Interesujące nas przykłady grup – podsumowanie

Grupą nazywamy zbiór wraz z działaniem dwuargumentowym określonym na tym zbiorze (i o wartościach w tymże zbiorze), spełniającym ogólnie przyjęte warunki, o których później. W swoich rozważaniach ograniczymy się do dwóch rodzin przykładów grup.

Grupa $\mathbb{Z}_n$, gdzie n jest liczbą całkowitą dodatnią.
Bardziej formalnie jest to para uporządkowana $(\mathbb{Z}_n, +_n)$, gdzie $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, a $+_n$ jest dodawaniem modulo n.

Grupa $\mathbb{Z}_p^*$, gdzie p jest liczbą pierwszą.
Bardziej formalnie jest to para uporządkowana $\left(\mathbb{Z}_p^*, \cdot_p\right)$, gdzie $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$, a $\cdot_p$ jest mnożeniem modulo p.

Odnotujmy wspólne własności powyższych struktur:
(i) Działanie jest łączne, czyli nie wymaga użycia nawiasów dla oznaczenia kolejności działań, a dokładniej:

$$(a +_n b) +_n c = a +_n (b +_n c) \qquad \text{dla } a, b, c \in \mathbb{Z}_n\,,$$

$$(a \cdot_p b) \cdot_p c = a \cdot_p (b \cdot_p c) \qquad \text{dla } a, b, c \in \mathbb{Z}_p^*\,.$$

(ii) Działanie jest przemienne, czyli jego wynik nie zależy od kolejności argumentów, a dokładniej:

$$a +_n b = b +_n a \qquad \text{dla } a, b \in \mathbb{Z}_n\,,$$

$$a \cdot_p b = b \cdot_p a \qquad \text{dla } a, b \in \mathbb{Z}_p^*\,.$$

(iii) W zbiorze istnieje element neutralny, czyli taki, którego dodanie/domnożenie nie daje żadnego efektu. W grupie $\mathbb{Z}_n$ takim elementem jest 0, a w grupie $\mathbb{Z}_p^*$ elementem neutralnym jest 1. Dokładniej:

$$a +_n 0 = 0 +_n a = a \qquad \text{dla } a \in \mathbb{Z}_n\,,$$

$$a \cdot_p 1 = 1 \cdot_p a = a \qquad \text{dla } a \in \mathbb{Z}_p^*\,.$$

(iv) Każdy element ma element przeciwny/odwrotny, czyli taki, którego dodanie/domnożenie prowadzi do elementu neutralnego, a dokładniej:
• dla każdego $a \in \mathbb{Z}_n$ istnieje taki element $-a \in \mathbb{Z}_n$, że

$$(-a) +_n a = a +_n (-a) = 0\,,$$

• dla każdego $a \in \mathbb{Z}_p^*$ istnieje taki element $a^{-1} \in \mathbb{Z}_p^*$, że

$$a^{-1} \cdot_p a = a \cdot_p a^{-1} = 1\,.$$

Warunki **(i)**, **(iii)** oraz **(iv)** występują w definicji grupy, natomiast warunek **(ii)** oznacza, że grupa jest przemienna. Ponieważ jednak wszystkie interesujące nas grupy są przemienne, nie musimy tego warunku w żaden sposób wyróżniać.

Niech teraz a będzie elementem grupy, a k liczbą całkowitą dodatnią. Dodając/mnożąc k kopii tego elementu przez siebie stosujemy następujące oznaczenia:

$$\underbrace{a +_n a +_n a +_n \ldots +_n a}_{k \text{ razy}} = ka \qquad \text{dla } a \in \mathbb{Z}_n\,,$$

$$\underbrace{a \cdot_p a \cdot_p a \cdot_p \ldots \cdot_p a}_{k \text{ razy}} = a^k \qquad \text{dla } a \in \mathbb{Z}_p^*\,.$$

Najmniejszą liczbę całkowitą dodatnią k, dla której otrzymamy w ten sposób element neutralny grupy, czyli w grupie $\mathbb{Z}_n$ lub $\mathbb{Z}_p^*$ odpowiednio

$$ka = 0 \qquad \text{lub} \qquad a^k = 1\,,$$

nazywamy rzędem elementu a (w tej grupie) i będziemy oznaczać odpowiednio przez $r_n^+(a)$ lub $r_p(a)$.

Generatorem grupy (skończonej) nazywamy element, którego rząd jest równy liczbie elementów grupy – wówczas każdy element jest wielokrotnością/potęgą generatora. Grupę posiadającą generator nazywamy grupą cykliczną.

Generatorem grupy $\mathbb{Z}_n$ jest liczba 1 (ale też każda liczba ze zbioru $\mathbb{Z}_n$ względnie pierwsza z n).

Grupa $\mathbb{Z}_p^*$ także ma generator, ale fakt ten nie jest już taki oczywisty, a wskazanie generatora w ogólnym przypadku nie jest łatwe. Wniosek z tego faktu jest następujący: Struktura grupy $\mathbb{Z}_p^*$ jest taka sama jak struktura grupy $\mathbb{Z}_{p-1}$, co najlepiej można zilustrować na przykładach.

