Rzędy Elementów Grupy Abelowej

Andrzej Nowicki

16 września 2015, wersja rz-15

Niech G będzie grupą z elementem neutralnym e i niech $a \in G$. Załóżmy, że istnieje co najmniej jedna dodatnia liczba całkowita n spełniająca równość $a^n = e$. Wówczas najmniejszą taką dodatnią liczbę całkowitą n nazywamy *rzędem elementu a w grupie G*.

Przedstawimy podstawowe własności rzędów. Omówimy rzędy elementów skończonych grup abelowych i w szczególności grup cyklicznych. Sporo miejsca przeznaczymy na rzędy elementów multyplikatywnych grup pierścieni $\mathbb{Z}_m$. Przedstawimy również pewne zastosowania rzędów w teorii ciał.

W tym opracowaniu liczbami naturalnymi nazywamy wszystkie dodatnie liczby całkowite. Zera nie zaliczamy tu do zbioru liczb naturalnych.

Spis treści

1 Rzędy elementów dowolnej grupy **1**
1.1 Rzędy i ich własności 2
1.2 Elementy rzędu 2 4

2 Rzędy elementów i grupy abelowe **5**
2.1 Własności rzędów elementów grup abelowych 6
2.2 Rzędy elementów skończonej grupy cyklicznej 7
2.3 Grupy z trywialnymi kwadratami 9
2.4 Liczba elementów rzędu 2 dla grup abelowych 10
2.5 Iloczyny elementów grupy abelowej 11

3 Multyplikatywna grupa modulo m **13**
3.1 Potęgi dwójki 14
3.2 Potęgi nieparzystej liczby pierwszej 16
3.3 Cykliczne grupy multyplikatywne modulo m 19
3.4 Przykłady 21

4 Pewne zastosowania rzędów w teorii ciał **23**

1 Rzędy elementów dowolnej grupy

W tym rozdziale G jest dowolną grupą (przemienną lub nieprzemienną) i e jest jej elementem neutralnym. Jeśli A jest skończonym zbiorem, to przez $|A|$ oznaczamy liczbę jego elementów.

1.1 Rzędy i ich własności

Stwierdzenie 1.1. *Jeśli grupa G jest skończona, to dla każdego jej elementu a istnieje taka dodatnia liczba całkowita n, że $a^n = e$ oraz $n \leqslant |G|$.*

Dowód. Niech $|G| = m$ oraz $a \in G$. Rozpatrzmy elementy $a, a^2, \ldots, a^{m+1}$. Są to elementy grupy G i jest ich więcej niż m. Istnieją więc dwie liczby $i, j \in \{1, 2, \ldots, m+1\}$ takie, że $i > j$ oraz $a^i = a^j$. Wtedy $a^{i-j} = e$, a zatem $a^n = e$ dla $n = i - j$. Mamy ponadto $1 \leqslant n \leqslant m$. ⊠

Niech $a \in G$. Najmniejszą liczbę naturalną n taką, że $a^n = e$ oznaczamy przez $\mathrm{ord}_G(a)$ i nazywamy *rzędem elementu a w grupie G*. Jeśli taka liczba naturalna n nie istnieje, to mówimy, że a jest elementem nieskończonego rzędu i piszemy $\mathrm{ord}_G(a) = \infty$. W przypadkach gdy grupa G jest ustalona, pisać będziemy często $\mathrm{ord}(a)$ zamiast $\mathrm{ord}_G(a)$. Wprost z definicji otrzymujemy, że $\mathrm{ord}_G(a) = 1 \iff a = e$.

Ze Stwierdzenia 1.1 wynika, że każdy element grupy skończonej ma skończony rząd i ten rząd nie przewyższa rzędu danej grupy. Jeśli każdy element danej grupy G ma skończony rząd, to grupa G nie musi być skończona. Taką grupą jest na przykład grupa ilorazowa $\mathbb{Q}/\mathbb{Z}$. Grupa ta nie jest skończona, a każdy jej element ma skończony rząd.

Dla danego elementu a grupy G oznaczmy przez $\langle a \rangle$ podgrupę grupy G generowaną przez element a, tzn.

$$\langle a \rangle = \{a^j;\ j \in \mathbb{Z}\}.$$

Stwierdzenie 1.2. *Niech G będzie dowolną grupą i niech a będzie jej elementem skończonego rzędu. Niech $\mathrm{ord}_G(a) = m$. Wtedy elementy $a^0 = e, a^1, \ldots, a^{m-1}$ są parami różne oraz*

$$\langle a \rangle = \left\{a^0,\ a^1,\ a^2,\ \ldots,\ a^{m-1}\right\}.$$

Dowód. Oznaczmy $A = \{a^0,\ a^1,\ a^2,\ \ldots,\ a^{m-1}\}$. Niech $j \in \mathbb{Z}$. Niech $j = km + r$, gdzie $k, r \in \mathbb{Z}$, $0 \leqslant r < m$. Wtedy $a^j = a^{km+r} = (a^m)^k \cdot a^r = e^k a^r = a^r$, czyli $a^j \in A$. Mamy więc inkluzję $A \subseteq \langle a \rangle$. Inkluzja w przeciwnym kierunku jest oczywista.

Przypuśćmy, że $a^i = a^j$ dla pewnych $i, j \in \{0, 1, \ldots, m-1\}$, $i > j$. Wtedy $a^{i-j} = e$ oraz $1 \leqslant i - j < m$ i mamy sprzeczność z własnością minimalności liczby m. ⊠

Z tego stwierdzenia wynika, że rząd elementu a w grupie G to nic innego jak rząd podgrupy $\langle a \rangle$. Z twierdzenia Lagrange'a otrzymujemy więc:

Stwierdzenie 1.3. *Jeśli G jest grupą skończoną rzędu m, to rząd każdego jej elementu jest dzielnikiem liczby m.*

Stąd następnie wynika następujące uogólnienie znanego twierdzenia Eulera.

Stwierdzenie 1.4. *Jeśli G jest grupą skończoną rzędu m, to dla każdego $a \in G$ zachodzi równość $a^m = e$.*

Dowód. Niech $a \in G$, niech $\mathrm{ord}_G(a) = r$. Wtedy $r \mid m$ (na mocy poprzedniego stwierdzenia). Niech $m = kr$. Mamy wtedy: $a^m = (a^r)^l = e^k = e$. $\boxtimes$

W wielu książkach z teorii grup lub z rozdziałami o teorii grup (patrz na przykład [2], [3], [1]) znajdziemy liczne fakty i informacje dotyczące rzędów. Udowodnimy teraz kilka podstawowych własności rzędów elementów grupy.

Stwierdzenie 1.5. *Niech $a \in G$, $\mathrm{ord}_G(a) = m < \infty$. Jeśli $j \in \mathbb{Z}$, to*

$$a^j = e \iff m \mid j.$$

Dowód. Niech $a^j = e$. Niech $j = km + r$, $k, r \in \mathbb{Z}$, $0 \leqslant r < m$. Przypuśćmy, że $r \geqslant 1$. Wtedy $a^r = e$, gdyż $e = a^j = (a^m)^k a^r = e^k a^r = a^r$ i mamy sprzeczność z własnością minimalności liczby m. Zatem $m \mid j$.

Jeśli $m \mid j$, to $j = km$, gdzie $k \in \mathbb{Z}$ i wtedy $a^j = (a^m)^k = e^k = e$. $\boxtimes$

Stwierdzenie 1.6. *Niech $a \in G$, $\mathrm{ord}_G(a) = m < \infty$. Jeśli $r \in \mathbb{Z}$, to*

$$\mathrm{ord}_G(a^r) = \frac{m}{(r, m)}.$$

Dowód. Oznaczmy $s = \mathrm{ord}_G(a^r)$ oraz $d = (r, m)$. Niech $r = ud$, $m = vd$, gdzie $u, v \in \mathbb{Z}$, $(u, v) = 1$. Należy pokazać, że $s = v$. Zauważmy, że $(a^r)^v = a^{udv} = a^{mu} = (a^m)^u = e^u = e$. Zatem $s \mid v$ (na mocy Stwierdzenia 1.5). Mamy również: $a^{rs} = (a^r)^s = e$, a więc $m \mid rs$, więc $vd \mid uds$, więc $v \mid us$. Ale liczby u, v są względnie pierwsze, więc $v \mid s$. Zatem $s = v = \frac{m}{(r,m)}$. $\boxtimes$

Z tego stwierdzenia otrzymujemy natychmiast:

Stwierdzenie 1.7. *Niech $a \in G$, $\mathrm{ord}_G(a) = m < \infty$ i niech $r \in \mathbb{Z}$.*

(1) *Jeśli $(r, m) = 1$, to $\mathrm{ord}_G(a^r) = m$.*

(2) *Jeśli $r \geqslant 1$ oraz $r \mid m$, to $\mathrm{ord}_G(a^r) = \frac{m}{r}$.*

(3) $\mathrm{ord}_G(a^{-1}) = \mathrm{ord}_G(a)$.

Z ostatniej równości otrzymujemy natychmiast:

Stwierdzenie 1.8. *W każdej grupie skończonej liczba elementów rzędu większego od* 2 *jest parzysta.*

Stwierdzenie 1.9. *Niech $m \geqslant 3$. W każdej grupie skończonej liczba elementów rzędu m jest parzysta.*

Następne stwierdzenia znajdziemy w [17] lub [14]. Literą G oznaczono dowolną grupę z mnożeniem oraz a, b, c są elementami grupy G.

Stwierdzenie 1.10. $\mathrm{ord}_G(ab) = \mathrm{ord}_G(ba)$.

Dowód. Jeśli rzędy elementów ab i ba są nieskończone, to nie ma czego dowodzić. Załóżmy, że $\mathrm{ord}_G(ab) = n < \infty$ i niech $(ba)^n = u$. Wtedy $au = (ab)^n a = a$, więc $u = e$. Zatem $(ba)^n = e$, czyli $\mathrm{ord}_G(ba) \leqslant n$. Jeśli więc $\mathrm{ord}_G(ab) < \infty$, to $\mathrm{ord}_G(ba) < \infty$ oraz $\mathrm{ord}_G(ba) \leqslant \mathrm{ord}_G(ab)$. Analogicznie wykazujemy, że $\mathrm{ord}_G(ab) \leqslant \mathrm{ord}_G(ba)$. ⊠

Stwierdzenie 1.11.

(1) $\mathrm{ord}_G(aba^{-1}) = \mathrm{ord}_G(b)$.

(2) $\mathrm{ord}_G(abc) = \mathrm{ord}_G(bca) = \mathrm{ord}_G(cab)$.

Dowód. Korzystamy z poprzedniego stwierdzenia. ⊠

Stwierdzenie 1.12. *Elementy abc i cba mogą mieć różne rzędy.*

Dowód. ([7] zadanie 5.3.6). Niech G będzie grupą S_3, permutacji zbioru $\{1, 2, 3\}$. Niech a, b, c będą następującymi cyklami: $a = (1, 2, 3)$, $b = (1, 2)$ oraz $c = (1, 3)$. Wtedy abc jest permutacją tożsamościową, więc jej rząd jest równy 1. Natomiast permutacja cba jest cyklem $(3, 2, 1)$, ma więc rząd równy 3. ⊠

Łatwy dowód następnego stwierdzenia znajdziemy na przykład w [3].

