zadarska smotra 3–4, 2016.

STUDIJE, RASPRAVE, ESEJI

Andrej Dujella

# Teorija brojeva i šifriranje

## Uvod

Teorija brojeva jedna je od najstarijih grana matematike. Važne su joj doprinose dali starogrčki matematičari Diofant i Euklid, a kasnije i neki od najznačajnijih matematičara u povijesti, poput Eulera i Gaussa. Međutim, tijekom te duge povijesti uvijek se smatrala dijelom "čiste" (teorijske) matematike i nije se očekivalo da bi od nje moglo biti nekih konkretnih primjena. Ni autor ovoga priloga, kad se, najprije kao učenik Osnovne škole *Novigrad*, a potom Osnovne škole *Stanovi* i Srednje škole *Juraj Baraković* u Zadru, počeo zanimati za matematiku i posebice teoriju brojeva, nije puno razmišljao o mogućim primjenama. Međutim, od sredine 70-ih godina 20. stoljeća dolazi do bitne promjene, tako da je danas teorija brojeva jedna od najvažnijih grana matematike za primjenu u kriptografiji (šifriranju) i sigurnoj razmjeni informacija. O ovoj temi nedavno sam održao predavanje najprije na znanstvenom skupu "Novigrad nekad i sad", a potom na Sveučilištu u Zadru kao dio serije predavanja nadarenim učenicima. Pokušat ću u ovom prilogu objasniti kako je teorija brojeva našla primjenu u kriptografiji, ali bez ulaženja u zahtjevnije matematičke detalje.

## Vrlo kratki uvod u teoriju brojeva

Teorija brojeva grana je matematike koja se prvenstveno bavi proučavanjem svojstava cijelih brojeva kao što su djeljivost, rastavljanje brojeva na proste faktore ili rješivost jednadžbi u cijelim brojevima. U ovom prilogu ograničit ćemo se na kratak prikaz nekoliko izabranih tema, s posebnim naglaskom na teme relevantne za primjenu u kriptografiji te na teme koje su u središtu interesa autora ovoga priloga (a i hrvatske istraživačke grupe iz teorije brojeva).

Pojam djeljivosti jedan je od najjednostavnijih, ali ujedno i najvažnijih pojmova u teoriji brojeva. Neka su $a$ i $b$ cijeli brojevi ($a \neq 0$). Kažemo da je $b$ djeljiv s $a$, odnosno da $a$ dijeli $b$, ako postoji cijeli broj $x$ takav da je $b = ax$. To zapisujemo sa $a|b$. Još kažemo da je $a$ dje-

Andrej Dujella

litelj od $b$, odnosno da je $b$ višekratnik od $a$. Ako su $a$ i $b$ cijeli brojevi od kojih je barem jedan različit od nule, onda postoji konačno mnogo njihovih zajedničkih djelitelja. Najveći među njima naziva se najveći zajednički djelitelj broja $a$ i $b$ te se označava s "nzd ($a$,$b$)". Ako je nzd($a$,$b$) = 1, onda kažemo da su brojevi $a$ i $b$ relativno prosti. Važna je činjenica (pogotovo za primjene) da se nzd($a$,$b$) može efikasno izračunati pomoću Euklidova algoritma. Štoviše, Euklidov algoritam daje nam i cijele brojeve $x$ i $y$ sa svojstvom da je $ax + by$ = nzd($a$,$b$).

Prirodan broj $p > 1$ jest prost ako $p$ nema niti jednoga djelitelja $d$ takvoga da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen. Već je starogrčki matematičar Euklid znao da prostih brojeva ima beskonačno mnogo. No, nije poznata niti jedna praktična formula koja bi producirala proste brojeve, što problem nalaženja velikih prostih brojeva čini teškim i zanimljivim. Trenutno je najveći poznati prosti broj $2^{74207281} - 1$ (ima 22 338 618 znamenaka), koji je pronađen 7. siječnja 2016.

Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je $a$ kongruentan $b$ modulo $m$ i pišemo $a \equiv b \pmod{m}$. Od brojnih važnih svojstava kongruencija, spomenimo ovdje samo Eulerov teorem, koji kaže da je $a^{\varphi(m)} \equiv 1 \pmod{m}$ za relativno proste brojeva $a$ i $m$ (ovdje je $\varphi(m)$ broj brojeva u nizu 1, 2, ..., $m$ koji su relativno prosti s $m$; $\varphi$ se naziva Eulerova funkcija). Direktna posljedica ovoga rezultata jest Mali Fermatov teorem, koji kaže da za svaki prost broj $p$ i svaki cijeli broj $a$ vrijedi kongruencija $a^p \equiv a \pmod{p}$ i predstavlja osnovu za većinu suvremenih metoda za testiranje i dokazivanje prostosti velikih brojeva.

Diofantske jednadžbe jesu jednadžbe u kojima rješenja tražimo u skupu cijelih brojeva. Jedna od povijesno najpoznatijih diofantskih jednadžbi jest Pitagorina jednadžba $x^2 + y^2 = z^2$, čija se rješenja nazivaju Pitagorine trojke, a predstavljaju katete i hipotenuzu pravokutnoga trokuta. Poznato je da Pitagorinih trojki ($x$, $y$, $z$) ima beskonačno mnogo, a neke su od njih (3, 4, 5), (6, 8, 10) i (5, 12, 13). Spomenimo i jedan diofantski problem koji ima vrlo dugu povijest (njime se bavio već starogrčki matematičar Diofant, po kojem je cijelo ovo područje matematike dobilo ime), a koji je predmet intenzivnoga istraživanja hrvatske grupe iz teorije brojeva. Skup od $m$ cijelih brojeva različitih od nule naziva se *Diofantova m-torka* ako umnožak svaka dva njihova različita elementa uvećan za 1 daje kvadrat. Ako su elementi skupa s istim svojstvom racionalni brojevi, onda takav skup nazivamo *racionalna Diofantova m-torka*. Primjerice, skup {1, 3, 8, 120} jedna je Diofantova četvorka (pronašao ga je Fermat). Zaista, $1 \cdot 3 + 1 = 2^2$, $1 \cdot 8 + 1 = 3^2$, $1 \cdot 120 + 1 = 11^2$, $3 \cdot 8 + 1 = 5^2$, $3 \cdot 120 + 1 = 19^2$, $8 \cdot 120 + 1 = 31^2$. Prirodno se nameće pitanje koliko veliki mogu biti skupovi s ovim svojstvom. U slučaju Diofantovih $m$-torki čiji su članovi cijeli brojevi (različiti od nule) na ovo je pitanje gotovo u potpunosti odgovoreno. Naime, poznato je (Dujella 2004) da ne postoji Diofantova šestorka te da postoji najviše konačno mnogo takvih petorki (slutnja je da nema petorki). Međutim,

u slučaju racionalnih Diofantovih *m*-torki nije poznata nikakva gornja ograda za njihovu duljinu. Prvi primjer racionalne Diofantove četvorke pronašao je sam Diofant: {1/16, 33/16, 17/3, 105/16}. Euler je pokazao da postoji beskonačno racionalnih Diofantovih petorki. Problem postojanja racionalnih Diofantovih šestorki ostao je otvoren nekoliko stoljeća. Prvu takvu šestorku našao je Gibbs 1999., a nedavno je dokazano da racionalnih Diofantovih šestorki ima beskonačno mnogo (Dujella, Kazalicki, Mikić, Szikszai 2016).

## Iz povijesti kriptografije

Ljudi su od davnina željeli sigurno komunicirati, ali bili su svjesni da njihove poruke često putuju nesigurnim komunikacijskim kanalima. Tijekom stoljeća načini su se prenošenja poruka uvelike mijenjali, ali je osnovni problem ostao isti: kako onemogućiti onoga tko može nadzirati kanal kojim se prenosi poruka da dozna njezin sadržaj? Načinima rješavanja ovoga problema bavi se znanstvena disciplina koja se naziva kriptografija. Sama riječ kriptografija grčkoga je podrijetla i mogla bi se doslovno prevesti kao *tajnopis*. U prošlosti je kriptografija često odlučivala ishode bitaka te sudbine špijuna i urotnika, a danas, uz i dalje važnu vojnu i diplomatsku komponentu, ima vrlo važnu ulogu u sigurnosti internetskih komunikacija i transakcija te je time postala zanimljivom puno širem krugu ljudi.

