Kongruencje

Beata Łojan

b.lojan@knm.katowice.pl

Koło Naukowe Matematyków
Uniwersytetu Śląskiego w Katowicach

www.knm.katowice.pl

III Liceum Ogólnokształcące im. Lucjana Szenwalda
w Dąbrowie Górniczej

Spis treści

Dąbrowa Górnicza, 14 listopada 2011

1. Kongruencje — wprowadzenie

1.1. Pojęcia wstępne — NWD i NWW

$\mathbb{N}$ – liczby naturalne
$\mathbb{Z}$ – liczby całkowite
$\mathbb{Q}$ – liczby wymierne
$\mathbb{R}$ – liczby rzeczywiste
$\mathbb{C}$ – liczby zespolone

Definicja 1.1. Niech $a, b \in \mathbb{Z}$ i $b \neq 0$. Wtedy a jest *podzielne z resztą* przez b jeśli istnieją takie liczby $q \in \mathbb{Z}$ oraz $r \in \mathbb{N} \cup \{0\}$, że $a = bq + r$ oraz $0 \leqslant r < |b|$.

Definicja 1.2. Niech $a, b \in \mathbb{Z}$ i $b \neq 0$. Mówimy, że a jest *podzielne* przez b jeśli istnieje taka liczba całkowita a, że $a = bq$ (czyli reszta z dzielenia $r = 0$). Wtedy b nazywamy *dzielnikiem* liczby a.
Oznaczenie: $b|a$ – b dzieli a, $b \not| a$ – b nie dzieli a.

Definicja 1.3. Niech $a, b \in \mathbb{Z}$ oraz $a \neq 0$ lub $b \neq 0$. *Największym wspólnym dzielnikiem* liczb a i b nazywamy taką liczbę naturalną d, że:

(i) $d|a \wedge d|b$

(ii) $\bigwedge\limits_{c \in \mathbb{N}} (c|a \wedge c|b) \Rightarrow c|d$

Oznaczenie: $\mathrm{NWD}(a, b) = d$.

Definicja 1.4. Niech $a, b \in \mathbb{Z}$ oraz $a \neq 0$ lub $b \neq 0$. Liczby a i b nazywamy *względnie pierwszymi* jeśli $\mathrm{NWD}(a, b) = 1$.

Definicja 1.5. Niech $a, b \in \mathbb{Z}$ oraz $a \neq 0$ i $b \neq 0$. *Najmniejszą wspólną wielokrotnością* liczb a i b nazywamy taką liczbę naturalną w, że:

(i) $a|w \wedge b|w$

(ii) $\bigwedge\limits_{c \in \mathbb{N}} (a|c \wedge b|c) \Rightarrow w|c$

Oznaczenie: $\mathrm{NWW}(a, b) = w$.

Twierdzenie 1.1. *Niech* $a, b \in \mathbb{N}$. *Wtedy* $ab = \mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b)$.

Przykład 1.1.

(i) $\mathrm{NWD}(8, 12) = \mathrm{NWD}(-8, 12) = 4$;

(ii) $\mathrm{NWW}(8, 12) = \mathrm{NWW}(-8, 12) = 24$;

(iii) $\mathrm{NWD}(2, 5) = 1$ co oznacza, że 2 i 5 są względnie pierwsze.

1.2. Definicja kongruencji

Definicja 1.6. Niech $m \in \mathbb{N}$ oraz $a, b \in \mathbb{Z}$. Mówimy, że liczba a *przystaje do* b *modulo* m jeśli $m|a - b$. Liczbę m nazywamy *modułem kongruencji*. Symbolicznie zapisujemy, to $a \equiv b (\mathrm{mod}\, m)$.

$$a \equiv b (\mathrm{mod}\, m) \Leftrightarrow m|(a - b) \Leftrightarrow \bigvee_{k \in \mathbb{Z}} a - b = k \cdot m$$

Kongruencja to sposób zapisu tego, że pewne dwie liczby całkowite a i b dają tę samą resztę przy dzieleniu przez liczbę naturalną m. Pozwalają w krótki sposób zapisywać rozwiązania zadań o podzielności liczb. Zapis $a \equiv b (\mathrm{mod}\, m)$ oznacza również, że reszta z dzielenia a przez m jest równa b, tzn.: $a = m \cdot q + b$. Zauważmy również, że jeśli $m|a$, to $a \equiv 0 (\mathrm{mod}\, m)$.

