UVOD

Kako matematički objasniti, odnosno prikazati označavanje proizvoda pomoću grafičkog prikaza?
Problem se sastoji u jednoznačnom označavanju svakog proizvoda, tj. njegove interpretacije.

Da bismo to pobliže objasnili potrebna nam je pomoć teorije brojeva.
Jedan od najvažnijih alata u elementarnoj teoriji brojeva jest MODULARNA ARITMETIKA tj, kongruencija. Jezik kongruencije razvio je Carl Friedrich Gauss, početkom 19.st. u djelu "DISQUISITIONES ARITMETICAE" ("ARITMETIČKA ISTRAŽIVANJA").

- Primjer 1
  Sat radi ili modulo 12 ili modulo 24, zatim imamo modulo 60 za minute i sekunde.

KONGRUENCIJA

Pretpostavimo da su brojevi *a, b, n* cijeli brojevi $(n \neq 0)$, tad kažemo da je *a* kongruentan *b* po modulu *n*, ako *n* dijeli *a-b*, s tim da je kvadrat svakog neparnog broja 1 modulo 8

- Primjer 2 $6 \equiv 2 (\mathrm{mod}\, 4), 9 \equiv 1 (\mathrm{mod}\, 8),$

Uvjet : $a \equiv b (\mathrm{mod}\, n)$ ako i samo ako postoji cijeli broj *q*, takav da je $a = b + qn$. Dakle, kongruenciju možemo prevesti kao jednadžbu s jednom nepoznanicom.

Svojstva :
1. Refleksivnost : Ako je *a* cijeli broj $a \equiv a (\mathrm{mod}\, n)$
2. Simetričnost : Ako je $a \equiv b (\mathrm{mod}\, n)$, tada je $b = a (\mathrm{mod}\, n)$
3. Tranzitivnost : Ako je $a \equiv b (\mathrm{mod}\, n)$ i $b \equiv c (\mathrm{mod}\, n)$, tada je $a \equiv c (\mathrm{mod}\, n)$

{ Izvedena svojstva i njihove dokaze potrazite u knjizi Darka Zubrinica Diskretna matematika, Element, Zagreb, 1997 ili na www.numbertheory.freeservers.com }

UNIVERSAL PRODUCT CODE (UPC)

Univerzalni proizvedni kod primjenjuje se u svijetu od 1972 godine. Kontrolne brojke, odnosno njihov grafički prikaz od velike su važnosti za današnju trgovinu. Pristuni su u banci, trgovini, prometu…
Velika većina proizvoda današnjice može se jednoznačno odrediti brojem nazvanim UPC. UPC je način prikazivanja broja s kombinacijom crno-cijelih vertikalnih linija različitih debljina. Zbog očitih razloga UPC je popularno nazvan Bar Code (eng. bars – rešetke).
UPC o kojem je ovdije riječ, sastoji se od 12 znamenki u obliku:

X – X X X X X – X X X X X - X , gdje su X-evi iz skupa {0,1,….,9}

Posljednja znamenka je kontrolna znamenka koja govori o ispravnosti predhodnih, a prva se koristi kod oznaka koda UPC.

{ Kod UPC sustava, kad se radi o broju proizvođača, ne rabe se slijedeće skupine brojeva
- brojevi koji počinju s više od dvije nule u nizu, tj. brojevi od 00000 do 00099
- brojevi od 01000 koji su rezervirani za LOCAL ASSINGED CODE }

- Primjer 3 0 – 67235 – 53276 – 8

Kontrolna brojka određena je pravilom:
3 (suma brojeva na neparnim pozicijama) + (suma brojeva na parnim pozicijama) $\equiv 0 \pmod{10}$

$$3*(0+7+3+5+2+6)+6+2+5+3+7 \equiv 0 \pmod{10}$$

$$69+23 \equiv 0 \pmod{10}$$

$$92 \equiv 0 \pmod{10} \qquad 10-2 = 8$$

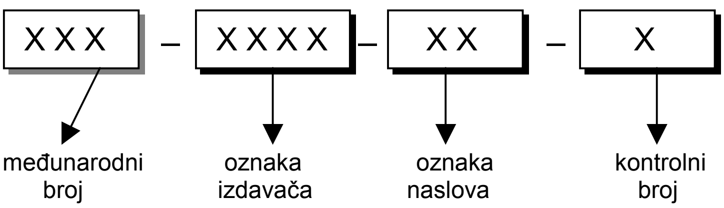
2

Za grafički prikaz brojeva preko UPC, možete pogledati Andrija Šijak:“PRUGASTI KOD, OD PROJEKTA DO PRIMJENE”, INFO CENTAR, ZAGREB 1997