Łatwo sprawdzić, że podane niżej przekształcenia zachowują działanie (sprecyzuj, co to znaczy). Aby skonstuować takie przekształcenie, wystarczy przypisać generatorowi grupy $\mathbb{Z}_{p-1}$ (najlepiej liczbie 1) generator grupy $\mathbb{Z}_p^*$ (znaleziony metodą prób i błędów), a wielokrotnościom jedynki przypisać odpowiednie potęgi generatora grupy $\mathbb{Z}_p^*$. Wówczas każdy element grupy $\mathbb{Z}_p^*$ jest przedstawiony jako potęga generatora, a mnożenie takich potęg sprowadza się do dodawania wykładników modulo $p-1$.

$\mathbb{Z}_4$		$\mathbb{Z}_5^*$
$+ \pmod 4$		$\cdot \pmod 5$
0	$\mapsto$	$1 = 2^0$
1	$\mapsto$	$2 = 2^1$
2	$\mapsto$	$4 = 2^2$
3	$\mapsto$	$3 = 2^3$

$\mathbb{Z}_4$		$\mathbb{Z}_5^*$
$+ \pmod 4$		$\cdot \pmod 5$
0	$\mapsto$	$1 = 3^0$
1	$\mapsto$	$3 = 3^1$
2	$\mapsto$	$4 = 3^2$
3	$\mapsto$	$2 = 3^3$

$\mathbb{Z}_6$		$\mathbb{Z}_7^*$
$+ \pmod 6$		$\cdot \pmod 7$
0	$\mapsto$	$1 = 3^0$
1	$\mapsto$	$3 = 3^1$
2	$\mapsto$	$2 = 3^2$
3	$\mapsto$	$6 = 3^3$
4	$\mapsto$	$4 = 3^4$
5	$\mapsto$	$5 = 3^5$

$\mathbb{Z}_6$		$\mathbb{Z}_7^*$
$+ \pmod 6$		$\cdot \pmod 7$
0	$\mapsto$	$1 = 5^0$
1	$\mapsto$	$5 = 5^1$
2	$\mapsto$	$4 = 5^2$
3	$\mapsto$	$6 = 5^3$
4	$\mapsto$	$2 = 5^4$
5	$\mapsto$	$3 = 5^5$

$\mathbb{Z}_{10}$		$\mathbb{Z}_{11}^*$
$+\,(\mathrm{mod}\ 10)$		$\cdot\,(\mathrm{mod}\ 11)$
0	$\mapsto$	$1=2^0$
1	$\mapsto$	$2=2^1$
2	$\mapsto$	$4=2^2$
3	$\mapsto$	$8=2^3$
4	$\mapsto$	$5=2^4$
5	$\mapsto$	$10=2^5$
6	$\mapsto$	$9=2^6$
7	$\mapsto$	$7=2^7$
8	$\mapsto$	$3=2^8$
9	$\mapsto$	$6=2^9$

$\mathbb{Z}_{12}$		$\mathbb{Z}_{13}^*$
$+\,(\mathrm{mod}\ 12)$		$\cdot\,(\mathrm{mod}\ 13)$
0	$\mapsto$	$1=2^0$
1	$\mapsto$	$2=2^1$
2	$\mapsto$	$4=2^2$
3	$\mapsto$	$8=2^3$
4	$\mapsto$	$3=2^4$
5	$\mapsto$	$6=2^5$
6	$\mapsto$	$12=2^6$
7	$\mapsto$	$11=2^7$
8	$\mapsto$	$9=2^8$
9	$\mapsto$	$5=2^9$
10	$\mapsto$	$10=2^{10}$
11	$\mapsto$	$7=2^{11}$

$\mathbb{Z}_{16}$		$\mathbb{Z}_{17}^*$
$+\,(\mathrm{mod}\ 16)$		$\cdot\,(\mathrm{mod}\ 17)$
0	$\mapsto$	$1=3^0$
1	$\mapsto$	$3=3^1$
2	$\mapsto$	$9=3^2$
3	$\mapsto$	$10=3^3$
4	$\mapsto$	$13=3^4$
5	$\mapsto$	$5=3^5$
6	$\mapsto$	$15=3^6$
7	$\mapsto$	$11=3^7$
8	$\mapsto$	$16=3^8$
9	$\mapsto$	$14=3^9$
10	$\mapsto$	$8=3^{10}$
11	$\mapsto$	$7=3^{11}$
12	$\mapsto$	$4=3^{12}$
13	$\mapsto$	$12=3^{13}$
14	$\mapsto$	$2=3^{14}$
15	$\mapsto$	$6=3^{15}$

