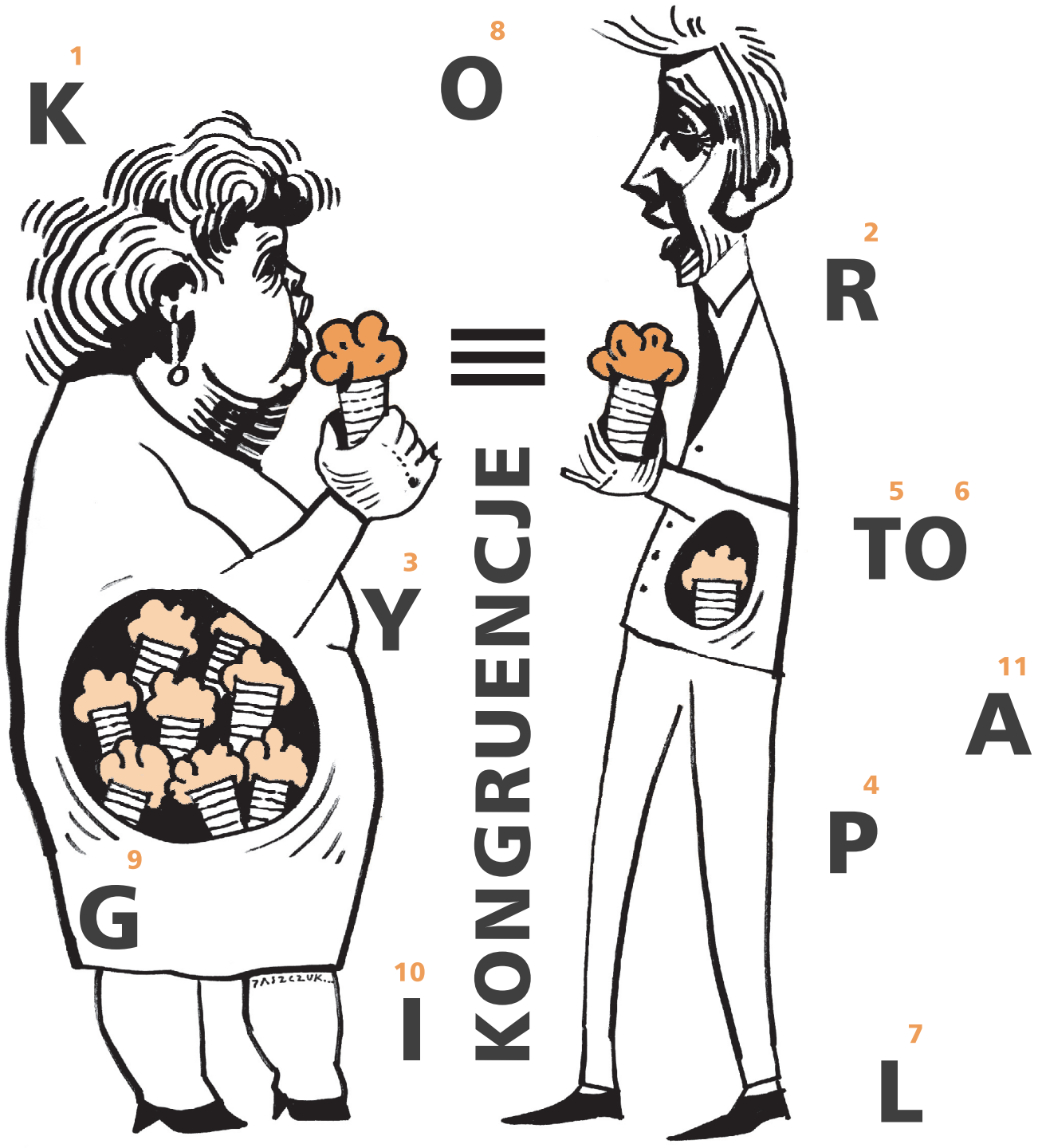
ISSN 1897-7464

Świat Matematyki
Pismo dla młodzieży szkolnej

DODATEK SPECJALNY 1



Drodzy Czytelnicy

Pierwszy numer dodatku specjalnego „Świata Matematyki” nie przez przypadek poświęcony jest kongruencjom. Jest to bowiem bardzo ważne pojęcie, przydatne w rozwiązywaniu wielu zagadnień matematycznych. Posługując się kongruencjami, można bez większego trudu poradzić sobie nawet z bardzo trudnymi, bo pojawiającymi się na olimpiadach matematycznych zadaniami. Niestety, umiejętność posługiwania się kongruencjami nie jest objęta programem nauczania matematyki w szkole i w związku z tym uczniom pozostaje opanowywanie tej umiejętności na własną rękę.

I właśnie temu ma służyć niniejszy dodatek specjalny „Świata Matematyki”. Został on zredagowany w taki sposób, że mogą go czytać nawet uczniowie z pierwszej klasy gimnazjum i nie będą mieli żadnych problemów ze zrozumieniem jego treści. Trzeba go tylko czytać systematycznie, a wówczas wrota, pozwalające rozwiązywać nawet skomplikowane zadania olimpijskie, zostaną otwarte na oścież. W następnych numerach „Świata Matematyki”, począwszy od czwartego, zaczną pojawiać się właśnie tego rodzaju zadania i każdy z naszych Czytelników będzie mógł sam się przekonać, że rzeczywiście bez kłopotów radzi sobie z rozwiązywaniem takich zadań.

Eugeniusz Sikorski
redaktor naczelny

Świat Matematyki
Pismo dla młodzieży szkolnej
DODATEK SPECJALNY

SPIS TREŚCI

Dodatek Specjalny „Świata Matematyki”
– pisma dla młodzieży szkolnej
pragnącego uczyć logicznego myślenia
przez zastosowanie technik matematycznych

Redaguje zespół:
Eugeniusz Sikorski – redaktor naczelny,
Jacek Orzechowski, Hubert Siuba, Agnieszka Malinowska, Paweł Jaszczuk – grafika, ilustracje,
Dariusz Tokarz – korekta

Wydawca:
Mediacom sp. z o.o., ul. Jeziorowa 27, Wrocław,
biuro@swiatmatematyki.pl
Druk:
Ultima-druk sp. z o.o., ul. Fabryczna 19, Wrocław

Kongruencje

dzięki znajomości których uczniowie rozwiązują nietypowe, bardzo rzadkie zadania, czym wprawiają w zdumienie swoich nauczycieli.

Zanim wyjaśnię Wam, co to takiego kongruencje, zajmiemy się dzieleniem z resztą, co jest bardzo ściśle związane z pojęciem kongruencji. Wiem, wiem, że każdy z Was umie dzielić z resztą, gdyż przerabia się to w trzeciej klasie szkoły podstawowej. I dlatego właśnie, że było to przerabiane bardzo dawno temu, w rzeczywistości okazuje się, iż wielu uczniów starszych klas ma kłopoty z dzieleniem sposobem pisemnym. Nauczyciele w starszych klasach na lekcjach tego nie przypominają, ponieważ nie mają na to czasu, gdyż muszą realizować obowiązujący program, a godzin na matematykę przeznaczonych jest w szkole niewiele. Z kolei uczniowie zapominali tego nawet kiedyś, gdy nie było kalkulatorów i komputerów, a co dopiero mówić obecnie, w dobie wszędobylskich kalkulatorów czy komputerów wraz z licznymi programami obliczeniowymi. Dlatego koniecznie trzeba to przypomnieć.

Podzielimy z resztą liczbę 34680 przez 57.
Dzielimy:

$$\overline{34680} : 57$$

W tym celu bierzemy najpierw pierwszą cyfrę dzielnej, czyli liczby 34680, i zapytujemy się siebie: ile razy dzielnik, a więc liczba 57, mieści się w 3 – w liczbie utworzonej przez pierwszą cyfrę dzielnej?

$$\overline{34680} : 57$$

(tę pierwszą cyfrę dzielnej zaznaczyliśmy na kolorowo). Oczywiście ani razu. Zatem nad 3, u góry, nie piszemy żadnej cyfry.
Bierzemy następnie drugą cyfrę dzielnej, czyli 4, i dołączamy ją do pierwszej cyfry. W ten sposób utworzona została liczba 34 (zaznaczona jest na kolorowo). Zapytujemy się siebie: ile razy dzielnik, czyli liczba 57, mieści się w 34 – w liczbie utworzonej przez dwie pierwsze cyfry dzielnej?

$$\overline{34680} : 57$$

Oczywiście również ani razu. Zatem u góry nad 4 także nie piszemy żadnej cyfry.
W kolejnym kroku bierzemy więc następną, trzecią cyfrę dzielnej, czyli 6, i dołączamy ją do dwóch pierwszych cyfr. W taki sposób utworzona zostaje liczba 346 (zaznaczona jest na kolorowo). Zapytujemy się siebie: ile razy liczba 57 mieści się w 346 – w liczbie utworzonej przez trzy pierwsze cyfry dzielnej?

$$\overline{34680} : 57$$

Na pewno mieści się, ale ile razy – to niestety trzeba odgadnąć (osoby mające w tym zakresie sporą wprawę potrafią szybko prawidłowo określić, ile razy się mieści). My jednak takiej wprawy nie mamy, więc odgadujemy. Przypuszczamy mianowicie, że 57 w 346 mieści się 5 razy.

Zatem u góry nad 6 piszemy cyfrę 5.

$$\begin{array}{r} 5 \\ \overline{34680} : 57 \end{array}$$

Następnie mnożymy 5 przez 57, otrzymując w rezultacie liczbę 285. Podpisujemy ją pod dzielną w taki sposób, aby jej ostatnia cyfra, czyli 5, znalazła się w jednym pionie z widoczną u samej góry 5.

$$\begin{array}{r} 5 \\ \overline{34680} : 57 \\ \underline{285} \end{array}$$

Teraz odejmujemy: od liczby 346 liczbę 285, i wynik zapisujemy niżej.

$$\begin{array}{r} 5 \\ \overline{34680} : 57 \\ -\underline{285} \\ 61 \end{array}$$

Jako różnicę otrzymaliśmy liczbę 61. Różnica musi być mniejsza od dzielnika, czyli w tym wypadku od liczby 57. Ponieważ liczba 61 jest większa od 57, to z tego wynika, że nasza próba odgadnięcia była błędna. Nie oznacza to jednak wcale, że nasza praca była daremna. Otrzymaliśmy bowiem pewną bardzo cenną informację: mianowicie z faktu, że różnica okazała się być większa od dzielnika, wynika, iż cyfra 5, znajdująca się u samej góry nad 6, jest za mała.

Zatem w miejscu 5, będącej u samej góry nad 6, musi znajdować się cyfra większa od 5, czyli jedna spośród czterech cyfr: 6, 7, 8 lub 9. Jak widać, błędne odgadnięcie pozwala zawęzić zbiór cyfr, które „wezmą udział" w kolejnej próbie odgadnięcia, ile razy liczba 57 mieści się w 346. Teraz przypuszczamy, że 57 w 346 mieści się aż 7 razy.

