Andrej Dujella: Teorija brojeva i kriptografija

Sažetak

U ovom prilogu novigradskog matematičara daje se kratak prikaz nekoliko tema iz teorije brojeva s posebnim naglaskom na one koje su u središtu interesa hrvatske istraživačke grupe iz teorije brojeva te se želi objasniti kako je teorija brojeva našla primjenu u kriptografiji. Navode se neke klasične i povijesno važne metode za šifriranje te neke suvremene koje se koriste metodama i algoritmima iz teorije brojeva.

Ključne riječi: Teorija brojeva; kriptografija.

Uvod

Teorija brojeva grana je matematike koja se bavi proučavanjem svojstava cijelih brojeva kao što su djeljivost, rastav na proste faktore ili rješivost jednadžbi u cijelim brojevima. Ona ima vrlo dugu i bogatu povijest, a važne su joj doprinose dali i neki od najvažnijih matematičara u povijesti, poput Euklida, Eulera i Gaussa. Tijekom te njene duge povijesti, teorija brojeva često se smatrala „najčišćom“ granom matematike, u smislu da je bila najdalja od bilo kakvih konkretnih primjena. Ni autor ovog priloga kad se, najprije kao učenik Osnovne škole Novigrad, a potom preko matematičkih natjecanja, počeo zanimati za matematiku i posebice za teoriju brojeva nije puno razmišljao o mogućim primjenama. Međutim, sredinom 70-ih godina 20. stoljeća, nastupa bitna promjena, tako da je danas teorija brojeva jedna od najvažnijih grana matematike za primjene u kriptografiji i sigurnoj razmjeni informacija.

Ljudi su od davnina željeli sigurno komunicirati, ali bili su svjesni da njihove poruke često putuju nesigurnim komunikacijskim kanalima. Kroz stoljeća su se načini 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 tog problema bavi se znanstvena disciplina koja se naziva kriptografija. U prošlosti je kriptografija često odlučivala o ishodima bitaka te sudbinama 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 zanimljiva puno širem krugu ljudi.

Metode koje su se u prošlosti najčešće rabile za šifriranje poruka bile su zamjena (supstitucija) i premještanje (transpozicija) osnovnih elemenata teksta (slova, blokova slova, bitova ili blokova bitova). Kombinaciju tih dviju metoda susrećemo i danas u suvremenim simetričnim kriptosustavima. Asimetrični kriptosustavi ili kriptosustavi s javnim ključem pojavili su se tek 70-ih godina 20. stoljeća. Kod njih se za šifriranje primjenjuju 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. U konstrukciji jednosmjernih funkcija rabe se „teški“ matematički problemi, koji uglavnom potječu iz algoritamske teorije brojeva, poput faktorizacije velikih prirodnih brojeva ili logaritmiranja u nekim konačnim grupama (glavni su primjeri multiplikativna grupa konačnog polja i grupa točaka na eliptičkoj krivulji nad konačnim poljem).

Neke teme iz teorije brojeva

U ovom prilogu nije moguće sustavno obraditi sve važne vidove teorije brojeva, stoga ćemo se ograničiti na kratak prikaz nekoliko izabranih tema, s posebnim naglaskom na teme relevantne za primjene u kriptografiji te na teme koje su u središtu interesa hrvatske istraživačke grupe iz teorije brojeva.

Djeljivost i kongruencije

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 kao $a|b$. Još kažemo da je a djelitelj b, odnosno da je b višekratnik 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 $nzd(a,b) = 1$, kažemo da su brojevi a i b relativno prosti. Važna je činjenica 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 $ax + by = nzd(a,b)$. Broj koraka u algoritmu proporcionalan je broju znamenaka manjem

od brojeva a i b (takve algoritme nazivamo efikasni ili polinomijalni, za razliku od eksponencijalnih kod kojih je broj koraka proporcionalan veličini ulaznih podataka (ili nekoj njihovoj potenciji)).
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 i φ se naziva Eulerova funkcija).

Prosti brojevi i faktorizacija

Za prirodan broj $p > 1$ kažemo da je prost ako p nema niti jedan djelitelj d takav 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 nijedna 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. u okviru GIMPS projekta u kojem skupina volontera, koristeći se programima za distribuirano računanje, sudjeluje u potrazi za velikim Mersenneovim prostim brojevima oblika $2^p - 1$.