$\mathbb{Z}_{18}$		$\mathbb{Z}_{19}^*$
$+\,(\mathrm{mod}\ 18)$		$\cdot\,(\mathrm{mod}\ 19)$
0	$\mapsto$	$1=2^0$
1	$\mapsto$	$2=2^1$
2	$\mapsto$	$4=2^2$
3	$\mapsto$	$8=2^3$
4	$\mapsto$	$16=2^4$
5	$\mapsto$	$13=2^5$
6	$\mapsto$	$7=2^6$
7	$\mapsto$	$14=2^7$
8	$\mapsto$	$9=2^8$
9	$\mapsto$	$18=2^9$
10	$\mapsto$	$17=2^{10}$
11	$\mapsto$	$15=2^{11}$
12	$\mapsto$	$11=2^{12}$
13	$\mapsto$	$3=2^{13}$
14	$\mapsto$	$6=2^{14}$
15	$\mapsto$	$12=2^{15}$
16	$\mapsto$	$5=2^{16}$
17	$\mapsto$	$10=2^{17}$

Liczbę całkowitą r nazywamy resztą kwadratową (odpowiednio: sześcienną i stopnia k) modulo p, jeżeli kongruencja

$$x^2 \equiv r \,(\mathrm{mod}\ p)$$

ma rozwiązanie całkowite x. Odpowiednio: $x^3 \equiv r \,(\mathrm{mod}\ p)$ i $x^k \equiv r \,(\mathrm{mod}\ p)$.

W przeciwnym razie resztę r nazywamy niereszą kwadratową (odpowiednio: sześcienną i stopnia k) modulo m.

W niektórych z poniższych zadań wolno skorzystać z następującego twierdzenia: Liczba 2 jest resztą kwadratową modulo p, gdzie p jest nieparzystą liczbą pierwszą, wtedy i tylko wtedy, gdy $p \equiv \pm 1 \,(\mathrm{mod}\ 8)$.

1. Korzystając z podanych wyżej przekształceń wskazać wszystkie generatory grup $\mathbb{Z}_p^*$ dla $p=5,7,11,13,17,19$.

2. Korzystając z podanych wyżej przekształceń wskazać wszystkie niezerowe reszty kwadratowe modulo p dla $p=11,13,17,19$.

3. Korzystając z podanych wyżej przekształceń wskazać wszystkie niezerowe reszty sześcienne modulo p dla $p=11,13,17,19$.

4. Korzystając z podanych wyżej przekształceń wskazać wszystkie niezerowe reszty bikwadratowe (czwartego stopnia) modulo p dla $p=11,13,17,19$.

5. Niech p będzie liczbą pierwszą. Ile wśród liczb 1, 2, 3, ..., $p-1$ jest reszt kwadratowych, a ile niereszt kwadratowych?

6. Niech p będzie liczbą pierwszą. Ile wśród liczb 1, 2, 3, ..., $p-1$ jest reszt sześciennych, a ile niereszt sześciennych?

7. Niech p będzie liczbą pierwszą. Ile wśród liczb 1, 2, 3, ..., $p-1$ jest reszt, a ile niereszt bikwadratowych (czwartego stopnia)?

8. Niech p będzie liczbą pierwszą. Ile wśród liczb 1, 2, 3, ..., $p-1$ jest reszt, a ile niereszt piątego stopnia?

9. Niech p będzie liczbą pierwszą. Ile wśród liczb 1, 2, 3, ..., $p-1$ jest reszt, a ile niereszt dziewiątego stopnia?

10. Niech p będzie liczbą pierwszą. Dowieść, że dowolny dzielnik pierwszy liczby 2^p-1 daje przy dzieleniu przez p resztę 1.

11. Niech p będzie liczbą pierwszą. Dowieść, że dowolny dzielnik pierwszy liczby 2^p+1 różny od 3 daje przy dzieleniu przez p resztę 1.

12. Dowieść, że istnieje nieskończenie wiele liczb pierwszych dających przy dzieleniu przez 6 resztę 1.

13. Dowieść, że istnieje nieskończenie wiele liczb pierwszych zakończonych cyfrą 1.

14. Niech k będzie liczbą naturalną. Dowieść, że dowolny dzielnik pierwszy liczby $2^{2^k}+1$ daje przy dzieleniu przez 2^{k+1} resztę 1.

15. Niech k będzie liczbą naturalną większą od 1. Dowieść, że dowolny dzielnik pierwszy liczby $2^{2^k}+1$ daje przy dzieleniu przez 2^{k+2} resztę 1.

16. Dowieść, że liczba 127 jest pierwsza nie wykonując żadnego dzielenia tej liczby przez mniejsze liczby.

17. Dowieść, że liczba $2^{16}+1$ jest pierwsza.

18. Dowieść, że liczba $2^{11}-1$ jest złożona.

19. Niech $p=4k+3>3$ będzie taką liczbą pierwszą, że liczba $q=2p+1$ też jest pierwsza. Dowieść, że liczba 2^p-1 jest złożona.

20. Wiadomo, że liczba $2^{32}+1$ ma dzielnik pierwszy mniejszy od 700. Wskazać ten dzielnik.