Przykład 1.2. Które kongruencje są prawdziwe?

(i) $10 \equiv 1 (\mathrm{mod}\, 9)$
Zauważmy, że $10 - 1 = 9$ oraz $9|9$, a zatem kongruencja jest prawdziwa.

(ii) $8 \equiv 5 (\mathrm{mod}\, 7)$
Mamy $8 - 5 = 3$ i $7 \not| 3$, a zatem kongruencja nie jest prawdziwa.

(iii) $-1 \equiv 113 (\mathrm{mod}\, 6)$

(iv) $-5 \equiv 31 (\mathrm{mod}\, 7)$

2. Własności kongruencji

Relacja równoważności jest to zwrotna, symetryczna i przechodnia relacja dwuargumentowa określona na pewnym zbiorze utożsamiająca ze sobą w pewien sposób jego elementy, co ustanawia podział tego zbioru na rozłączne podzbiory według tej relacji.

Przystawanie modulo m jest relacją równoważności:

(i) zwrotność:
$$a \equiv a (\mathrm{mod}\, m)$$

(ii) symetryczność:
$$a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$$

(iii) przechodniość:
$$a \equiv b (\mathrm{mod}\, m) \wedge b \equiv c (\mathrm{mod}\, m) \Rightarrow a \equiv c (\mathrm{mod}\, m)$$

Twierdzenie 2.1. *Niech* $a, b, c, d \in \mathbb{Z}$ *oraz* $m, m_1, m_2 \in \mathbb{N}$. *Wówczas:*

(i) *jeśli* $a \equiv b (\mathrm{mod}\, m)$ *i* $c \equiv d (\mathrm{mod}\, m)$, *to*

(i_a) $a + c \equiv b + d (\mathrm{mod}\, m)$;

(i_b) $a - c \equiv b - d (\mathrm{mod}\, m)$;

(i_c) $a \cdot c \equiv b \cdot d (\mathrm{mod}\, m)$;

(ii) *jeśli* $ad \equiv bd (\mathrm{mod}\, m)$ *i* $\mathrm{NWD}(d, m) = 1$, *to* $a \equiv b (\mathrm{mod}\, m)$;

(iii) *jeśli* $a \equiv b (\mathrm{mod}\, m_1)$ *i* $a \equiv b (\mathrm{mod}\, m_2)$, *to* $a \equiv b (\mathrm{mod}\ \mathrm{NWW}(m_1, m_2))$.

Wniosek 2.1. *W szczególności, jeśli* $a \equiv b (\mathrm{mod}\, m)$, *to dla dowolnych liczb całkowitych* $k_0, \ldots, k_n$ *mamy:*

$$k_n a^n + \cdots + k_1 a + k_0 \equiv k_n b^n + \cdots + k_1 b + k_0 (\mathrm{mod}\, m).$$

Zauważmy, że po obu stronach mamy wielomiany stopnia n *i powyższą kongruencję możemy zapisać:* $f(a) \equiv f(b) (\mathrm{mod}\, m)$, *gdzie* $f(X) = a_n X^n + \cdots + a_1 X + a_0$.

Cechy podzielności

W tej części pokażemy jak za pomocą kongruencji można wykazać znane nam cechy podzielności liczb.

Dowolną liczbę całkowitą a w systemie dziesiątkowym możemy zapisać w postaci:

$$a = (a_0 a_1 \dots a_n)_{10} = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n.$$

Jeśli zatem $f(X) = a_n X^n + \cdots + a_1 X + a_0$ to wówczas $a = f(10)$.

Przykład 2.1. (Cecha podzielności przez 9) Jak wiemy liczba podzielna jest przez 9 wtedy i tylko wtedy, gdy suma jej cyfr podzielna jest przez 9.

