IMIĘ i NAZWISKO (DRUKOWANE): .....

Nr grupy: .....

40 pkt.

Kolokwium II – 3 lutego 2023 r. – Zestaw B

1. W zbiorze $\mathbb{Z}$ określono relację równoważności R:

10 pkt.

$$xRy \qquad \Longleftrightarrow \qquad x^2 \equiv y^6 \pmod 5.$$

Wyznacz klasy abstrakcji względem tej relacji.

Rozwiązanie: Ponieważ 5 jest liczbą pierwszą, to z małego twierdzenia Fermata wynika, że $y^5 \equiv y \pmod 5$ dla dowolnego $y \in \mathbb{Z}$. Możemy wiec definicję relacji R przepisać w postaci

$$xRy \qquad \Longleftrightarrow \qquad x^2 \equiv y^2 \pmod 5.$$

(Oczywiście spokojnie można zostawić y^6 i liczyć tak samo. Dla y^2 jest po prostu trochę szybciej.) Teraz wystarczy sprawdzić, do jakich klas należą liczby postaci $5k + i$ dla $i \in \{0, 1, 2, 3, 4\}$. Mamy

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \colon x^2 \equiv 0 \pmod 5\} = \{5k \colon k \in \mathbb{Z}\},\\
[1] = [4] &= \{x \in \mathbb{Z} \colon x^2 \equiv 1 \pmod 5\} = \{5k+1 \colon k \in \mathbb{Z}\} \cup \{5k+4 \colon k \in \mathbb{Z}\},\\
[2] = [3] &= \{x \in \mathbb{Z} \colon x^2 \equiv 4 \pmod 5\} = \{5k+2 \colon k \in \mathbb{Z}\} \cup \{5k+3 \colon k \in \mathbb{Z}\}.
\end{aligned}$$

□

2. Rozwiąż układ kongruencji

$$\begin{cases} x \equiv 9 \pmod 7, \\ 5x \equiv 2 \pmod{13}, \\ 6x \equiv 5 \pmod{29}. \end{cases}$$

10 pkt.

Rozwiązanie: Ponieważ $6 \cdot 5 \equiv 1 \pmod{29}$, to z trzeciej kongruencji wynika, że $x \equiv 25 \pmod{29}$, czyli $x = 25 + 29k$ dla $k \in \mathbb{Z}$. Wstawiając otrzymany wynik do drugiej kongruencji, dostajemy $125 + 145k \equiv 2 \pmod{13}$, co jest równoważne z $2k \equiv 7 \pmod{13}$. Mnożąc tę kongruencję przez 7, widzimy, że $k \equiv 10 \pmod{13}$, czyli $k = 10 + 13l$ dla $l \in \mathbb{Z}$, co daje $x = 315 + 13 \cdot 29l$. Po wstawieniu tego wyniku do pierwszej kongruencji mamy (po redukcji modulo 7) $-l \equiv 2 \pmod 7$, więc $l = -2 + 7m$, $m \in \mathbb{Z}$. Ostatecznie

$$x = -439 + 7 \cdot 13 \cdot 29m = 2200 + 7 \cdot 13 \cdot 29m', \qquad m, m' \in \mathbb{Z}.$$

□

3. Uzasadnij, że liczba

$$2^{7^{2023}} - 23$$

jest podzielna przez 105.

10 pkt.

Rozwiązanie: Sposób 1. Z chińskiego twierdzenia o resztach wynika, że liczba całkowita x jest podzielna przez $105 = 3 \cdot 5 \cdot 7$ wtedy i tylko wtedy, gdy

$$\begin{cases} x \equiv 0 \pmod 3, \\ x \equiv 0 \pmod 5, \\ x \equiv 0 \pmod 7. \end{cases}$$

Sprawdźmy zatem, jakie są reszty z dzielenia $x = 2^{7^{2023}} - 23$ przez 3, 5 i 7. Ponieważ $2^{2k+1} = 4^k \cdot 2 \equiv 2 \pmod 3$ dla dowolnego $k \in \mathbb{N}$, to (7^{2023} jest liczbą nieparzystą) $x \equiv 2 - 23 \equiv 0 \pmod 3$. Podobnie $2^{2k+1} = 4^k \cdot 2 \equiv -2 \pmod 5$, więc $x \equiv -2 - 23 \equiv 0 \pmod 5$. Aby natomiast znaleźć resztę z dzielenia x przez 7, zauważmy, że $2^{3k} \equiv 1 \pmod 7$ oraz $7^k \equiv 1 \pmod 3$. Stąd