Stwierdzenie 1.13. *Niech $f : G \to H$ będzie homomorfizmem grup. Niech $a \in G$ oraz $\mathrm{ord}_G(a) < \infty$. Wtedy $\mathrm{ord}_H(f(a)) < \infty$ oraz liczba $\mathrm{ord}_H(f(a))$ jest dzielnikiem liczby $\mathrm{ord}_G(a)$. Jeśli f jest injekcją, to $\mathrm{ord}_H(f(a)) = \mathrm{ord}_G(a)$.*

1.2 Elementy rzędu 2

Wykażemy teraz, że każda skończona grupa parzystego rzędu ma co najmniej jeden element rzędu 2 i przy tym liczba wszystkich jej elementów rzędu 2 jest nieparzysta.

Niech G będzie dowolną grupą. Rozważmy relację $\sim$ w G zdefiniowaną następująco:

$$a \sim b \ \text{ jeśli } b = a \ \text{ lub } \ b = a^{-1}$$

dla $a, b \in G$. Z łatwością sprawdzamy, że $\sim$ jest relacją typu równoważności. Oznaczmy przez $[a]$ klasę abstrakcji elementu $a \in G$ względem tej relacji oraz oznaczmy przez $d(a)$ liczbę elementów klasy abstrakcji $[a]$. Jest jasne, że $[a] = \{a, a^{-1}\}$, $1 \leqslant d(a) \leqslant 2$ oraz $d(e) = 1$. Jeśli a jest elementem różnym od e, to

$$d(a) = 1 \iff a = a^{-1} \iff \mathrm{ord}_G(a) = 2.$$

Dla wszystkich elementów $a \in G \setminus \{e\}$ o rzędzie większym od 2 liczba $d(a)$ jest więc równa 2.

Ponieważ relacja $\sim$ jest typu równoważności, więc G jest sumą mnogościową parami rozłącznych klas abstrakcji. Załóżmy, że grupa G jest skończona oraz $\{a_0 =$

$e, a_1, \ldots, a_s\}$ jest wyborem jej reprezentantów względem relacji $\sim$. Mamy wówczas równość

$$|G| = 1 + d(a_1) + d(a_2) + \cdots + d(a_s).$$

Jeśli grupa G nie ma żadnego elementu rzędu 2, to wszystkie liczby $d(a_1), \ldots, d(a_s)$ są równe 2 i wtedy po prawej stronie powyższej równości jest liczba nieparzysta. Stąd wynika następujące stwierdzenie, które często występuje jako zadanie w książkach z teorii grup (patrz na przykład [17], [6], [1]).

Stwierdzenie 1.14. *Grupa skończona parzystego rzędu zawsze ma co najmniej jeden element rzędu* 2*.*

Załóżmy teraz, że w powyższym wyborze reprezentantów elementy $a_1, \ldots, a_k$ są rzędu 2, a pozostałe elementy $a_{k+1}, \ldots, a_s$ mają rzędy większe od 2. Mamy wówczas równość

$$|G| = 1 + k + 2(s - k),$$

z której otrzymujemy:

Stwierdzenie 1.15. *Jeśli G jest skończoną grupą parzystego rzędu, to liczba jej wszystkich elementów rzędu* 2 *jest nieparzysta.*

Z powyższego stwierdzenia (oraz Stwierdzenia 1.3) wynika, że nie ma takiej grupy skończonej, która ma dokładnie 2 elementy rzędu 2. Grupa abelowa $\mathbb{Z}_2 \times \mathbb{Z}_2$ ma dokładnie 3 elementy rzędu 2. Grupa dihedralna D_4 (która nie jest abelowa) ma takich elementów 5. Później udowodnimy, że nie ma takiej grupy abelowej, która ma dokładnie 5 lub dokładnie 9 elementów rzędu 2 (patrz Stwierdzenie 2.14).

Zajmowaliśmy się elementami rzędu 2. Jeśli co najmniej jeden taki element występuje, to jak powyżej wykazaliśmy, liczba wszytkich takich elementów jest nieparzysta. Przypomnijmy (patrz Stwierdzenie 1.9), że jeśli $m \geqslant 3$ jest liczbą naturalną, to w każdej grupie skończonej liczba elementów rzędu m jest parzysta. W tym przypadku ta liczba może być oczywiście równa 0.

---

2 Rzędy elementów i grupy abelowe

Teraz zajmować się będziemy skończonymi grupami abelowymi. W pewnych miejscach zakładać będziemy, że Czytelnik zna poniższe twierdzenie o strukturze skończonych grup abelowych.

Twierdzenie 2.1. *Każda skończona grupa abelowa rozkłada się jednoznacznie na iloczyn prosty swoich podgrup cyklicznych, których rzędy są potęgami liczb pierwszych dzielących rząd grupy.*

2.1 Własności rzędów elementów grup abelowych

Udowodnimy najpierw następujące dwa stwierdzenia.

Stwierdzenie 2.2. *Niech G będzie grupą abelową. Niech $a, b \in G$. Załóżmy, że $n = \mathrm{ord}_G(a) < \infty$ oraz $m = \mathrm{ord}_G(b) < \infty$. Jeśli $(n, m) = 1$, to $\mathrm{ord}_G(ab) = nm$.*

Dowód. Niech $s = \mathrm{ord}_G(ab)$. Mamy: $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$, a więc $s \mid nm$ na mocy Stwierdzenia 1.5.

Mamy również: $e = (ab)^{sn} = (a^n)^s b^{sn} = e^s b^{sn} = b^{sn}$ i stąd $m \mid sn$. Ale $(n, m) = 1$, więc $m \mid s$. Podobnie: $e = (ab)^{sm} = a^{ms}(b^n)^s = a^{sm}e^s = a^{sm}$ i stąd $n \mid sm$. Ale $(n, m) = 1$, więc $n \mid s$. Zatem $m \mid s$ oraz $n \mid s$ i stąd (ponieważ liczby m, n są względnie pierwsze) mamy podzielność $nm \mid s$. Wykazaliśmy więc, że $s = nm$. ⊠

Stwierdzenie 2.3. *Niech G będzie grupą abelową. Niech $a \in G$ oraz $n = \mathrm{ord}_G(a) < \infty$. Załóżmy, że dla każdego elementu $b \in G$ zachodzi nierówność $\mathrm{ord}_G(b) \leqslant m$. Wtedy rząd każdego element grupy G jest dzielnikiem liczby m. W szczególności $b^m = e$ dla wszystkich $b \in G$.*

Dowód. Niech $b \in G$ i niech $r = \mathrm{ord}_G(b)$. Wiemy, że $r \leqslant m$. Należy pokazać, że $r \mid m$. Przypuśćmy, że $r \nmid m$. Niech $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $r = p_1^{\beta_1} \cdots p_s^{\beta_s}$, gdzie $p_1, \ldots, p + s$ są parami różnymi liczbami pierwszymi oraz wykładniki $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_s$ są nieujemnymi liczbami całkowitymi. Ponieważ $r \nmid m$, więc istnieje $j \in \{1, \ldots, s\}$ takie, że $\beta_j > \alpha_j$. Oznaczmy $p = p_j$, $\alpha = \alpha_j$ oraz $\beta = \beta_j$. Mamy wtedy: $m = m'p^\alpha$, $r = r'p^\beta$, gdzie $\alpha < \beta$ oraz m', r' są liczbami naturalnymi niepodzielnymi przez p.

Rozważmy elementy a^{p^α} oraz $b^{r'}$. Ze Stwierdzenia 1.7(2) wynika, że

$$\mathrm{ord}_G\left(a^{p^\alpha}\right) = m', \quad \mathrm{ord}_G\left(b^{r'}\right) = p^\beta.$$

Ponieważ grupa g jest abelowa oraz liczby m' i p^β są względnie pierwsze, więc (na mocy Stwierdzenia 2.2) element $a^{p^\alpha} \cdot b^{r'}$ ma rząd równy $m'p^\beta$. Rząd ten jest większy od m. Istotnie:

$$m'p^\beta = \frac{m}{p^\alpha}p^\beta = m\frac{p^\beta}{p^\alpha} > m.$$

Przypuszczenie $r \nmid m$ prowadzi więc do sprzeczności. Zatem $r \mid m$. Stąd dalej wynika, że $m = ur$, gdzie $u \in \mathbb{Z}$ i mamy: $b^m = (b^r)^u = e^u = e$. ⊠

Uwaga 2.4. W powyższych dwóch stwierdzeniach założenie o abelowości grupy G jest istotne. Dla grup nieabelowych już takie stwierdzenia nie muszą być prawdziwe. Załóżmy dla przykładu, że G jest grupą symetryczną S_3. Wszystkie elementy tej grupy mają rzędy mniejsze lub równe 3 oraz istnieją elementy rzędu 3 i istnieją elementy rzędu 2. Ale $2 \nmid 3$, więc w tym przypadku nieabelowy odpowiednik Stwierdzenia 2.3 nie jest prawdziwy. Liczby $2, 3$ są oczywiście względnie pierwsze. Nie ma tu jednak elementu rzędu $6 = 2 \cdot 3$. Gdyby taki element rzędu 6 istniał, to nieabelowa grupa S_3 (która jest rzędu 6) byłaby grupą cykliczną; sprzeczność. Nie ma więc również nieabelowego odpowiednika Stwierdzenia 2.2. ⊠

2.2 Rzędy elementów skończonej grupy cyklicznej

W tym podrozdziale zbadamy rzędy elementów cyklicznej grupy $\mathbb{Z}_n$ z dodawaniem $+$, gdzie $n \geqslant 2$ jest liczbą naturalną. Jeśli $a \in \mathbb{Z}_n$, to w tym przypadku rzędem elementu a w $\mathbb{Z}_n$ jest najmniejsza liczba naturalna $m \geqslant 1$ taka, że w $\mathbb{Z}_n$ zachodzi równość $ma = 0$, tzn. taka, że $am \equiv 0 \pmod{n}$. W tym przypadku ten rząd oznaczać będziemy przez $\mathrm{ord}_n(a)$. Wprost z definicji otrzymujemy, że $\mathrm{ord}_n(a) = 1 \iff a = 0$.

Odpowiednie stwierdzenia z Rozdziału 1 można teraz zapisać w następującej postaci.

Stwierdzenie 2.5. *Niech $a, b \in \mathbb{Z}_n$, $r \in \mathbb{Z}$ oraz $m = \mathrm{ord}_n(a)$, $s = \mathrm{ord}_n(b)$. Wtedy:*

(1) $ra \equiv 0 \pmod{n} \iff \mathrm{ord}_n(a) \mid r$ (Stwierdzenie 1.5);

(2) $\mathrm{ord}_n(a) \mid n$ (Stwierdzenie 1.3);

(3) $\mathrm{ord}_n(ra) = \frac{m}{(r,m)}$ (Stwierdzenie 1.6);

(4) *jeśli* $(r, m) = 1$, *to* $\mathrm{ord}_n(ra) = m$ (Stwierdzenie 1.7);

(5) *jeśli* $r \geqslant 1$ *oraz* $r \mid m$, *to* $\mathrm{ord}_n(ra) = \frac{m}{r}$ (Stwierdzenie 1.7);

(6) $\mathrm{ord}_n(-a) = \mathrm{ord}_n(a)$ (Stwierdzenie 1.7);

(7) *jeśli* $(m, s) = 1$, *to* $\mathrm{ord}_n(a + b) = ms$ (Stwierdzenie 2.2).

Zanotujmy następne stwierdzenia.

