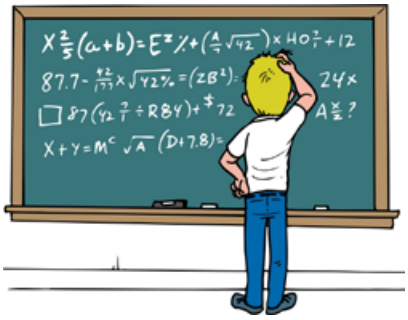

Niedostrzegalne i mniej efektowne niż kryptografia są ustandaryzowane kody bankowe i sklepowe (pomimo ich powszechności). A przecież są one jednym z filarów, na których opiera się współczesne społeczeństwo.

Będąc w sklepie i obserwując pracę kasjerki, widzimy, że tylko przesuwa ona towar nad czytnikiem i otrzymuje kwotę do zapłaty bez wielkiego wysiłku. Wystarczy jednak chwilę się zastanowić, aby stwierdzić, że dla kodów tam występujących priorytetem musi być jednoznaczność i precyzja w identyfikacji produktów.

A więc trochę opowieści na ten temat

Kody na co dzień
(czyli o matematyce życia codziennego)

Krystyna Nowicka
Centrum Nauczania Matematyki i Kształcenia na Odległość

Wstęp

Chcąc objaśnić kody kreskowe czy kody kart kredytowych, potrzebna jest znajomość kilku prostych faktów z matematyki. Właściwie jest to wiedza z tzw. arytmetyki modularnej i to też na poziomie liczb naturalnych.

Niech a, b, m będą liczbami naturalnymi. Piszemy $a = b \ (mod\ m)$ (czytamy a równa się b modulo m) jeżeli reszta z dzielenia a przez m wynosi b.

Można też stwierdzić, że $a = b \ (mod\ m)$ wtedy i tylko wtedy, gdy $a - b$ jest wielokrotnością m. I tak np. $127 = 7 \ (mod\ 12)$ $(a = 127, b = 7, m = 12)$ $a - b = 120 = 12 \cdot 10 = 10m$, $60 = 0 \ (mod\ 10)$ $(a = 60, b = 0, m = 1, a - b = 60 = 6 \cdot 10 = 6m)$. W dalszej części opisywanych kodów będzie zawsze $m = 10$.

Innym ważnym pojęciem jest kod liniowy *modulo m*.

Załóżmy, że kod zawiera n-cyfrowe słowo kodowe $a_1, a_2, \ldots, a_{n-1}, a_n$, (są to cyfry z systemu dziesiętnego, czyli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Ostania cyfra (tj. a_n) jest tzw. cyfrą kontrolną, a jej wartość jest ustalana tak, aby wyrażenie liniowe $w_1a_1 + w_2a_2 + \ldots + w_na_n$ dawało resztę b z dzielenia przez m dla odpowiednio ustalonych tzw. współczynników wagowych $w_1, w_2, \ldots, w_n$ (są to konkretne liczby dla danego kodu).

Pojęcie kodu liniowego *modulo m* jest dość często spotykane w kodowaniu.

W rozważanych tu kodach $m = 10$, zaś $b = 0$.

Niezbędne jest również pojęcie tzw. iloczynu zmodyfikowanego $x \circ y$ (x, y – liczby ze zbioru $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) i związanego z nim zmodyfikowanego kodu liniowego modulo m.

Iloczyn zmodyfikowany $x \circ y$ jest określony następująco: $x \circ y$ = suma cyfr z wyniku zwykłego iloczynu $x \cdot y$. I tak np. $2 \circ 3 = 6$, $1 \circ 5 = 5$, ale $2 \circ 5 = 1$, ponieważ $2 \cdot 5 = 10$, stąd $1 + 0 = 1$, podobnie $2 \circ 9 = 9$, $2 \cdot 9 = 18$, a stąd $1 + 8 = 9$.

