentu $a|p^{k-1}$. Jadi $a = p^i$ untuk suatu $0 \le i < k$ dan n berbentuk $n = (p-1)p^i$. Andaikan $n \neq (p-1)p^{k-1}$, maka $n|(p-1)p^{k-2}$. Tetapi ini berakibat $r^{(p-1)p^{k-2}} \equiv 1(mod\ p^k)$, yaitu setiap pembangun $\underline{r}$ dari U_p tidak memenuhi (12). Maka harus $n = (p-1)p^{k-1}$ sehingga U_{p^k} siklik.

Dalil 26. Jika p prim ganjil, maka U_{2p^k} siklik untuk setiap aslian k.

Bukti: Karena U_{p^k} siklik, maka $\langle \underline{r} \rangle = U_{p^k}$ untuk suatu r. Kita dapat mengasumsikan bahwa r ganjil sebab andaipun r genap maka $s = r + pk$ (yang juga wakil dari r) ganjil dan $\langle s \rangle = U_{p^k}$. Karena $(r, 2) = 1$ dan $(r, p^k) = 1$ dengan $(2, p^k) = 1$, maka berdasarkan Dalil 6, $(r, 2p^k) = 1$, jadi $\underline{r} \in U_{2p^k}$. Akan dibuktikan $\langle \underline{r} \rangle = U_{2p^k}$.

Misal n order dari r di U_{2p^k}, jadi berdasarkan Dalil 16, n berupa faktor dari

$$|U_{2p^k}| = \varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k). \quad (17)$$

Tetapi $r^n \equiv 1(mod\ 2p^k)$ berakibat $r^n \equiv 1(mod\ p^k)$, berhubung $\langle \underline{r} \rangle = U_{p^k}$ maka $\varphi(p^k) = o(r)$ adalah faktor dari n. Maka $n = \varphi(p^k) = |U_{p^{2k}}|$ sehingga U_{2p^k} siklik.

Bukti dari kedua dalil terakhir di atas juga menyimpulkan bahwa Dalil 27. Jika U_{p^k} dibangun oleh r, maka U_{2p^k} dibangun oleh r atau $r + p^k$.

4. KESIMPULAN

Berdasarkan hasil dan pembahasan, diperoleh kesimpulan yaitu Dalil Gauss untuk akar primitif yang menyatakan U_n siklik apabila $n = 2,4, p^k, 2p^k$ dapat dibuktikan ulang menggunakan berbagai landasan teori. Dimulai dengan menunjukkan U_{ab} tidak siklik dimana $a, b > 2, (a, b) = 1$. Maka syarat perlu agar U_n siklik harus $n = 2^k, p^k, 2p^k$ dimana p sebarang prim ganjil dan k aslian. Kemudian didapati U_{2^k} siklik hanya apabila $k = 1,2$ dan menggunakan induksi, diperoleh U_{p^k} siklik. Terakhir, didapati pula bahwa U_{2p^k} siklik sehingga Dalil Gauss terbukti. Penulisan ini hanya bertujuan untuk menunjukkan kesiklikan pada U_n (yang berarti apabila U_n siklik, maka U_n memiliki pembangun) tanpa mencari tahu apa pembangunnya. Maka dari itu, untuk penelitian selanjutnya dapat diselidiki pembangun dari U_n yang telah diketahui kesiklikannya, terlebih untuk mencari tahu pembangun terkecilnya. Sebab tentu akan jauh lebih mudah melakukan operasi aritmatika pada angka yang lebih kecil.

REFERENSI

Amri, S. (2020). *Order Element*. Diakses pada 5 April 2021 dari https://www.youtube.com/watch?v=ijoslmLiJME.

Burton, D. M. (2010). *Elementary Number Theory* (7th Ed.). McGraw-Hill, New York.

Gallian, J. A. (2012). *Contemporary Abstract Algebra* (8th Ed.). Cengage Learning, Duluth.

Gauss, C. F. (1966). *Disquisitiones Arithmeticae*. Terjemahan dari Disquisitiones Arithmeticae, oleh Arthur A. Clarke, Yale University Press, New Haven.