Stwierdzenie 2.6. *Jeśli $a \in \mathbb{Z}_n$, to $\mathrm{ord}_n(a) = n \iff (n, a) = 1$.*

Dowód. Jest oczywiste, że $\mathrm{ord}_n(1) = n$. Załóżmy, że $(n, a) = 1$. Wtedy (na mocy 2.5(4)): $\mathrm{ord}_n(a) = \mathrm{ord}_n(a \cdot 1) = \mathrm{ord}_n(1) = n$. Załóżmy teraz, że $\mathrm{ord}_n(a) = n$, Mamy wówczas (na mocy 2.5(3)) $n = \mathrm{ord}_n(a) = \mathrm{ord}_n(a \cdot 1) = \frac{n}{(n,a)}$ i stąd $(n, a) = 1$. ⊠

Stwierdzenie 2.7. *Jeśli $d \mid n$, to $\mathrm{ord}_n\left(\frac{n}{d}\right) = d$.*

Dowód. Korzystamy ze Stwierdzenia 2.5(5):

$$\mathrm{ord}_n\left(\frac{n}{d}\right) = \mathrm{ord}_n\left(\frac{n}{d} \cdot 1\right) = \frac{\mathrm{ord}_n(1)}{n/d} = \frac{n}{n/d} = d$$

i to kończy dowód ⊠

Teraz możemy udowodnić:

Twierdzenie 2.8. *Jeśli d jest naturalnym dzielnikiem liczby n, to w grupie $\mathbb{Z}_n$ istnieje dokładnie $\varphi(d)$ elementów rzędu d.*

Dowód. Niech $d \mid n$. Niech $n = ud$, gdzie $1 \leqslant u \in \mathbb{Z}$. Oznaczmy:

$$M_n(d) = \{b \in \mathbb{Z}_n;\ \mathrm{ord}_n(b) = d\} \quad \text{oraz} \quad \Psi(d) = |M_n(d)|.$$

Ze Stwierdzenia 2.7 wiemy, że $\mathrm{ord}_n(u) = d$. Niech $j \in \{1, 2, \ldots, d\}$ będzie takie, że $(j, d) = 1$. Wtedy $\mathrm{ord}_n(ju) = \mathrm{ord}_n(u) = d$ (na mocy 2.5(4)). Stąd wynika, że $\Psi(d) \geqslant \varphi(d)$. Należy pokazać, że $\Psi(d) = \varphi(d)$. Zauważmy, że (na mocy 2.5(2)) mamy równość

$$\sum_{d|n} \Psi(d) = n.$$

Przypuśćmy, że istnieje taki naturalny dzielnik d liczby n, że $\Psi(d) > \varphi(d)$. Mamy wtedy sprzeczność:

$$n = \sum_{d|n} \Psi(d) > \sum_{d|n} \varphi(d) = n.$$

Wykorzystaliśmy dobrze znaną równość $\sum\limits_{d|n} \varphi(d) = n$ (patrz [15], [16] lub [11]). ⊠

Stąd wynika w szczególności, że skończona grupa cykliczna ma co najwyżej jeden element rzędu 2. Zapamiętajmy:

Stwierdzenie 2.9. *Niech G będzie skończoną grupą cykliczną. Jeśli $|G|$ jest liczbą nieparzystą, to G nie ma elementów rzędu 2. Jeśli natomiast $|G|$ jest liczbą parzystą, to G ma dokładnie jeden element rzędu 2.*

Zapamiętajmy również łatwą do udowodnienia konsekwencję powyższego stwierdzenia.

Stwierdzenie 2.10. *Niech $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, gdzie $r \geqslant 2$ oraz $n_1, \ldots, n_s$ są liczbami naturalnymi większymi od 1. Grupa G ma co najmniej dwa elementy rzędu 2 wtedy i tylko wtedy, gdy co najmniej dwie spośród liczb $n_1, \ldots, n_r$ są parzyste.*

Jeśli $d \mid n$, to niech $M_n(d)$ oznacza zbiór tych wszystkich elementów $b \in \mathbb{Z}_n$, których rząd $\mathrm{ord}_n(b)$ jest równy d. Takie oznaczenie wprowadziliśmy już w dowodzie Twierdzenia 2.8. Dla każdego $n \geqslant 2$ zachodzi równość $M_n(1) = \{0\}$ oraz $M_n(n)$ jest zbiorem tych wszystkich liczb naturalnych mniejszych od n, które są względnie pierwsze z liczbą n.

2.11. *Przykłady:*

$M_4(2) = \{2\}$, $M_4(4) = \{1, 3\}$;
$M_6(2) = \{3\}$, $M_6(3) = \{2, 4\}$, $M_6(6) = \{1, 5\}$;
$M_8(2) = \{4\}$, $M_8(4) = \{2, 6\}$, $M_8(8) = \{1, 3, 5, 7\}$;
$M_9(3) = \{3, 6\}$, $M_9(9) = \{1, 2, 4, 5, 7, 8\}$;
$M_{10}(2) = \{5\}$, $M_{10}(5) = \{2, 4, 6, 8\}$, $M_{10}(10) = \{1, 3, 7, 9\}$;
$M_{12}(2) = \{6\}$, $M_{12}(3) = \{4, 8\}$, $M_{12}(4) = \{3, 9\}$, $M_{12}(6) = \{2, 10\}$;
$M_{14}(2) = \{7\}$, $M_{14}(7) : \{2, 4, 6, 8, 10, 12\}$, $M_{14}(14) = \{1, 3, 5, 9, 11, 13\}$.

W poniższych tabelach podano zestawienia rzędów elementów grupy $\mathbb{Z}_n$ dla pewnych n. W pierwszych kolumnach podano dzielniki naturalne d liczby n większe od 1. W drugich kolumnach występują wszystkie elementy rzędu d, a w trzecich są liczby elementów z drugich kolumn.

	$n = 15$	
3	$5, 10$	2
5	$3, 6, 9, 12$	4
15	$1, 2, 4, 7, 8, 11, 13, 14$	8

	$n = 16$	
2	8	1
4	$4, 12$	2
8	$2, 6, 10, 14$	4
16	$1, 3, 5, 7, 9, 11, 13, 15$	8

	$n = 18$	
2	9	1
3	$6, 12$	2
6	$3, 15$	2
9	$2, 4, 8, 10, 14, 16$	6
18	$1, 5, 7, 11, 13, 17$	6

	$n = 20$	
2	10	1
4	$5, 15$	2
5	$4, 8, 12, 16$	4
10	$2, 6, 14, 18$	4
20	$1, 3, 7, 9, 11, 13, 17, 19$	8

	$n = 30$	
2	15	1
3	$10, 20$	2
5	$6, 12, 18, 24$	4
6	$5, 25$	2
10	$3, 9, 21, 27$	4
15	$2, 4, 8, 14, 16, 22, 26, 28$	8
30	$1, 7, 11, 13, 17, 19, 23, 29$	8

	$n = 42$	
2	21	1
3	$14, 28$	2
6	$7, 35$	2
7	$6, 12, 18, 24, 30, 36$	6
14	$3, 9, 15, 27, 33, 39$	6
21	$2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38, 40$	12
42	$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$	12

2.3 Grupy z trywialnymi kwadratami

Rozpoczynamy ten podrozdział od następującego, łatwego do udowodnienia, stwierdzenia.

Stwierdzenie 2.12. *Jeśli dla każdego elementu a grupy G zachodzi równość $a^2 = e$, to grupa G jest abelowa.*

Dowód. Równość $a^2 = e$ jest równoważna równości $a^{-1} = a$. Jeśli więc $a, b \in G$, to $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. $\boxtimes$

Niech m będzie liczbą naturalną. Załóżmy, że dla każdego elementu a danej grupy G zachodzi równość $a^m = e$. Wykazaliśmy przed chwilą, że jeśli $m = 2$, to grupa G jest abelowa. Czy abelowość grupy G można również wykazać w przypadku gdy $m = 3$ lub $m = 4$?. Okazuje się, że nie można. Elegancki dowód na to, że tego wykazać nie

można znajdziemy w książce Czesława Bagińskiego [1]. Teraz przedstawimy ten dowód. W tym celu najpierw wprowadzimy grupy, które oznaczać będziemy przez $\mathcal{B}(R)$.

Niech R będzie pieścieniem przemiennym z jedynką. Jeśli $a, b, c \in R$, to przez $[a, b, c]$ oznaczać będziemy 3×3 macierz trójkątną o wierszach $(1, a, b)$, $(0, 1, c)$ oraz $(0, 0, 1)$. Zapamiętajmy:

$$[a, b, c] = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}.$$

Zbiór wszystkich tego rodzaju macierzy oznaczać będziemy przez $\mathcal{B}(R)$. Łatwo sprawdzić, że ten zbiór jest grupą ze względu na mnożenie macierzowe. Elementem neutralnym jest macierz $[0, 0, 0]$. Wzory na mnożenie i element odwrotny są takie:

$$\begin{aligned} [a_1, b_1, c_1] \cdot [a_2, b_2, c_2] &= [a_1 + a_2,\ b_1 + b_2 + a_1 c_2,\ c_1 + c_2], \\ [a, b, c]^{-1} &= [-a,\ ac - b,\ -c]. \end{aligned}$$

Niech $x = [1, 0, 0]$, $y = [0, 0, 1]$. Wtedy $xy = [1, 1, 1]$ oraz $yx = [1, 0, 1]$, a zatem $xy \neq yx$. Dla każdego pierścienia R, przemiennego z jedynką, $\mathcal{B}(R)$ jest grupą i nie jest to grupa abelowa.

Za pomocą łatwej indukcji wykazujemy, że jeśli $a, b, c \in R$, to dla dowolnej liczby naturalnej n zachodzi równość

$$(*) \qquad [a, b, c]^n = \left[na,\ nb + \frac{n(n-1)}{2} ac,\ nc\right].$$

Stąd natychmiast wynika:

Stwierdzenie 2.13 ([1]). *Rozważmy grupę $\mathcal{B}(\mathbb{Z}_p)$, gdzie p jest nieparzystą liczbą pierwszą. Grupa ta nie jest abelowa i dla każdego jej elementu a zachodzi równość $a^p = e$.*

W szczególności $\mathcal{B}(\mathbb{Z}_3)$ jest nieabelową grupą (rzędu 27) i dla każdego jej elementu a zachodzi równość $a^3 = e$. Z równości $(*)$ wynika, że $\mathcal{B}(\mathbb{Z}_2)$ jest nieabelową grupą i dla każdego jej elementu a zachodzi równość $a^4 = e$. Jest to grupa rzędu 8, izomorficzna z grupą izometrii kwadratu D_4. W podobny sposób dla każdej liczby naturalnej $m \geqslant 3$ wykazujemy, że istnieje taka nieabelowa grupa G, że $a^m = e$ dla wszystkich $a \in G$.

2.4 Liczba elementów rzędu 2 dla grup abelowych

Udowodniliśmy (patrz Stwierdzenie 1.15, że jeśli G jest skończoną grupą (niekoniecznie abelową) parzystego rzędu, to liczba jej wszystkich elementów rzędu 2 jest nieparzysta. Dla grup abelowych tę liczbę można opisać dokładniej.