Zmodyfikowany kod liniowy modulo m jest wyróżnieniem liniowym postaci $w_1 \circ a_1 + w_2 \circ a_2 + \ldots + w_{n-1} \circ a_{n-1} + w_n \circ a_n$, gdzie $w_1, w_2, \ldots, w_n$ – współczynniki wagowe, zaś $\circ$ – oznacza iloczyn zmodyfikowany.

Należy może podać jeszcze klika faktów historycznych. Karty kredytowe są kodowane w sposób zmodyfikowanego kodu liniowego. Metoda ta, zwana metodą Luhana, została opracowana przez grupę matematyków w 1960 r. Algorytm ten został nazwany na cześć Hansa Luhana – niemieckiego inżyniera, który wstępnie go opracował.

Pierwszy zaś system kodów kreskowych został opatentowany 7 października 1952 r. przez dwóch Amerykanów. Kody te były jednak inne od obecnie używanych.

Niemniej dało to możliwość dalszego rozwoju i pierwsze oficjalne użycie kodu kreskowego w sklepie miało miejsce w 1974 r. w Stanach Zjednoczonych.

Ogromne zaś zasługi w kodowaniu położył George J. Laurer – potomek niemieckich emigrantów, pracownik IBM.

W maju 1973 r. zaakceptowano jego projekt zwany UPC (Universal Product Code). Każdy produkt był w nim opisany 11-cyfrowym kodem, zakończony dodatkową cyfrą.

Po pewnym czasie dopisano na początku kodu jeszcze jedną cyfrę – kod kraju. Dzięki temu kod UPC nazwany w Europie EAN – 13 (European Article Number) rozpoczął swój triumfalny pochód przez świat.

Może jeszcze na jedną rzecz należy zwrócić uwagę. Aby komputer zrozumiał informację, musi być ona przetłumaczona w tzw. języku dwójkowym. Język ten składa się z 2 cyfr – 0 i 1 (to te paski na kodzie kreskowym). I tak np. liczba dziesiętna *9780* w zapisie dwójkowym wynosi *10011000110100*.

Karty kredytowe

Karty kredytowe są identyfikowane przez pewien ciąg liczb. Ich weryfikacji dokonuje się za pomocą algorytmu, który jest oparty na arytmetyce modularnej. Większość kart ma numer składający się z 16 cyfr dziesiętnych. Są one grupowane po cztery, aby ułatwić odczytywanie karty. Każda grupa czterech cyfr koduje pewną informację. Pierwsza odpowiada numerowi identyfikacyjnemu banku (lub innej jednostki, która tę kartę wydała). Piąta cyfra oznacza rodzaj karty i określa instytucję finansową, która zarządza kontem.

Kolejne 10 cyfr opisuje unikalny identyfikator dla każdej karty (np. rodzaj karty, dostępny limit, odsetki na koncie). Na końcu kodu znajduje się cyfra kontrolna, która jest wyznaczona na podstawie poprzednich cyfr zgodnie z algorytmem Luhana. W metodzie tej używa się zmodyfikowanego kodu liniowego modulo 10 o współczynnikach wagowych równych 2 dla wyrazów nieparzystych i 1 dla wyrazów parzystych.

Stąd karta kredytowa jest poprawnie zakodowana, jeżeli wyrażenie $2 \circ a_1 + a_2 + 2 \circ a_3 + a_4 + 2 \circ a_5 + a_6 + 2 \circ a_7 + a_8 + 2 \circ a_9 + a_{10} + 2 \circ a_{11} + a_{12} + 2 \circ a_{13} + a_{14} + 2 \circ a_{15} + a_{16}$ jest podzielone przez 10 bez reszty (tu $\circ$ oznacza zmodyfikowany iloczyn).