Kod ispitivanja je li neki konkretni broj p prost, vrlo je neefikasno (a za velike brojeve i praktički nemoguće) to raditi ispitujući je li broj djeljiv s brojevima d između 1 i p (jedno očito, ali i dalje nedovoljno efikasno ubrzanje jest da se provjerava djeljivost samo brojevima do $\sqrt{p}$). Stoga se u pravilu ispituje zadovoljava li broj p neko od svojstava koje vrijedi za sve proste brojeve (ali ih mogu zadovoljiti i neki složeni brojevi). Jedno od takvih svojstava, koje je polazište za većinu praktičnih testova za testiranje prostosti, jest Mali Fermatov teorem. Taj teorem kaže da za svaki prost broj p i svaki cijeli broj a vrijedi kongruencija $a^p \equiv a \pmod{p}$. Istinitost te kongruencije može se efikasno provjeriti (čak i za vrlo velike brojeve p) primjenom metode „kvadriraj i množi“ koja se koristi binarnim zapisom broja p. Tako, slično kao kod Euklidova algoritma, imamo algoritam kojem je broj koraka proporcionalan broju znamenaka ulaznih podataka.

Ako prirodan broj n ne prođe neki od testova za testiranje prostosti, onda znamo da je sigurno složen, no ti testovi u pravilu nam ne daju faktore od n. Faktorizacija velikih prirodnih brojeva težak je problem i upravo su na njegovoj težini zasnovane neke od suvremenih metoda za

šifriranje. Zajednička osobina većine modernih metoda za faktorizaciju jest da u zadnjem koraku netrivijalni faktor (različit od 1 i n) nalaze računanjem nzd(n,x), za prikladno odabrani broj x. Ovdje je ponovno vrlo važna činjenica da se najveći zajednički djelitelj može efikasno izračunati pomoću Euklidova algoritma.

Diofantske jednadžbe

Diofantske jednadžbe su jednadžbe u kojima rješenja tražimo u skupu cijelih brojeva. Najjednostavnije diofantske jednadžbe su linearne diofantske jednadžbe s dvije nepoznanice. Primjerice, $3x+5y = 28$ jedna je takva jednadžba. Jedno je njezino rješenje $(x,y)=(1,5)$, a iz njega se sva rješenja dobivaju formulama $(x,y)=(1+5t,5-t)$. Čak i ako takva jednadžba ima vrlo velike koeficijente, rješenje je moguće efikasno pronaći Euklidovim algoritmom.

Spomenimo i dvije diofantske jednadžbe drugog stupnja. Prva je Pitagorina jednadžba $x^2+y^2=z^2$, čija se rješenja u prirodnim brojevima nazivaju Pitagorine trojke, a predstavljaju katete i hipotenuzu pravokutnog 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). Druga važna diofantska jednadžba drugog stupnja jest Pellova jednadžba. To je jednadžba oblika $x^2 - dy^2 = 1$, gdje je d prirodan broj koji nije kvadrat. Poznato je da i ta jednadžba ima beskonačno mnogo rješenja u prirodnim brojevima (iako često najmanje rješenje može biti vrlo veliko). Rješenja su u uskoj vezi s jako dobrim racionalnim aproksimacijama iracionalnog broja $\sqrt{d}$ (što je tema kojom se bavi dio teorije brojeva koji se naziva „diofantske aproksimacije“). Primjerice, rješenja jednadžbe $x^2 - 2y^2 = 1$ jesu $(x,y) = (3,2), (17,12), (99,70), (577,408), (3363,2378), ...$, a tim rješenjima pridruženi razlomci $p/q = 3/2, 17/12, 99/79, 577/408, 3363/2378, ...$ svi zadovoljavaju nejednakost $|\sqrt{2} - p/q| < 1/q^2$.

Spomenimo i jedan diofantski problem koji ima vrlo dugu povijest (njime se bavio već starogrčki matematičar Diofant, po kojem je cijelo to područje matematike dobilo ime), a koji je predmet intenzivnog 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*. Glavno pitanje vezano uz taj pojam jest koliko veliki mogu biti skupovi s tim svojstvom. U slučaju Diofantovih m-torki čiji su članovi cijeli brojevi (različiti od nule), na to je pitanje gotovo potpuno odgovoreno. Naime, lako je vidjeti da postoji beskonačno mnogo Diofantovih

četvorki (npr. $\{k - 1, k + 1, 4k, 16k^3 - 4k\}$ za $k > 1$; za $k = 2$ dobiva se poznata četvorka {1,3,8,120} koju je pronašao Fermat). S druge strane, 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.).

