MEMO pripreme 2019., Teorija brojeva

sastavio: Matko

4. 6. 2019.

1 Osnove

Osnovni teorem aritmetike. Svaki prirodan broj n na jedinstven se način može prikazati kao

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

gdje su $k, a_1, \ldots, a_k$ nenegativni cijeli brojevi, te $p_1, \ldots, p_k$ prosti brojevi,

Euklidov algoritam. Za cijele brojeve a, b vrijedi $M(a, b) = M(a, a - b)$. Njegova posljedica je da su brojevi a, b su relativno prosti ako i samo ako postoje cijeli brojevi $x, y \in \mathbb{Z}$ takvi da je $ax + by = 1$. Nadalje, jednadžba $ax + by = c$ ima rješenja ako i samo ako $D(a, b) \mid c$.

Nužni i dovoljni uvjeti djeljivosti iz decimalnog zapisa. Sjetite se kada je broj n djeljiv s brojem $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 25, 100$, ovisno o njegovom decimalnom zapisu.

2 Kongruencije

Za dva cijela broja a i b kažemo da su kongruentni po modulu n ako je njihova razlika $a - b$ djeljiva s n. Može se reći i da su a i b kongruentni ako daju isti ostatak pri dijeljenju s n. Pišemo:

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$$

Kongruencijama se služimo jako slično kao i znakom jednako, tj. možemo ih zbrajati, oduzimati, množiti, potencirati. Dakle, ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, vrijedi:

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^m \equiv b^m \pmod{n}$, za bilo koji $m \in \mathbb{N}$. **Oprez:** obrat ne vrijedi, npr: $1^6 \equiv 2^6 = 64 \pmod{7}$, ali $1 \not\equiv 2 \pmod{7}$.
- $am \equiv bm \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{M(n,m)}}$, gdje $M(m, n)$ označava najveću zajedničku mjeru (djelitelj) brojeva m i n.

Koristeći kongruencije lako se sljedeća tvrdnja.

Lema za polinome s cjelobrojnim koeficijentima. Dan je polinom $P(x)$ s cjelobrojnim koeficijentima, te različiti cijeli brojevi a, b. Tada je $P(a) - P(b)$ djeljivo s $a - b$.

Ova tvrdnja, uz "polinom koji je najviše n-tog stupnja i u $n+1$ je točaka je jednak nuli", je ključna i gotovo jedina bitna u rješavanju zadataka s polinomima s cjelobrojnim koeficijentima.

3 Diofantske jednadžbe

Osnovne metode - kongruencije i faktorizacije

Gotovo sve Diofantske jednadžbe na kraju se svedu na kongruencije i faktorizacije. Prvo ispitivanjem nekih modula saznamo više o nepoznanicama, kojeg su oblika, a zatim tu informaciju iskoristimo u faktorizaciji.

Kod kongruencija mogu pomoći Fermatov i Eulerov teorem.

Fermatov (mali) teorem. Neka su a i p prirodni brojevi pri čemu je p prost. Tada vrijedi $a^p \equiv a \ (mod\ p)$.
Ekvivalentna formulacija: Neka su a i p cijeli brojevi pri čemu je p prost. Ako $M(a,p) = 1$, tada vrijedi $a^{p-1} \equiv 1 \ (mod\ p)$.

Eulerov teorem. Neka su a i n prirodni brojevi takvi da je $M(a,n) = 1$. Neka je $\varphi(n)$ broj prirodnih brojeva manjih ili jednakih n koji su relativno prosti s n. Tada vrijedi $a^{\varphi(n)} \equiv 1 \ (mod\ p)$.

Eulerova φ funkcija ima i zatvorenu formulu:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) = p_1^{a_1-1}\cdots p_k^{a_k-1}(p_1-1)\cdots(p_k-1).$$

Kod kongruencija korisno je znati česte kvadratne, kubne i ostale ostatke koje koristimo. Npr: kvadrat broja pri dijeljenju s 3 i 4 daje ostatke $0, 1$, modulo 8 daje $0, 1, 4$; kub prirodnog broja modulo 7 daje $0, 1, 6$. Općenito, m-ta potencija prirodnog broja daje "malo" ostataka modulo n ako je $m = \varphi(n)$ (ti ostatci su 0 i 1) ili $2m = \varphi(n)$ (ti ostatci su 0 i ± 1).

