Računske tehnike za deljivost binomskih koeficientov

dr. Katja Berčič in dr. Russ Woodroofe

Fakulteta za matematiko in fiziko, Univerza v Ljubljani
Fakulteta za matematiko, naravoslovje in informacijske tehnologije, Univerza na Primorskem

1 Binomi

Za celi števili $0 \leq k \leq n$ lahko definiramo *binomski koeficient* $\binom{n}{k}$ s predpisom

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

Binomski koeficienti so zanimivi, saj štejejo koristne stvari. Binomski koeficient $\binom{n}{k}$ predstavlja število možnih izbir podmnožice s k elementi iz množice z n elementi. Tu predpostavljamo, da lahko predmete razločimo, ter da nas ne zanima vrstni red elementov.

Binomski koeficienti se pojavijo, kot že ime pove, kot koeficienti v razčlenjeni obliki potence binoma $(1+x)^n$. Če to razvijemo na običajen način, in za trenutek pozabimo, da je $1 \cdot x = x \cdot 1$, dobimo 2^n členov oblike $\_\ \_\ \_ \cdots \_$, kjer je vsak $\_$ bodisi 1 ali x. Na primer,

$$\begin{aligned}(1+x)^3 = {} & 1\cdot 1\cdot 1 + 1\cdot 1\cdot x + 1\cdot x\cdot 1 + x\cdot 1\cdot 1 + \\ & 1\cdot x\cdot x + x\cdot 1\cdot x + x\cdot x\cdot 1 + x\cdot x\cdot x.\end{aligned}$$

Koeficient člena x^k v izrazu $(1+x)^n$ predstavlja število načinov, da izberemo k podčrtajev, na katere bomo postavili x.

Iz definicije sledi, da velja $\binom{n}{k} = \binom{n}{n-k}$, da $\binom{n}{0} = \binom{n}{n} = 1$, ter da za $1 \leq k \leq n-1$ velja $\binom{n}{k} > 1$.

2 Vprašanje deljivosti

Naslednje vprašanje se je pojavilo pri delu drugega avtorja z Johnom Shareshianom.

Vprašanje 1. *Ali je za dano celo število n vedno mogoče najti praštevili p in r, tako da je vsak nenetrivialni binomski koeficient $\binom{n}{k}$ deljiv bodisi s p, bodisi z r?*

Z netrivialno tu mislimo »različno od 1«. Zavržemo torej $\binom{n}{0}$ in $\binom{n}{k}$ ter zahtevamo, da so preostali binomski koeficienti $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ deljivi s p ali z r. Zaradi simetrije je seveda dovolj, če obravnavamo le binomske koeficiente $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{\lfloor n/2 \rfloor}$.

Motivacija za to vprašanje izhaja iz teorije grup (matematične teorije simetrij). Tu je $\binom{n}{k}$ razmerje med skupnim številom načinov za preurejanje množice $1, \ldots, n$ ter številom načinov za preurejanje, pri katerih ohranimo $1, \ldots, k$ (v nekem vrstnem redu) na prvih k mestih.

Primer 2. Za $n = 15$ ni težko izračunati nenetrivialnih binomskih koeficientov: to so 15, 105, 455, 1365, 3003, 5005, 6435. Lahko opazimo, da sta praštevili $p = 3$ in $r = 5$ primerni, da na vprašanje odgovorimo z »da«. Morda ni tako očitno, vendar pa deluje tudi $r = 13$, če je p bodisi 3 bodisi 5.

Naredimo prvo opazko:

Lema 3. Če praštevili p in r vodita do odgovora »da«, potem vsaj eno deli $n = \binom{n}{1}$.

Nadaljevali bomo s predpostavko, da praštevilo p deli n.

Primer 4. Za $n = 1$ milijon $= 10^6$ preverimo, da je $r = 999.983$ tudi praštevilo. To je koristno, saj je $n!$ deljivo z r, vendar je $k!$ deljivo z r le, sče je $k \geq r$, $(n-k)!$ pa je deljivo z r le še, da je $k \leq (n-r)$. Sledi, da so vsi binomski koeficienti deljivi z r, razen $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{17}$ in simetričnih binomskih koeficientov na koncu seznama.

Ker je $n = 10^6 = 2^6 \cdot 5^6$, moramo zdaj preveriti le še, da števili 2 ali 5 delita teh 17 koeficientov. Delita jih obe števili, zato je odgovor na vprašanje »da« za $n = 10^6$.

Ideje iz Primera 4 se da močno posplošiti. Naslednji izrek je dokazan na enak način kot v primeru.

Lema 5 (Velika praštevila veliko pomagajo, angl. *large primes help a lot*)**.** Če je praštevilo r manjše od n, potem velja

$$r \mid \binom{n}{k} \text{ razen če } k \leq (n-r) \text{ ali } k \geq r.$$

Poleg tega potrebujemo še pogoj, ki nam bo pomagal pri obravnavi primera $k \leq (n-r)$. Kot smo opazili, bomo za to potrebovali praštevilski delitelj števila n. Naslednja lema (katere dokaz ni težak, a presega obseg tega kratkega članka) bo prišla prav.