Stwierdzenie 2.14. *Liczba wszystkich elementów rzędu 2 skończonej grupy abelowej jest postaci $2^s - 1$, gdzie $s \geqslant 0$.*

Dowód. Jeśli G jest skończoną grupą abelową (z dodawaniem $+$), to oznaczmy przez $\delta(G)$ liczbę tych wszystkich elementów $a \in G$, dla których zachodzi równość $2a = 0$, czyli $a + a = 0$. Ponieważ $2 \cdot 0 = 0$, więc $\delta(G) \geqslant 1$. Z łatwością wykazujemy, że:

(a) $\delta(G \times H) = \delta(G)\delta(H)$ dla wszystkich skończonych grup abelowych G, H;

(b) $\delta(\mathbb{Z}_{2^s}) = 2$ dla $s \geqslant 1$;

(c) jeśli G jest grupą nieparzystego rzędu, to $\delta(G) = 1$.

Niech G będzie dowolną skończoną grupą abelową. Z twierdzenia o strukturze skończonych grup abelowych (patrz Twierdzenie 2.1) wynika, że $G = G_1 \times G_2$, gdzie G_2 jest skończoną grupą abelową nieparzystego rzędu oraz G_1 jest grupą abelową postaci $\mathbb{Z}_{2^{n_1}} \times \cdots \times \mathbb{Z}_{2^{n_s}}$ (przy czym $s \geqslant 0$). Korzystamy z własności $(a), (b), (c)$ i otrzymujemy równość $\delta(G) = 2^s$. W grupie G jest więc dokładnie 2^s takich elementów a, że $2a = 0$. Wśród nich jest element zerowy (który ma rząd 1). Pozostałe elementy są rzędu 2; jest więc ich $2^s - 1$. $\boxtimes$

Liczby postaci $2^s - 1$, występujące w powyższym twierdzeniu, nazywają się *liczbami Mersenne'a*. W [15], [16] lub [12] przedstawiono przeróżne własności i zastosowania liczb Mersenne'a. Zwróćmy uwagę, że dla każdej liczby naturalnej s istnieje taka skończona grupa abelowa G, która ma dokładnie $2^s - 1$ elementów rzędu 2. Taką grupą jest na przykład $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots\ldots \mathbb{Z}_2$ (s czynników).

W Stwierdzeniu 2.14 rozważaliśmy elementy rzędu 2. Modyfikując nieco dowód tego stwierdzenia otrzymujemy:

Stwierdzenie 2.15. *Niech p będzie liczbą pierwszą. Liczba wszystkich elementów rzędu p skończonej grupy abelowej jest zawsze postaci $p^s - 1$, gdzie $s \geqslant 0$.*

Nie ma więc takiej grupy abelowej, która ma dokładnie 5 lub dokładnie 6 elementów rzędu 3. Dla każdej liczby naturalnej s istnieje taka skończona grupa abelowa G, która ma dokładnie $p^s - 1$ elementów rzędu p. Taką grupą jest na przykład $\mathbb{Z}_p \times \mathbb{Z}_p \times \ldots\ldots \mathbb{Z}_p$ (s czynników).

2.5 Iloczyny elementów grupy abelowej

Spójrzmy jeszcze raz na wprowadzoną na stronie 4 relację typu równoważności $\sim$. Przypomnijmy, że $a \sim b$ jeśli $b = a$ lub $b = a^{-1}$. Grupa G jest sumą mnogościową parami rozłącznych klas abstrakcji względem tej relacji. Załóżmy, że grupa G jest skończona i załóżmy, że $\{a_0 = e, a_1, \ldots, a_s\}$ jest wyborem reprezentantów względem tej relacji. Mamy wówczas równość

$$G = \{e\} \cup [a_1] \cup [a_2] \cup \cdots \cup [a_s],$$

w której $[a_i] = \{a_i, a_i^{-1}\}$ dla $i = 1, \ldots, s$. Elementy $a_1, \ldots, a_s$ są różne od e. Jeśli a_i jest elementem rzędu 2, to $a_i = a_i^{-1}$ i wtedy zbiór $[a_i]$ jest jednoelementowy; $[a_i] = \{a_i\}$. Jeśli natomiast rząd elementu a_i jest większy od 2, to $a_i \neq a_i^{-1}$ i wtedy zbiór $[a_i]$ ma dokładnie dwa elementy. Stąd natychmiast wynika następująco stwierdzenie dla skończonych grup abelowych.

Stwierdzenie 2.16. *Niech G będzie skończoną grupą abelową i niech w będzie iloczynem wszystkich jej elementów. Jeśli grupa G nie ma żadnego elementu rzędu 2, to w jest elementem neutralnym. Jeśli grupa G ma dokładnie jeden element a rzędu 2, to $w = a$.*

Wyjaśnijmy jeszcze co się dzieje z iloczynem wszystkich elementów w przypadku gdy liczba elementów rzędu 2 jest większa od 1.

Stwierdzenie 2.17. *Jeśli skończona grupa abelowa ma co najmniej dwa elementy rzędu 2, to iloczyn jej wszystkich elementów jest elementem neutralnym.*

Dowód. Niech G będzie skończoną grupą abelową i dodawaniem $+$. Wówczas elementem neutralnym jest zero oraz "iloczyn" jest "sumą". Przez $s(G)$ oznaczać będziemy sumę wszystkich elementów grupy G. Należy więc udowodnić, że jeśli G ma co najmniej dwa elementy rzędu 2, to $s(G)$ jest równe 0. Przypomnijmy jeszcze, że element rządu 2, to taki niezerowy element a grupy G, dla którego zachodzi równość $2a = 0$, czyli $a + a = 0$.

Załóżmy więc, że grupa G ma co najmniej dwa elementy rzędu 2. Z twierdzenia o strukturze skończonych grup abelowych (patrz Twierdzenie 2.1) wiemy, że wtedy z dokładnością do izomorfizmu mamy równość postaci

$$G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r},$$

w której $n_1, \ldots, n_r$ są liczbami naturalnymi większymi od 1. Ponieważ skończona grupa cykliczna ma tylko co najwyżej jeden element rzędu 2, więc w naszym przypadku $r \geqslant 2$. Jeśli wszystkie liczby $n_1, \ldots, n_r$ są nieparzyste, to G nie ma elementu rzędu 2. Jeśli wśród tych liczb jest tylko jedna liczba parzysta, to G ma dokładnie jeden element rzędu 2. Z założenia, że G ma co najmniej dwa elementy rzędu 2 wynika więc, że wśród liczb $n_1, \ldots, n_r$ są co najmniej dwie parzyste (patrz Stwierdzenie 2.10).

Jest jasne, że $s(\mathbb{Z}_n) = \frac{n(n-1)}{2}$ oraz $s(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}) = \left(n_2 \frac{n_1(n_1-1)}{2},\ n_1 \frac{n_2(n_2-1)}{2}\right)$. Stosując łatwą indukcję wykazujemy, że w naszym przypadku $s(G) = (u_1, \ldots, u_r)$, gdzie

$$u_i = n_1 n_2 \cdots n_r \frac{n_i - 1}{2}$$

dla wszystkich $i = 1, \ldots r$. Zauważmy teraz, że jeśli co najmniej dwie spośród liczb $n_1, \ldots, n_r$ są parzyste (a tak jest w naszym przypadku), to liczby $u_1, \ldots, u_r$ są podzielne odpowiednio przez $n_1, \ldots, n_r$. Zatem $u_1, \ldots, u_r$ są zerami odpowiednio w $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_r}$. Wykazaliśmy więc, że $s(G) = (0, 0, \ldots, 0)$. Suma wszystkich elementów grupy G jest więc elementem zerowym. $\boxtimes$

Zanotujmy teraz Stwierdzenia 2.16 oraz 2.17 w postaci jednego następującego twierdzenia, które można znaleźć jako zadanie (bez rozwiązania) w książce [5].

Twierdzenie 2.18. *Niech G będzie skończoną grupą abelową i niech w będzie iloczynem wszystkich jej elementów. Jeśli G ma dokładnie jeden element a rzędu 2, to $w = a$. W pozostałych przypadkach w jest elementem neutralnym.*

Z tego twierdzenia szybko wynikają następne dwa stwierdzenia.

Stwierdzenie 2.19. *Jeśli skończona grupa abelowa ma co najmniej dwa elementy rzędu 2, to iloczyn jej wszystkich elementów rzędu 2 jest elementem neutralnym.*

Dowód. Niech G będzie skończoną grupą abelową i niech $\{a_0 = e, a_1, \ldots, a_s\}$ jest wyborem reprezentantów względem relacji $\sim$. Załóżmy, że elementy $a_1, \ldots, a_k$ są rzędu 2, a pozostałe elementy $a_{k+1}, \ldots, a_s$ mają rzędy większe od 2. Niech w będzie iloczynem wszystkich elementów grupy G i niech v będzie iloczynem wszystkich elementów rzędu 2. Wtedy $w = e$ (na mocy Twierdzenia 2.18) oraz $v = a_1 \cdots a_k$. Mamy więc

$$e = w = e \cdot a_1 \cdots a_k \cdot a_{k+1} \cdot a_{k+1}^{-1} \cdot \cdots \cdot a_s \cdot a_s^{-1} = eve = v,$$

a więc $v = e$. $\boxtimes$

Stwierdzenie 2.20. *Jeśli w jest iloczynem wszystkich elementów skończonej grupy abelowej, to w^2 jest elementem neutralnym.*

Dowód. (Sposób I). Wynika to natychmiast z Twierdzenia 2.18.

(Sposób II). Niech $G = \{g_1, g_2, \ldots, g_n\}$. Wtedy $\left\{g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right\} = G$ i mamy: $w^2 = g_1 g_2 \cdots g_n \cdot g_1^{-1} g_2^{-1} \cdots g_n^{-1} = e$. $\boxtimes$

W Stwierdzeniu 2.19 mamy iloczyn elementów rzędu 2. Łatwo wykazać podobne stwierdzenie dla iloczynu wszystkich elementów ustalonego rzędu większego od 2.

Stwierdzenie 2.21. *Niech $m \geqslant 3$. Jeśli skończona grupa abelowa ma co najmniej jeden element rzędu m, to iloczyn jej wszystkich elementów rzędu m jest elementem neutralnym.*

Dowód. Wynika to z równości $\mathrm{ord}_G(g) = \mathrm{ord}_G(g^{-1})$. $\boxtimes$

---

3 Multyplikatywna grupa modulo m

Przez $\mathbb{Z}_m^*$ oznaczamy multyplikatywną grupę pierścienia $\mathbb{Z}_m$. Jest to grupa abelowa rzędu $\varphi(m)$. Element $a \in \mathbb{Z}_m$ należy do $\mathbb{Z}_m^*$ wtedy i tylko wtedy, gdy $\mathrm{nwd}(a, m) = 1$. Jeśli a jest elementem grupy $\mathbb{Z}_m^*$, to rząd tego elementu w tej grupie oznaczać będziemy przez $\mathrm{ord}_n^*(a)$. Przykłady: $\mathrm{ord}_6^*(5) = 2$, $\mathrm{ord}_{13}^*(4) = 6$, $\mathrm{ord}_{14}^*(11) = 3$. Liczba $\mathrm{ord}_m^*(a)$ jest najmniejszą liczbą naturalną $s \geqslant 1$ taką, że $a^s \equiv 1 \pmod{m}$. Jest jasne, że $\mathrm{ord}_m^*(a) = 1 \iff a = 1$. Wiemy również (patrz Stwierdzenie 1.3), że liczba $\mathrm{ord}_m^*(a)$ jest naturalnym dzielnikiem liczby $\varphi(m)$. Zwróćmy uwagę, że ze Stwierdzenia 1.4 wynika natychmiast znane twierdzenie Eulera: *jeśli* $\mathrm{nwd}(a, m) = 1$, *to* $m \mid a^{\varphi(m)} - 1$.