Baker i Davenport dokazali su da se trojka {1,3,8} ne može proširiti do (cjelobrojne) Diofantove petorke (Baker, Davenport, 1969.). Problem proširenja Diofantove trojke do četvorke usko je vezan uz pojam eliptičkih krivulja, koje su vrlo važne za moderne primjene u kriptografiji. Konkretno, proširenje trojke {1,3,8} vodi do proučavanja cjelobrojnih i racionalnih točaka na krivulji $y^2 = (x+1)(3x+1)(8x+1)$ (dakle, imamo Diofantsku jednadžbu trećeg stupnja), za koju se može pokazati da ima beskonačno mnogo racionalnih točaka, ali samo tri cjelobrojne: $(x,y) = (-1,0), (0,1)$ i $(120,6479)$.

Kratka povijest kriptografije

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija grčkog je podrijetla i mogla bi se doslovno prevesti kao *tajnopis*.

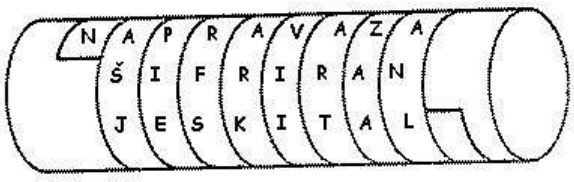
Glavne metode klasične kriptografije jesu:
• transpozicija (premještanje): NOVIGRAD → DONIVRAG

• supstitucija (zamjena): NOVIGRAD → OPWJHSBE

Transpozicijske šifre

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 kojeg 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.



Slika 1: Starogrčka naprava za šifriranje skital

U praksi najupotrebljavanija transpozicijska šifra bila je *stupčana transpozicija*. Kod nje se otvoreni tekst upisuje u pravokutnik po redcima, a zatim se poruka čita po stupcima, ali s promijenjenim poretkom stupaca. Ako se posljednji redak ne ispuni do kraja, onda se prazna mjesta popune proizvoljnim slovima *(nulama)* koja ne mijenjaju sadržaj poruke. Za primjer šifrirajmo sljedeću rečenicu iz Šenoina romana *Kletva*: „Tvrdi Novigrad kraj mora visio je u burnu noć kao crna, rogata glava ogromne nemani.“ (ovdje se možemo prisjetiti da se dio radnje romana *Kletva* Augusta Šenoe odvija u novigradskoj Fortici). Koristimo se ključem (redoslijed stupaca) 4613752.

4	6	1	3	7	5	2
T	V	R	D	I	N	O
V	I	G	R	A	D	K
R	A	J	M	O	R	A
V	I	S	I	O	J	E
U	B	U	R	N	U	N
O	Ć	K	A	O	C	R
N	A	R	O	G	A	T
A	G	L	A	V	A	O
G	R	O	M	N	E	N
E	M	A	N	I	X	Y

Dakle, šifrirana poruka glasi:
RGJSUKRLOAOKAENRTONYDRMIRAOMNTVRVUONAGE
NDRJUCAAEXVIAIMĆAGRMIAOONOGVNI.

Drugi popularan način za realizaciju transpozicijskih šifara jest pomoću tzv. rešetki. To su geometrijski likovi, najčešće kvadrati, koji su podijeljeni na male kvadratiće. Neki od tih kvadratića predstavljaju otvore u koje se upisuje otvoreni tekst. Ako su otvori izabrani sasvim proizvoljno, onda se nakon upisivanja slova rešetka makne, a preostala se mjesta pokušaju dopuniti tako da konačan rezultat bude neki bezazleni tekst. Primalac bi trebao imati identičnu

rešetku (tj. geometrijsku figuru s otvorima na istim mjestima), pa je staviti kao „masku“ na primljenu geometrijsku figuru i pročitati tajnu poruku.

Supstitucijske šifre

Znameniti rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog 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 zadnjeg slova Z ponovo dolaze A, B, C. Ako bismo upotrijebili današnju međunarodnu abecedu od 26 slova, onda bi ime novigradske utvrde iz rimskog vremena CASTRUM NOVUM bilo šifrirano kao FDVWUXP QRYXP.