Dla przykładu weźmy kartę o numerze *1234567890123452*

(tu $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, $a_5 = 5$, $a_6 = 6$, $a_7 = 7$, $a_8 = 8$, $a_9 = 9$, $a_{10} = 0$, $a_{11} = 1$, $a_{12} = 2$, $a_{13} = 3$, $a_{14} = 4$, $a_{15} = 5$, $a_{16} = 2$). Postępując zgodnie z algorytmem Luhana mamy $2 \circ 1 + 2 + 2 \circ 3 + 4 + 2 \circ 5 + 6 + 2 \circ 7 + 8 + 2 \circ 9 + 0 + 2 \circ 1 + 2 + 2 \circ 3 + 4 + 2 \circ 5 + 2 = 60$.

Wynikiem jest *60*, co jest wielokrotnością *10*.

Tak więc powyższy numer karty jest poprawny. Jak widać pozornie losowe cyfry na karcie kredytowej podlegają ścisłym matematycznym zasadom, co więcej, jeżeli wiadomo, że mamy do czynienia z prawidłowym numerem karty kredytowej i zapomnieliśmy jedną cyfrę, to stosując ten algorytm można ją odzyskać. I tak na przykład mając *4539 4512 03X8 7356* gdzie *X* – zapomniana cyfra, to stosując metodę Luhana można wyliczyć, że $X = 9$, czyli pełny numer karty kredytowej to *4539 4512 0398 7356*.

Kody kreskowe

Współczesne kody kreskowe składają się z czarnych pasków, które odpowiadają jedynkom i białych przerw między nimi (które odpowiadają zerom). Są one zwykle wydrukowane na etykietach, z których są odczytywane przez urządzenia optyczne.

Istnieje wiele standardowych kodów kreskowych. Jednak najbardziej jest rozpowszechniona 13-cyfrowa wersja kodu EAN. Pozwala on na szybkie zidentyfikowanie dowolnego produktu. Kod kreskowy EAN-13 składa się z 13 cyfr reprezentowanych za pomocą 30 czarnych pasków i białych odstępów, które wspólnie tworzą do odczytania kod dwójkowy.

Cyfry są rozmieszczone w 3 grupach. Pierwsza grupa składa się z 2 lub 3 cyfr i oznacza kod kraju (np. kod Polski to *590*, zaś Wielkiej Brytanii *50*), zaś druga składa się z 9 lub 10 cyfr i identyfikuje producenta i produkt. Trzecia grupa jednocyfrowa, to kod kontrolny.

W celu stwierdzenia poprawności kodu używa się kodu liniowego modulo 10 o zerowej reszcie i współczynnikach wagowych 1 dla wyrazów nieparzystych i 3 dla wyrazów parzystych, tj. $a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13}$.

Dla przykładu, sprawdźmy, czy kod kreskowy na szkatułce, którą kupiłam reprezentowany przez cyfry *5901162215163* jest poprawny

$5 + 3 \cdot 9 + 0 + 3 \cdot 1 + 1 + 3 \cdot 6 + 2 + 3 \cdot 2 + 1 + 3 \cdot 5 + 1 + 3 \cdot 6 + 3 = 100 = 10 \cdot 10$

Wniosek: kod jest poprawny.

Spróbujmy jeszcze ustalić wartość nieczytelnej cyfry w kodzie kreskowym (jest nią X).

4013 3200 03X497

Stosując wspomniany algorytm mamy

$64 + 3X = 0 \ (mod\ 10)$

Stad można wyznaczyć $X = 6$

4013 3200 036497

Inne

Klasyfikację czasopism umożliwia kod ISSN (International Standard Serial Numbers), zaś odpowiednikiem kodu dla książek jest ISBN (International Standard Book Number).

Każdy obywatel Polski ma nadany kod PESEL. Jest to 11-cyfrowy kod liniowy modulo 10 ze współczynnikami wagowymi *1,3,7,9,1,3,7,9,1,3,1* oraz resztą z dzielenia równą 0. Pierwszych sześć cyfr w tym kodzie, to data urodzin w układzie rok – miesiąc – dzień. Jeżeli ktoś urodził się już w XXI wieku, to liczba miesiąca jest powiększona o 20 (styczeń 21, luty 22, …, grudzień 32). Kolejne cztery cyfry pozwalają odróżnić ludzi

urodzonych tego samego dnia. Czwarta z nich dodatkowo oznacza płeć (nieparzysta – mężczyzna, parzysta – kobieta). Ostania cyfra w kodzie to cyfra kontrolna.