$$x \equiv 2^{3k+1} - 23 \equiv 2 - 23 \equiv 0 \pmod 7.$$

Sposób 2. Ponieważ jedynym dzielnikiem pierwszym liczby $2^{7^{2023}}$ jest 2, to $\mathrm{NWD}(2^{7^{2023}}, 105) = 1$. Ponadto $\phi(105) = \phi(3) \cdot \phi(5) \cdot \phi(7) = 2 \cdot 4 \cdot 6 = 48$, więc na mocy twierdzenia Eulera otrzymujemy $2^{48} \equiv 1 \pmod{105}$ i w konsekwencji

$$2^{48k} \equiv 1 \pmod{105}$$

dla dowolnego $k \in \mathbb{N}$. (Oczywiście tę własność można również otrzymać z „tabelki", ale jest to droga bardziej pracochłonna — lepiej użyć tw. Eulera.) Ponadto $7^{2k} \equiv 1 \pmod{48}$, więc

$$7^{2023} \equiv 7 \pmod{48}.$$

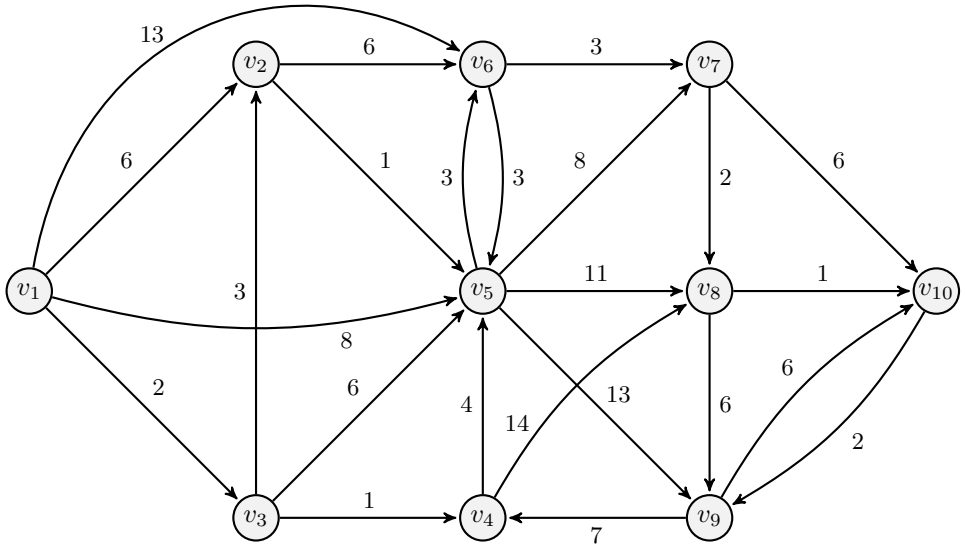
Ostatecznie

$$2^{7^{2023}} \equiv 2^{7^{2023} \bmod 48} = 2^7 \equiv 23 \pmod{105},$$

więc $2^{7^{2023}} - 23 \equiv 0 \pmod{105}$. □

4. Wyznacz, przy pomocy algorytmu Dijkstry, najkrótsze ścieżki łączące wierzchołek v_1 ze wszystkimi pozostałymi dla grafu

10 pkt.



Rozwiązanie: Postępując zgodnie z algorytmem Dijkstry, otrzymujemy

L	$D(2)$	$D(3)$	$D(4)$	$D(5)$	$D(6)$	$D(7)$	$D(8)$	$D(9)$	$D(10)$
$\emptyset$	6	2	13	8	∞	∞	∞	∞	∞
$\{v_2\}$	5	2	13	8	3	∞	∞	∞	∞
$\{v_2, v_4\}$	5	2	13	7	3	∞	17	∞	∞
$\{v_2, v_4, v_3\}$	5	2	11	6	3	∞	17	∞	∞
$\{v_2, v_4, v_3, v_5\}$	5	2	9	6	3	14	17	19	∞
$\{v_2, v_4, v_3, v_5, v_6\}$	5	2	9	6	3	12	17	19	∞
$\{v_2, v_4, v_3, v_5, v_6, v_9\}$	5	2	9	6	3	12	14	19	18
$\{v_2, v_4, v_3, v_5, v_6, v_9, v_8\}$	5	2	9	6	3	12	14	19	15
$\{v_2, v_4, v_3, v_5, v_6, v_9, v_8, v_7\}$	5	2	9	6	3	12	14	19	15
$\{v_2, v_4, v_3, v_5, v_6, v_9, v_8, v_7, v_{10}\}$	5	2	9	6	3	12	14	17	15

□