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 NOVIGRAD DALMATINSKI pomoću ključne riječi 5, 7, 3, 9 bio bi šifriran kao SVYRLYDM IHOVFALWXRL. Iako naizgled mala modifikacija Cezarove šifre, Vigenèreova šifra znatno je sigurnija, ponajprije zbog velikog broja mogućih ključeva, a potom i zbog toga što se identična slova u otvorenom tekstu, ovisno o položaju u tekstu, šifriraju na različite načine, čime se sprječavaju napadi koji se koriste poznatim činjenicama o frekvenciji slova u jeziku otvorenog teksta (primjerice, u hrvatskom jeziku najfrekventnija su slova A, I, O, E, N). Stoga je nekoliko stoljeća to bila najpopularnija šifra, koja je bila u primjeni tijekom važnih povijesnih događaja, poput Američkoga građanskog rata.

Njemački pronalazač Artur Scherbius 1918. godine izumio je rotorsku napravu koju je nazvao ENIGMA. Masovna uporaba ENIGME započela 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 pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička *rotora* (*šifrarnika*) i električne prespojne ploče. U standardnoj verziji s 10 prespojnih kabela pružala je golem 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, velik problem bila je razmjena ključeva. Svaki mjesec operateri ENIGME dobili bi novu knjigu s ključevima u kojoj bi se specificiralo 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, kako se dnevno šifrirao golem 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 dnevnog ključa. Poljski su kriptoanalitičari predvođeni Rejewskim uspjeli iskoristili protokol koji se pritom primjenjivao (za koji su prethodno saznali Francuzi metodama klasične špijunaže) za kriptoanalitički napad (više vidi u (Čavrak, 2004.) i (Dujella, Maretić, 2007.).

Kriptografija javnog ključa

Sigurnost svih do sada navedenih kriptosustava leži u tajnosti ključa. I tu se pojavljuje vrlo važan i težak problem, a to je kako sigurno razmijeniti ključ. Naime, polazna pretpostavka u kriptografiji jest da imamo dvije strane koje ne mogu sigurno razmijeniti poruke (jer netko nagleda komunikacijski kanal preko kojeg komuniciraju), a od njih se traži da sigurno razmijene ključ. Taj se problem pokušavao riješiti na različite načine, ali često (kao u slučaju ENIGME) rješenja su bila bitno nekvalitetnija od same šifre. Sredinom 70-ih godina 20. stoljeća konačno je pronađeno zadovoljavajuće rješenje problema razmjene ključeva. Ideje koje su se pritom primijenile uskoro su primijenjene i na druge probleme koje je donijela moderna uporaba kriptografije, poput digitalnog potpisa.

Osnovna ideja jest korištenje „jednosmjernih funkcija“, tj. funkcija koje se računaju lako, ali se njihov inverz računa jako teško. Osnova za konstrukciju „jednosmjernih funkcija“ jesu „teški“ matematički problemi. Ovdje „teški“ ne znači nužno da ih je teško razumjeti (u smislu da iza njih stoji vrlo duboka teorija) već ponajprije to da ih je teško riješiti za konkretne (velike) ulazne podatke. Tipični takvi problemi jesu:

• faktorizacija velikih složenih brojeva;

• problem diskretnog logaritma (DLP):

za zadane a, b i p naći x takav da vrijedi $a^x \equiv b \pmod{p}$;

• eliptički diskretni logaritam (ECDPL).

Diffie-Hellmanov protokol za razmjenu ključeva

Godine 1976. Whitfield Diffie i Martin Hellman ponudili su moguće rješenje problema razmjene ključeva zasnovano na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. Pretpostavimo da se osobe A i B žele dogovoriti o jednom tajnom slučajnom elementu u konačnoj cikličkoj grupi $G=\{1, g, g^2, \ldots, g^{n-1}\}$ reda n (grupi s n elemenata), koji bi onda poslije mogli rabiti kao ključ za šifriranje u nekom simetričnom kriptosustavu. Oni taj svoj dogovor moraju provesti preko nekog nesigurnog komunikacijskog kanala a da prethodno nisu razmijenili bilo kakvu informaciju. Jedina informacija koju imaju jest grupa G i njezin generator g.