A więc u samej góry nad 6 piszemy cyfrę 7.

$$\begin{array}{r} 7 \\ \hline 34680 : 57 \end{array}$$

Następnie mnożymy 7 przez 57, otrzymując w rezultacie liczbę 399. Podpisujemy ją pod dzielną w taki sposób, aby jej ostatnia cyfra, czyli 9, znalazła się w jednym pionie z widoczną u samej góry 7.

$$\begin{array}{r} 7 \\ \hline 34680 : 57 \\ -\underline{399} \end{array}$$

Ponieważ różnica nie może być ujemna, zatem liczba odejmowana nie może być większa od liczby, od której się ją odejmuje, a w naszym przypadku tak jest – liczba 399 jest większa od 346. Z tego wniosek, że również i teraz nasza próba odgadnięcia jest błędna. Dostarczyła nam jednak bardzo istotnej informacji: mianowicie z faktu, że liczba, która ma być odjęta, jest większa od liczby, od której ma zostać odjęta, wynika, iż cyfra 7, znajdująca się u samej góry nad 6, jest za duża.

Zatem w miejscu 7, znajdującej się u samej góry nad 6, musi być cyfra mniejsza od 7, czyli jedna spośród siedmiu cyfr: {0, 1, 2, 3, 4, 5, 6}. Wcześniej jednak ustaliliśmy, że u samej góry nad 6 musi znajdować się cyfra większa od 5, czyli jedna spośród czterech cyfr: {6, 7, 8, 9}. A więc w interesującym nas miejscu musi być cyfra należąca jednocześnie do obu zbiorów, czyli do zbioru cyfr większych od 5 i zarazem do zbioru cyfr mniejszych od 7. Jest tylko jedna taka cyfra: cyfra 6. I to właśnie ona powinna znaleźć się w rozpatrywanym przez nas miejscu, czyli u samej góry nad 6. Wstawiamy ją tam.

$$\begin{array}{r} 6 \\ \hline 34680 : 57 \end{array}$$

Następnie mnożymy 6 przez 57, otrzymując w rezultacie liczbę 342. Podpisujemy ją pod dzielną w wiadomy sposób, czyli tak, aby jej ostatnia cyfra – cyfra 2 – znalazła się w jednym pionie z widoczną u samej góry 6.

$$\begin{array}{r} 6 \\ \hline 34680 : 57 \\ -\underline{342} \end{array}$$

Teraz odejmujemy: od liczby 346 liczbę 342, i wynik zapisujemy niżej

$$\begin{array}{r} 6 \\ \hline 34680 : 57 \\ -\underline{342} \\ 4 \end{array}$$

Jako różnicę otrzymaliśmy liczbę 4. Ponieważ różnica jest mniejsza od dzielnika, czyli od liczby 57, więc widoczna u samej góry 6 jest cyfrą prawidłowo określającą, ile razy liczba 57 mieści się w 346.

Następnie tuż obok 4, będącej przed chwilą obliczoną różnicą, dopisujemy 8, którą uprzednio spuszczamy z dzielnej (czwarta cyfra dzielnej, przedostatnia).

$$\begin{array}{r} 6 \\ \hline 34680 : 57 \\ -\underline{342\downarrow} \\ 48 \end{array}$$

W ten sposób otrzymaliśmy u dołu liczbę 48. Zapytujemy się siebie: ile razy w 48 mieści się liczba 57? Oczywiście ani razu.

W poprzednich przypadkach, gdy 57 nie mieściła się w danej liczbie ani razu, w odpowiednim miejscu u samej góry nie pisaliśmy żadnej cyfry, lecz pozostawialiśmy to miejsce puste. To prawda, nie pisaliśmy zera, ale tylko dlatego, że na początku liczb nie pisze się zer. Nikt rozsądny nie napisze przecież liczby na przykład 21 w taki sposób: 021. Jednak w środku i na końcu liczb pisze się zera. Dlatego właśnie u samej góry, nad cyfrą 8, wstawiamy zero.

$$\begin{array}{r} 60 \\ \hline 34680 : 57 \\ -\underline{342} \\ 48 \end{array}$$

Gdyby w miejscu przed chwilą napisanego u samej góry zera stała jakakolwiek inna cyfra, to pomnożylibyśmy ją przez 57 i otrzymywany wynik podpisalibyśmy pod 48. W przypadku, gdy u samej góry jest 0 (tak jak my teraz mamy), postępujemy inaczej: mianowicie tuż obok liczby 48, z prawej strony, dopisujemy 0, które uprzednio spuszczamy z dzielnej (ostatnia cyfra dzielnej).

$$\begin{array}{r} 60 \\ \hline 34680 : 57 \\ -\underline{342\ \downarrow} \\ 480 \end{array}$$

W ten sposób otrzymaliśmy u dołu liczbę 480. Zapytujemy się siebie: ile razy w 480 mieści się liczba 57? I znowu trzeba, tak jak było to w przypadku 6, rozpocząć proces odgadywania. Teraz jednak mamy już pewne doświadczenie i w związku z tym od razu odgadujemy właściwą cyfrę. Jest nią 8. Wstawiamy ją u samej góry, w pionie, nad spuszczoną ostatnio cyfrą.

$$\begin{array}{r} 608 \\ \hline 34680 : 57 \\ -\underline{342} \\ 480 \end{array}$$

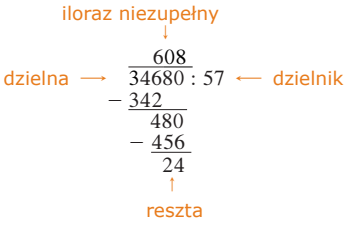
Następnie mnożymy 8 przez 57, otrzymując w rezultacie liczbę 456. Podpisujemy ją pod 480 w odpowiedni sposób – tak jak widać to niżej – i odejmujemy: od liczby 480 liczbę 456.

$$\begin{array}{r} 608 \\ 34680 : 57 \\ -\,342 \\ \hline 480 \\ -\,456 \\ \hline 24 \end{array}$$

Jako różnicę otrzymaliśmy liczbę 24. Ponieważ jest ona mniejsza od liczby 57, zatem widoczna u samej góry 8 jest cyfrą prawidłowo określającą, ile razy liczba 57 mieści się w 480.

Ponieważ z góry z dzielnej nie możemy już spuścić żadnej cyfry, gdyż takowej już nie ma, więc dzielenie z resztą sposobem pisemnym liczby 34680 przez 57 zostało zakończone. Widoczna u dołu liczba 24 jest resztą z tego dzielenia.

Teraz opiszemy, jak nazywają się poszczególne liczby występujące w tym dzieleniu.



Wynik dzielenia z resztą zapisujemy w następujący sposób:

$$34680 : 57 = 608 \text{ reszta } 24.$$

Zapewne każdy z Was wie, że poprawność wykonanego dzielenia sposobem pisemnym sprawdza się, mnożąc iloraz (wynik dzielenia) przez dzielnik. Jeżeli dzielenie zostało wykonane prawidłowo, to powinniśmy otrzymać dzielną.

A jak sprawdza się poprawność wykonanego dzielenia z resztą sposobem pisemnym? Mnożąc iloraz niezupełny przez dzielnik i dodając do otrzymanego iloczynu resztę. Na przykład wykonane przez nas dzielenie z resztą należałoby sprawdzić następująco:

$$608 \cdot 57 + 24 = 34680.$$

Umiemy już dzielić z resztą sposobem pisemnym, możemy zatem zająć się kongruencjami.

Liczby całkowite a i b przystają modulo m (gdzie m jest ustaloną liczbą naturalną), jeżeli obie dzielone z resztą przez m dają tę samą resztę. O liczbach takich mówimy też, że są kongruentne modulo m.

Fakt, że liczby a i b są kongruentne modulo m, zapisujemy krótko:

$$a \equiv b \pmod{m}.$$

Przykład

Liczby 95 i 147 przystają modulo 13, gdyż:

$$\begin{array}{r} 7 \\ 95 : 13 \\ -91 \\ \hline 4 \end{array} \qquad\qquad \begin{array}{r} 11 \\ 147 : 13 \\ -13 \\ \hline 17 \\ -13 \\ \hline 4 \end{array}$$

Jak widać z powyższego, obie dzielone z resztą przez 13 dają tę samą resztę – resztę 4.

Piszemy więc

$$95 \equiv 147 \pmod{13}.$$

– – – – – – – – – – –

Gdyby nauczyciel w szkole dał polecenie: znajdźcie resztę z dzielenia liczby $21 \cdot 15 + 53$ przez 15, to zdecydowana większość uczniów najpierw znalazłaby przedstawienie tej liczby w postaci zapisu dziesiętnego:

$$21 \cdot 15 + 53 = 368 \quad \longleftarrow \text{zapis dziesiętny,}$$

a dopiero później wykonałaby dzielenie z resztą sposobem pisemnym liczby 368 przez 15:

$$\begin{array}{r} \underline{24} \\ 368 : 15 \\ \underline{-30} \\ 68 \\ \underline{-60} \\ 8 \end{array}$$

Reszta, którą polecił znaleźć nauczyciel – jak widać – wynosi 8.

Tylko nieliczna garstka uczniów – tych najbystrzejszych – postąpiłaby inaczej. Mianowicie zamiast najpierw obliczać liczbę 368, a potem jeszcze dzielić ją przez 15, to od razu podzieliłaby z resztą przez 15 liczbę 53:

$$\begin{array}{r} \underline{3} \\ 53 : 15 \\ \underline{-45} \\ 8 \end{array}$$

otrzymując, jak widać, prawidłową resztę.

Nie jest to żaden przypadek, lecz prawidłowość. Mając bowiem zapisaną liczbę w postaci sumy, gdzie jeden ze składników jest iloczynem, w którym jako czynnik występuje właśnie ta liczba, przez którą mamy dzielić z resztą, to wówczas dla znalezienia tej reszty wystarczy jedynie podzielić z resztą ten drugi składnik sumy. Nie potrzeba znajdować całej liczby.

Wyjaśnimy teraz, dlaczego tak jest. $53 = 3 \cdot 15 + 8$, więc do wyrażenia $21 \cdot 15 + 53$ w miejsce liczby 53 wstawiamy wyrażenie $3 \cdot 15 + 8$, otrzymując w ten sposób

$$21 \cdot 15 + 3 \cdot 15 + 8.$$

Liczbę 15, będącą wspólnym czynnikiem w obu iloczynach: $21 \cdot 15$ i $3 \cdot 15$, wyciągamy poza nawias, korzystając w tym przypadku z własności rozdzielności mnożenia względem dodawania:

$$\mathbf{(a + b) \cdot c = a \cdot c + b \cdot c}$$

Jak przechodzimy od strony lewej do prawej widocznego w ramce zapisu, to wówczas nazywa się to otwieraniem nawiasu, gdy natomiast przechodzimy od strony prawej do lewej, to wtedy określa się to jako wyciąganie wspólnego czynnika poza nawias.

W rozpatrywanym przez nas przypadku $21 \cdot 15 + 3 \cdot 15 + 8$ liczbę 15, występującą w obu iloczynach, wyciągamy poza nawias, otrzymując wyrażenie:

$$(21 + 3) \cdot 15 + 8,$$

które po dodaniu liczb występujących w nawiasie przyjmuje postać:

$$24 \cdot 15 + 8.$$

Zauważmy, że tę samą widoczną wyżej postać otrzymalibyśmy również podczas sprawdzania poprawności wykonania dzielenia z resztą sposobem pisemnym liczby 368 przez 15.

$$368 : 15 = 24 \text{ reszta } 8, \quad 53 : 15 = 3 \text{ reszta } 8,$$

Widać z tego, że przedstawienie liczby, będącej wartością wyrażenia $21 \cdot 15 + 53$, najpierw w postaci zapisu dziesiętnego, a dopiero potem podzielenie jej z resztą przez 15, nie spowodowało zmiany reszty w stosunku do podzielenia z resztą 53 przez 15, a jedynie wpłynęło na zmianę ilorazu niezupełnego.