W tym rozdziale przedstawimy znane fakty dotyczące struktury grupy $\mathbb{Z}_m^*$. Istotną rolę w dowodach tych faktów odgrywać będą rzędy elementów grupy $\mathbb{Z}_m^*$.

3.1 Potęgi dwójki

Grupy $\mathbb{Z}_2^* = \{1\}$ oraz $\mathbb{Z}_4^* = \{1,3\}$ są cykliczne. Natomiast grupa $\mathbb{Z}_8^* = \{1,3,5,7\}$ już nie jest cykliczna. Mamy tu $\mathrm{ord}_8^*(3) = \mathrm{ord}_8^*(5) = \mathrm{ord}_8^*(7) = 2$. Nie ma elementu rzędu $\varphi(8) = 4$. Udowodnimy, że jeśli $m = 2^n$, gdzie $n \geqslant 3$, to grupa $\mathbb{Z}_m^*$ nie jest cykliczna.

Lemat 3.1 ([15] 176). *Jeśli a jest nieparzystą liczbą całkowitą, to dla każdej liczby naturalnej n istnieje liczba całkowita k_n taka, że*

$$a^{2^n} = 1 + 2^{n+2}k_n.$$

Dowód. Indukcja ze względu na n. Liczba a jest postaci $4b \pm 1$, gdzie $b \in \mathbb{Z}$. Dla $n = 1$ mamy $a^{2^1} = 16b^2 \pm 8b + 1 = 1 + 2^3 k_1$, gdzie $k_1 = 2b^2 \pm b \in \mathbb{Z}$. Załóżmy, że to jest prawdą dla pewnego $n \geqslant 1$. Mamy wtedy

$$\begin{aligned} a^{2^{n+1}} &= \left(a^{2^n}\right)^2 = (1 + 2^{n+2}k_n)^2 = 2^{2n+4}k_n^2 + 2^{n+3}k_n + 1 \\ &= 2^{n+3}\left(2^{n+1}k_n^2 + k_n\right) + 1 = 1 + 2^{(n+1)+2}k_{n+1}, \end{aligned}$$

gdzie $k_{n+1} = 2^{n+1}k_n^2 + k_n$ jest liczbą całkowitą. ⊠

Twierdzenie 3.2. *Jeśli $n \geqslant 3$, to grupa $\mathbb{Z}_{2^n}^*$ nie jest cykliczna.*

Dowód. Niech $n \geqslant 3$ i niech $G = \mathbb{Z}_{2^n}^*$. Grupa G ma dokładnie $\varphi(2^n) = 2^{n-1}$ elementów. Przypuśćmy, że jest to grupa cykliczna. Istnieje wtedy taki element $a \in G$, że $\mathrm{ord}_{2^n}^*(a) = 2^{n-1}$. Najmniejszą liczbą naturalną s taką, że $a^s \equiv 1 \pmod{2^n}$ jest więc $s = 2^{n-1}$. Tymczasem, na mocy Lematu 3.1, mamy $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, a więc 2^{n-1} nie jest taką najmniejszą liczbą s; liczba 2^{n-2} jest mniejsza od 2^{n-1}. ⊠

Z tego dowodu oraz Stwierdzenia 2.3 wynika, że jeśli $n \geqslant 3$, to rząd każdego elementu grupy $\mathbb{Z}_{2^n}^*$ jest dzielnikiem liczby 2^{n-2}.

Udowodnimy teraz, że grupa $\mathbb{Z}_{2^n}^*$ (dla $n \geqslant 3$) jest izomorficzna z produktem grup cyklicznych $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. Podamy jawnę postać izomorfizmu. Dowód, który przedstawimy można znaleźć w różnych książkach z teorii liczb (patrz na przykład [15], [18], [16], [9]). Rozpoczynamy od lematów.

Lemat 3.3. *Dla każdej liczby całkowitej $r \geqslant 0$ zachodzi kongruencja*

$$5^{2^r} \equiv 1 + 2^{r+2} \pmod{2^{r+3}}.$$

Dowód. Indukcja ze względu na r. Dla $r = 0$ jest to oczywiste. Załóżmy, że jest to prawdą dla pewnego $r \geqslant 0$. Wtedy $5^{2^r} = 1 + 2^{r+2} + 2^{r+3}c$, gdzie $c \in \mathbb{Z}$. Zatem

$$\begin{aligned} 5^{2^{r+1}} &= \left(5^{2^r}\right)^2 = (1 + 2^{r+2} + 2^{r+3}c)^2 = 1 + 2^{2r+4} + 2^{2r+6}c^2 + 2^{r+3} + 2^{r+4}c + 2^{2r+6}c \\ &= 1 + 2^{r+3} + 2^{r+4}\left(2^r + 2^{r+2}c + c + 2^{r+2}c\right), \end{aligned}$$

a więc $5^{2^{r+1}} \equiv 1 + 2^{r+3} \pmod{2^{r+4}}$. ⊠

Lemat 3.4. *Niech $n \geqslant 3$. Wtedy $\operatorname{ord}^*_{2^n}(5) = 2^{n-2}$. Innymi słowy, najmniejszą liczbą naturalną b taką, że $5^b \equiv 1 \pmod{2^n}$ jest $b = 2^{n-2}$.*

Dowód. Już wiemy (patrz Lemat 3.3), że $5^{2^{n-2}} \equiv 1 \pmod{2^n}$.

Przypuśćmy, że istnieje liczba naturalna b taka, że $5^b \equiv 1 \pmod{2^n}$ oraz $b < 2^{n-2}$. Niech $b = 2^r c$, gdzie $r \geqslant 0$, $2 \nmid c$. Mamy wtedy (na mocy Lematu 3.3):

$$5^b = \left(5^{2^r}\right)^c \equiv \left(1 + 2^{r+2}\right)^c = 1 + \binom{c}{1}2^{r+2} + \binom{c}{2}2^{2r+4} + \cdots \equiv 1 + 2^{r+2} \pmod{2^{r+3}}.$$

Ale $b < 2^{n-2}$ czyli $2^r c < 2^{n-2}$, więc $2^r < 2^{n-2}$, więc $r < n-2$, więc $r+3 \leqslant n$. Zatem $5^b \equiv 1 \pmod{2^{r+3}}$ (ponieważ $5^b \equiv 1 \pmod{2^n}$ oraz $r+3 \leqslant n$). Mamy więc dwie kongruencje

$$5^b \equiv 1 + 2^{r+2} \pmod{2^{r+3}}, \quad 5^b \equiv 1 \pmod{2^{r+3}},$$

które prowadzą do sprzecznej podzielności $2^{r+3} \mid 2^{r+2}$. ⊠

Z tego lematu oraz Stwierdzenia 1.5 wynika

Lemat 3.5. *Jeśli $n \geqslant 3$ oraz $b \in \mathbb{Z}$, to*

$$5^b \equiv 1 \pmod{2^n} \iff 2^{n-2} \mid b.$$

Zanotujmy jeszcze kolejny lemat.

Lemat 3.6. *Niech $a, a', b, b' \in \mathbb{Z}$ i niech $n \geqslant 3$. Jeśli $a \equiv a' \pmod 2$ oraz $b \equiv b' \pmod{2^{n-2}}$, to $(-1)^a 5^b \equiv (-1)^{a'} 5^{b'} \pmod{2^n}$.*

Dowód. Z kongruencji $a \equiv a' \pmod 2$ wynika, że $(-1)^a = (-1)^{a'}$. Niech $b \equiv b' \pmod{2^{n-2}}$. Niech $b = b' + 2^{n-2}k$, gdzie $k \in \mathbb{Z}$. Z Lematu 3.4 (lub z Lematu 3.5) wiemy, że $5^{2^{n-2}} \equiv 1 \pmod{2^n}$. Zatem, $5^b = 5^{b'+2^{n-2}k} = b^{b'}\left(5^{2^{n-2}}\right)^k \equiv 5^{b'}1^k = 5^{b'} \pmod{2^n}$ i to kończy dowód. ⊠

Niech $n \geqslant 3$ i niech A, B, C będą ideałami pierścienia $\mathbb{Z}$ generowanymi odpowiednio przez 2, 2^{n-2} oraz 2^n. Mamy wtedy $\mathbb{Z}_2 = \mathbb{Z}/A$, $\mathbb{Z}_{2^{n-2}} = \mathbb{Z}/B$ oraz $\mathbb{Z}_{2^n} = \mathbb{Z}/C$. Rozpatrzmy odwzorowanie $f : \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \to \mathbb{Z}^*_{2^n}$ określone wzorem

$$f\Big((a + A, b + B)\Big) = (-1)^a 5^b + C,$$

dla wszystkich $a, b \in \mathbb{Z}$. Z Lematu 3.6 oraz z tego, że $(-1)^a 5^b + C$ należy do grupy $\mathbb{Z}^*_{2^n}$ wynika, że f jest dobrze zdefiniowaną funkcją. Bez trudu stwierdzamy, że funkcja ta jest homomorfizmem grup.

Lemat 3.7. *Powyższe odwzorowanie f jest różnowartościowe.*

Dowód. Już wiemy, że f jest homomorfizmem grup. Wystarczy zatem wykazać, że f ma trywialne jądro. Załóżmy, że $(a + A, b + B)$ należy do jądra odwzorowania f. Wtedy $(-1)^a 5^b \equiv 1 \pmod{2^n}$. Ponieważ $n \geqslant 3$, więc $(-1)^a 5^b \equiv 1 \pmod 4$, czyli $(-1)^a \equiv 1 \pmod 4$ i stąd wynika, że a jest parzyste. Wiemy więc już, że $(a+A, b+B) = (0 + A, b + B)$ oraz $5^b \equiv 1 \pmod{2^n}$. Z Lematu 3.5 wynika, że liczba b jest podzielna przez 2^{n-2}. Zatem $(a+A, b+B) = (0+A, 0+B)$. Wykazaliśmy więc, że odwzorowanie f ma trywialne jądro. ⊠

Teraz możemy udowodnić:

Twierdzenie 3.8. *Jeśli $n \geqslant 3$, to grupy $\mathbb{Z}_{2^n}^*$ oraz $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ są izomorficzne.*

Dowód. Wiemy, że powyżej określone odwzorowanie $f : \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \to \mathbb{Z}_{2^n}^*$ jest różnowartościowym homomorfizmem grup. Ponieważ są to grupy skończone i ich rzędy są jednakowe (każda z tych grup ma dokładnie 2^{n-1} elementów), więc to odwzorowanie f jest również surjekcją. Zatem f jest izomorfizmem grup. ⊠

Spójrzmy na to twierdzenie i jego dowód gdy $n = 3$ oraz $n = 4$.