1. Osoba A generira slučajan prirodan broj a iz $\{1, 2, \ldots, n - 1\}$. Ona pošalje osobi B element g^a.
2. Osoba B generira slučajan prirodan broj b iz $\{1, 2, \ldots, n - 1\}$, te pošalje osobi A element g^b.
3. Osoba A izračuna $(g^b)^a = g^{ab}$.
4. Osoba B izračuna $(g^a)^b = g^{ab}$.

Sada je njihov tajni ključ $K = g^{ab}$.

Dakle, na kraju komunikacije osobe A i B uspjele su razmijeniti podatak K koji ni u jednom trenutku nije prenesen preko njihova nesigurnog komunikacijskog kanala. Njihov protivnik koji može prisluškivati njihovu komunikaciju preko nesigurnog komunikacijskog kanala zna sljedeće podatke: G, g, g^a, g^b te iz tih podataka treba izračunati g^{ab}. Ako protivnik iz poznavanja g i g^a može izračunati a (tj. ako može riješiti problem diskretnog logaritma), onda i on može pomoću a i g^b izračunati g^{ab}. Da bi protokol funkcionirao, grupa G treba biti izabrana tako da je u njoj problem diskretnog logaritma dovoljno težak. Jedna je mogućnost multiplikativna grupa konačnog polja $\boldsymbol{F}_p$ (skup $\{1,2,\ldots,p-1\}$ 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 $\{g, g^2, \ldots, g^{p-1}\}$ daju različite ostatke pri dijeljenju s p (često se može uzeti da je $g = 2$).

RSA kriptosustav

Prvi, a ujedno i najpopularniji i najšire rabljen kriptosustav s javnim ključem jest RSA kriptosustav koji su izumili Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Njegova sigurnost zasnovana je na teškoći faktorizacije velikih prirodnih brojeva. Slijedi opis izbora parametara RSA kriptosustava:

1. Izabiremo tajno dva velika prosta broja p i q od preko 150 znamenaka, tako da q ima nekoliko znamenaka više od p. To radimo tako da pomoću nekog generatora slučajnih brojeva generiramo prirodan broj m s traženim brojem znamenaka, a zatim korištenjem nekog testa za testiranje prostosti tražimo prvi prosti broj veći ili jednak m;
2. Izračunamo $n = pq$ i $\varphi(n) = (p - 1)(q - 1) = n + 1 - p - q$ (Eulerova funkcija);
3. Izaberemo na slučajno broj e takav da je $e < \varphi(n)$ i $nzd(\varphi(n), e) = 1$. To se može napraviti slično kao pod 1. Nakon toga tajno izračunamo d, tako da je $de \equiv 1 \pmod{\varphi(n)}$ (riješimo linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$ pomoću Euklidova algoritma);.
4. Stavimo ključ za šifriranje (n, e) u javni direktorij.

Sada je (n, e) javni ključ (koji treba znati svatko tko vam šalje poruke), a (p, q, d) tajni je (osobni) ključ (koji trebate znati samo vi). 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 navedenog Eulerova teorema. Uočimo da je ovdje e_k „jednosmjerna funkcija“. Naime, iz $e_k(x) = x^e \bmod n$, tj. uz poznavanje samo javnog ključa (n, e), ne možemo naći tajni ključ d, odnosno inverznu funkciju $d_k(y) = y^d \bmod n$. Za to nam je potreban „dodatni podatak“, a to je u ovom slučaju faktorizacija od n.