Dowód. Zauważmy, że $10 \equiv 1 (\mathrm{mod}\, 9)$, zatem na mocy wniosku (2.1) mamy, że $f(10) \equiv f(1) (\mathrm{mod}\, 9)$. Rozważmy następujące kongruencje:

$$\begin{aligned} 10^0 = 1 &\equiv 1 (\mathrm{mod}\, 9) \\ 10^1 = 10 &\equiv 1 (\mathrm{mod}\, 9) \\ 10^2 = 100 &\equiv 1 (\mathrm{mod}\, 9) \\ &\vdots \\ 10^n &\equiv 1 (\mathrm{mod}\, 9) \end{aligned}$$

Pomnóżmy każdą z tych kongruencji odpowiednio przez $a_0, a_1, a_2, \dots, a_n$. Wówczas mamy:

$$\begin{aligned} a_0 &\equiv a_0 (\mathrm{mod}\, 9) \\ 10 \cdot a_1 &\equiv a_1 (\mathrm{mod}\, 9) \\ 10^2 \cdot a_2 &\equiv a_2 (\mathrm{mod}\, 9) \\ &\vdots \\ 10^n \cdot a_n &\equiv a_n (\mathrm{mod}\, 9) \end{aligned}$$

Następnie dodajmy je wszystkie stronami:

$$a = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \equiv a_0 + a_1 + \cdots + a_n (\mathrm{mod}\, 9)$$

■

Przykład 2.2. (Cecha podzielności przez 11) Liczba podzielna jest przez 11 wtedy i tylko wtedy, gdy naprzemienna suma jej cyfr podzielna jest przez 11.

Dowód. Zauważmy, że $10 \equiv -1 (\mathrm{mod}\, 11)$, zatem na mocy wniosku (2.1) mamy, że $f(10) \equiv f(-1) (\mathrm{mod}\, 11)$. Rozważmy następujące kongruencje:

$$\begin{aligned} 10^0 = 1 &\equiv 1 (\mathrm{mod}\, 11) \\ 10^1 = 10 &\equiv -1 (\mathrm{mod}\, 11) \\ 10^2 = 100 &\equiv 1 (\mathrm{mod}\, 11) \\ &\vdots \\ 10^n &\equiv (-1)^n (\mathrm{mod}\, 11) \end{aligned}$$

Pomnóżmy każdą z tych kongruencji odpowiednio przez $a_0, a_1, a_2, \dots, a_n$, a następnie dodajmy je stronami i otrzymamy wtedy:

$$\begin{aligned} a &\equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n (\mathrm{mod}\, 11) \\ a &\equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) (\mathrm{mod}\, 11) \end{aligned}$$

■

3. Funkcja Eulera

Definicja 3.1. Niech $n \in \mathbb{N}$, Zbiór $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ nazywamy *zbiorem reszt modulo* n. Przez $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \colon \text{NWD}(x, n) = 1\}$ oznaczamy *zbiór elementów odwracalnych*.

Przykład 3.1.

(i) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$,
$U(\mathbb{Z}_4) = \{1, 3\}$;
Zauważmy również, że „5" w $\mathbb{Z}_4$ jest równe 1 (dzielimy z resztą 5 przez 4). Zatem zbiór $\mathbb{Z}_4$ jest zbiorem wszystkim możliwych reszt z dzielenia przez 4.

(ii) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$,
$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$;

(iii) $\mathbb{Z}_{25} = \{0, 1, 2, 3, \ldots, 23, 24\}$,
$U(\mathbb{Z}_{25}) = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$;

(iv) $\mathbb{Z}_{31} = \{0, 1, 2, 3, \ldots, 29, 30\}$,
$U(\mathbb{Z}_{31}) = \{0, 1, 2, 3, \ldots, 29, 30\}$;

(v) Ogólnie jeśli p jest liczbą pierwszą, to wówczas

$$\begin{matrix} \mathbb{Z}_p = \{0, 1, \ldots, p-1\} \\ U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^* \end{matrix}.$$

Leonard Euler był szwajcarskim matematykiem i fizykiem. Uważany za czołowego matematyka XVIII wieku i jednego z najwybitniejszych w historii. Jego prace dotyczą prawie wszystkich dziedzin ówczesnej matematyki. W roku 1736 Euler rozwiązał problem znany jako zagadnienie mostów królewieckich – opis tego zagadnienia uznawany jest za pierwszą publikację z teorii grafów. Wprowadził pojęcie funkcji i jako pierwszy zastosował zapis $f(x)$ dla oznaczenia funkcji f argumentu x.

Definicja 3.2. Funkcję $\varphi \colon \mathbb{N} \longrightarrow \mathbb{N}$ taką, że $\varphi(m)$ jest równe liczbie elementów zbioru $U(\mathbb{Z}_m)$ nazywamy *funkcją Eulera*.

Przykład 3.2. Obliczymy $\varphi(10)$. Zgodnie z definicją jest to moc zbioru $U(\mathbb{Z}_{10})$. Zauważmy, że $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$, czyli moc tego zbioru to 4. Zatem $\varphi(10) = 4$.