Ten ostatni wniosek będzie miał doniosłe znaczenie podczas wykazywania pewnych własności kongruencji.

– – – – – – – – – – – – –

Rozpatrzmy dwie kongruencje:

$$422 \equiv 219 \pmod{29}$$
$$502 \equiv 328 \pmod{29}$$

o wspólnym module. Obie są prawdziwe, co łatwo sprawdzić. W przypadku pierwszej kongruencji, dzieląc z resztą obie liczby: 422 oraz 219 przez 29, otrzymamy w obu przypadkach, jak widać niżej,

$$\begin{array}{r} \underline{14} \\ 422 : 29 \\ \underline{-29} \\ 132 \\ \underline{-116} \\ 16 \end{array} \qquad \begin{array}{r} \underline{7} \\ 219 : 29 \\ \underline{-203} \\ 16 \end{array}$$

tę samą resztę – resztę 16, co świadczy o prawdziwości pierwszej kongruencji. Natomiast w przypadku drugiej kongruencji, dzieląc z resztą liczby 502 i 328 przez 29, także otrzymamy tę samą resztę, teraz z kolei równą 9:

$$\begin{array}{r} 17 \\ 502 : 29 \\ -29 \\ \hline 212 \\ -203 \\ \hline 9 \end{array} \qquad \begin{array}{r} 11 \\ 328 : 29 \\ -29 \\ \hline 38 \\ -29 \\ \hline 9 \end{array}$$

co świadczy o prawdziwości drugiej kongruencji.

Dodajmy obie kongruencje stronami, otrzymując w ten sposób kongruencję

$$422 + 502 \equiv 219 + 328 \pmod{29},$$

która po uproszczeniu przyjmuje postać:

$$924 \equiv 547 \pmod{29}.$$

Czy jest to prawdziwa kongruencja, czy też nie? Przekonajmy się.
Obie strony kongruencji podzielmy z resztą przez 29:

$$\begin{array}{r} 31 \\ 924 : 29 \\ -87 \\ \hline 54 \\ -29 \\ \hline 25 \end{array} \qquad \begin{array}{r} 18 \\ 547 : 29 \\ -29 \\ \hline 257 \\ -232 \\ \hline 25 \end{array}$$

Jak widać z powyższego, w obu przypadkach dostaliśmy tę samą resztę równą 25. Zatem kongruencja $924 \equiv 547 \pmod{29}$ jest prawdziwa.

Czy jest to przypadek, czy prawidłowość, która ma zawsze miejsce? Przekonajmy się.

$$422 : 29 = 14 \text{ reszta } 16 \quad \text{i} \quad 219 : 29 = 7 \text{ reszta } 16,$$

co możemy zapisać w następującej postaci:

$$422 = 14 \cdot 29 + 16 \quad \text{oraz} \quad 219 = 7 \cdot 29 + 16,$$

Dalej:

$$502 : 29 = 17 \text{ reszta } 9 \quad \text{i} \quad 328 : 29 = 11 \text{ reszta } 9,$$

co z kolei zapisujemy w postaciach:

$$502 = 17 \cdot 29 + 9 \quad \text{oraz} \quad 328 = 11 \cdot 29 + 9.$$

Dodajemy:

$$\begin{aligned} &422 + 502 = \\ &= \underbrace{14 \cdot 29 + 16}_{422} + \underbrace{17 \cdot 29 + 9}_{502} = \\ &= 14 \cdot 29 + 17 \cdot 29 + 16 + 9 = \\ &= (14 + 17) \cdot 29 + 16 + 9 = \\ &= 31 \cdot 29 + 16 + 9 \end{aligned}$$

$$\begin{aligned} &219 + 328 = \\ &= \underbrace{7 \cdot 29 + 16}_{219} + \underbrace{11 \cdot 29 + 9}_{328} = \\ &= 7 \cdot 29 + 11 \cdot 29 + 16 + 9 = \\ &= (7 + 11) \cdot 29 + 16 + 9 = \\ &= 18 \cdot 29 + 16 + 9 \end{aligned}$$

Z postaci wyrażenia $31 \cdot 29 + 16 + 9$ widać natychmiast, że reszta z dzielenia liczby będącej wartością tego wyrażenia przez 29 jest taka sama, jak reszta z dzielenia sumy $16 + 9$ przez 29. Wynika to bezpośrednio z poczynionych wcześniej ustaleń. Po prostu na resztę z dzielenia przez 29 nie ma żadnego wpływu składnik $31 \cdot 29$, który występuje w rozpatrywanym przez nas wyrażeniu i który jest wielokrotnością liczby 29. Podobnie sprawa wygląda w przypadku wrażenia $18 \cdot 29 + 16 + 9$. Tutaj także reszta z dzielenia przez 29 uzależniona jest tylko i wyłącznie od sumy $16 + 9$. A więc otrzymany wcześniej rezultat nie był dziełem przypadku.

Kongruencje o wspólnym module można dodawać stronami

Jeżeli $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, to $a + c \equiv b + d \pmod{m}$

Teraz rozpatrzmy dwie inne kongruencje o wspólnym module:

$$381 \equiv 17 \pmod{7}$$
$$305 \equiv 25 \pmod{7}$$

Obie są prawdziwe, co łatwo może każdy z Was sprawdzić sam (tak samo jak to było robione poprzednio)

Pomnóżmy obie kongruencje stronami, otrzymując w ten sposób kongruencję

$$381 \cdot 305 \equiv 17 \cdot 25 \pmod 7,$$

która po uproszczeniu przyjmuje postać:

$$116\,205 \equiv 425 \pmod 7.$$

Otrzymana kongruencja jest również prawdziwa, co łatwo sprawdzić, dzieląc z resztą liczby występujące po obu stronach kongruencji przez moduł, czyli przez 7. W obu przypadkach otrzymamy tę samą resztę równą 5, co dowodzi prawdziwości kongruencji.

Ale czy to, że po pomnożeniu obu stron kongruencji otrzymaliśmy kongruencję prawdziwą, było tylko dziełem przypadku, czy też jest to prawidłowość, która zawsze zachodzi? Popatrzmy:

$$381 = 54 \cdot 7 + 3, \qquad 17 = 2 \cdot 7 + 3,$$
$$305 = 43 \cdot 7 + 4, \qquad 25 = 3 \cdot 7 + 4.$$

Teraz pomnóżmy liczby będące lewymi stronami kongruencji, czyli pomnóżmy 381 przez 305. Otrzymujemy:

$$381 \cdot 305 = (54 \cdot 7 + 3)(43 \cdot 7 + 4) = 54 \cdot 7 \cdot 43 \cdot 7 + 54 \cdot 7 \cdot 4 + 3 \cdot 43 \cdot 7 + 3 \cdot 4 =$$

Po wyciągnięciu z zaznaczonej części wspólnego czynnika poza nawias – tym wspólnym czynnikiem jest oczywiście 7 – otrzymujemy:

$$= (54 \cdot 43 \cdot 7 + 54 \cdot 4 + 3 \cdot 43) \cdot 7 + 3 \cdot 4.$$

Na wielkość reszty, jaka będzie rezultatem podzielenia przez 7 liczby będącej wartością powyższego wyrażenia, nie ma żadnego wpływu ta część wyrażenia, która jest wielokrotnością 7 (ta część wyrażenia została zaznaczona na kolorowo). Aby zatem znaleźć ową resztę, nie potrzeba wcale obliczać wartości wyrażenia ujętego w nawias – wystarczy jedynie obliczyć resztę z dzielenia liczby będącej wartością iloczynu $3 \cdot 4$, czyli resztę z dzielenia 12 przez 7. A to natychmiast oblicza się w pamięci:

$$12 : 7 = 1 \text{ reszta } 5.$$

A teraz zobaczymy, co będzie, jak pomnożymy liczby będące prawymi stronami kongruencji, czyli jak pomnożymy 17 przez 25. Obliczamy:

$$17 \cdot 25 = (2 \cdot 7 + 3)(3 \cdot 7 + 4) = 2 \cdot 7 \cdot 3 \cdot 7 + 2 \cdot 7 \cdot 4 + 3 \cdot 3 \cdot 7 + 3 \cdot 4 =$$

Po wyciągnięciu z zaznaczonej części wspólnego czynnika wynoszącego 7 poza nawias dostajemy:

$$= (2 \cdot 3 \cdot 7 + 2 \cdot 4 + 3 \cdot 3) \cdot 7 + 3 \cdot 4.$$

Z tych samych powodów co poprzednio, na resztę z dzielenia przez 7 liczby będącej wartością ostatniego wyrażenia nie ma żadnego wpływu iloczyn $(2 \cdot 3 \cdot 7 + 2 \cdot 4 + 3 \cdot 3) \cdot 7$. Reszta ta zależy tylko i wyłącznie od pozostałej części wyrażenia, czyli od iloczynu $3 \cdot 4$. Jest więc taka sama, jak w przypadku mnożenia liczb będących lewymi stronami kongruencji, czyli również wynosi 5.

Z przeprowadzonych wyżej rozważań widać od razu, dlaczego

kongruencje o wspólnym module można mnożyć stronami

Jeżeli $a \equiv b \pmod m$ i $c \equiv d \pmod m$, to $a \cdot c \equiv b \cdot d \pmod m$.

Ponieważ kongruencja

$$c \equiv c \pmod m$$

jest zawsze prawdziwa dla dowolnego modułu, zatem

do obu stron kongruencji można dodawać tę samą liczbę

Jeżeli $a \equiv b \pmod m$, to $a + c \equiv b + c \pmod m$,

oraz

obie strony kongruencji można mnożyć przez tę samą liczbę

Jeżeli $a \equiv b \pmod m$, to $a \cdot c \equiv b \cdot c \pmod m$.

Wśród kongruencji o tym samym module zachodzi następujący związek:

Jeżeli $a \equiv b \pmod m$ oraz $b \equiv c \pmod m$, to $a \equiv c \pmod m$.

Wyjaśnienie tego faktu jest natychmiastowe. Najlepiej to zrobić na konkretnym przykładzie.

Mamy dwie kongruencje

$$47 \equiv 11 \pmod 9 \quad \text{oraz} \quad 11 \equiv 101 \pmod 9,$$

obie prawdziwe, co każdy może sam łatwo sprawdzić. Teraz popatrzmy na dwie niżej widoczne ramki. Ta z lewej strony dotyczy kongruencji $47 \equiv 11 \pmod 9$, a ta z prawej strony kongruencji $11 \equiv 101 \pmod 9$.