Metode koje su se u prošlosti najčešće koristile za šifriranje poruka bile su zamjena (supstitucija) i premještanje (transpozicija) osnovnih elemenata teksta (slova, blokova slova, bitova).

Neki elementi kriptografije bili su prisutni već kod starih Grka. Tako su Spartanci u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu *skital*. To je bio drveni štap oko kojega se namotavala vrpca od pergamenta, pa se na nju okomito pisala poruka. Nakon upisivanja poruke vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.

Znameniti rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenoga teksta zamjenjivala slovima što su se nalazila tri mjesta dalje od njih u abecedi (A → D, B → E itd.). Pretpostavljamo da se abeceda ciklički nastavlja, tj. da nakon zadnjega slova Z ponovno dolaze A, B, C. Ako bismo upotrijebili današnju međunarodnu abecedu od 26 slova, onda bi JADER bilo šifrirano kao MDGHU.

Francuski diplomat Blaise de Vigenère 1586. godine objavio je knjigu *Traicte de Chiffres*, u kojoj se nalazilo sve što se u to vrijeme znalo o kriptografiji. U njoj je opisano više originalnih polialfabetskih sustava. Sustav koji se danas naziva Vigenèreova šifra definiran je na sljedeći način. Ključna riječ sastoji se od $m$ brojeva $k_1, k_2, \ldots, k_m$. Prvo slovo u tekstu pomiče se za $k_1$ mjesta u alfabetu, drugo za $k_2$, ..., $m$-to za $k_m$ mjesta, pa ($m$+1)-vo slovo ponovno za $k_1$ mjesta itd. Primjerice, otvoreni tekst ZADARSKA SMOTRA pomoću ključne riječi 5, 8, 4, 9, 5 bio bi šifriran kao HEMFZWTF AQXYZE. Vigenèreova šifra znatno je sigurnija od Cezarove, ponajprije zbog velikoga broja mogućih ključeva, a potom i zbog toga što se identična slova u otvorenom tekstu, ovisno o položaju u tekstu, šifriraju na različite načine te se time sprje-

čavaju napadi koji koriste poznate činjenice o frekvenciji slova u jeziku otvorenoga teksta (primjerice, u hrvatskom jeziku najfrekventija su slova A, I, O, E, N). Stoga je nekoliko stoljeća bila najpopularnija šifra te je korištena u važnim povijesnim događajima, poput Američkoga građanskog rata.

Njemački pronalazač Artur Scherbius 1918. godine izumio je napravu za šifriranje koju je nazvao *ENIGMA*. Do masovne uporabe ENIGME došlo je neposredno prije i za vrijeme Drugoga svjetskog rata. Razbijanje njezine šifre (kombinacijom kriptoanalize i klasične špijunaže) imalo je važnu ulogu za tijek i ishod Drugoga svjetskog rata. ENIGMA je bila elektromehanička naprava koja se sastojala od tipkovnice s 26 tipki poput pisaćega stroja, zaslona s 26 žaruljica za prikaz šifriranoga izlaza, tri mehanička *rotora* (*šifrarnika*) i električne prespojne ploče. U standardnoj verziji s 10 prespojnih kabela pružala je golemi broj od 150 738 274 937 250 mogućih kombinacija te je napad ispitivanjem svih mogućih kombinacija bio nemoguć. Pa ipak, dvije grupe matematičara kriptoanalitičara uspjele su pronaći način za dekriptiranje ENIGME. Bile su to poljska grupa, koju je predvodio Marian Rejewski, te britanska grupa, koju je predvodio Alan Turing. Kao i kod svih klasičnih šifara, veliki problem predstavljala je razmjena ključeva. Svaki mjesec operateri ENIGME dobili bi novu knjigu s ključevima koja je specificirala koji se ključ rabi koji dan. Što se tiče orijentacije rotora, svaki rotor imao je alfabet ugraviran na vanjskom omotaču, pa bi operater rotirao rotor sve dok se na vrhu ne bi pojavila slova specificirana u dnevnom ključu. Svaki dan vrijedila je druga šifra, no budući da se dnevno šifrirao golemi broj poruka, bilo je potrebno nekako postići da se sve ne šifriraju doslovno istim ključem jer bi to znatno smanjilo sigurnost. Stoga su Nijemci uveli distribuciju "ključa za poruku" pomoću dnevnoga ključa. Poljski su kriptoanalitičari predvođeni Rejewskim uspjeli iskoristiti protokol koji se pritom koristio (za koji su prethodno saznali Francuzi metodama klasične špijunaže) za kriptoanalitički napad (više vidi u Čavrak 2004 i Dujella, Maretić 2007).