Uwaga 3.1. Jak obliczyć wartość funkcji φ? Weźmy liczbę naturalną m. Wówczas

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right),$$

dla $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gdzie p_i są parami różmymi liczbami pierwszymi, a $\alpha_1 \in \mathbb{N}$.

Uwaga 3.2. (Własności funkcji Eulera)

(i) Jeśli $n, m \in \mathbb{N}$ oraz $\text{NWD}(n, m) = 1$, to $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

(ii) Jeśli p jest liczbą pierwszą, to $\varphi(p^k) = p^{k-1}(p-1)$.
W szczególności $\varphi(p) = p - 1$.

Przykład 3.3. Obliczymy $\varphi(10)$ (innym sposobem niż w poprzednim przykładzie). Wiemy, że $10 = 2 \cdot 5$. Zatem

$$\varphi(10) = 10\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4.$$

Twierdzenie 3.1. (Eulera) *Jeśli* $m > 1$ *oraz* $\text{NWD}(a, m) = 1$, *to*

$$a^{\varphi(m)} \equiv 1 (\text{mod}\, m).$$

Zastosowanie twierdzenia Eulera

Przykład 3.4. Wyznaczymy ostatnią cyfrę liczby 7^{14}. W tym celu musimy sprawdzić do czego przystaje liczba 7^{14} modulo 10. Ponieważ $\text{NWD}(7, 10) = 1$, to na mocy twierdzenia Eulera wiemy, że $7^{\varphi(10)} \equiv 1 (\text{mod}\,(10)$. Mamy:

$$\varphi(10) = 10\left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4.$$

Czyli $7^4 \equiv 1 (\text{mod}\, 10)$. Zauważmy, że

$$7^{14} = 7^{4\cdot 3+2} = \left(7^4\right)^3 \cdot 7^2 \equiv 7^2 (\text{mod}\, 10).$$

Ostatecznie $7^{14} \equiv 49 (\text{mod}\, 10)$, zatem $7^{14} \equiv 9 (\text{mod}\, 10)$. Zatem ostatnią cyfrą liczby 7^{14} jest 9.

Przykład 3.5. Wyznaczymy trzy ostatnie cyfry liczby 3^{2004}. Musimy sprawdzić do czego przystaje liczba 3^{2004} modulo 1000. Ponieważ $\text{NWD}(3, 1000) = 1$, to na mocy twierdzenia Eulera wiemy, że $3^{\varphi(1000)} \equiv 1 (\text{mod}\, 1000)$. Mamy:

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = 2^2(2-1) \cdot 5^2(5-1) = 400.$$

Zatem $3^{400} \equiv 1 (\text{mod}\, 1000)$. Zauważmy, że

$$3^{2004} = 3^{400\cdot 5+4} = \underbrace{\left(3^{400}\right)^5}_{\equiv 1} \cdot 3^4 \equiv 3^4 (\text{mod}\, 1000)$$

Ponieważ $3^4 = 81$, zatem trzy ostatnie cyfry liczby 3^{2004}, to 081.

Twierdzenie 3.2. (Małe twierdzenie Fermata) *Dla dowolnych liczb* $a \in \mathbb{N}$ *oraz* $p \in \mathbb{P}$ *takich, że* $p \nmid a$ *mamy* $a^{p-1} \equiv 1 (\text{mod}\, p)$.

4. Rozwiązywanie kongruencji

Kongruencje możemy rozwiązywać (tak jak zwykle równania); zajmiemy się kongruencjami liniowymi, tzn.: postaci $aX + b$, gdzie $a, b \in \mathbb{Z}$. Dla uproszczenia zapisu kongruencje liniowe zapisujemy następująco:

$$aX \equiv b (\text{mod}\, m)$$

Gdy rozwiązujemy równanie $aX = b$ w zbiorze liczb rzeczywistych (czyli gdy $a, b \in \mathbb{R}$), to mnożymy obie jego strony przez liczbę odwrotną do a. Podobnie jest w przypadku kongruencji, powstaje jednak pytanie jak wyznaczyć ten element odwrotny.