Przykład 3.9. Dla $n = 3$ mamy: $\mathbb{Z}_2 = \mathbb{Z}_{2^{n-2}} = \{0, 1\}$ oraz $\mathbb{Z}_{2^n}^* = \mathbb{Z}_8^* = \{1, 3, 5, 7\}$ i wiemy, że $\mathbb{Z}_2 \times \mathbb{Z}_2 \approx \mathbb{Z}_8^*$. Izomorfizm $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_8^*$ jest tutaj określony następująco: $f(0,0) = 1$, $f(0,1) = (-1)^0 5^1 = 5$, $f(1,0) = (-1)^1 5^0 = -1 = 7$, $f(1,1) = (-1)^1 5^1 = -5 = 3$. ⊠

Przykład 3.10. Dla $n = 4$ mamy: $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_{2^{n-2}} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ oraz $\mathbb{Z}_{2^n}^* = \mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ i wiemy, że $\mathbb{Z}_2 \times \mathbb{Z}_4 \approx \mathbb{Z}_{16}^*$. Izomorfizm $f : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_{16}^*$ jest tutaj określony następująco: $f(0,0) = 1$, $f(0,1) = (-1)^0 5^1 = 5$, $f(0,2) = (-1)^0 5^2 = 9$, $f(0,3) = (-1)^0 5^3 = -3 = 13$, $f(1,0) = (-1)^1 5^0 = -1 = 15$, $f(1,1) = (-1)^1 5^1 = -5 = 11$. $f(1,2) = (-1)^1 5^2 = -9 = 7$, $f(1,3) = (-1)^1 5^3 = 3$. ⊠

Łatwo udowodnić:

Stwierdzenie 3.11. *Niech $G_n = \mathbb{Z}_{2^n}^*$. Jeśli $n \geqslant 3$, to grupa G_n ma dokładnie 3 elementy rzędu 2. Jeśli $n \geqslant 4$, to grupa G_n ma dokładnie 4 elementy rzędu 4. Jeśli $n \geqslant 5$, to grupa G_n ma dokładnie 8 elementów rzędu 8. Ogólniej, Jeśli $n \geqslant s + 2$ gdzie $s \geqslant 2$, to grupa G_n ma dokładnie 2^s elementów rzędu 2^s.*

3.2 Potęgi nieparzystej liczby pierwszej

Udowodnimy, że jeśli p jest nieparzystą liczbą pierwszą, to każda grupa $\mathbb{Z}_{p^n}^*$ jest cykliczna. Dowód, który przedstawimy został opracowany na podstawie książek [15], [18], [16] oraz [9]). Rozpoczynamy od lematów.

Lemat 3.12. *Niech $p \geqslant 3$ będzie liczbą pierwszą, $n \geqslant 1$ liczbą naturalną oraz a liczbą całkowitą niepodzielną przez p. Wtedy*

$$(1 + ap)^{p^{n-1}} \equiv 1 + ap^n \pmod{p^{n+1}}.$$

Dowód. Indukcja względem n. Dla $n = 1$ jest to oczywiste. Załóżmy, że dla pewnego $n \geqslant 1$ rozważana kongruencja jest prawdziwa. Niech $(1+ap)^{p^{n-1}} = 1 + ap^n + cp^{n+1}$, gdzie $c \in \mathbb{Z}$. Wtedy modulo p^{n+2} mamy:

$$\begin{aligned}
(1+ap)^{p^n} &= \left((1+ap)^{p^{n-1}}\right)^p = ((1+ap^n)+cp^{n+1})^p \\
&= (1+ap^n)^p + \binom{p}{1}(1+ap^n)^{p-1}cp^{n+1} + \binom{p}{2}(1+ap^n)^{p-2}c^2p^{2n+2} + \cdots \\
&\equiv (1+ap^n)^p = 1 + \binom{p}{1}ap^n + \binom{p}{2}a^2p^{2n} + \cdots \\
&\equiv 1 + ap^{n+1}
\end{aligned}$$

i to kończy dowód. ⊠

Lemat 3.13. *Niech $p \geqslant 3$ będzie liczbą pierwszą, $n \geqslant 1$ liczbą naturalną oraz a liczbą całkowitą niepodzielną przez p. Wtedy $\operatorname{ord}^*_{p^n}(1+ap) = p^{n-1}$. Innymi słowy, najmniejszą liczbą naturalną b taką, że*

$$(1+ap)^b \equiv 1 \pmod{p^n}$$

jest $b = p^{n-1}$.

Dowód. Niech $b = \operatorname{ord}^*_{p^n}(1+ap)$. Z Lematu 3.12 wynika, że $(1+ap)^{p^{n-1}} \equiv 1 \pmod{p^n}$. Wiemy zatem (na mocy Stwierdzenia 1.5), że $b \mid p^{n-1}$. Przypuśćmy, że $b < p^{n-1}$. Mamy wtedy $b = p^r$, gdzie $r < n-1$. Zatem $(1+ap)^{p^r} \equiv 1 \pmod{p^n}$ oraz (na mocy Lematu 3.12)

$$(1+ap)^{p^r} \equiv 1 + ap^{r+1} \pmod{p^{r+2}}.$$

Ale $r < n-1$ więc $r+2 \leqslant n$, a zatem

$$(1+ap)^{p^r} \equiv 1 \pmod{p^{r+2}}.$$

Mamy więc dwie kongruencje modulo p^{r+2}, z których wynika, że $ap^{r+1} \equiv 0 \pmod{p^{r+2}}$ i stąd, że $p \mid a$; wbrew temu, że $p \nmid a$. ⊠

Lemat 3.14. *Niech $p \geqslant 3$ będzie liczbą pierwszą i niech g będzie liczbą całkowitą taką, że $g^{p-1} = 1+ap$, gdzie a jest pewną liczbą całkowitą. Niech $h = g+p$. Wtedy $h^{p-1} = 1+bp$, gdzie $b \in \mathbb{Z}$. Jeśli $p \mid a$, to $p \nmid b$.*

Dowód. Mamy:

$$\begin{aligned}
h^{p-1} &= (g+p)^{p-1} = y^{p-1} + \binom{p-1}{1}g^{p-2}p + \binom{p-1}{2}g^{p-3}p^2 + \cdots \\
&= 1 + ap + (p-1)g^{p-2}p + \cdots = 1 + (a - g^{p-2})\,p + up^2 \\
&= 1 + (a - g^{p-2} + up)\,p,
\end{aligned}$$

gdzie u jest pewną liczbą całkowitą. Stąd wynika, że $b = a - g^{p-2} + up$. Jeśli więc $p \mid a$, to $p \nmid b$, gdyż $p \nmid g^{p-2}$. ⊠

Załóżmy, że $p \geqslant 3$ będzie liczbą pierwszą. Wiemy, że wtedy pierścień $\mathbb{Z}_p$ jest skończonym ciałem. Jego grupa multyplikatywna $\mathbb{Z}_p^*$ jest (patrz Twierdzenie 4.1) grupą cykliczną. Istnieje więc element $a \in \mathbb{Z}_p^*$, którego rząd w $\mathbb{Z}_p^*$ jest równy $p-1$. Mówić będziemy w tym przypadku, że *a jest generatorem grupy* $\mathbb{Z}_p^*$. Często taki element a jest nazywany *pierwiastkiem pierwotnym modulo p* (patrz na przykład [15], [18], [16]).

Twierdzenie 3.15. *Każda grupa postaci $\mathbb{Z}_{p^n}^*$, gdzie p jest nieparzystą liczbą pierwszą oraz $n \geqslant 1$ jest liczbą naturalną, jest grupą cykliczną.*

Dowód. Niech $p \geqslant 3$ będzie liczbą pierwszą i niech $n \geqslant 1$ będzie liczbą naturalną. Oznaczmy przez G grupę $\mathbb{Z}_{p^n}^*$. Jeśli $n = 1$, to cykliczność grupy G wynika z Twierdzenia 4.1. Zakładamy więc dalej, że $n \geqslant 2$. Należy wykazać, że w grupie G istnieje element rzędu $\varphi(p^n) = (p-1)p^{n-1}$.

Niech $g \in \{2, 3, \ldots, p^2-1\}$ będzie generatorem grupy $\mathbb{Z}_p^*$. Wtedy $g^{p-1} \equiv 1 \pmod{p}$, a więc $g^{p-1} = 1 + ap$, gdzie a jest pewną liczbą całkowitą. Jeśli $p \mid a$, to zastępujemy element g elementem $g + p$. Możemy więc założyć (na mocy Lematu 3.14), że $p \nmid a$. Udowodnimy, że g jest elementem rzędu $\varphi(p^n) = (p-1)p^{n-1}$.

Niech s będzie rzędem elementu g w grupie G, tzn. $s = \mathrm{ord}_{p^n}^*(g)$, czyli $s = \mathrm{ord}_G(g)$. Wtedy $g^s \equiv 1 \pmod{p^n}$ i stąd w szczególności $g^s \equiv 1 \pmod{p}$. Ale g jest generatorem grupy cyklicznej $\mathbb{Z}_p^*$ (rzędu $p-1$), więc liczba s jest podzielna przez $p-1$.

Z Lematu 3.13 wiemy, że rzędem element g^{p-1} w G jest p^{n-1}. Korzystamy teraz ze Stwierdzenia 1.6 i mamy

$$p^{n-1} = \mathrm{ord}_G(g^{p-1}) = \frac{\mathrm{ord}_G(g)}{\mathrm{nwd}(p-1, \mathrm{ord}_G(g))} = \frac{s}{(p-1, s)} = \frac{s}{p-1},$$

a zatem $s = (p-1)p^{n-1} = \varphi(p^n) = |G|$. Wykazaliśmy, że w grupie G istnieje element rzędu $|G|$. Wykazaliśmy więc, że G jest grupą cykliczną. ⊠

Z tego dowodu wynika następujące twierdzenie.

Twierdzenie 3.16. *Niech p będzie nieparzystą liczbą pierwszą i niech g będzie generatorem grupy $\mathbb{Z}_p^*$. Jeśli $g^{p-1} \not\equiv 1 \pmod{p^2}$, to element g jest generatorem każdej grupy $\mathbb{Z}_{p^n}^*$ dla $n \geqslant 1$. Jeśli natomiast $g^{p-1} \equiv 1 \pmod{p^2}$, to element $g + p$ jest generatorem każdej grupy $\mathbb{Z}_{p^n}^*$ dla $n \geqslant 1$.*

Spójrzmy na przypadek $p = 3$. Jedynym generatorem grupy cyklicznej $\mathbb{Z}_3^* = \{1, 2\}$ jest 2. Zauważmy, że $2^2 \not\equiv 1 \pmod{9}$. Mamy zatem:

Stwierdzenie 3.17. *Dl a każdej liczby naturalnej n liczba 2 jest generatorem grupy cyklicznej $\mathbb{Z}_{3^n}^*$.*

Podobnie jest dla $p = 5$. Grupa cykliczna $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ ma dokładnie $2 = \varphi(\varphi(6))$ elementów maksymalnego rzędu $4 = \varphi(5)$. Są to 2 oraz 3. Tutaj również mamy: $2^4 \not\equiv 1 \pmod{25}$ oraz $3^4 \not\equiv 1 \pmod{25}$. Z Twierdzenia 3.16 wynika zatem:

Stwierdzenie 3.18. *Dl a każdej liczby naturalnej n liczba 2 jest generatorem grupy cyklicznej $\mathbb{Z}_{5^n}^*$. Liczba 3 jest również generatorem każdej takiej grupy.*

Podobnego typu stwierdzenia zachodzą dla wszystkich nieparzystych liczb pierwszych p mniejszych od 29. Dla takich p wszystkie generatory g grupy $\mathbb{Z}_p^*$ są takie, że

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Dla $p = 29$ elementami maksymalnego rzędu (czyli rzędu 28) są liczby:

$$2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27$$

(12 liczb). Dla generatora 14 zachodzi kongruencja $14^{28} \equiv 1 \pmod{29^2}$. Dla wszystkich pozostałych generatorów tego typu kongruencji nie ma.

Dla liczb pierwszych p mniejszych od 200 tego typu sytuacja pojawia się, gdy p jest jedną z liczb: $29, 37, 43, 71, 103, 109, 113, 131, 181, 191$.