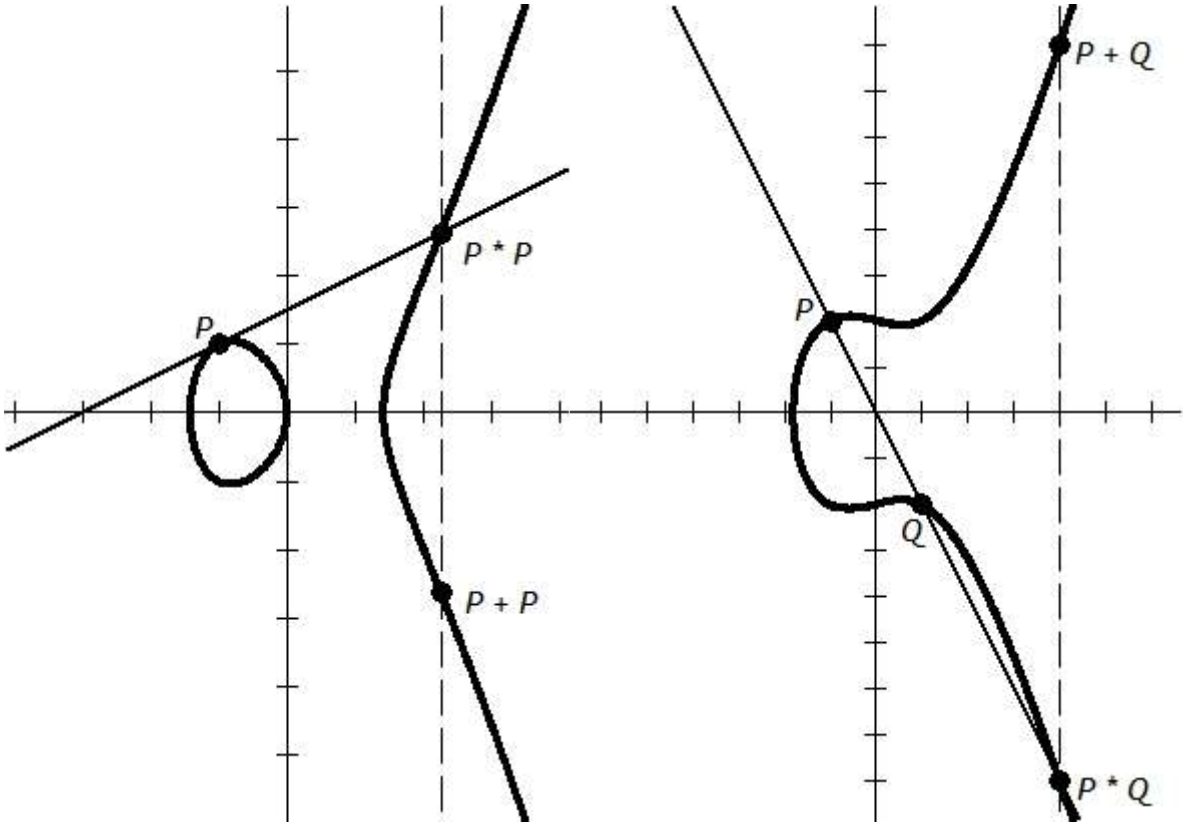
Dakle, sigurnost RSA kriptosustava leži u teškoći faktorizacije velikih brojeva. Zaista, onaj tko zna ili može otkriti faktore p i q javno poznatog broja n može izračunati $\varphi(n) = (p - 1)(q - 1)$ te saznati tajni eksponent d rješavajući linearnu diofantsku jednadžbu $de - t\,\varphi(n) = 1$.

Kad se kaže da je teško faktorizirati velik prirodan broj n, ta je tvrdnja dosta neprecizna (pa doslovno shvaćeno i netočna). Naravno da ima vrlo velikih brojeva koje je lako faktorizirati (primjerice, $10^{200} = 2^{200} \cdot 5^{200}$, a ima i manje očitih primjera, recimo brojeva koji su produkt

dva bliska broja). Dakle, ono što se zapravo hoće reći jest da je teško faktorizirati n koji je produkt dva velika pažljivo odabrana prosta broja p i q (s barem stotinjak znamenaka). No tu dolazimo naizgled do podjednako teškog (a onda možda i nerješivog) problema, a to je kako naći (tajno) veliki prosti broj. „Školskim" načinom (dijeleći redom s 2, 3...) čini se da je to podjednako teško kao i faktorizirati veliki prirodni broj slične veličine. I tu je ključno ono što smo već spomenuli u poglavlju o teoriji brojeva – da se testirati (pa i dokazati) prostost velikih brojeva može puno efikasnije nego „školski", dok za faktorizaciju nemamo algoritama koji bi bili drastično brži od „školskog". Kao ilustraciju navedimo da najveći broj za koji je dokazano da je prost ima 22.338.618 znamenaka, dok najveći broj n koji zadovoljava sve savjete za izbor modula u RSA kriptosustavima, a za koji javno objavljena uspješna faktorizacija, ima 232 decimalne znamenke.