Zauważmy, że w przypadku liczb rzeczywistych elementem odwrotnym do a jest liczba postaci $\frac{1}{a}$ oraz że zachodzi wówczas warunek $a \cdot \frac{1}{a} = 1$. W przypadku kongruencji musimy uwzględnić moduł kongruencji m oraz fakt, iż działamy na liczbach całkowitych. Rozwiązując więc równanie kongruencyjne $aX \equiv b (\text{mod}\, m)$ musimy znaleźć taką liczbę całkowitą a', aby dla $a, a' \in \mathbb{Z}$ zachodził warunek:

$$a \cdot a' \equiv 1 (\text{mod}\, m).$$

O tym kiedy takie równania mają rozwiązanie mówi nam następujące twierdzenie:

Twierdzenie 4.1. *Niech* $a, b \in \mathbb{Z}$ *i* $n \in \mathbb{N}$. *Kongruencja* $aX \equiv b(\mathrm{mod}\, m)$ *ma rozwiązanie wtedy i tylko wtedy, gdy* $\mathrm{NWD}(a, m)|b$.

Przykład 4.1.

(i) $2X \equiv 3(\mathrm{mod}\, 6)$ nie ma rozwiązania, bo $\mathrm{NWD}(2, 6) = 2$, a $2 \nmid 3$.

(ii) $2X \equiv 3(\mathrm{mod}\, 5)$ ma rozwiązanie, bo $\mathrm{NWD}(2, 5) = 1$, a $1|3$. Szukamy takiego $a \in \{1, 2, 3, 4\}$, że $2 \cdot a \equiv 1(\mathrm{mod}\, 5)$. Mnożąc $2X \equiv 3(\mathrm{mod}\, 5)$ przez 3 dostaniemy, że $X \equiv 4(\mathrm{mod}\, 5)$. Zatem $X = 5t + 4$, czyli rozwiązaniem są liczby, które przy dzieleniu przez 5 dają resztę 4.

4.1. Chińskie twierdzenie o resztach

Chińskie twierdzenie o resztach zostało odkryte i wykorzystane już w średniowiecznych Chinach.

Twierdzenie 4.2. (chińskie o resztach) *Niech* $n \in \mathbb{N}$, $n \geqslant 2$, *a* $m_1, \ldots, m_n$ *będą takimi liczbami naturalnymi, że* $\mathrm{NWD}(m_i, m_j) = 1$, *dla* $i \neq j$. *Niech ponadto liczby* $r_1, \ldots, r_n$ *będą dowolnymi liczbami całkowitymi. Wtedy istnieje rozwiązanie układu kongruencji:*

$$\begin{cases} X \equiv r_1(\mathrm{mod}\, m_1) \\ X \equiv r_2(\mathrm{mod}\, m_2) \\ \vdots \\ X \equiv r_n(\mathrm{mod}\, m_n) \end{cases}$$

Rozwiązanie, to jest jedyne modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_n$, *czyli*

$$X \equiv \text{␣}(\mathrm{mod}\, (m_1 \cdot m_2 \cdot \ldots \cdot m_n).$$

Chińskie twierdzenie o resztach mówi nam, że zawsze możemy znaleźć liczbę r spełniającą warunku postaci: „niech r dzieli się przez q_i z resztą r_i". Oczywiście pod warunkiem, iż nie wykluczają się one wzajemnie.

Przykład 4.2. Rozważmy układ równań

$$\begin{cases} X \equiv -2(\mathrm{mod}\, 5) \\ X \equiv 1(\mathrm{mod}\, 7) \end{cases}$$

Układ ten ma rozwiązanie, bo $\mathrm{NWD}(5, 7) = 1$. Z pierwszej kongruencji układu X jest postaci $X = 7k + 1$. Zatem

$$\begin{aligned} 7k + 1 &\equiv -2(\mathrm{mod}\, 5) \\ 2k &\equiv -3(\mathrm{mod}\, 5) \\ 2k &\equiv 2(\mathrm{mod}\, 5) \\ k &\equiv 1(\mathrm{mod}\, 5) \end{aligned}$$

Stąd k jest postaci $k = 5l + 1$. Wstawiając, to do $X = 7k + 1$ dostajemy, że $X = 35l + 7 + 1 = 35l + 8$. Ostatecznie $X \equiv 8(\mathrm{mod}\, 35)$.

5. Zastosowania

Wykorzystując kongruencje w łatwy sposób możemy odpowiedzieć na pytanie w jakim dniu tygodnia miało miejsce interesujące nas wydarzenie.