Lema 6 (Kummer, 1852)**.** Če je a pozitivno celo število in p praštevilo, tako da velja $p^a \mid n$, potem velja

$$p \mid \binom{n}{k} \text{ razen, kadar } p^a \mid k.$$

Zaključek 7. Če sta p in r praštevili, tako da velja $p^a \mid n$ in $r < n$, hkrati pa velja $p^a + r > n$, potem p in r vodita do odgovora »da« na vprašanje.

3 Kaj je znano

Odgovora na splošno ne poznamo. Čeprav nas Sklep 7 pogosto usmerja k odgovoru »da«, včasih ne deluje.

Primer 8 (Poučna zgodba)**.** Za $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ lahko preverimo, da je naslednje manjše praštevilo 199. Na žalost velja $199 + 7 < 210$. Vendar pa velja $206 = 103 \cdot 2$, in podoben argument kot v Primeru 4 pokaže, da so edini binomski koeficienti, ki niso deljivi z 103, tisti pri $k = 1, 2, 3, 4, 103, 104, 105$, in simetrični binomski koeficienti, ki so večji od $105 = 210/2$. Po Kummerjevi lemi so vsi ti, razen $\binom{210}{105}$, deljivi s 5 (brez računanja). S preštevanjem števila petic v števcu in imenovalcu lahko preverimo, da je tudi $\binom{210}{105}$ deljivo s 5.

Tako $p = 5$ in 103 vodita do odgovora »da« na vprašanje, a za to je potrebno nekaj dela!

Problem 1 (Ne preveč preprosto)**.** Najdi praštevili p in r, ki vodita do odgovora »da« na vprašanje za $n = 31.416$.

To, kar vemo o vprašanju, je naslednje:

Izrek 9 (Guralnick, Shareshian, in Woodroofe [2])**.** *Odgovor na vprašanje je »da« za vsa $n \leq 10^{15}$.*

Izrek 10 (Shareshian in Woodroofe [3], Teräväinen [4])**.** *Odgovor na vprašanje je »da« za skoraj vsa števila n. (Tu ima »skoraj vsa« poseben tehnični pomen.)*

4 Računske tehnike

Če se soočite z vprašanjem, na katerega ne poznate odgovora, je smiselno preveriti majhne vrednosti s pomočjo računalnika. Če vas zanimajo večje vrednosti, potem lahko bodisi program poganjate dlje časa, kupite hitrejši računalnik, ali pa izboljšate algoritem. Izboljšave algoritma imajo običajno največji učinek.

Izboljšave algoritma, ki so sčasoma privedle do Izreka 9, so primer tega.

1. Naiven, grob pristop, zapisan v programskem jeziku GAP, interpretiranem računalniškem algebrskem sistemu, nas je pripeljal do približno 10^4.

2. Sklep 7 nam omogoča hitro preveriti okoli 99.9% vrednosti. Potrebujemo seznam praštevil in največjih praštevilskih potenc. Z naivno faktorizacijo s tem trikom smo z GAP-om računali do 10^9.

3. Potrebujemo hitro metodo za pridobivanje vseh praštevil v velikem intervalu celih števil. Lahko uporabimo Eratostenovo sito, ki ste ga morda že videli. To je zelo hitro, vendar kljub nekaterim izboljšavam zahteva $O(\sqrt{n})$ pomnilnika. Z GAP-om smo računali do približno 10^{12} v nekaj dneh.

4. Ko zmanjka drugih idej, je smiselno optimizirati: prešli smo na jezik C za 20-kratno pospešitev. Izognemo se upoštevanju večjih praštevilskih faktorjev, pozorni smo na zmogljivost medpomnilnika, uporabljamo krožna faktorizacijo (angl. *wheel factorization*) in vrsto drugih manjših trikov za dodaten 50% pospešek. Na večjedrnem računalniku smo pognali 15 vzporednih kopij in tako v desetih dneh dosegli 10^{15}, kot v Izreku 9.

Triki, uporabljeni v (4), so nekoliko pomagali, vendar pa je največji napredek prišel pri (3). Več o Eratostenovem situ si lahko preberete v [1] in mnogih drugih virih.

Rada bi se zahvalila Bobu Guralnicku in Johnu Shareshianu za mnoge zanimive diskusije in večletno sodelovanje pri raziskovanju deljivosti binomskih koeficientov.

Literatura

[1] Richard Crandall and Carl Pomerance, *Prime numbers: a computational perspective*, second ed., Springer, New York, 2005.

[2] Robert M. Guralnick, John Shareshian, and Russ Woodroofe, *On invariable generation of alternating groups by elements of prime and prime power order*, Math. Comp. **92** (2023), no. 341, 1349–1361.

[3] John Shareshian and Russ Woodroofe, *Divisibility of binomial coefficients and generation of alternating groups*, Pacific J. Math. **292** (2018), no. 1, 223–238, arXiv:1505.05143.

[4] Joni Teräväinen, *Almost all alternating groups are invariably generated by two elements of prime order*, (2023), 16 pages, arXiv:2203.05427, accepted to Int. Math. Res. Not.