Eliptičke krivulje u kriptografiji

Eliptičke krivulje imaju važnu ulogu u više područja matematike (teorija brojeva, algebarska geometrija, kompleksna analiza), a odnedavno su postale i vrlo bitne za primjene u kriptografiji. Eliptička krivulja može se definirati nad proizvoljnim poljem. U teoriji brojeva najvažniji je slučaj polja racionalnih brojeva $\boldsymbol{Q}$, dok su za promjene najvažnija konačna polja. Ako je polje karakteristike različite od 2 i 3 (a takvo je $\boldsymbol{Q}$ te polja $\boldsymbol{F}_p$ za $p > 2$), onda eliptička krivulja ima jednadžbu oblika $y^2 = x^3 + ax + b$, uz uvjet da je $4a^3 + 27b^2 \neq 0$ (da bi krivulja bila nesingularna, tj. imala tangentu u svakoj točki). Vrlo je važna činjenica da se na skupu svih točaka na eliptičkoj krivulji (točke (x,y) koje zadovoljavaju jednadžbu uz dodatak još jedne „točke u beskonačnosti") može na prirodan način uvesti operacija („zbrajanje točaka"), uz koju taj skup postaje komutativna grupa. Operaciju možemo opisati geometrijski (ako za trenutak uzmemo da krivulju promatramo nad poljem realnih brojeva $\boldsymbol{R}$). Točke P i Q zbrajamo tako da kroz njih povučemo pravac (sekantu). Taj pravac siječe krivulju u točno još jednoj točki koju označimo s $P * Q$. Sada definiramo da je $P + Q$ osnosimetrična točka točki $P * Q$ s obzirom na os x. Ako je $P = Q$, onda umjesto sekante povlačimo tangentu na krivulju u točki P (vidi skice).



Slika 2: Zbrajanje točaka na eliptičkim krivuljama

Ideju o tome da bi eliptičke krivulje mogle biti korisne u konstrukciji kriptosustava s javnim ključem prvi su javno iznijeli Koblitz i Miller 1985. godine. U grupi točaka na eliptičkoj krivulji nad konačnim poljem razlika u težini izmedu potenciranja i logaritmiranja još je veća nego u standarno korištenoj grupi $\boldsymbol{F}_p$, stoga istu sigurnost postižemo uz manju duljinu ključa (umjesto ključa duljine 1024 bita, što je danas standardna duljina kod RSA kriptosustava te onih koji koriste $\boldsymbol{F}_p$, dovoljan je ključ duljine 160 bitova). To je osobito važno kod onih primjena (kao što su npr. „pametne kartice“) kod kojih je prostor za pohranu ključeva vrlo ograničen.

Za problem eliptičkog diskretnog logaritma (osim za neke vrlo specijalne eliptičke krivulje) nisu poznati bolji algoritmi od algoritama za općenite grupe, kojima je složenost približno $\sqrt{n}$, gdje je n red grupe. To su algoritam „malih i velikih koraka“ – BSGS (nepoznati broj $x < n$ tražimo u obliku $x = [\sqrt{n}]\, a + b$, $0 \leq a, b < \sqrt{n}$) i Pollardov ρ-algoritam (povezan s paradoksom rođendana). Za problem diskretnog logaritma u grupi $\boldsymbol{F}_p$ postoje dosta efikasniji (subeksponencijalni) algoritmi zasnovani na „Index calculus metodi“.

Ideja te metode u tome je da se elementi od $\boldsymbol{F}_p$ shvate kao cijeli brojevi, tj. elementi od $\boldsymbol{Z}$, te da ih se prikaže kao produkt malih prostih brojeva (za uspjeh te metode bitno je da prostih brojeva ima beskonačno mnogo). Ako bismo istu ideju htjeli primijeniti na eliptičke krivulje nad $\boldsymbol{F}_p$, mogli bismo shvatiti eliptičku krivulju nad $\boldsymbol{F}_p$ kao eliptičku krivulju nad $\boldsymbol{Q}$, koja može imati veći broj generatora (broj generatora naziva se *rang*). Za realizaciju te ideje trebale bi nam krivulje ranga barem 180, a danas nije poznata nijedna krivulja ranga većeg od 28.