$47 : 9 = 5$ reszta $\square$
$11 : 9 = 1$ reszta 2

$11 : 9 = 1$ reszta 2
$101 : 9 = 11$ reszta $\square$

Zachodzenie widocznych w ramkach, ustawionych pionowo, kolorowych znaków równości jest oczywiste. Wynika to z samej definicji kongruencji. W takim razie możemy napisać następującą równość:

$$\square = 2 = \square .$$

Jaka cyfra powinna znaleźć się w obu krateczkach? Oczywiście 2. Zatem na miejsce:

$$47 : 9 = 5 \text{ reszta } 2 \quad \text{oraz} \quad 101 : 9 = 11 \text{ reszta } 2,$$

co z kolei oznacza zachodzenie kongruencji

$$47 \equiv 101 \pmod 9.$$

Z zachodzenia obu kongruencji $47 \equiv 11 \pmod 9$ oraz $11 \equiv 101 \pmod 9$ wykazaliśmy prawdziwość kongruencji $47 \equiv 101 \pmod 9$, i to nie na drodze bezpośredniego sprawdzenia, lecz wyjaśniając cały mechanizm za to odpowiedzialny. Tym samym dowiedliśmy, że

Jeżeli $a \equiv b \pmod m$ oraz $b \equiv c \pmod m$, to $a \equiv c \pmod m$

Zadania, których rozwiązanie wymaga posłużenia się kongruencjami, często występują na różnych konkursach i olimpiadach matematycznych. Ale nie tylko. Kongruencje mają także zastosowanie przy rozwiązywaniu bardzo skomplikowanych równań w liczbach całkowitych, a także – o czym będziecie mogli przekonać się w trakcie lektury ostatniego artykułu z niniejszego numeru – w kryptologii, czyli dyscyplinie zajmującej się szyfrowaniem i deszyfrowaniem.

Iloczyn $a \cdot a \cdot \ldots \cdot a$, w którym występuje n czynników, a każdy z nich równy jest liczbie a, nazywamy potęgą. Iloczyn taki zapisujemy w skrócie:

$$\underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{n razy}} = a^n$$

podstawa potęgi → a^n ← wykładnik potęgi

Przykłady

$$2^6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$$

$$\left(\frac{3}{4}\right)^3 = \frac{3}{4} : \frac{3}{4} : \frac{3}{4} = \frac{27}{64}$$

Teraz na konkretnym przykładzie wykażę pewien wzór dotyczący działań na potęgach, który będzie bardzo przydatny przy rozwiązywaniu zadań, jakie za moment się pojawią.

$$2^5 \cdot 2^3 = (2 \cdot 2 \cdot 2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8$$

Przechodząc od wyrażenia $(2 \cdot 2 \cdot 2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2)$ do wyrażenia $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$, opuściłem tylko nawiasy, co wolno mi było zrobić, ponieważ mnożenie jest działaniem łącznym. Z powyższego wynika, że

$$2^5 \cdot 2^3 = 2^8.$$

Co zauważyliście? Mianowicie, że

$$2^5 \cdot 2^3 = 2^{5+3} = 2^8.$$

Uogólnimy to.

Dla dowolnej liczby a i naturalnych liczb n oraz m prawdziwy jest wzór

$$a^n \cdot a^m = a^{n+m}$$

A teraz zapowiedziane wcześniej nietypowe, bardzo rzadkie zadania, które dzięki znajomości kongruencji z łatwością rozwiązują uczniowie, czym wprawiają w zdumienie własnych nauczycieli.

Wszystkie te zadania pojawiły się w swoim czasie na różnych konkursach, olimpiadach i innych zawodach matematycznych.

ZNAJDŹ RESZTĘ Z DZIELENIA PRZEZ 43...

Znajdź resztę z dzielenia przez 43 liczby 7^{1000}.

ROZWIĄZANIE

Może jednak, zanim przejdziemy do właściwego rozwiązania, wyjaśnię Wam, dlaczego uczniowie rozwiązują z łatwością tego typu zadania, czym wprawiają w zdumienie swoich nauczycieli. Otóż starając się znaleźć resztę z dzielenia jakiejś liczby naturalnej przez inną liczbę naturalną, zwykle postępuje się tak, jak to opisałem na samym początku niniejszego artykułu, czyli wykonuje się dzielenie z resztą sposobem pisemnym. Umiejętność takiego dzielenia jest powszechna i powinny ją posiadać dzieci dziewięcioletnie. Teraz jednak w dobie ogólnodostępnych urządzeń liczących nierzadko zdarza się tak, że młodsi uczniowie umieją dzielić z resztą sposobem pisemnym, gdy natomiast ich starsi koledzy zdążyli już to zapomnieć. Ale dlaczego o tym piszę? Otóż ta powszechna znajomość dzielenia z resztą sposobem pisemnym powoduje, że jak tylko pojawi się polecenie znajdź resztę z dzielenia... to natychmiast każdy chciałby najpierw przedstawić liczbę, będącą wartością danego wyrażenia, w postaci dziesiętnego zapisu pozycyjnego i dopiero potem dzielić ją z resztą w ogólnie znany sposób. Nauczyciele spodziewają się więc, że jak ich uczniowie ujrzą, że aby liczbę będącą wartością potęgi 7^{1000} przedstawić w postaci dziesiętnego zapisu pozycyjnego, należy 7 pomnożyć przez siebie aż 1000 razy, to się od razu przestraszą zadania i nie będą nawet próbowali zaczynać je rozwiązywać.

Z praktycznego punktu widzenia przedstawienie liczby 7^{1000} w postaci dziesiętnego zapisu pozycyjnego nie ma najmniejszego sensu, gdyż – jak łatwo oszacować – liczba ta miałaby ponad 825 cyfr. Skąd to wiem? Sami popatrzcie:

$$7^4 = 7 \cdot 7 \cdot 7 \cdot 7 = 2401 > 2000 = 2 \cdot 1000 = 2 \cdot 10^3.$$

Z tego wniosek, że $7^4 > 2 \cdot 10^3$.

$$\left.\begin{array}{l} 7^4 > 2 \cdot 10^3 \\ 7^4 > 2 \cdot 10^3 \\ \vdots \\ 7^4 > 2 \cdot 10^3 \end{array}\right\} \text{250 razy}$$

Wymnóżmy te wszystkie nierówności stronami. Otrzymujemy:

$$\underbrace{7^4 \cdot 7^4 \cdot \ldots \cdot 7^4}_{\text{250 razy}} > \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{\text{250 razy}} \cdot \underbrace{10^3 \cdot 10^3 \cdot \ldots \cdot 10^3}_{\text{250 razy}}$$

Po zastosowaniu wzoru, który omawiałem wcześniej – chodzi o wzór $a^n \cdot a^m = a^{n+m}$ – dostajemy:

$$7^{\underbrace{4+4+\ldots+4}_{\text{250 razy}}} > 2^{250} \cdot 10^{\underbrace{3+3+\ldots+3}_{\text{250 razy}}}$$

Ponieważ

$$\underbrace{4 + 4 + \ldots + 4}_{\text{250 razy}} = 4 \cdot 250 = 1000\,, \qquad \underbrace{3 + 3 + \ldots + 3}_{\text{250 razy}} = 3 \cdot 250 = 750,$$

zatem ostatnią nierówność możemy zapisać w postaci:

$$7^{1000} > 2^{250} \cdot 10^{750}.$$

$2^{10} = 1024$, co łatwo obliczyć, mnożąc bezpośrednio 2 przez siebie dziesięć razy.
Ponieważ $2^{10} = 1024 > 1000 = 10^3$, zatem $2^{10} > 10^3$.

Teraz popatrzmy:

$$2^{250} = 2^{\underbrace{10+10\ldots+10}_{\text{25 razy}}} = \underbrace{2^{10} \cdot 2^{10} \cdot \ldots \cdot 2^{10}}_{\text{25 razy}} > \underbrace{10^3 \cdot 10^3 \cdot \ldots \cdot 10^3}_{\text{25 razy}} = 10^{\underbrace{3+3\ldots+3}_{\text{25 razy}}} = 10^{3 \cdot 25} = 10^{75}.$$

Z tego wynika, że

$$2^{250} > 10^{75}.$$

Jeżeli w nierówności $7^{1000} > 2^{250} \cdot 10^{750}$ liczbę 2^{250} zastąpimy mniejszą liczbą – na przykład 10^{75} – to nierówność będzie oczywiście zachowana. Więc postąpmy tak: 2^{250} zastępujemy przez 10^{75}. W rezultacie otrzymujemy nierówność:

$$7^{1000} > 10^{75} \cdot 10^{750}.$$

Ponieważ $10^{75} \cdot 10^{750} = 10^{75+750} = 10^{825}$, zatem

$$7^{1000} > 10^{825}.$$

Liczbę 10^{825} w dziesiętnym zapisie pozycyjnym tworzy jedna jedynka i ustawionych za nią 825 zer:

$$\underbrace{100\ldots0}_{\text{825 zer}}.$$

Z nierówności $7^{1000} > 10^{825}$ wynika, że liczba 7^{1000} jest większa od liczby 10^{825}, czyli od liczby $\underbrace{100\ldots0}_{\text{825 zer}}$.

W każdym systemie pozycyjnym – a więc również w dziesiętnym – jest tak, że większa liczba ma nie mniej cyfr od liczby mniejszej. Z tego wniosek, że liczba 7^{1000} ma nie mniej cyfr od liczby $\underbrace{100\ldots0}_{\text{825 zer}}$, czyli nie mniej niż 826 cyfr.

Być może rozumowanie, które przeprowadziłem w wyżej widocznej kolorowej wstawce, jest dla niektórych z Was niezbyt zrozumiałe, gdyż jest nieco skrótowe. Nie szkodzi. Nie ma ono bowiem żadnego znaczenia dla rozwiązania naszego zadania. Wyjaśnia tylko, dlaczego uczeń potrafiący obliczyć resztę z dzielenia liczby 7^{1000} przez

43 wprowadza w zdumienie swych nauczycieli. A czy Wy na miejscu swoich nauczycieli nie bylibyście zdumieni tym, że Wasz uczeń potrafi precyzyjnie określić resztę z dzielenia niewyobrażalnej wręcz liczby – bo liczącej ponad 825 cyfr – przez liczbę 43? Całe rozumowanie objęte kolorową wstawką służyło jedynie pokazaniu, że liczba 7^{1000} ma ponad 825 cyfr. Dla rozwiązania naszego zadania jest to nieistotne, dlatego jeśli ktoś z Was nie zrozumiał tego rozumowania, to nic się nie stało, jeżeli natomiast pojął je, to świadczy o tym, że ma duże uzdolnienia matematyczne.

A teraz przechodzimy do właściwego rozwiązania naszego zadania.

ROZWIĄZANIE WŁAŚCIWE

Ponieważ $7^2 = 49$ i $49 : 43 = 1$ reszta 6, zatem zachodzi następująca kongruencja:

$$7^2 \equiv 6 \pmod{43}.$$

6 podzielone przez 43 daje oczywiście resztę 6, gdyż

$$\begin{array}{r} 0 \\ \hline 6 : 43 \\ -0 \\ \hline 6 \end{array} \longleftarrow \text{reszta}$$

Kongurencję $7^2 \equiv 6 \pmod{43}$ napiszmy trzykrotnie jedna pod drugą:

$$\begin{aligned} 7^2 &\equiv 6 \pmod{43} \\ 7^2 &\equiv 6 \pmod{43} \\ 7^2 &\equiv 6 \pmod{43} \end{aligned}$$

Pomnóżmy je stronami:

$$7^2 \cdot 7^2 \cdot 7^2 \equiv 6 \cdot 6 \cdot 6 \pmod{43}.$$

Ponieważ $7^2 \cdot 7^2 \cdot 7^2 = 7^{2+2+2} = 7^{3 \cdot 2} = 7^6$, a $6 \cdot 6 \cdot 6 = 216$, zatem kongruencję $7^2 \cdot 7^2 \cdot 7^2 \equiv 6 \cdot 6 \cdot 6 \pmod{43}$ możemy zapisać w postaci:

$$7^6 \equiv 216 \pmod{43}.$$

Dzieląc z resztą 216 przez 43, otrzymujemy: $216 : 43 = 5$ reszta 1. Z tego wynika, że zachodzi następująca kongruencja:

$$216 \equiv 1 \pmod{43}.$$

Skoro $7^6 \equiv 216 \pmod{43}$ oraz $216 \equiv 1 \pmod{43}$, to zachodzi kongruencja

$$7^6 \equiv 1 \pmod{43}.$$

(Skorzystałem tutaj z dowiedzionego wcześniej faktu: mianowicie jeżeli $a \equiv b \pmod{m}$ oraz $b \equiv c \pmod{m}$, to $a \equiv c \pmod{m}$.