3.3 Cykliczne grupy multyplikatywne modulo m

Jeśli A jest pierścieniem przemiennym z jedynką, to jego grupę multyplikatywną oznacza się często przez A^*. Takie oznaczenie będziemy tu stosować. Zapamiętajmy:

$$A^* = \left\{ a \in A;\ \exists_{b \in A}\ ab = 1 \right\}.$$

Zanotujmy następujące oczywiste stwierdzenie.

Stwierdzenie 3.19. *Jeśli A, B są pierścieniami przemiennymi z jedynkami, to grupy $(A \times B)^*$ oraz $A^* \times B^*$ są izomorficzne.*

Przypomnijmy również:

Twierdzenie 3.20 (Twierdzenie Chińskie o Resztach). *Niech n, m będą względnie pierwszymi liczbami naturalnymi. Wtedy pierścienie $\mathbb{Z}_{nm}$ oraz $\mathbb{Z}_n \times \mathbb{Z}_m$ są izomorficzne.*

Z powyższych faktów otrzymujemy:

Twierdzenie 3.21. *Jeśli p jest nieparzystą liczbą pierwszą, to każda grupa postaci $\mathbb{Z}_{2p^n}^*$, gdzie $n \geqslant 1$ jest liczbą naturalną, jest grupą cykliczną.*

Dowód. Niech $p \geqslant 3$ będzie liczbą pierwszą i niech $n \geqslant 1$. Wtedy liczby 2 oraz p^n są względnie pierwsze i wobec tego (na mocy Twierdzenia Chińskiego o Resztach) pierścień $\mathbb{Z}_{2p^n}$ jest izomorficzny z pierścieniem $\mathbb{Z}_2 \times \mathbb{Z}_{p^n}$. Grupa $\mathbb{Z}_{2p^n}^*$ jest więc (na mocy Stwierdzenia 3.19) izomorficzna z grupą $\mathbb{Z}_2^* \times \mathbb{Z}_{p^n}^*$. Ale $\mathbb{Z}_2^*$ jest grupą zerową. Grupy $\mathbb{Z}_{2p^n}^*$ oraz $\mathbb{Z}_{p^n}^*$ są więc izomorficzne. Wiemy z Twierdzenia 3.15, że grupa $\mathbb{Z}_{p^n}^*$ jest cykliczna. Zatem grupa $\mathbb{Z}_{2p^n}^*$ jest również cykliczna. ⊠

Twierdzenie 3.22. *Niech $m \geqslant 2$. Grupa $\mathbb{Z}_m^*$ jest cykliczna wtedy i tylko wtedy, gdy liczba m jest jedną z następujących czterech postaci*

(1) $m = 2$;
(2) $m = 4$;
(3) $m = p^n$, *gdzie* $n \geqslant 1$ *oraz* $p \geqslant 3$ *jest liczbą pierwszą;*
(4) $m = 2p^n$, *gdzie* $n \geqslant 1$ *oraz* $p \geqslant 3$ *jest liczbą pierwszą.*

Dowód. ([15] 175). Udowodniliśmy już wcześniej, że jeśli liczba m jest jedną z powyższych czterech postaci, to grupa $\mathbb{Z}_m^*$ jest cykliczna. Należy więc wykazać, że innych przypadków nie ma.

Załóżmy, że $\mathbb{Z}_m^*$ jest grupą cykliczną i załóżmy, że $a \in \mathbb{Z}_m^*$ jest elementem rzędu $|\mathbb{Z}_m^*| = \varphi(m)$. Niech $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ będzie rozkładem kanonicznym liczby m. Ponieważ liczba a jest względnie pierwsza z m, więc jest względnie pierwsza z każdą z liczb $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$ i wobec tego (na mocy twierdzenia Eulera) mamy następujący ciąg kongruencji:

$$a^{\varphi\left(p_1^{\alpha_1}\right)} \equiv 1 \pmod{p_1^{\alpha_1}}, \quad \ldots, \quad a^{\varphi(p_s^{\alpha_s})} \equiv 1 \pmod{p_s^{\alpha_s}},$$

Załóżmy, że N jest liczbą naturalną podzielną przez każdą z liczb

$$(*) \qquad \varphi\left(p_1^{\alpha_1}\right), \quad \varphi\left(p_2^{\alpha_2}\right), \quad \ldots, \quad \varphi\left(p_s^{\alpha_s}\right).$$

Mamy wtedy ciąg kongruencji: $a^N \equiv 1 \pmod{p_1^{\alpha_1}}$, $\ldots$, $a^N \equiv 1 \pmod{p_s^{\alpha_s}}$ i wobec tego liczba $a^N - 1$ jest podzielna przez wszystkie liczby $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$. Ale liczby te są parami względnie pierwsze, więc liczba $a^N - 1$ jest podzielna przez iloczyn tych liczb czyli przez liczbą m. Zatem wtedy $a^N \equiv 1 \pmod{m}$.

Przypuśćmy teraz, że w ciągu $(*)$ występują co najmniej dwie liczby parzyste. Wtedy $N = \frac{1}{2}\varphi(m) = \frac{1}{2}\varphi\left(p_1^{\alpha_1}\right) \cdots \varphi\left(p_s^{\alpha_s}\right)$ jest liczbą naturalną podzielną przez każdą z liczb ciągu $(*)$. Zatem wtedy $a^{\varphi(m)/2} \equiv 1 \pmod{m}$ i mamy sprzeczność:

$$\varphi(m) = \operatorname{ord}_m^*(a) \leqslant \frac{\varphi(m)}{2}.$$

Zatem w ciągu $(*)$ może występować co najwyżej jedna liczba parzysta. Liczba postaci $\varphi(n)$ jest nieparzysta tylko dla $n = 1$ oraz $n = 2$. W pozostałych przypadkach jest to zawsze liczba parzysta. Jest więc teraz oczywiste, że w rozkładzie kanonicznym liczby m może występować co najwyżej jedna liczba pierwsza nieparzysta. Jeśli jej nie ma, to m jest potęgą dwójki i wtedy (na mocy Twierdzenia 3.2) liczba m jest równa 2 lub 4. Jeśli natomiast w rozkładzie kanonicznym liczby m występuje dokładnie jedna liczba pierwsza nieparzysta p, to może to być jedynie gdy $m = p^n$ lub $m = 2p^n$. Przypadki $m = 4p^n$, $m = 8p^n, \ldots$ nie są możliwe, gdyż w takich przypadkach w ciągu $(*)$ występują dwie liczby parzyste. ☒

Znamy więc już wszystkie grupy cykliczne postaci $\mathbb{Z}_m^*$. Zanotujmy następujące twierdzenie wynikające z Twierdzenia 2.8.

Twierdzenie 3.23. *Jeśli $\mathbb{Z}_m^*$ jest grupą cykliczną, to dla każdego dzielnika naturalnego liczby $\varphi(m)$ istnieje w grupie $\mathbb{Z}_m^*$ dokładnie $\varphi(d)$ elementów rzędu d. W szczególności w grupie $\mathbb{Z}_m^*$ istnieje dokładnie $\varphi(\varphi(m))$ elementów maksymalnego rzędu $\varphi(m)$.*

W grupie $\mathbb{Z}_p^*$ istnieje więc dokładnie $\varphi(p-1)$ elementów maksymalnego rzędu $p-1$ ([15] 185, [16] 274).

Następne stwierdzenie znajdziemy na przykład w [15], [16] lub jako zadanie E2080 w czasopiśmie *The American Mathematical Monthly* 4(1969) 417 -418.

Stwierdzenie 3.24. *Jeśli $\mathbb{Z}_m^*$ jest grupą cykliczną, to iloczyn wszystkich jej elementów przystaje do -1 modulo m. W pozostałych przypadkach ten iloczyn przystaje do 1 modulo m.*

Dowód. Dla $m = 2$ jest to oczywiste. Niech $m \geqslant 3$. Wtedy $\varphi(m)$ jest liczbą parzystą, a zatem $\mathbb{Z}_m^*$ jest grupą parzystego rzędu. Jeśli $\mathbb{Z}_m^*$ jest grupą cykliczną to oczywiście zawiera dokładnie jeden element rzędu 2 (patrz Stwierdzenie 2.9) i tym elementem jest -1. Jeśli natomiast $\mathbb{Z}_m^*$ nie jest grupą cykliczną, to ma co najmniej dwa elementy rzędu 2. Teza wynika zatem ze Stwierdzenia 2.18. ⊠

Zwróćmy uwagę, że powyższe stwierdzenie jest uogólnieniem znanego Twierdzenia Wilsona: *jeśli p jest liczbą pierwszą, to* $(p-1)! \equiv -1 \pmod{p}$. Inne uogólnienia tego twierdzenia znajdziemy na przykład w [13]. Jedno z takich uogólnień podamy w następnym rozdziale w Twierdzeniu 4.3.

3.4 Przykłady

Każda z grup $\mathbb{Z}_3^*$, $\mathbb{Z}_4^*$, $\mathbb{Z}_6^*$ jest grupą cykliczną izomorficzną z grupą $\mathbb{Z}_2$.

Grupy $\mathbb{Z}_{20}^*$ oraz $\mathbb{Z}_{30}^*$ nie są cykliczne. Zauważmy, że $\mathbb{Z}_{20}^* \approx \mathbb{Z}_4^* \times \mathbb{Z}_5^* \approx \mathbb{Z}_2 \times \mathbb{Z}_4$ oraz

$$\mathbb{Z}_{30}^* \approx \mathbb{Z}_{2\cdot 3}^* \times \mathbb{Z}_5^* \approx \mathbb{Z}_3^* \times \mathbb{Z}_5^* \approx \mathbb{Z}_2 \times \mathbb{Z}_4.$$

Są to więc grupy izomorficzne. Mamy również: $\mathbb{Z}_{15}^* \approx \mathbb{Z}_{16}^* \approx \mathbb{Z}_2 \times \mathbb{Z}_4$. Istnieją więc dokładnie 4 liczby naturalne n (mianowicie $n = 15, 16, 20$ oraz 30) takie, że grupa $\mathbb{Z}_n^*$ jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Istnieją również dokładnie 4 takie liczby naturalne n, że grupa $\mathbb{Z}_n^*$ jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_3$. Są to $n = 7, 9, 14$ oraz $n = 18$.

Istnieje dokładnie 7 takich liczb naturalnych n, że grupa $\mathbb{Z}_n^*$ jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$. Są to: $n = 35, 39, 45, 52, 70, 78$ oraz $n = 90$.

Istnieje dokładnie 8 takich liczb naturalnych n, że grupa $\mathbb{Z}_n^*$ jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$. Są to: $n = 104, 105, 112, 140, 144, 156, 180$ oraz $n = 210$.