Spomenimo da se neke informacije o povijesti kriptografije u Hrvatskoj mogu naći u Kapitanović 2012. Tako se navodi djelo *Cryptographia nova seu Ars cryptographica noviter inventa* (Nova kriptografija ili nedavno izmišljena kriptografska vještina), objavljeno 1732. godine, koje se pripisuje hrvatskom latinistu Ivanu Krstitelju Prusu.

## Kriptografija javnoga ključa

Asimetrični kriptosustavi ili kriptosustavi s javnim ključem pojavili su se tek 70-ih godina 20. stoljeća. Kod njih se za šifriranje koriste funkcije koje su "jednosmjerne" (one se računaju lako, ali njihov inverz vrlo teško). To znači da funkcija za šifriranje može biti javna, dok samo funkcija za dešifriranje mora biti tajna. Time se rješava glavni problem klasične kriptografije, a to je sigurna razmjena ključeva. Naime, polazna pretpostavka u kriptografiji jest da imamo dvije strane koje ne mogu sigurno razmijeniti poruke (jer netko nadgleda komunikacijski kanal preko kojega komuniciraju), a od njih se traži da sigurno razmijene ključ. Taj se problem pokušavao riješiti na različite načine, ali često su (kao u slučaju ENIGME) rješenja bila bitno nekvalitetnija od same šifre. U konstrukciji jednosmjernih funkcija koriste se "teški" mate-

matički problemi, koji uglavnom potječu iz algoritamske teorije brojeva, poput faktorizacije velikih prirodnih brojeva ili logaritmiranja u nekim konačnim grupama (glavni su primjeri multiplikativna grupa konačnoga polja i grupa točaka na eliptičkoj krivulji nad konačnim poljem).

Godine 1976. Whitfield Diffie i Martin Hellman ponudili su jedno moguće rješenje problema razmjene ključeva, zasnovano na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. Pretpostavimo da se dvije osobe (nazovimo ih Ana i Branko; u engleskoj literaturi obično se koriste imena Alice i Bob) žele dogovoriti o jednom tajnom slučajnom elementu u cikličkoj grupi $G$ koji bi onda poslije mogli koristi kao ključ za šifriranje u nekom simetričnom kriptosustavu. Oni taj svoj dogovor moraju provesti preko nekoga nesigurnog komunikacijskog kanala koji prisluškuje treća osoba (nazovimo ju Eva), a da prethodno nisu razmijenili bilo kakvu informaciju. Jedina informacija koju imaju jest grupa $G$ i njezin generator $g$.

1. Ana generira slučajan prirodan broj $a$ iz $\{1, 2, \dots, |G| - 1\}$. Ona pošalje Branku element $g^a$.
2. Branko generira slučajan prirodan broj $b$ iz $\{1, 2, \dots, |G| - 1\}$ te pošalje Ani element $g^b$.
3. Ana izračuna $(g^b)^a = g^{ab}$.
4. Branko izračuna $(g^a)^b = g^{ab}$.

Sada je Anin i Brankov tajni ključ $K = g^{ab}$.