Ile razy 6 mieści się w 1000? Aby to stwierdzić, wystarczy podzielić z resztą 1000 przez 6:

$$\begin{array}{r} 166 \\ \hline 1000 : 6 \\ -\underline{6} \\ 40 \\ -\underline{36} \\ 40 \\ -\underline{36} \\ 4 \end{array}$$

A więc 6 mieści się w 1000 aż 166 razy.

W takim razie kongruencję $7^6 \equiv 1 \pmod{43}$ napiszemy 166 razy jedna pod drugą:

$$\left.\begin{aligned} 7^6 &\equiv 1 \pmod{43} \\ 7^6 &\equiv 1 \pmod{43} \\ &\cdot \quad\quad \cdot \\ &\cdot \quad\quad \cdot \\ &\cdot \quad\quad \cdot \\ 7^6 &\equiv 1 \pmod{43} \end{aligned}\right\} \text{166 razy}$$

Pomnóżmy je wszystkie stronami:

$$\underbrace{7^6 \cdot 7^6 \cdot \ldots \cdot 7^6}_{166 \text{ razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{166 \text{ razy}} \pmod{43}.$$

Ponieważ $\underbrace{7^6 \cdot 7^6 \cdot \ldots \cdot 7^6}_{166 \text{ razy}} = 7^{\underbrace{6+6+\ldots+6}_{166 \text{ razy}}} = 7^{166 \cdot 6} = 7^{996}$, a 1 obojętnie ile razy pomnożona przez siebie zawsze daje 1, zatem kongruencję $\underbrace{7^6 \cdot 7^6 \cdot \ldots \cdot 7^6}_{166 \text{ razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{166 \text{ razy}} \pmod{43}$ możemy zapisać w następującej postaci:

$$7^{996} \equiv 1 \pmod{43}.$$

Teraz podpisujemy jedna pod drugą kongruencję $7^{996} \equiv 1 \pmod{43}$ oraz dwukrotnie kongruencję $7^2 \equiv 6 \pmod{43}$:

$$\begin{aligned} 7^{996} &\equiv 1 \pmod{43} \\ 7^2 &\equiv 6 \pmod{43} \\ 7^2 &\equiv 6 \pmod{43} \end{aligned}$$

Mnożymy je obustronnie, otrzymując kongruencję

$$7^{996} \cdot 7^2 \cdot 7^2 \equiv 1 \cdot 6 \cdot 6 \pmod{43}.$$

Ponieważ $7^{996} \cdot 7^2 \cdot 7^2 = 7^{996+2+2} = 7^{1000}$, a $1 \cdot 6 \cdot 6 = 36$, zatem ostatnią kongruencję możemy zapisać w postaci

$$7^{1000} \equiv 36 \pmod{43}.$$

Z tej ostatniej postaci widać od razu, że reszta z dzielenia liczby 7^{1000} przez 43 wynosi 36. Zapisujemy to w postaci:

$$7^{1000} : 43 = \underset{\substack{\uparrow \\ \text{iloraz niezupełny nieznany}}}{\square} \text{ reszta } 36$$

Znaleźliśmy, jak widać, resztę, nie znając ilorazu niezupełnego. Ale w naszym zadaniu chodziło tylko o znalezienie reszty, i to uczyniliśmy.

Odpowiedź: reszta z dzielenia liczby 7^{1000} przez 43 wynosi 36.

WYKAŻ, ŻE 7 DZIELI...

Wykaż, że 7 dzieli liczbę $2222^{5555} + 5555^{2222}$.

ROZWIĄZANIE

Plan rozwiązania zadania:

- Najpierw znajdziemy resztę z dzielenia liczby 2222^{5555} przez 7 (I etap).
- Następnie znajdziemy resztę z dzielenia liczby 5555^{2222} przez 7 (II etap).
- Na końcu znajdziemy resztę z dzielenia sumy obu powyższych liczb, czyli liczby $2222^{5555} + 5555^{2222}$ przez 7 (III etap).

Etap I

Ponieważ

$$\begin{array}{r} 317 \\ 2222 : 7 \\ -21 \\ \hline 12 \\ -7 \\ \hline 52 \\ -49 \\ \hline 3 \end{array}$$

Możemy więc napisać

$$2222 : 7 = 317 \text{ reszta } 3.$$

Zachodzi zatem kongruencja:

$$2222 \equiv 3 \pmod{7}.$$

Zapiszmy tę kongruencję, jedna pod drugą, 6 razy:

$$\left.\begin{array}{l} 2222 \equiv 3 \pmod 7 \\ 2222 \equiv 3 \pmod 7 \\ \quad . \qquad . \\ \quad . \qquad . \\ \quad . \qquad . \\ 2222 \equiv 3 \pmod 7 \end{array}\right\} \text{6 razy}$$

Pomnóżmy je wszystkie stronami:

$$\underbrace{2222 \cdot 2222 \ldots \cdot 2222}_{\text{6 razy}} \equiv \underbrace{3 \cdot 3 \cdot \ldots \cdot 3}_{\text{6 razy}} \pmod 7.$$

Lewą stronę powyższej kongruencji zapisujemy w postaci potęgi

$$2222^6,$$

a prawą stronę – po wymnożeniu sześciu 3 – w postaci dziesiętnego zapisu pozycyjnego:

$$3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 729.$$

Po zrobieniu tego ostatnia kongruencja przyjmuje postać:

$$2222^6 \equiv 729 \pmod 7.$$

Ponieważ

$$\begin{array}{r} \underline{104} \\ 729 : 7 \\ \underline{-7} \\ 29 \\ \underline{-28} \\ 1 \end{array}$$

zachodzi więc następująca kongruencja:

$$729 \equiv 1 \pmod 7.$$

Z faktu, że prawdziwe są dwie kongruencje: $2222^6 \equiv 729 \pmod 7$ oraz $729 \equiv 1 \pmod 7$, wynika zachodzenie następującej kongruencji:

$$2222^6 \equiv 1 \pmod 7$$

(skorzystaliśmy tu z własności: jeżeli $a \equiv b \pmod m$ oraz $b \equiv c \pmod m$, to $a \equiv c \pmod m$.

Ile razy 6 mieści się w 5555? Aby to stwierdzić, wystarczy podzielić z resztą 5555 przez 6:

$$\begin{array}{r} \underline{925} \\ 5555 : 6 \\ \underline{-54} \\ 15 \\ \underline{-12} \\ 35 \\ \underline{-30} \\ 5 \end{array}$$

A zatem 6 mieści się w 5555 aż 925 razy.

W takim razie kongruencję $2222^6 \equiv 1 \pmod 7$ napiszmy 925 razy jedna pod drugą:

$$\left.\begin{array}{l} 2222^6 \equiv 1 \pmod 7 \\ 2222^6 \equiv 1 \pmod 7 \\ \quad . \qquad . \\ \quad . \qquad . \\ \quad . \qquad . \\ 2222^6 \equiv 1 \pmod 7 \end{array}\right\} \text{925 razy}$$

Pomnóżmy je wszystkie stronami:

$$\underbrace{2222^6 \cdot 2222^6 \cdot \ldots \cdot 2222^6}_{\text{925 razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{\text{925 razy}} \pmod 7$$

Ponieważ $\underbrace{2222^6 \cdot 2222^6 \cdot \ldots \cdot 2222^6}_{\text{925 razy}} \equiv 2222^{\underbrace{6+6+\ldots+6}_{\text{925 razy}}} = 2222^{925 \cdot 6} = 2222^{5550}$, a 1 obojętnie ile razy pomnożone przez siebie zawsze daje 1, zatem kongruencję $\underbrace{2222^6 \cdot 2222^6 \cdot \ldots \cdot 2222^6}_{\text{925 razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{\text{925 razy}} \pmod 7$ możemy zapisać w następującej postaci:

$$2222^{5550} \equiv 1 \pmod 7.$$

Na początku rozwiązania ustaliliśmy, że zachodzi kongruencja $2222 \equiv 3 \pmod 7$. Napiszmy ją jedna pod drugą pięć razy:

$$2222 \equiv 3 \pmod 7$$
$$2222 \equiv 3 \pmod 7$$
$$2222 \equiv 3 \pmod 7$$
$$2222 \equiv 3 \pmod 7$$
$$2222 \equiv 3 \pmod 7$$

Po pomnożeniu ich stronami otrzymujemy kongruencję:

$$2222^5 \equiv 3^5 \pmod 7.$$

Ponieważ $3^5 = 243$, więc w powyższej kongruencji potęgę 3^5 możemy zastąpić przez 243, otrzymując w ten sposób kongruencję

$$2222^5 \equiv 243 \pmod 7.$$

Biorąc pod uwagę, że $243 : 7 = 34$ reszta 5, dostajemy kolejną kongruencję:

$$243 \equiv 5 \pmod 7.$$

Z prawdziwości kongruencji $2222^5 \equiv 243 \pmod 7$ oraz $243 \equiv 5 \pmod 7$ wynika zachodzenie kongruencji:

$$2222^5 \equiv 5 \pmod 7.$$

Kongruencję $2222^{5550} \equiv 1 \pmod 7$, której prawdziwość wykazaliśmy wcześniej, i kongruencję $2222^5 \equiv 5 \pmod 7$, której zachodzenie pokazaliśmy przed chwilą, piszemy jedna pod drugą:

$$2222^{5550} \equiv 1 \pmod 7$$
$$2222^5 \equiv 5 \pmod 7$$

i następnie mnożymy je stronami:

$$2222^{5550} \cdot 2222^5 \equiv 1 \cdot 5 \pmod 7.$$

Ponieważ $2222^{5550} \cdot 2222^5 = 2222^{5550+5} = 2222^{5555}$, zatem ostatnią kongruencję możemy zapisać jako

$$\boxed{2222^{5555} \equiv 5 \pmod 7}\ .$$

I właśnie o znalezienie tej kongruencji chodziło w pierwszym etapie. Z jej postaci widać od razu, że reszta z dzielenia liczby 2222^{5555} przez 7 wynosi 5.

Przechodzimy więc do drugiego etapu.