Przyporządkujmy dniom tygodnia cyfry od 0 do 6:

0 – niedziela
1 – poniedziałek
2 – wtorek
3 – środa
4 – czwartek
5 – piątek
6 – sobota

Rok zwykły ma 365 i zauważmy, że $365 = 350 + 14 + 1$, więc $365 \equiv 1 (\mathrm{mod}\, 7)$. Z tego wynika, że po upływie roku zwykłego wypada o jeden dzień tygodnia dalszy, w porównaniu z rokiem poprzednim. Ponieważ rok przestępny ma ma 366 dni, to $366 \equiv 2 (\mathrm{mod}\, 7)$, a zatem po upływie roku przestepnego numer dnia tygodnia wzrasta o 2.

Przykład 5.1. Druga wojna światowa rozpoczęła się 1 września 1939 roku. Jaki to dzień tygodnia?

Oznaczmy poszukiwany przez nas dzień tygodnia przez d. Dla wygody sprawdzamy jakim dniem tygodnia był 1 września 2011 – był to czwartek. Od września 1939 do 1 września 2011 upłynęły 72 lata. Sprawdzamy ile lat przestępnym było w tym okresie: $72 : 4 = 18$ – mamy więc 18 lat przestępnych. Zatem szukany przez nas dzień d spełnia kongruencję:

$$\mathrm{d} \equiv 4 - 72 - 18 (\mathrm{mod}\, 7),$$

czyli $\mathrm{d} \equiv -86 (\mathrm{mod}\, 7)$. Zauważmy, że $-86 = -91 + 5$, czyli $\mathrm{d} \equiv 5 (\mathrm{mod}\, 7)$. Oznacza to, że druga wojna światowa rozpoczęła się w piątek.

Przy sięganiu do dat sprzed roku 1582, należy uwzględnić zmianę kalendarza juliańskiego na kalendarz gregoriański. W kalendarzu juliańskim każdy rok o numerze podzielnym przez 4 był przestępny i miał 366 dni, a pozostałe lata były zwykłe i miały po 365 dni. Kalendarz gregoriański wprowadził wyjątki od tej zasady: rok o numerze podzielnym przez 100, ale nie podzielnym przez 400, jest rokiem zwykłym. Dotychczas spośród lat o numerach podzielnych przez 4 latami zwykłymi były następujące trzy: 1700, 1800, 1900. Ponadto pominięto w kalendarzu 10 dat: od 5 do 14 października 1582 roku.

Kalendarz gregoriański jest to zreformowany kalendarz juliański, który koryguje różnicę narosłą od wprowadzenia kalenarza juliańskiego (Kalendarz juliański spóźnia się o 1 dzień na 128 lat, natomiast opóźnienie kalendarza gregoriańskiego wynosi 1 dzień na ok. 3000 lat.) Należy tu również wspomnieć, iż nie wszystkie kraje od razu przeszły z kalendarza juliańskiego na gregoriański. W 1582 roku po ukazaniu się bulli papieża natychmiast przeszły głównie kraje katolickie – w tym Polska. Najdłużej zwlekały kraje prawosławne. Niektóre cerkwie prawosławne – mimo oficjalnego przejścia państw na kalendarz gregoriański – do obliczania świąt ruchomych nadal używa kalendarza juliańskiego.

Przykład 5.2. Sprawdzimy w jakim dniu była bitwa pod Grunwaldem, która rozpoczęła się 15 lipca 1410. Można sprawdzić w kalendarzu, że 15 lipca 2011 był piątek i była wówczas 601 rocznica tego wydarzenia. Gdyby nie wspomniane „poprawki" kalendarza to szukany dzień d rozpoczęcia bitwy spełniałby kongruencję:

$$\mathrm{d} \equiv 5 - 601 - 150 (\mathrm{mod}\, 7)$$

Po uwzględnieniu 10 usuniętych dat oraz dodatkowych lat, które nie były przestępne (1700, 1800, 1900) mamy:

$$\mathrm{d} \equiv 5 - 601 - 150 + 10 + 3 (\mathrm{mod}\, 7)$$

Zatem $\mathrm{d} \equiv -733 (\mathrm{mod}\, 7)$. Ponieważ $-733 = -700 - 35 + 2$, to $\mathrm{d} \equiv 2 (\mathrm{mod}\, 7)$, więc bitwa pod Grunwaldem rozpoczęła się we wtorek.