Współczynniki wagowe i podstawa *modulo* dla kodów NIP-u czy REGON-u są tajne i należałoby się zwrócić do GUS-u z prośbą o udostępnienie ich.

Jednak ambitni informatycy mogą doświadczalnie, próbując różne wagi i podstawy modulo, odtworzyć te prawidłowe. I tak oto przyszło nam stwierdzić, że w świecie, w którym żyjemy pełno jest kodów i liczb.

P.S.

Przypomniał też mi się protest mojego studenta (gdy rozmawialiśmy na ten temat), że nie chce on być żadnym PESEL, NIP czy jeszcze innym numerem identyfikacyjnym. On po prostu chce być, powiedzmy, Janem Kowalskim.

Być sobą w ciągłym poszukiwaniu Wywiad z prof. Anielą Kitą cz. 1

Danuta Siemińska
Klub Seniora

Jakie były powody decyzji Pani Profesor, aby po ukończeniu szkoły podstawowej podjąć naukę w Państwowym Liceum Technik Plastycznych w Gdyni Orłowie?
O, to nie było tak od razu, ponieważ zupełnie nie wiedziałam, kim chciałabym być w przyszłości. Wprawdzie nauczyciele namawiali mnie, bym poszła do Liceum Pedagogicznego w Wejherowie, ale ja odpowiadałam, że nigdy w życiu nie będę nauczycielem (sic!). Namówiona przez koleżankę złożyłam papiery do Technikum Poligraficznego w Sopocie. Ponieważ w szkole podstawowej wszystkie prace artystyczne mnie powierzano, uznałam, że to dobry wybór. Zawsze lubiłam malować. Fascynował mnie kolor. Pomyślnie zdałam egzamin wstępny z mocnym, jak na czternastolatkę przystało, postanowieniem, że zostanę drukarzem i będę drukować kolorowe książki! W szkole bardzo mi się podobało, ale cotygodniowe praktyki w drukarni tak dalece wpłynęły na moje zdrowie (kontakt z ołowiem), że zgodnie z zaleceniami lekarzy, mowy być nie mogło o kontynuowaniu nauki. Mimo usilnych nalegań dyrektora szkoły, że szkoda, bo taka dobra uczennica, posłuchałam lekarzy i zrezygnowałam.

Zadowolona licealistka na plenerze malarskim w Charzykowach, Kaszuby 1956 r.

Ponownie znalazła się Pani w punkcie wyjścia.
No tak. Miałam piętnaście lat, były wakacje, a ja z rozterką w sercu co ze sobą zrobić? Szczęśliwym dla mnie (jak się później okazało) zbiegiem okoliczności, w moim kościele parafialnym pw. św. Wawrzyńca w Gdyni Wielkim Kacku trwały prace nad artystycznym wystrojem wnętrz, których wykonawcą był wszechstronnie utalentowany, pochodzący z Wilna malarz i rzeźbiarz pan Waldemar Kaczyński. Z powodów politycznych został w 1952 roku pozbawiony wolności. Proboszcz zwrócił się zatem do Kazimierza Ostrowskiego. Tak, tego słynnego „Kacha", który przygotował piękne, rysowane węglem kartony, obrazujące życie św. Wawrzyńca. Pokazane publicznie bardzo się wszystkim podobały – mnie również. Przychodziłam prawie codziennie, by z zachwytem patrzeć, jak ten artysta pracuje. Aż pewnego dnia zapytał mnie: „No, co mała, podoba Ci się? A może chciałabyś spróbować? Z wrażenia zaniemówiłam i tylko kiwnęłam potakująco głową. Szybko na ścianie