Zadanie *1* (oprac. *Anna Wrochna*) Niech m będzie liczbą całkowitą dodatnią. Udowodnij, że jeśli m jest liczbą złożoną, to $\{1, \ldots, m-1\}$ z operacją mnożenia mod$m$ nie jest grupą.

Rozwiązanie. Jeśli m jest liczbą złożoną, to istnieją takie liczby całkowite dodatnie p i q, że $m = pq$. Oczywiście należą one do zbioru $\{1, \ldots, m-1\}$, natomiast ich iloczyn mod$m$ wynosi 0. Zbiór $\{1, \ldots, m-1\}$ nie jest zatem domknięty na możenie mod$m$.

Zadanie *4* (oprac. *Anna Wrochna*) Skonstruuj ciało $GF(11)$ z dodawaniem i mnożeniem modulo 11. Znajdź wszystkie elementy pierwotne. Wyznacz rzędy pozostałych elementów.

Rozwiązanie. Dodawanie i mnożenie w $GF(11)$ wyglądają następująco:

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

$*$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Potęgi kolejnych elementów wynoszą odpowiednio:

x^y	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

Rzędem elementu (zapisanego w pierwszej kolumnie) jest numer kolumny, w którym występuje druga jedynka. Mamy więc:

- 1 element rzędu 1: 1
- 1 element rzędu 2: 10
- 4 elementy rzędu 5: 3, 4, 5, 9
- 4 elementy rzędu 10, czyli elementy pierwotne: 2, 6, 7, 8

Zadanie *5* (oprac. *Anna Wrochna*) Pokaż, że każde ciało skończone ma element pierwotny.
Rozwiązanie. Rozważmy ciało o q elementach. Jego grupa multiplikatywna ma wówczas $q-1$ elementów.
Niech a będzie elementem maksymalnego rzędu w tym ciele, ktory oznaczymy przez m. Zauważmy, że dla każdych elementów x, y zachodzi:

$$ord(xy) = NWW(ord(x), ord(y))$$

Niech b będzie elementem tego ciała. Wówczas

$$ord(ab) = NWW(ord(a), ord(b)) = NWW(m, ord(b)) = m$$

gdyż m jest maksymalnym rzędem. Mamy więc, że dla dowolnego elementu b zachodzi $ord(b)|m$, a zatem $b^m - 1 = 0$. Skoro wielomian $x^m - 1$ ma $q-1$ pierwiastków, to

$$m \geq q-1$$

Z drugiej strony, maksymalny rząd elementu nie może przekraczać liczby elementów w grupie, czyli

$$m \leq q-1$$

Wynika stąd, że element maksymalnego rzędu jest elementem rzędu $q-1$, czyli pierwiastkiem pierwotnym.

Zadanie *8* (oprac. *Anna Wrochna*) Pokaż, że $p(X) = X^5 + X^3 + 1$ jest nieredukowalny nad $GF(2)$.
Rozwiązanie. $p(X)$ jest wielomianem stopnia 5, wystarczy więc sprawdzić, czy nie dzieli się przez wielomian nieredukowalny stopnia mniejszego niż 3.
Zauważmy, że $p(0) = p(1) = 1$. Oznacza to, że $p(X)$ nie ma pierwsiastków, a zatem nie jest podzielny przez żaden wielomian stopnia 1.
Wielomiany stopnia 2 nad $GF(2)$ są następujące:

- X^2 - podzielny przez X
- $X^2 + 1$ - podzielny przez $X + 1$
- $X^2 + X$ - podzielny przez X
- $X^2 + X + 1$ - nieredukowalny.

Podzielimy więc $p(X)$ przez $X^2 + X + 1$ „szkolnym" algorytmem dzielenia (ale utożsamiając dodawanie i odejmowanie w $GF(2)$ utożsamiamy):
$\underline{X^3 + X^2 + X}$
$X^5 + X^3 + 1 : X^2 + X + 1$
$\underline{+X^5 + X^4 + X^3}$
$X^4 + 1$
$\underline{+X^4 + X^3 + X^2}$
$X^3 + X^2 + 1$
$\underline{+X^3 + X^2 + X}$
$X + 1$
Otrzymaliśmy resztę $X + 1$, co dowodzi, że $p(X)$ nie jest podzielny przez $X^2 + X + 1$, a zatem jest nieredukowalny.
Zadanie *9* (oprac. *Anna Wrochna*) Niech $f(X)$ będzie wielomianem stopnia n nad $GF(2)$. Wielomianem odwrotnym do $f(X)$ jest $f^*(X) = X^n f(\frac{1}{X})$.

1. Dowiedz, że $f^*(X)$ jest nieredukowalny nad $GF(2)$ wtw $f(X)$ jest nieredukowalny.
2. Dowiedz, że $f^*(X)$ jest pierwotny wtw $f(X)$ jest pierwotny.

Rozwiązanie.

Obserwacja 1 *Operacja $\cdot^*$ jest inwolucją, czyli $(f^*(X))^* = f(X)$.*

Dowód:

$$(f^*(X))^* = (X^n f(1/X))^* = (1/X)^n X^n f\left(1/\frac{1}{X}\right) = f(X)$$

$\diamond$

1. Przypuśćmy, że $f(X)$ jest redukowalny. Wówczas, dla pewnych nietrywialnych wielomianów $p(X)$ i $q(X)$, mamy:

$$f(X) = p(X)q(X)$$

Zatem

$$f^*(X) = X^n p(1/X) q(1/X) = p^*(X) q^*(X)$$

co oznacza, że $f^*(X)$ jest redukowalny. Analogicznie, redukowalność $f^*(X)$ implikuje redukowalność $f(X)$.

2. Niech $f(X)|X^k+1$. Pokażemy, że jest to równoważne warunkowi $f^*(X)|X^k+1$. Mamy:

$$X^k + 1 = f(X)p(X)$$

dla pewnego nietrywialnego wielomianu $p(X)$. Podstawiając w miejsce X $1/X$ otrzymujemy:

$$X^{-k} + 1 = f(1/X)p(1/X)$$

Mnożymy stronami przez X^k:

$$1 + X^k = X^k f(1/X)p(1/X)$$

Wiedząc, że $deg\ f + deg\ p = k$, możemy napisać:

$$1 + X^k = f^*(X)p^*(X)$$

co oznacza, że $f^*(X)|X^k + 1$.
Oczywiście $deg\ f = deg\ f^* = n$. Jeśli zatem najmniejszą liczbą k taką, że $f(X)|X^k + 1$ jest $2^n - 1$, to dla wielomianu f^* jest analogicznie (i odwrotnie, korzystając z obserwacji udowodnionej powyżej).