Dakle, na kraju komunikacije Ana i Branko uspjeli su razmijeniti podatak $K$ koji niti u jednome trenutku nije prenesen preko njihova nesigurnog komunikacijskog kanala. Eva prisluškivanjem njihove komunikacije preko nesigurnoga komunikacijskog kanala može saznati $G$, $g$, $g^a$, $g^b$ te treba iz ovih podataka izračunati $g^{ab}$. Ako iz poznavanja $g$ i $g^a$ može izračunati $a$ (tj. ako može riješiti problem diskretnoga logaritma), onda i ona može pomoću $a$ i $g^b$ izračunati $g^{ab}$. Dakle, da bi protokol funkcionirao, grupa $G$ treba biti izabrana tako da je u njoj problem diskretnoga logaritma dovoljno težak. Jedna je mogućnost multiplikativna grupa konačnoga polja $\boldsymbol{F}_p$ (skup $\{1, 2, \dots, p - 1\}$ uz operaciju množenja modulo $p$) za dovoljno velik prost broj $p$ (barem 300 znamenaka). Tada je $g$ primitivni korijen modulo $p$, tj. broj sa svojstvom da brojevi $\{g, g^2, \dots, g^{p-1}\}$ daju različite ostatke pri dijeljenju s $p$ (često se može uzeti da je $g = 2$). Ako je, primjerice, $p = 11$ (što je, naravno, premali broj za stvarnu primjenu) i $g = 2$, onda vidimo da potencije $g^i$, za $i = 1, 2, \dots, 10$ daju redom ostatke 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 pri dijeljenju s 11, pa se zaista svi ostatci (osim 0) pojavljuju točno jednom.

Još efikasniji protokol dobivamo ako umjesto grupe $\boldsymbol{F}_p$ koristimo grupu točaka na eliptičkoj krivulji (nesingularnoj kubnoj krivulji) nad konačnim poljem. Naime, u toj grupi je problem diskretnoga logaritma još teži, pa stoga istu sigurnost postižemo uz manju duljinu ključa (umjesto ključa duljine 1024 bita, što je danas standardna duljina kod protokola koji koriste $\boldsymbol{F}_p$, a slično je i s onima koji koriste problem faktorizacije, dovoljan je ključ duljine 160 bitova). Više o primjeni eliptičkih krivulja u kriptografiji vidi u Dujella, Maretić 2007.

Prvi, a ujedno i najpopularniji i najšire korišteni kriptosustav s javnim ključem je RSA-kriptosustav, koji su izumili Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Njegova sigurnost zasnovana je na teškoći faktorizacije velikih prirodnih brojeva. U njemu najprije izabiremo tajno dva velika prosta broja $p$ i $q$ od preko 150 znamenaka (ovdje je vrlo važna

činjenica da postoje efikasni testovi prostosti pomoću kojih se to može napraviti) te izračunamo $n = pq$ i $\varphi(n) = (p - 1)(q - 1) = n + 1 - p - q$ (Eulerova funkcija). Zatim izaberemo broj $e$ takav da je $e < \varphi(n)$ i $\text{nzd}(\varphi(n), e) = 1$ te tajno izračunamo $d$ tako da je $de \equiv 1 \pmod{\varphi(n)}$ (rješimo linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$ pomoću Euklidova algoritma). Sada je $(n, e)$ naš javni ključ (koji treba znati svatko tko nam šalje poruke), a $(p, q, d)$ tajni je (osobni) ključ (koji trebamo znati samo mi). Poruka (razbijena na blokove koji odgovaraju brojevima manjim od $n$ – tipično $n$ ima oko 1024 bita) šifrira se ovako: $e_k(x) = x^e \bmod n$, a dobiveni šifrat dešifrira se ovako: $d_k(y) = y^d \bmod n$. Da su funkcije $e_k$ i $d_k$ inverzne, slijedi iz prije navedenoga Eulerova teorema.

Sigurnost RSA-kriptosustava leži u teškoći faktorizacije velikih brojeva. Zaista, onaj tko zna ili može otkriti faktore $p$ i $q$ javno poznatoga broja $n$, taj može izračunati $\varphi(n) = (p - 1)(q - 1)$ te saznati tajni eksponent $d$ rješavajući linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$.

**Literatura**


Čavrak, H. 2004. Enigma, *Math.e*: 3.

Dujella, A. 2004. There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* 566: 183–214.

Dujella, A.; Kazalicki, M.; Mikić, M.; Szikszai, M. 2016. There are infinitely many rational Diophantine sextuples, *Int. Math. Res. Not. IMRN* (objavljuje se).

Dujella, A.; Maretić, M. 2007. *Kriptografija*. Zagreb: Element.

Kapitanović, V. 2012. *Povijesna vrela i pomoćne znanosti*. Split: Filozofski fakultet.