Oczywiście oprócz sprawdzania w jakim dniu tygodnia miało miejsce jakieś wydarzenie, możemy również sprawdzić w jakim dniu tygodnia coś dopiero będzie.

Przykład 5.3. Sprawdzimy w jakim dniu rozpocznie się nowe stulecie, czyli jakim dniem jest 1 stycznia 2100. Dla wygody spradzamy, że 1 stycznia 2011 roku była sobota. Od tej daty do 2100 roku będzie jeszcze 89 lat, w tym 22 lata przestępne. Zatem szukany przez nas dzień d spełnia kongruencję:

$$d \equiv 6 + 89 + 22 (\mathrm{mod}\, 7),$$

czyli $d \equiv 117 (\mathrm{mod}\, 7)$. Ponieważ $117 = 112 + 5$, więc $d \equiv 5 (\mathrm{mod}\, 7)$ co oznacza, że 1 stycznia 2100 roku będzie piątkiem.

6. Zadania

Zadanie 6.1. Wyprowadź cechy podzielności przez 7,13,27,37,101.
Wskazówka: skorzystaj z kongruencji $100 \equiv 1 (\mathrm{mod}\, 11)$, $100 \equiv -1 (\mathrm{mod}\, 101)$, $1000 \equiv -1 (\mathrm{mod}\, 7, 13, 11)$, $100 \equiv 1 (\mathrm{mod}\, 27, 37)$

Zadanie 6.2. Wyznacz dwie ostatnie cyfry następujących liczb:

(a) 289^{289}

(b) 2^{241}

(c) 7^{9^9}

(d) $14^{14^{14}}$

Zadanie 6.3. Wykaż, że liczba $53^{53} - 33^{33}$ jest podzielna przez 10.

Zadanie 6.4. Rozwiąż kongruencje:

(a) $3X \equiv 1 (\mathrm{mod}\, 5)$;

(b) $3X \equiv 8 (\mathrm{mod}\, 13)$;

(c) $25X \equiv 15 (\mathrm{mod}\, 7)$;

(d) $4X \equiv 7 (\mathrm{mod}\, 6)$;

Zadanie 6.5. Rozwiąż układy kongruencji:

(a)
$$\begin{cases} X \equiv 4 (\mathrm{mod}\, 5); \\ X \equiv 1 (\mathrm{mod}\, (12) \\ X \equiv 7 (\mathrm{mod}\, 14) \end{cases}$$

(b)
$$\begin{cases} X \equiv 1 (\mathrm{mod}\, 25); \\ X \equiv 2 (\mathrm{mod}\, (4) \\ X \equiv 3 (\mathrm{mod}\, 9) \end{cases}$$

Zadanie 6.6. W sadzie zebrano jabłka, których nie było więcej niż 1000. Gdyby podzielić jabłka równo do 7 koszy, to zostanie 1 jabłko. Gdyby podzielić jabłka równo do 13 koszy, to zostanie 6 jabłek. Można jednak podzielic jabłka równo na 11 części. Ile zebrano jabłek?

Zadanie 6.7. Dopisać z prawej strony liczby 523 takie trzy cyfry, aby otrzymana liczba sześciocyfrowa była podzielna przez 7, 8 i 9.

Zadanie 6.8. Znajdź cyfry x, y, z wiedząc, że liczba $xyz138$ dzieli się przez 7, liczba $138xyz$ przy dzieleniu przez 13 daje resztę 6, a liczba $x1y3z8$ przy dzieleniu przez 11 daje resztę 5.

Zadanie 6.9. (Olimpiada Matematyczna) Znajdź cyfry x, y, z wiedząc, że liczba $13xy45z$ dzieli się przez 792.

Zadanie 6.10. (Olimpiada Matematyczna) Wykaż, że jeżeli $m \equiv n (\mathrm{mod}\, 4)$, to liczba $53^m - 33^n$ jest podzielna przez 10.

Zadanie 6.11. (Olimpiada Matematyczna) Znajdź wszystkie liczby naturalne n, aby liczba $1! + 2! + \cdots + n!$ była

(a) kwadratem pewnej liczby naturalnej;

(b) sześcianem pewnej lizby naturalnej.

Literatura

[1] M.Bryński, *Jaki dzień tygodnia*, „Delta”, 2010/03, strony 12-13

[2] N.Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa, 1995

[3] W.Sierpiński, *Wstęp do teorii liczb*, Biblioteczka Matematyczna 25, PZWS, Warszawa 1965.