Druga razlika, i potencijalna prednost, grupe $E(\boldsymbol{F}_p)$ u odnosu na $\boldsymbol{F}_p$ jest da je red multiplikativne grupe polja $\boldsymbol{F}_p$ potpuno određen s p (jednak je p - 1), dok red grupe $E(\boldsymbol{F}_p)$, za različite krivulje E i fiksirani p, može poprimiti bilo koju vrijednost unutar Hasseova intervala $\langle p+1-2\sqrt{p},\ p+1+2\sqrt{p}\rangle$. Jedna primjena te ideje jest u faktorizaciji velikih prirodnih brojeva. Polazište je Pollardova p - 1 metoda koja se koristi Malim Fermatovim teoremom. Neka je n prirodni broj čiji prosti faktor p želimo pronaći. Kad bismo znali neki višekratnik m od p - 1, onda bismo p mogli naći (Euklidovim algoritmom) kao zajednički djelitelj od a^m - 1 i n. Pitanje je medutim kako naći višekratnik od p - 1 kad ne znamo p. To možemo efikasno napraviti u slučaju kada broj p - 1 ima samo male proste faktore, što, naravno, ne mora biti općenito zadovoljeno. Ipak, pokazuje se da je unutar Hasseova intervala uvijek moguće pronaći broj koji je dovoljno „gladak“ (ima samo male proste faktore), a time i eliptičku krivulju nad $E(\boldsymbol{F}_p)$ dovoljno glatkog reda. Prevođenjem Pollardove metode u grupu eliptičkih krivulja (što je 1987. godine predložio Lenstra) dobiva se jedna od najefikasnijih (subeksponencijalnih) danas poznatih metoda za faktorizaciju. Daljnja poboljšanja te metode (Dujella, Najman, 2012.) dobivaju se promatranjem eliptičkih krivulja koje imaju veliku torzijsku grupu (grupu točaka konačnog reda) nad $\boldsymbol{Q}$ ili nad poljima algebarskih brojeva malog stupnja, čime se može unaprijed osigurati da red od $E(\boldsymbol{F}_p)$ ima neki netrivijalni faktor (jednak redu torzijske grupe). Konstrukcija eliptičkih krivulja velikog ranga sa zadanom torzijskom grupa još je jedna od tema na kojoj aktivno i uspješno radi hrvatska grupa iz teorije brojeva.

Kriptografija u Hrvatskoj

Neke informacije o povijesti kriptografije u Hrvatskoj mogu se naći u knjizi (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.

Možda je zanimljivo spomenuti da transpozicijsko šifriranje pomoću Cardanove rotirajuće rešetke igra važnu ulogu u romanu Julesa Vernea *Mathias Sandorf* iz 1885. godine. U romanu se opisuje kako tri ugarska plemića: grof Mathias Sandorf i njegovi suradnici Stjepan Bathory i Ladislav Zathmar u Trstu 1867. godine pripremaju urotu za odcjepljenje Mađarske od Austro-Ugarske. Međutim, urota nije uspjela jer je skitnica Sarcany uhvatio goluba koji je prenosio zavjereničku šifriranu poruku i dešifrirao je tako što je ukrao rešetku za dešifriranje. Veliki dijelovi romana odvijaju se u hrvatskim krajevima: Istri (Pazin, Limski kanal, Rovinj) i Dubrovniku. Posebno je detaljan opis pazinskoga Kaštela i jame, uključujući i ilustracije Leona Benetta, prema fotografijama koje je Verne dobio od tadašnjega gradonačelnika Pazina Giuseppea Cecha.

Danas, u Hrvatskoj se kriptografija i sigurnost informacija izučavaju na fakultetima (Matematički odsjek PMF-a u Zagrebu, PMF u Splitu, Odjel za matematiku u Osijeku, FER u Zagrebu, FOI u Varaždinu) te u državnim agencijama zaduženima za sigurnost.

Na kraju priloga napominjemo da su ideje za većinu spomenutih autorovih rezultata iz teorije brojeva i njihovih primjena u kriptografiji nastale za vrijeme boravaka u Novigradu u obiteljskoj kući kod crkve svetog Nikole.

Literatura

Baker, A., Davenport, H. (1969.): The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser. (2)* 20, 129-137.

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*, to appear.

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

Dujella, A., Najman, F. (2012.): Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization, *Period. Math. Hungar.* 65, 193-203.

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

Summary

In this contribution the author, a native of Novigrad, gives short overview of certain topics in number theory with special emphasis on main reseach topics of Croatian number theory reseach group, and explains applications of number theory in cryptography. The contribution discusses some classical and historically important, as well as some modern cryptosystems based on methods and algorithms from number theory.

Keywords: Number theory; cryptography.