INTERNATIONAL STANDARD BOOK NUMBER (ISBN)

Od 1968.g., večini knjiga dodijeljen je desetoznamenkasti broj nazva ISBN, koji jednoznačno identificira zemlju izdavača, izdavača i naslov knjige, odnosno publikacije. Ustvari sve bitne informacije sadržane su u prvih 9 znamenki, dok deseta služi za provjeru predhodnih brojeva.

$$1 * a_1 + 2 * a_2 + 3 * a_3 + \ldots + 9*a_9 + 10 * a_{10} \equiv 0 \pmod{11}$$



ISBN se dodjeljuje publikacijama pod kontrolom Međunarodnog ureda za ISBN sa sjedištem u Berlinu, a u Republici Hrvatskoj ga dodjeljue Hrvatski ured za ISBN (npr. međunarodni broj Republike Hrvatske je 953).

- Primjer 4 953 – 6071 – 14 – 2

$$X=10*a_{10}$$

$$1 * 9 + 2 * 5 + 3 * 3 + 4 * 6 + 5 * 0 + 6 * 7 + 7 * 1 + 8 * 1 + 9 * 4 + X \equiv 0 \pmod{11}$$

$$145 \equiv X \pmod{11}$$

$$145:11=13$$

2

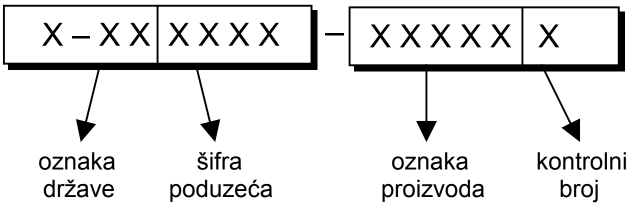
x=2

EUROPEAN ARTICLE NUMBERING (EAN)

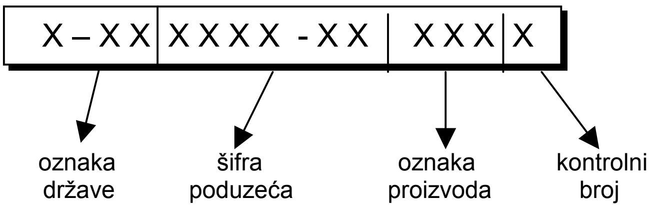
Godine 1974. Proizvođači i trgovci iz europskih zemalja sastali su se sa zadaćom da se ispita mogućnost razvoja jedinstvenog sustava označavanja proizvoda, a nekoliko godina kasnije, tj. 1977.g. osnovano je i udruženje EAN sa sjedištem u Bruxellesu. Tada je potpisan sporazum o njegovom formiranju sa ciljem da djeluje kao neprofitna međunarodna organizacija. Organizacija se brzo širila a 1981.g. promjenila je ime u IANA EAN (INTERNATIONAL ARTICLE NUMBERING ASSOCIATION EAN).

<u>Kod EAN je prilagođen UPC-u.</u>

(za 100 000 proizvoda)



(za 1000 proizvoda)



(suma brojeva na neparnim pozicijama) + 3 * (suma brojeva na parnim pozicijama) $\equiv$ 0(mod10)

- Prmjer 5 3 – 850146 – 011111

$$3 + 5 + 1 + 6 + 1 + 1 + X + 3 * (8 + 0 + 4 + 0 + 1 + 1) \equiv 0(\text{mod}10)$$

$$X + 59 \equiv 0(\text{mod}10)$$

$$59=(10-X) (\text{mod}10)$$

59 :10 = 5
9

X – ostatak pri cijelobrojnom dijeljenju
10-X – kontrolni broj

<u>X=1</u>

Napomena:

Iz dosad viđenog, da se primjetiti da ovi testovi s kongruencijom detektiraju greške u kodu, temeljem kontrolnog broja. S druge strane, moguća je greška koju nemožemo primjetiti u kontrolnom broju (ako dvije brojke ponište razliku u ulogama koda).