Što se tiče faktorizacija, postoje razne i teško ih je sve pobrojati. Navodimo neke ideje: $(x + A)(y + B) = C$, kvadratna jednadžba, korištenje algebarskih identiteta (razlika kvadrata, kubova i sl), supstitucija motivirana Vietom ($a := mn, b := m + n$) faktorizacija polinoma u kompleksnim nultočkama. Također, postoji i jedan pomalo zaboravljeni identitet:

Identitet Sophie Germain:

$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2).$$

Također, kod faktorizacija, pomaže i uvođenje mjere nepoznanica, kako bi se pokrilo više slučajeva. Izrazito korisno u eksponencijalnim jednadžbama. Također, uvođenje mjere nam omogućuje da imamo zaključke poput: umnožak dva relativno prosta broja je k-ta potencija prirodnog broja ako i samo ako su oba broja k-ta potencija prirodnog broja.

Ograničavanje/smještanje među kvadrate i kubove

Ograničavanje se bazira na nejednakostima - dokazujemo da neka jednadžba nema rješenja (osim nekih jednostavnih) zbog toga što je jedna strana jednakosti veća od druge. Često kod faktorijela i Diofantskih jednadžbi iskazanih u racionalnom formatu.

Poseban slučaj je smještanje među kvadrate: ako primijetimo da se neki izraz nalazi između dva kvadrata (primjerice n^2 i $(n+1)^2$), tada zaključujemo da on ne može biti potpun kvadrat. Ponekad nećemo smještati između kvadrata, nego kubova, ili nekih većih potencija. Također, ponekad nećemo smještati između dva uzastopna kvadrata (ako je neki izraz potpun kvadrat, a nalazi se između $(x-1)^2$ i $(x+1)^2$, tada jedino što preostaje je da je on jednak broju x^2).

Beskonačni spust

Metoda kojom dokazujemo da jednadžba nema rješenja. Zasniva se na tome da prilikom rješavanja jednadžbe u nekom koraku opet dobijemo početnu jednadžbu, ali s "manjim" varijablama.

Prilikom zapisa, ne budite škrti tako da samo napišete "beskonačni spust". Koristite fraze poput "pretpostavimo da je (x, y) rješenje s minimalnom sumom/sumom kvadrata/ i sl", ili indukciju.

Jednadžbe s beskonačno rješenja

Pitagorine trojke. Neka su (a, b, c) prirodni brojevi koji zadovoljavaju $a^2+b^2 = c^2$. Tada postoje prirodni brojevi k, m, n t.d. su m, n relativno prosti brojevi različite parnosti takvi da je

$$a = k(m^2 - n^2),\ b = 2kmn,\ c = k(m^2 + n^2).$$

Kad već spominjemo Pitagorine trojke, podsjećamo na to da rješenja ne postoje ako se potencije 2 zamijene većima.

Veliki Fermatov teorem. Za $n \geq 3$ ne postoji rješenje jednadžbe $a^n + b^n = c^n$ u prirodnim brojevima.

Pellove jednadžbe. Jednadžba $x^2 - dy^2 = 1$, za d kvadratno slobodan broj veći od 1, naziva se Pellova jednadžba. Ona ima beskonačno rješenja u prirodnim brojevima zadana rekurzijom

$$(x_n + \sqrt{d}y_n) = (x_1 + \sqrt{d}y_1)^n,$$

gdje je (x_1, y_1) *najmanje* rješenje.
Postoje i Pellovske jednadžbe: $x^2 - dy^2 = N$, za neki cijeli N, s nešto drugačijim svojstvima.
Dobri materijali Link 1, Link 2.

Vieta jumping. Metoda kojom se može pokazivati beskonačnost rješenja i nepostojanje rješenja (poseban slučaj beskonačnog spusta). Ugrubo: Diofantsku jednadžbu u varijablama x, y gledamo kao kvadratnu jednadžbu po x s fiksiranim

y, koja ima dva rješenja: x i x'. Koristeći Vietove formule dokazujemo da je x' također prirodan broj, te ostala njegova svojstva (da je veći od x, ako želimo beskonačno rješenja, ili da je manji od x, ako želimo beskonačan spust). Jedan primjer Vieta jumpinga, i općenito više o Vieta jumpingu vidjeti na linku.

3.1 Nešto dijeli nešto

Nije metoda, ali je tip zadatka (odredi sve prirodne brojeve m, n takve da je neki razlomak cijeli broj). Pored svih ostalih navedenih metoda, česta ideja je koristeći osnovna svojstva djeljivosti (zbroj dva broja djeljiva s d djeljiv je s d i sl) da u nazivniku dobijemo broj koji je veći od brojnika. Opširnije, koristite sljedeće:

- $ab = cd \implies a \mid cd,\ b \mid cd,\ c \mid ab,\ d \mid ab$
- $p \mid ab \implies p \mid a$ ili $p \mid b$
- $c \mid ab,\ M(a,c) = 1 \implies c \mid b$
- $ab \mid c,\ M(a,c) = 1 \implies b \mid c$
- $a \mid c, b \mid c,\ M(a,b) = 1 \implies ab \mid c$
- $c \mid a,\ c \mid b \implies c \mid \alpha a + \beta b,\ \forall \alpha, \beta \in \mathbb{Z}$

  (Ovo se ponekad koristi i kada je jedan od brojeva a, b jednak c; tj. ako znamo samo da izraz A dijeli izraz B, tada ćemo najćešće raditi transformacije oblika $A \mid \alpha A + \beta B$.)
- $c \mid a \implies |a| \geq |c|$ ili $a = 0$

3.2 Kongruencije - nešto naprednije tvrdnje

Korištenjem malog Fermatovog teorema može se pokazati i sljedeća lema.

Poznata lema. Broj oblika $n^2 + 1$ nema prostih faktora oblika $4k + 3$.

Posljedica toga je jedna od sljedećih tvrdnji:

Zapis prirodnog broja kao zbroj nekoliko kvadrata. Broj prikaziv kao zbroj dva kvadrata cijela broja ako i samo ako mu je svaki prost faktor oblika $4k+3$ na parnu potenciju u rastavu. Broj je prikaziv kao zbroj tri kvadrata cijela broja ako i samo ako nije oblika $4^a(8b + 7)$. Svaki prirodan broj je prikaziv kao zbroj četiri kvadrata cijela broja.

Oprez: u gornjim tvrdnjama dopuštena je 0 u zbrojevima.

Što se tiče kvadratnih neostataka, postoje još neke tvrdnje poput: broj oblika n^2+2 nema prostih faktora oblika $8k+5$, $8k+7$; broj oblika n^2+3 nema prostih faktora oblika $6k + 5$. One su posljedice *Gaussovog zakona reciprociteta.* Za one koji žele znati više: link.

Uz Feromatov i Eulerov teorem veže se pojam reda.

Red od a modulo n. Broj r zovemo red od a modulo n (oznaka: $r = \mathrm{ord}_n\, a$) ako je najmanji prirodan broj takav da je $a^r \equiv 1\ (mod\ n)$. Jedno njegovo svojstvo:

$a^k \equiv 1 \ (mod\ n) \iff \mathrm{ord}_n\, a \mid k$. Eulerov teorem tvrdi da red uvijek postoji za relativno proste a, n.

Multiplikativni inverzi. Prirodan broj a je multiplikativni inverz broja b modulo n ako je $ab \equiv 1 (mod\ n)$. Ako su a, n relativno prosti, postoji i jedinstven je modulo n (egzistencija: $b = a^{\varphi(n)-1}$; jedinstvenost: oduzmi dva).

Multiplikativni inverzi korisni kad znate da postoje, i da znate da kongruencija $a/b \equiv c \ (mod\ n)$ ima smisla ($1/b$ označava multiplikativni inverz od b).

Možete se pitati postoji li element kojemu je red upravo jednak $\varphi(n)$. Postoji u posebnim slučajevima.

Teorem o primitivnom korijenu. Primitivni korijen modulo n (broj koji potenciran redom na $1, 2, 3 \ldots, \varphi(n)$ daje različite ostatke modulo n) postoji ako i samo ako je $n = 2, 4, p^j$ ili $2p^j$, za neparan prost p.

Posebno, ovo znači da za sve proste brojeve možete naći k takav da k potenciran na sve potencije $1, 2, \ldots, p-1$, u uniji s 0, čini potpun sustav ostataka modulo n.

4 Funkcije u teoriji brojeva

Osim Eulerove φ funkcije, postoje još neke funkcije s ružnim formulama. One su multiplikativne: za relativno proste m, n vrijedi $f(mn) = f(m) \cdot f(n)$, $f(1) = 1$. Zadane su preko rastava na proste faktore:

$$n = p_1^{a_1} \cdots p_k^{a_k}.$$

Broj djelitelja broja n. Funkcija $d(n)$ (ponekad $\tau(n)$), broj djelitelja od n, dana je formulom

$$d(n) = (1 + a_1)(1 + a_2) \cdots (1 + a_k).$$

Iz ove formule, ali i mnogo lakše (uparivanjem djelitelja), vidimo da je $d(n)$ neparan ako i samo ako je n potpun kvadrat.