Etap II

Ponieważ $5555 : 7 = 793$ reszta 4, zatem zachodzi kongruencja $5555 \equiv 4 \pmod 7$. Piszemy ją trzykrotnie jedna pod drugą:

$$5555 \equiv 4 \pmod 7$$
$$5555 \equiv 4 \pmod 7$$
$$5555 \equiv 4 \pmod 7$$

Po pomnożeniu ich stronami otrzymujemy:

$$5555^3 \equiv 4^3 \pmod 7.$$

Biorąc pod uwagę, że $4^3 = 64$, ostatnią kongruencję zapisujemy jako

$$5555^3 \equiv 64 \pmod 7.$$

Ponieważ $64 : 7 = 9$ reszta 1, zatem prawdziwa jest kongruencja

$$64 \equiv 1 \pmod 7.$$

Zachodzenie kongruencji $5555^3 \equiv 64 \pmod 7$ oraz $64 \equiv 1 \pmod 7$ pociąga za sobą prawdziwość kongruencji

$$5555^3 \equiv 1 \pmod 7.$$

Ile razy 3 mieści się w 2222? Proste podzielenie z resztą $2222 : 3 = 740$ reszta 2 ujawnia, że 740 razy.

Zatem kongruencję $5555^3 \equiv 1 \pmod 7$ piszemy 740 razy jedna pod drugą:

$$\left.\begin{array}{l} 5555^3 \equiv 1 \pmod 7 \\ 5555^3 \equiv 1 \pmod 7 \\ \quad\vdots \\ 5555^3 \equiv 1 \pmod 7 \end{array}\right\} \text{740 razy}$$

Pomnóżmy je wszystkie stronami:

$$\underbrace{5555^3 \cdot 5555^3 \cdot \ldots \cdot 5555^3}_{740 \text{ razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{740 \text{ razy}} \pmod 7$$

Ponieważ $\underbrace{5555^3 \cdot 5555^3 \cdot \ldots \cdot 5555^3}_{740 \text{ razy}} = 5555^{\overbrace{3+3+\ldots+3}^{740 \text{ razy}}} = 5555^{740 \cdot 3} = 5555^{2220}$, zatem kongruencję widoczną dalej

$\underbrace{5555^3 \cdot 5555^3 \cdot \ldots \cdot 5555^3}_{740 \text{ razy}} \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{740 \text{ razy}} \pmod 7$ można zapisać w następującej postaci:

$$5555^{2220} \equiv 1 \pmod 7.$$

Teraz podpisujemy jedna pod drugą kongruencję $5555^{2220} \equiv 1 \pmod 7$ oraz dwukrotnie kongruencję $5555 \equiv 4 \pmod 7$:

$$\begin{aligned} 5555^{2220} &\equiv 1 \pmod 7 \\ 5555 &\equiv 4 \pmod 7 \\ 5555 &\equiv 4 \pmod 7 \end{aligned}$$

Mnożymy je obustronnie, otrzymując kongruencję

$$5555^{2220} \cdot 5555 \cdot 5555 \equiv 1 \cdot 4 \cdot 4 \pmod 7.$$

Ostatnią kongruencję możemy zapisać w postaci:

$$5555^{2222} \equiv 16 \pmod 7.$$

Ponieważ $16 : 7 = 2$ reszta 2, więc zachodzi kongruencja

$$16 \equiv 2 \pmod 7.$$

Z zachodzenia kongruencji $5555^{2222} \equiv 16 \pmod 7$ oraz $16 \equiv 2 \pmod 7$ wynika prawdziwość kongruencji

$$\boxed{5555^{2222} \equiv 2 \pmod 7}$$

Znalezienie tej kongruencji jest ukoronowaniem drugiego etapu.
Z jej postaci widać od razu, że reszta z dzielenia liczby 5555^{2222} przez 7 wynosi 2.
Przechodzimy zatem do trzeciego etapu.

Etap III

Teraz podpisujemy jedna pod drugą kongruencje ujęte w ramki, czyli te, których znalezienie było ukoronowaniem pierwszego i drugiego etapu rozwiązania zadania:

$$\begin{aligned} 2222^{5555} &\equiv 5 \pmod 7 \\ 5555^{2222} &\equiv 2 \pmod 7 \end{aligned}$$

Następnie dodajemy je stronami, otrzymując w ten sposób kongruencję:

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \pmod 7,$$

skąd

$$2222^{5555} + 5555^{2222} \equiv 7 \pmod 7.$$

Ponieważ $7 \equiv 0 \pmod 7$, więc biorąc pod uwagę zachodzenie kongruencji $2222^{5555} + 5555^{2222} \equiv 7 \pmod 7$ oraz $7 \equiv 0 \pmod 7$, dochodzimy do wniosku – na mocy dobrze nam znanej własności kongruencji, bo kilkakrotnie już wykorzystywanej – że prawdziwa jest również kongruencja:

$$\boxed{2222^{5555} + 5555^{2222} \equiv 0 \pmod 7},$$

która oznacza nic innego, tylko to, że

$$(2222^{5555} + 5555^{2222}) : 7 = \square \text{ reszta } 0.$$

$\square$ – iloraz niezupełny nieznany

Otrzymany wynik oznacza, że liczba $2222^{5555} + 5555^{2222}$ dzieli się przez 7, co właśnie należało udowodnić.

ZNAJDŹ TRZY OSTATNIE CYFRY...

Znajdź trzy ostatnie cyfry liczby 13^{100}.

ROZWIĄZANIE

Co wiąże powyższe zadanie z kongruencjami? Zobaczmy, czym faktycznie jest znalezienie trzech ostatnich cyfr liczby 13^{100}.

Podzielmy w tym celu jakąś dowolną liczbę – na przykład $27\,839$ – przez 1000:

$$\begin{array}{r} 27 \\ 27839 \\ -\ 2000 \\ \hline 7839 \\ -\ 7000 \\ \hline 839 \end{array} : 1000$$

Zatem $27839 : 1000 = 27$ reszta 839.

Przykład ten pokazuje nam, że znalezienie trzech ostatnich cyfr jakiejś dowolnej liczby sprowadza się do otrzymania reszty z dzielenia tej liczby przez 1000.

Zatem znalezienie trzech ostatnich cyfr liczby 13^{100} polega na obliczeniu reszty z dzielenia tej liczby przez 1000, a to już umiemy świetnie realizować, umiejętnie posługując się kongruencjami. Zaczynamy.

Ponieważ $13^3 = 2197$ i $2197 : 1000 = 2$ reszta 197, zatem zachodzi kongruencja:

$$13^3 \equiv 197 \pmod{1000}.$$

Powyższą kongruencję mnożymy stronami przez siebie, otrzymując w ten sposób nową kongruencję:

$$13^3 \cdot 13^3 \equiv 197 \cdot 197 \pmod{1000},$$

skąd

$$13^6 \equiv 809 \pmod{1000},$$

(skorzystaliśmy tu z faktu, że $197 \cdot 197 = 28\,809$ i że $28\,809 : 1000 = 28$ reszta 809). Ostatnio otrzymaną kongruencję znowu mnożymy stronami przez siebie, w rezultacie czego dostajemy kongruencję

$$13^6 \cdot 13^6 \equiv 809 \cdot 809 \pmod{1000},$$

skąd

$$13^{12} \equiv 481 \pmod{1000}$$

(skorzystaliśmy tu z faktu, że $809 \cdot 809 = 654\,481$ i że $654\,481 : 1000 = 654$ reszta 481). Ostatnią kongruencję jeszcze raz mnożymy stronami przez siebie, dochodząc w ten sposób do kongruencji

$$13^{12} \cdot 13^{12} \equiv 481 \cdot 481 \pmod{1000},$$

skąd

$$13^{24} \equiv 361 \pmod{1000}$$

(skorzystaliśmy tu z faktu, że $481 \cdot 481 = 231\,361$ i że $231\,361 : 1000 = 231$ reszta 361). I jeszcze raz ostatnią kongruencję mnożymy stronami przez siebie, otrzymując następną kongruencję

$$13^{24} \cdot 13^{24} \equiv 361 \cdot 361 \pmod{1000},$$

skąd

$$13^{48} \equiv 321 \pmod{1000}$$

(skorzystaliśmy tu z faktu, że $361 \cdot 361 = 130\,321$ i że $130\,321 : 1000 = 130$ reszta 321).

Uff. Teraz już po raz ostatni ostatnią kongruencję mnożymy stronami przez siebie, otrzymując w rezultacie kongruencję

$$13^{48} \cdot 13^{48} \equiv 321 \cdot 321 \pmod{1000},$$

skąd

$$13^{96} \equiv 41 \pmod{1000}$$

(skorzystaliśmy tu z faktu, że $321 \cdot 321 = 103\,041$ i że $103\,041 : 1000 = 103$ reszta 41).

Już jesteśmy bardzo blisko końca. Pod kongruencją $13^{96} \equiv 41 \pmod{1000}$ podpisujemy kongruencję, którą otrzymaliśmy na samym początku, czyli kongruencję $13^3 \equiv 197 \pmod{1000}$:

$$13^{96} \equiv 41 \pmod{1000}$$
$$13^{3} \equiv 197 \pmod{1000}$$

Obie kongruencje mnożymy stronami:

$$13^{96} \cdot 13^{3} \equiv 41 \cdot 197 \pmod{1000},$$

skąd

$$13^{99} \equiv 77 \pmod{1000}$$

(skorzystaliśmy tu z faktu, że $41 \cdot 197 = 8077$ i że $8077 : 1000 = 8$ reszta 77).

Teraz już nie mnożymy kongruencji stronami, lecz obie strony ostatniej kongruencji mnożymy przez liczbę 13:

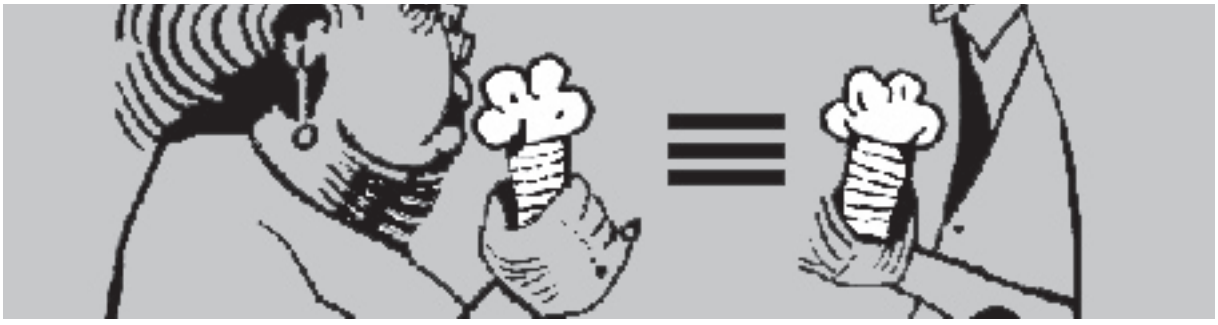
$$13 \cdot 13^{99} \equiv 13 \cdot 77 \pmod{1000},$$

a stąd dostajemy, że

$$13^{100} \equiv 1 \pmod{1000},$$

(skorzystaliśmy tu z faktu, że $13 \cdot 77 = 1001$ i że $1001 : 1000 = 1$ reszta 1).

Z ostatniej kongruencji widać bezpośrednio, że trzy ostatnie cyfry liczby 13^{100} tworzą blok 001.