OSTALE PRIMJENE KONGRUENCIJE

Kongruencija postoji od oko 350.g., odakle seže kineskii teorem ostatka, čiju primjenu nalazimo, između ostalog, u određivanju brojeva po njihovom ostatku i kriptografiji.

KRIPTOGRAFIJA

Želimo li nekim javnim telekomunikacijskim kanalom poslati poruku, datoteku, sliku ili neki drugi elektronski materijal, a tajnost nam je od važnosti, koristit ćemo neki oblik kriptografije. Kriptografija se razvila iz potrebe za razmjenom tajnih poruka koje su uvijek prisutne u diplomatskom i vojnom dijelokrugu. Kriptografija je strogo čuvana nauka koja obuhvača kriptografiju i kriptoanalizu. Kriptografija je nauka o šifriranju, a kriptoanaliza je nauka koja se bavi dešifriranjem. Cilj kriptografije je da poruka bude nerazumljiva "uljezima". Povijest kriptografije seže do Julija Cezara ali s današnjeg gledišta, te su nam metode "primitivne".

- Primjer 6

Danas je jedan od najsigurnijih načina šifriranja RSA kriptosustav. RSA su razvili 1978.g. na MIT-u Rivest, Shamir i Adleman, a sam algoritam se temelji upravo na kongruenciji. To je asimetričan sustav, tj. koristi se tajni i javni ključ. Princip se zasniva na funkciji koja se lako računa, a izračunavanje njene inverzne funkcije je gotovo neizvedivo.

Princip rada:

1. Odaberu se prosti brojevi P i Q, koji su dio tajnog ključa. Izračuna se N = P*Q i L=(P-1)*(Q-1).
2. Odaberu se (ili se izračunaju) brojevi d i e tako da vrijedi:
   nzm (P, Q) < d < L (nzm - najveća zajednička mjera)
   $0<e<L$
   $e * d \equiv 1 (\text{mod } L)$, što je isto kao da odredimo najmanji k za koji vrijedi $e * d = k * L + 1$
3. Par (N, e) se objave kao javni ključ.
4. Šifriranje se izvodi tako da je $M^e \equiv C$ (mod N), pri čemu je M broj koji se šifrira, a C broj koji se dobije šifriranjem.
5. Dešifriranje se izvodi tako da je $C^d \equiv M$ (mod N).

Napomena: $0 \leq M < N$

- Primjer 6.1

P = 11, Q=13 $\Rightarrow$ N = P * Q = 143, L = (P – 1) * (Q – 1) = 10 * 12 = 120
$e * d = k * L + 1$, za k = 4 odabire se e = 37 i d=13.
Slovo koje je predstavljeno kao broj 47 (ASCII "/") nakon šifriranja bit će zamijenjeno slovom koje predstavlja broj 86 (ASCII "V"), $47^{37} \equiv 86$ (mod143).
Isto tako će dešifriranjem broj 86 biti zamijenjen s 47 ($86^{13} \equiv 47$(mod143)).

ZAKLJUČAK

Naučili smo da jedna matematička metoda poput kongruencije može imati nebrojeno mnogo korisnih primjena u današnjem svijetu. Mnogi matematiku tretiraju kao dosadnu i bespotrebnu znanost, ali ona to, zapravo nije. Može postati takva uz nerazumjevanje i bez želje za znanjem. Napokon, gdje bismo danas bili bez nje?! Ako samo jedna metoda ima toliko primjena, što je sa matematikom općenito? Matematika je ograničavajuća samo u ograničenom umu. Nadalje spoznali smo da zajednički rad, proučavanje, učenje, obogačuje znanjem i spoznajama sve pojedince u grupi. Možda bi otišli tako daleko i matematiku uvrstili u jednu od najbitnijih znanosti, jer ona i jest jedna od znanosti koja bitno označava današnje društvo.

Popis Literature:

- Darko Žubrinić “Diskretna matematika”, Element, Zagreb, 1997.

- Andrija Šijak “Prugasti kod, od projekta do primjene”, Info Centar, Zagreb 1997

- www.numbertheory.freeservers.com

- E.G. Godaire, M.M. Parmeter: “Discrete mathematics with graph theory”