Niech $\gamma(n_1, n_2, \ldots, n_s)$ oznacza liczbę tych wszystkich liczb naturalnych n, dla których grupa $\mathbb{Z}_n^*$ jest izomorficzna z grupą $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$. Z powyższych przykładów mamy:

$$\gamma(2) = 3, \quad \gamma(2,3) = 4, \quad \gamma(2,4) = 4, \quad \gamma(2,3,4) = 7, \quad \gamma(2,2,3,4) = 8.$$

Spójrzmy na następne przykłady otrzymane za pomocą komputera.

$$\begin{array}{ll}
\gamma(2,4,5)=5, & \gamma(2,3,4,5,7)=13,\\
\gamma(2,2,3,7)=6, & \gamma(2,2,3,4,9)=14,\\
\gamma(2,4,5,9)=9, & \gamma(2,2,2,3,4,5)=15,\\
\gamma(2,3,4,25)=10, & \gamma(2,2,2,3,5,11)=16,\\
\gamma(2,3,4,5)=11, & \gamma(2,2,3,4,5)=17,\\
\gamma(2,2,3,5,7)=11, & \gamma(2,2,2,3,3,4,5)=18,\\
\gamma(2,3,4,13)=12, & \gamma(2,2,3,4,5,9)=29,\\
\gamma(2,2,3,4,7)=12, & \gamma(2,2,3,4,5,7)=30.
\end{array}$$

Następne przykłady również otrzymano za pomocą komputera. W przykładach tych przez G_n oznaczono grupę $\mathbb{Z}_n^*$. Jeśli grupa G_n jest ustalona, to przez R_k oznaczono zbiór wszystkich jej elementów rzędu k, a liczbę elementów zbioru R_k oznaczono przez r_k. Ponieważ liczba r_1 jest zawsze równa 1, więc będziemy ją pomijamy. Iloczyn prosty $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ oznaczono przez $[n_2, n_2 \ldots, n_s]$.

Dla $n = 30$ mamy: $G_{30} = \{1,7,11,13,17,19,23,29\} \approx [2,4]$, $|G_{30}| = 8$, $R_2 = \{11,19,29\}$, $r_2 = 3$, $R_4 = \{7,13,17,23\}$, $r_4 = 4$. Innymi słowy, grupa $\mathbb{Z}_{30}^*$ jest 8-elementowa, jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_4$, ma 3 elementy rzędu 2 oraz ma 4 elementy rzędu 4.

Dla $n = 36$ mamy: $G_{36} = \{1,5,7,11,13,17,19,23,25,29,31,35\} \approx [2,2,3]$, $|G_{36}| = 12$, $R_2 = \{17,19,35\}$, $r_2 = 3$, $R_3 = \{13,25\}$, $r_3 = 2$, $R_6 = \{5,7,11,23,29,31\}$, $r_6 = 6$. Innymi słowy, grupa $\mathbb{Z}_{36}^*$ jest 12-elementowa, jest izomorficzna z grupą $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, ma 3 elementy rzędu 2, ma dwa elementy rzędu 2 oraz ma 6 elementów rzędu 6.

Poniższa tabelka przedstawia następne tego typu przykłady.

n	$\lvert G\rvert$	$\approx$	r
12	4	$[2,2]$	$r_2 = 3$
18	6	$[2,3]$	$r_2 = 1,\ r_3 = 2,\ r_6 = 2$
20	8	$[2,4]$	$r_2 = 3,\ r_4 = 4$
24	8	$[2,2,2]$	$r_2 = 7$
28	12	$[2,2,3]$	$r_2 = 3,\ r_3 = 2,\ r_6 = 6$
35	24	$[2,3,4]$	$r_2 = 3.\ r_3 = 2,\ r_4 = 4,\ r_6 = 6,\ r_{12} = 8$
40	16	$[2,2,4]$	$r_2 = 7.\ r_4 = 8$
50	20	$[4,5]$	$r_2 = 1.\ r_4 = 4,\ r_5 = 4,\ r_{10} = 4,\ r_{20} = 8$
65	48	$[3,4,4]$	$r_2 = 3,\ r_3 = 2,\ r_4 = 12,\ r_6 = 6,\ r_{12} = 24$
75	40	$[2,4,5]$	$r_2 = 3.\ r_4 = 4,\ r_5 = 4,\ r_{10} = 12,\ r_{20} = 16$
100	40	$[2,4,5]$	$r_2 = 3.\ r_4 = 4,\ r_5 = 4,\ r_{10} = 12,\ r_{20} = 16$
200	80	$[2,2,4,5]$	$r_2 = 7.\ r_4 = 8,\ r_5 = 4,\ r_{10} = 28,\ r_{20} = 32$
500	200	$[2,4,25]$	$r_2 = 3.\ r_4 = 4,\ r_5 = 4,\ r_{10} = 12,\ r_{20} = 16$ $r_{25} = 20,\ r_{50} = 60,\ r_{100} = 80$
1000	400	$[2,2,4,25]$	$r_2 = 7.\ r_4 = 8,\ r_5 = 4,\ r_{10} = 28,\ r_{20} = 32$ $r_{25} = 20,\ r_{50} = 140,\ r_{100} = 160$
1200	320	$[2,2,4,4,5]$	$r_2 = 15.\ r_4 = 48,\ r_5 = 4,\ r_{10} = 60,\ r_{20} = 192$

4 Pewne zastosowania rzędów w teorii ciał

Twierdzenie 4.1. *Multyplikatywna grupa ciała skończonego jest cykliczna.*

Dowód. Niech K będzie ciałem skończonym i niech $|K^*| = n$, gdzie $K^* = K \setminus \{0\}$. Przypuśćmy, że w grupie $G = K^*$ nie ma elementu rzędu n. Wtedy rzędy wszystkich elementów tej grupy są ostro mniejsze od n. Niech $a \in G$ będzie elementem maksymalnego rzędu. Niech $m = \mathrm{ord}_G(a)$. Wtedy, na mocy Stwierdzenia 2.3, dla każdego $b \in G$ zachodzi równość $b^m = 1$. Wielomian $x^m - 1 \in K[x]$ ma więc $n = |K^*|$ pierwiastków. Doszliśmy do sprzeczności, gdyż jest to wielomian stopnia m o współczynnikach z ciała K i przy tym $m < n$. $\boxtimes$

Niech K będzie dowolnym ciałem i niech $n \geqslant 1$. Oznaczmy:

$$U_n(K) = \Big\{ b \in K;\ b^n = 1 \Big\}.$$

Zbiór $U_n(K)$ jest grupą abelową. Jest to podgrupa multyplikatywnej grupy ciała K, czyli grupy $K^* = K \setminus \{0\}$. Jest to grupa skończona, gdyż wielomian $x^n - 1$ ma co najwyżej n pierwiastków.

Twierdzenie 4.2. *Jeśli K jest ciałem, to dla każdego $n \geqslant 1$ grupa $U_n(K)$ jest cykliczna.*

Dowód. Niech $G = U_n(K)$ i niech $|G| = s$. Oczywiście $s \leqslant n$. Przypuśćmy, że grupa G nie jest cykliczna. Niech $a \in G$ będzie elementem maksymalnego rzędu. Wtedy $m < s$ oraz (na mocy Stwierdzenia 2.3) dla każdego elementu b grupy G zachodzi równość $b^m = 1$. Wielomian $x^m - 1 \in K[x]$ ma więc s pierwiastków. Doszliśmy do sprzeczności, gdyż jest to wielomian stopnia m o współczynnikach z ciała K i przy tym $m < s$. $\boxtimes$

Wiemy dobrze, że jeśli p jest liczbą pierwszą, to pierścień $\mathbb{Z}_p$ jest ciałem. W poprzednim rozdziale udowodniliśmy (patrz Stwierdzenie 3.24) pewne uogólnienie twierdzenia Wilsona mówiącego o tym, że iloczyn wszystkich niezerowych elementów ciała $\mathbb{Z}_p$ jest równy -1. Udowodnimy, że to samo zachodzi dla dowolnego ciała skończonego.

Twierdzenie 4.3. *Iloczyn wszystkich niezerowych elementów dowolnego ciała skończonego jest równy -1.*

Dowód. Niech p będzie liczbą pierwszą i niech K będzie ciałem skończonym charakterystyki p. Liczba wszystkich elementów ciała K jest wtedy potęgą liczby p; przyjmijmy, że $|K| = p^s$, gdzie $s \geqslant 1$.

Niech $G = K \setminus \{0\}$ będzie grupą multyplikatywną ciała K. Mamy wtedy: $|G| = p^s - 1$. Wiemy (patrz Twierdzenie 4.1), że G jest grupą cykliczną.

Załóżmy najpierw, że $p \geqslant 3$. W tym przypadku G jest skończoną grupą cykliczną parzystego rzędu. Grupa ta ma więc (na mocy Stwierdzenia 2.9) dokładnie jeden element rzędu 2. Tym elementem jest oczywiście -1. Ze Stwierdzenia 2.18 wynika zatem, że iloczyn wszystkich elementów grupy G, czyli iloczyn wszystkich niezerowych elementów ciała K, jest równy -1.

Pozostał przypadek $p = 2$. W tym przypadku G jest grupą cykliczną nieparzystego rzędu. Grupa G nie ma więc żadnego elementu rzędu 2. Iloczyn jej wszystkich elementów, na mocy Stwierdzenia 2.18, jest równy 1. Ale w tym przypadku K jest ciałem charakterystyki 2, więc $1 = -1$. $\boxtimes$

Literatura

[1] Cz. Bagiński, *Wstęp do Teorii Grup*, SCRIPT, Warszawa 2012.

[2] J. Browkin, *Wybrane Zagadnienia Algebry*, PWN, Warszawa, 1968.

[3] J. Browkin, *Teoria Ciał*, PWN, Warszawa, 1977.

[4] M. Hall, *The theory of groups*, The MacMillan Company, New York, 1959 (wydanie rosyjskie: Moskwa 1962).

[5] I. N. Herstein, *Topics in Algebra*, John Wiley & Sons, 1975.

[6] M. I. Kargapołow, J. I. Mierzlakow, *Podstawy Teorii Grup*, Nauka, Moskwa, 1982 (wydanie polskie: PWN, Warszawa, 1989).

[7] A. I. Kostrykin, *Zbiór zadań z algebry*, PWN, Warszawa, 1995.

[8] S. Lang, *Algebra*, Addison–Wesley Publ. Comp. 1965.

[9] F. Lemmermeyer, *Introduction to Number Theory*, Preprint, 2000, 1-100.

[10] A. Nowicki, *Liczby Pierwsze*, Podróże po Imperium Liczb, cz.4, Wydanie Drugie, Wydawnictwo OWSIiZ, Toruń, Olsztyn, 2012.

[11] A. Nowicki, *Funkcje Arytmetyczne*, Podróże po Imperium Liczb, cz.5, Wydanie Drugie, Wydawnictwo OWSIiZ, Toruń, Olsztyn, 2012.

[12] A. Nowicki, *Liczby Mersenne'a, Fermata i Inne Liczby*, Podróże po Imperium Liczb, cz.8, Wydanie Drugie, Wydawnictwo OWSIiZ, Toruń, Olsztyn, 2012.

[13] A. Nowicki, *Silnie i Symbole Newtona*, Podróże po Imperium Liczb, cz.11, Wydanie Drugie, Wydawnictwo OWSIiZ, Toruń, Olsztyn, 2013.

[14] J. Rutkowski, *Algebra Abstrakcyjna w Zadaniach*, PWN, Warszawa 2000.

[15] W. Sierpiński, *Teoria Liczb*, Warszawa - Wrocław, 1950.

[16] W. Sierpiński, *Elementary Theory of Numbers*, Editor: A. Schinzel, North-Holland Mathematical Library, Vol. 31, 1988.

[17] K. Szymiczek i inni, *Zbiór Zadań z Teorii Grup*, Uniwersytet Śląski, Katowice, 1979.

[18] I. Winogradow, *Elementy Teorii Liczb*, PWN, Warszawa, 1954.

Nicolaus Copernicus University, Faculty of Mathematics and Computer Science,
87-100 Toruń, Poland, (e-mail: anow@mat.uni.torun.pl).