Tajemnice szyfrów

Nierzucająca się w oczy willa na przedmieściach stolicy jednego z państw Bliskiego Wschodu. Zza żaluzji widać kilka zwykłych komputerów. Do budynku wchodzą i wychodzą co jakiś czas młodzi ludzie w wytartych dżinsach, z niedbałymi fryzurami i kolczykami w uszach. Wchodzi również młody dwudziestokilkuletni chłopak w dżinsach z wielkimi dziurami na kolanach, z dwoma kolczykami: jeden w uchu, a drugi w nosie, oraz z czerwonymi włosami na głowie, zrobionymi „na irokeza". To pułkownik wywiadu, kierownik rządowego ośrodka wojny elektronicznej, jeden z najbliższych i najbardziej zaufanych oraz cenionych doradców premiera. Po ukończeniu matematyki utrzymywał się z hakerstwa. To znaczy na zlecenie jednych firm włamywał się do sieci informatycznych konkurencji albo w celu jej dezorganizacji, albo dla pozyskania jakichś cennych informacji. Schwytany w końcu przez policję, otrzymał propozycję: albo pójdzie za kratki, albo obejmie kierownictwo rządowego ośrodka wojny elektronicznej. Domyślacie się, co wybrał. I właśnie w ten sposób został jednym z najbardziej cenionych doradców premiera.

Anthony Zboralski – jeden z legendarnych hakerów, który w 1994 roku jako 19-letni geniusz komputerowy o pseudonimie „Frantic" przez 7 miesięcy buszował po archiwach FBI i który po odsiedzeniu za to wyroku we Francji wyemigrował do Indonezji, gdzie kieruje firmą ochrony komputerowych sieci Bellua Asia Pacific – komentuje to tak:

– Moim zdaniem sytuacja jest coraz gorsza. Coraz więcej komputerów, coraz więcej ludzi, a coraz mniej ekspertów, którzy rzeczywiście wiedzą, o co chodzi w ochronie cyberprzestrzeni.

Oczywiście ochroną cyberprzestrzeni, jak i wojną elektroniczną nie mogą zajmować się osoby, które ukończyły kierunki humanistyczne. Świat potrzebuje coraz więcej ludzi z wykształceniem ścisłym, a więc informatyków, elektroników, matematyków, fizyków i tak dalej. Mianem kierunków ścisłych określa się wszystkie te kierunki, na których matematyka odgrywa istotną rolę. W Rosji przy wielu wydziałach matematycznych powstały nawet kierunki kryptologii. Nie bez powodu więc hakerzy rosyjscy i chińscy uchodzą za najgroźniejszych na świecie. Mają bowiem solidne wykształcenie matematyczne.

A sprawa nie jest błaha, gdyż armie i rządy prowadzą dziś wojny za pośrednictwem hakerów. Ofiarami sieciowego szpiegostwa lub sabotażu padały już – oczywiście w różnym czasie – systemy informatyczne różnych ministerstw i innych ważnych centralnych urzędów w Niemczech, Wielkiej Brytanii, Francji, Japonii czy Stanach Zjednoczonych. Co prawda na razie ze skutkami takich ataków lepiej lub gorzej radzą sobie specjaliści od bezpieczeństwa sieci, ale należy wziąć pod uwagę, że obecnie hakerzy rekrutowani są w ten sposób, że przyłapani na gorącym uczynku są szantażowani i aby uniknąć więzienia, decydują się na pracę dla władz. Są to na ogół bardzo młodzi ludzie, bez

specjalistycznego wykształcenia. Można śmiało powiedzieć: hakerzy amatorzy. Co za tym idzie, ich ataki nie są zbyt wyrafinowane. Całkiem inaczej sprawa może wyglądać, gdy wezmą się za to prawdziwi zawodowcy, posiadający specjalistyczne przygotowanie w zakresie matematyki. Prof. Ryszard Tadeusiewicz, wybitny cybernetyk i informatyk z Akademii Górniczo-Hutniczej w Krakowie, twierdzi, że profesjonalni hakerzy są w stanie obejść wszelkie odmiany internetowej policji. Ci hakerzy, którzy potrafią operować na podstawowym, zero-jedynkowym poziomie, mogą ustalić na nowo pierwotne zasady działania komputerów. Mogą wówczas przeprowadzić atak, wobec którego mogłyby się okazać niewystarczające wszelkie dotychczasowe zabezpieczenia.

W naszym niedużym objętościowo czasopiśmie nie jesteśmy oczywiście w stanie omówić całokształtu zagadnień związanych z bezpieczeństwem sieci informatycznych. Chcielibyśmy naszym Czytelnikom przedstawić pewien drobny fragment tych zagadnień, a mianowicie zapoznać ich z jednym z najbardziej rozpowszechnionych obecnie kryptosystemów z kluczem publicznym – systemem RSA. Tym bardziej że w tym roku mija 30 lat od jego powstania.

30 LAT RSA

W 1978 roku trzech matematyków z MIT (Massachusetts Institute of Technology), który uznawany jest za najlepszą uczelnię techniczną na świecie, opracowało taki sposób kodowania wiadomości, że:

a) **każdy może ogłosić publicznie (na przykład w gazecie): adresowane do mnie wiadomości proszę szyfrować tak a tak;**
b) **zaszyfrowaną wiadomość może wysłać każdy, ale odczytać ją – jedynie adresat.**

Twórcami RSA – kryptosystemu z kluczem publicznym – są Ron Rivest, Adi Shamir i Leonard Adleman. Nazwa systemu RSA powstała z pierwszych liter ich nazwisk.

W dowodzie tego, że z praktycznego punktu widzenia szyfr jest nie do złamania, wykorzystuje się twierdzenie teorii automatów. Po prostu dwie bardzo duże liczby pierwsze (liczące na przykład po kilkaset cyfr każda) pomnożyć z wykorzystaniem komputera jest łatwo, ale postąpić odwrotnie, to znaczy mając jedynie ów iloczyn, a nie znając tych liczb pierwszych, obliczyć je, czyli inaczej mówiąc, rozłożyć ów iloczyn na czynniki pierwsze, nawet najszybszemu i najlepiej zaprogramowanemu komputerowi zabiera to zbyt dużo czasu (mogą to być nawet lata pracy).

Teraz pokażemy, jak się w praktyce szyfruje i deszyfruje w systemie RSA. Ponieważ „Świat Matematyki" jest czasopismem matematycznym o profilu edukacyjnym, dlatego dla łatwości i przejrzystości obliczeń użyjemy bardzo małych liczb pierwszych. Najpierw zaszyfrujemy, a potem przeprowadzimy deszyfrację otrzymanego wcześniej szyfrogramu. Uczynimy to na przykładzie słowa

S Z Y F R

Najpierw sporządzimy tabelkę z ponumerowanymi literami alfabetu polskiego:

numer	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
znak	spacja	A	Ą	B	C	Ć	D	E	Ę	F	G	H	I	J	K	L	Ł

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
M	N	Ń	O	Ó	P	Q	R	S	Ś	T	U	V	W	X	Y	Z	Ź	Ż

Następnie opiszemy procedurę szyfrowania w RSA w sześciu punktach:

1. **Wybieramy dwie liczby pierwsze p i q.**
2. **Obliczamy $n = pq$.**
3. **Wybieramy liczbę e względnie pierwszą z $(p - 1)(q - 1)$.**
4. **Wyznaczamy liczbę całkowitą d, $0 < d < (p - 1)(q - 1)$, taką że $ed + a(p - 1)(q - 1) = 1$.**
5. **Udostępniamy parę (n, e) jako nasz klucz publiczny RSA.**
6. **Zachowujemy w tajemnicy parę (n, d) jako nasz klucz tajny RSA.**

Przystępujemy do szyfrowania słowa SZYFR.

① Jako dwie liczby pierwsze wybieramy 7 oraz 13.
② Obliczamy ich iloczyn $7 \cdot 13 = 91$.
③ Wybieramy liczbę e względnie pierwszą z $(7 - 1) \cdot (13 - 1) = 6 \cdot 12 = 72$. Liczba e względnie pierwsza z 72 to taka liczba, że największy wspólny dzielnik liczby e oraz 72 wynosi 1. Taką liczbą e może być na przykład 11.

④ Wyznaczamy liczbę całkowitą d, gdzie $0 < d < 72$, taką że $11d + 72a = 1$. Do równania $ed + a(p - 1)(q - 1) = 1$ w miejsce e wstawiliśmy liczbę 11 (wybraliśmy ją w ③ jako liczbę e), a w miejsce $(p - 1)(q - 1)$ wstawiliśmy liczbę 72, którą obliczyliśmy wcześniej również w ③. Równanie $11d + 72a = 1$ jest równaniem nieoznaczonym pierwszego stopnia z dwiema niewiadomymi.

Umiejętność rozwiązywania tego rodzaju równań jest bardzo ważna w matematyce, a mimo tego nie jest objęta w Polsce programem nauczania matematyki w szkole. Tego rodzaju równań nie umieją rozwiązywać nawet uczniowie z klas maturalnych o profilu matematycznym. Równania nieoznaczone pierwszego stopnia z dwiema niewiadomymi rozwiązuje się za pomocą bardzo interesującego i na dodatek łatwego algorytmu, na tyle łatwego, że bez trudu opanowują go nawet 11-latkowie (sam to sprawdziłem na kółku matematycznym w piątej klasie szkoły podstawowej). Nie będę tego algorytmu tutaj przytaczał, gdyż po pierwsze nie ma teraz na to miejsca, a po drugie został on bardzo szczegółowo objaśniony w pierwszym numerze „Świata Matematyki" w artykule „Stare francuskie zadanie z XVIII wieku" przy okazji rozwiązywania zadania „Handlarze winem i celnicy". Jeśli ktoś z naszych Czytelników nie ma tego numeru, to może go zamówić, korzystając z naszej strony internetowej: www.swiatmatematyki.pl

Nie będę więc równania $11d + 72a = 1$ rozwiązywał, tylko podam samo jego rozwiązanie, a konkretnie wartość niewiadomej d, która spełnia warunek $0 < d < 72$. Bo tylko ona jest tu nam potrzebna jako klucz tajny RSA. Poszukiwana wartość d wynosi 59.

⑤ Udostępniamy parę (91, 11) jako nasz klucz publiczny RSA.

⑥ Zachowujemy w tajemnicy parę (91, 59) jako nasz klucz tajny RSA.

Mając klucz publiczny RSA, którym w naszym przypadku jest para (91, 11), możemy przystąpić do szyfrowania wiadomości brzmiącej SZYFR. W tym celu znaki występujące w tym słowie zastępujemy cyframi, według wcześniej sporządzonej tabelki.

S	Z	Y	F	R
25	33	32	09	24

Tekst jawny zapisany cyfrowo:

25 : 33 : 32 : 09 : 24

szyfrujemy według wzoru:

$$E(x) = x^e \pmod n$$

gdzie x oznacza numer danego znaku, $e = 11$, a $n = 91$.

$$E(25) = 25^{11} \pmod{91}$$

Ponieważ kongruencje zostały omówione bardzo szczegółowo we wcześniejszym artykule niniejszego numeru, więc nikt z Czytelników nie powinien mieć trudności ze zrozumieniem, o co tu właściwie chodzi. $E(25)$ oznacza nic innego, tylko resztę z dzielenia liczby 25^{11} przez 91. Obliczamy. Ponieważ $25^2 = 625$, a z kolei $625 : 91 = 6$ reszta 79, zatem

$$25^2 \equiv 79 \pmod{91}.$$

Powyższą kongruencję mnożymy stronami przez siebie:

$$25^2 \equiv 79 \pmod{91}$$
$$25^2 \equiv 79 \pmod{91}$$

Po pomnożeniu otrzymujemy:

$$25^4 \equiv 79^2 \pmod{91}.$$

Ponieważ $79^2 = 6241$, a $6241 : 91 = 68$ reszta 53, zatem

$$79^2 \equiv 53 \pmod{91}.$$

Teraz korzystamy z faktu, że jeżeli $25^4 \equiv 79^2 \pmod{91}$ i $79^2 \equiv 53 \pmod{91}$, to

$$25^4 \equiv 53 \pmod{91}.$$

Powyższą kongruencję znów mnożymy przez siebie stronami

$$25^4 \equiv 53 \pmod{91}$$
$$25^4 \equiv 53 \pmod{91}$$

otrzymując

$$25^8 \equiv 53^2 \pmod{91}.$$

Ponieważ $53^2 = 2809$, a $2809 : 91 = 30$ reszta 79, zatem

$$53^2 \equiv 79 \pmod{91}.$$

Teraz korzystamy z faktu, że jeżeli $25^8 \equiv 53^2 \pmod{91}$ i $53^2 \equiv 79 \pmod{91}$, to

$$25^8 \equiv 79 \pmod{91}.$$

Teraz z kolei mnożymy stronami trzy kongruencje:

$$25^8 \equiv 79 \pmod{91}$$
$$25^2 \equiv 79 \pmod{91}$$
$$25 \equiv 25 \pmod{91}$$

w rezultacie otrzymując

$$25^{8+2+1} \equiv 79 \cdot 79 \cdot 25 \pmod{91},$$

skąd

$$25^{11} \equiv 156\,025 \pmod{91}.$$

Uwzględniając fakt, że $156\,025 : 91 = 1714$ reszta 51, mamy

$$156\,025 \equiv 51 \pmod{91}.$$

Z tego, że $25^{11} \equiv 156\,025 \pmod{91}$ i $156\,025 \equiv 51 \pmod{91}$, dostajemy kongruencję:

$$25^{11} \equiv 51 \pmod{91}.$$

Zatem

$$E(25) = 25^{11} \pmod{91} = 51.$$

Po prostu reszta z dzielenia liczby 25^{11} przez 91 wynosi 51.
Podobne obliczenia przeprowadzamy w przypadku szyfrowania pozostałych znaków:

$$E(25) = 25^{11} \pmod{91} = 51$$
$$E(33) = 33^{11} \pmod{91} = 80$$
$$E(32) = 32^{11} \pmod{91} = 37$$
$$E(09) = \ 9^{11} \pmod{91} = 81$$
$$E(24) = 24^{11} \pmod{91} = 19$$

W ten sposób otrzymaliśmy zapisany cyfrowo szyfrogram:

$$51 : 80 : 37 : 81 : 19.$$

A jak ma przeprowadzić deszyfrację ten, kto otrzymał powyższy szyfrogram? Dzięki kluczowi tajnemu RSA. Deszyfrujemy bowiem według wzoru:

$$D(x) = x^d \pmod{n}$$

gdzie x oznacza liczbę występującą w szyfrogramie, $d = 59$, a $n = 91$.

$$D(51) = 51^{59} \pmod{91}$$

$D(51)$ oznacza resztę z dzielenia liczby 51^{59} przez 91. Obliczamy. Ponieważ $51^2 = 2601$, a $2601 : 91 = 28$ reszta 53, zatem

$$51^2 \equiv 53 \pmod{91}.$$

Powyższą kongruencję mnożymy stronami przez siebie:

$$51^2 \equiv 53 \pmod{91}$$
$$51^2 \equiv 53 \pmod{91}$$

W rezultacie otrzymujemy:

$$51^4 \equiv 53^2 \pmod{91}.$$

Ponieważ $53^2 = 2809$, a $2809 : 91 = 30$ reszta 79, zatem

$$53^2 \equiv 79 \pmod{91}.$$

Teraz korzystamy z faktu, że jeżeli $51^4 \equiv 53^2 \pmod{91}$ i $53^2 \equiv 79 \pmod{91}$, to

$$51^4 \equiv 79 \pmod{91}.$$

Ostatnią kongruencję mnożymy stronami przez siebie, w rezultacie otrzymując:

$$51^8 \equiv 79^2 \pmod{91}.$$

Ponieważ $79^2 = 6241$, a $6241 : 91 = 68$ reszta 53, zatem

$$79^2 \equiv 53 \pmod{91}.$$

Jeżeli $51^8 \equiv 79^2 \pmod{91}$ i $79^2 \equiv 53 \pmod{91}$, to

$$51^8 \equiv 53 \pmod{91}.$$

Teraz mnożymy stronami dwie kongruencje:

$$51^8 \equiv 53 \pmod{91}$$
$$51^4 \equiv 79 \pmod{91}$$

w rezultacie otrzymując:

$$51^{8+4} \equiv 53 \cdot 79 \pmod{91},$$

a stąd

$$51^{12} \equiv 4187 \pmod{91}.$$

Ponieważ $4187 : 91 = 46$ reszta 1, więc

$$51^{12} \equiv 1 \pmod{91}.$$

Mnożymy stronami aż siedem kongruencji:

$$51^{12} \equiv 1 \pmod{91}$$
$$51^{12} \equiv 1 \pmod{91}$$
$$51^{12} \equiv 1 \pmod{91}$$
$$51^{12} \equiv 1 \pmod{91}$$
$$51^8 \equiv 53 \pmod{91}$$
$$51^2 \equiv 53 \pmod{91}$$
$$51 \equiv 51 \pmod{91}$$

Po pomnożeniu otrzymujemy:

$$51^{12+12+12+12+8+2+1} \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 53 \cdot 53 \cdot 51 \pmod{91},$$

skąd

$$51^{59} \equiv 143\,259 \pmod{91}.$$

Ponieważ $143\,259 : 91 = 1574$ reszta 25, zatem

$$51^{59} \equiv 25 \pmod{91}.$$

Oznacza to, że reszta z dzielenia liczy 51^{59} przez 91 wynosi 25.

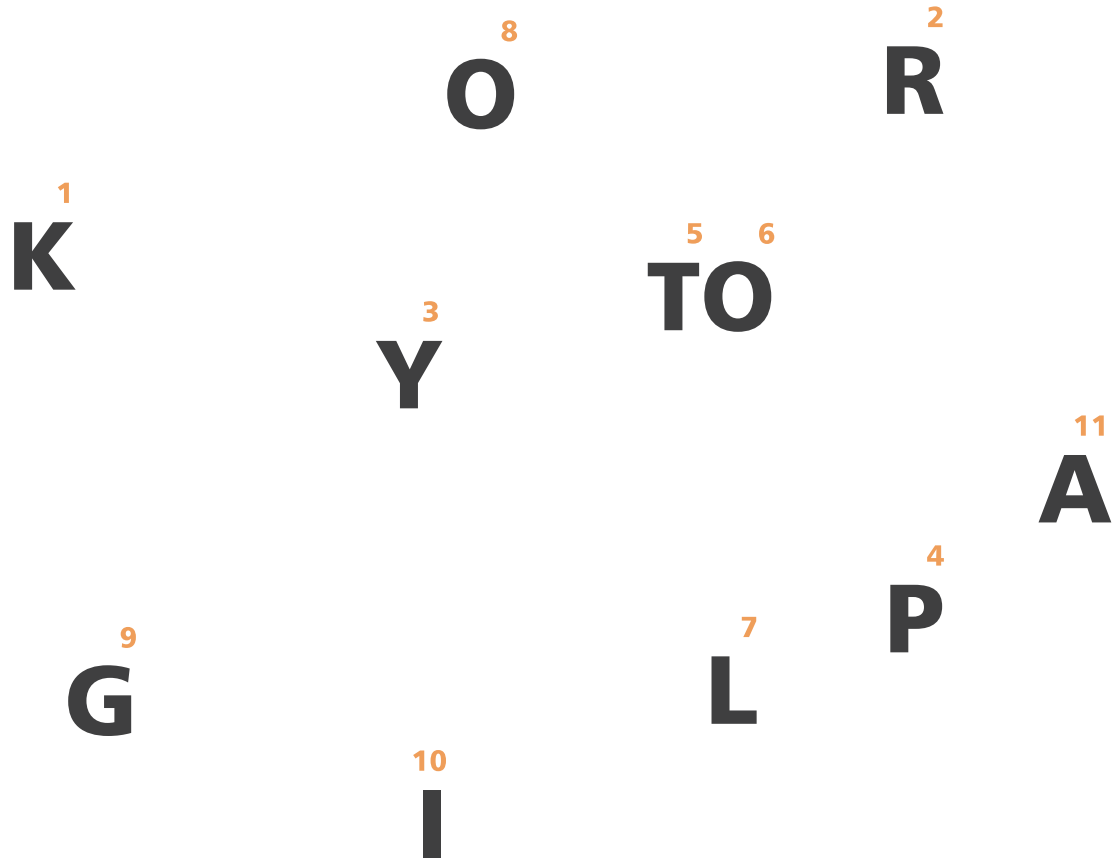
Jak widać, otrzymaliśmy z powrotem liczbę 25, która w tabeli jest numerem litery S. Klucz tajny RSA pozwoli nam na deszyfrację całego szyfrogramu:

$$D(51) = 51^{59} \pmod{91} = 25,$$
$$D(80) = 80^{59} \pmod{91} = 33,$$
$$D(37) = 37^{59} \pmod{91} = 32,$$
$$D(81) = 81^{59} \pmod{91} = 9,$$
$$D(19) = 19^{59} \pmod{91} = 24.$$

Widać, że wszystko się zgadza.

Na pewno niektórzy z Was zetknęli się już nieraz z systemem RSA, gdyż jest on podstawą konstrukcji tak zwanych certyfikatów elektronicznych, potwierdzających na przykład autentyczność niektórych stron internetowych. Jeżeli otwierałeś kiedyś strony za pomocą bezpiecznego protokołu internetowego (większość przeglądarek wyświetla wówczas ikonę zamkniętej kłódki), to na pewno z systemu RSA korzystałeś.

Czytelnicy, których niniejszy artykuł zainteresował, mogą przeczytać więcej na ten temat w bardzo przystępnie napisanej książeczce, będącej 19. tomikiem z serii „Miniatury Matematyczne", wydawanej przez Wydawnictwo „Aksjomat" z Torunia.



Claude Elwood Shannon

30.04.1916 – 24.02.2001

Amerykański matematyk i inżynier,
profesor MIT.
Jako jeden z pierwszych
pojął doniosłość kodu binarnego,
twierdząc, że da się nim opisać
tekst, obraz i dźwięk.
Jego najsłynniejsze dzieło to
„Matematyczna teoria komunikacji”
wydana w 1948 r.

Alan Mathison Turing

23.06.1912 – 7.06.1954

Angielski matematyk,
twórca maszyny Turinga,
jeden z ojców informatyki.
Na przełomie 1939 i 1940 r.
zaprojektował tzw. bombę Turinga
(częściowo w oparciu o prace
polskich kryptologów,
m.in. Mariana Rejewskiego),
urządzenie do łamania
kodu Enigmy.

Marian Adam Rejewski

16.08.1905 – 13.02.1980

Polski matematyk i kryptolog.
W 1932 r. złamał kod Enigmy,
najważniejszej maszyny szyfrującej,
używanej przez hitlerowskie Niemcy.
Autor „bomby kryptologicznej”,
skonstruowanej w 1938 r.
do odczytywania szyfrów Enigmy.