Zbroj djelitelja broja n. Funkcija $\sigma(n)$, zbroj djelitelja od n, dana je formulom

$$\begin{aligned}\sigma(n) &= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1} \\ &= (1 + p_1 + p_1^2 + \cdots p_1^{a_1})(1 + p_2 + p_2^2 + \cdots p_2^{a_2}) \cdots (1 + p_k + p_k^2 + \cdots p_k^{a_k})\end{aligned}$$

Tri navedene funkcije imaju svojstvo multiplikativnosti. Uočite i da njihovi umnošci i omjeri imaju to svojstvo. Ponekad je to korisno. Neke funkcijske jednadžbe u teoriji brojeva se isto lakše rješavaju kada znate da su multiplikativne, njihovo ponašanje treba samo definirati na potencijama prostih.

Funkcije u nastavku više nisu multiplikativne.

Najveći zajednički višekratnik i najmanji zajednički djelitelj. Definicije za $M(a, b)$ i $V(a, b)$. Najpoznatija relacija: $ab = M(a, b) \cdot V(a, b)$.

Najveće cijelo $\lfloor x \rfloor$ je najveći cijeli broj koji je manji ili jednak od x. Primjer: $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$.

Najmanje cijelo $\lceil x \rceil$ je najmanji cijeli broj koji je veći ili jednak od x. Primjer: $\lceil \pi \rceil = 4$, $\lceil -\pi \rceil = -3$.

Razlomljeni dio $\{x\}$ se definira kao $x - \lfloor x \rfloor$. Primjer: $\{\pi\} = 0.1415\ldots$, $\{-\pi\} = 0.8584\ldots$.

Svojstva:

1. $\lfloor x \rfloor = -\lceil -x \rceil$, za sve x.
2. $x - 1 < \lfloor x \rfloor \leq x$, uz jednakost kada je x cijeli broj.
3. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, ako je n cijeli broj.
4. $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$.
5. $\lfloor x \cdot y \rfloor \geq \lfloor x \rfloor \cdot \lfloor y \rfloor$, za sve pozitivne x, y.

Uz najveće cijelo se veže i sljedeća tvrdnja.

Rastav broja $n!$ na proste faktore. U rastavu broja $n!$ na proste faktore, eksponent na prostom broju p jednak je

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

5 Jaki teoremi

Kineski teorem o ostatcima. Neka su $n_1, n_2, \ldots, n_k$ relativno prosti prirodni brojevi. Tada za svaki izbor cijelih brojeva $a_1, a_2, \ldots a_k$ postoji rješenje sustava

$$x \equiv a_1 \ (mod\ n_1)$$

$$x \equiv a_2 \ (mod\ n_2)$$

$$\ldots$$

$$x \equiv a_k \ (mod\ n_k).$$

To je rješenje jedinstveno $(mod\ n_1 n_2 \ldots n_k)$.

Dirichletov teorem. *Ne miješati s Dirichletovim principom.* Svaki aritmetički niz kojemu su prvi član i razlika niza relativno prosti sadrži beskonačno mnogo prostih brojeva. (Drugim riječima, ako je $M(a, b) = 1$, tada niz $a, a+b, a+2b, a+3b, \ldots$ sadrži beskonačno mnogo prostih brojeva).

Wilsonov teorem. Za prirodan broj p vrijedi da je prost ako i samo ako vrijedi $(p-1)! \equiv -1 \ (mod\ p)$.

Bertrandov postulat. Za svaki prirodan broj n postoji barem jedan prost broj p takav da je $n \leq p \leq 2n$. Nadalje, za svaki prirodan broj $n > 3$ postoji barem jedan prost broj p takav da je $n < p < 2n - 2$.

6 Još jači teoremi

Lifting the exponent lemma. Teorija koja u sebi sadrži više tvrdnji poput sljedeće. Neka su x, y cijeli brojevi čija je razlika djeljiva s neparnim prostim brojem p. Tada je

$$v_p\left(x^n - y^n\right) = v_p(x-y) + v_p(n),$$

gdje je $v_p(z)$ najveći nenegativan cijeli broj m t.d $p^m \mid z$. Detaljnije na linku.

Mihăilescu theorem (ili Catalan conjecture). Jedine dvije potencije (eksponent veći od 1) prirodnih brojeva koje se razlikuju za 1 su 3^2 i 2^3.

Zsigmondyjev teorem. Neka su a, b relativno prosti prirodni brojevi, a n prirodan broj. Tada (osim u nekim izuzetcima) postoji prost broj p koji dijeli $a^n - b^n$, a ne dijeli $a^k - b^k$ ni za koji drugi $k < n$. Izuzetci su: $n = 1, a - b = 1$; $n = 2, a + b = 2^\alpha$; $n = 6, a = 2, b = 1$. Nadalje, analogna tvrdnja vrijedi za izraz $a^n + b^n$, uz izuzetak $2^3 + 1^3 = 9$.

Lucasov teorem. Neka je p prost, te m, n prirodni brojevi, gdje su $\overline{m_k m_{k-1} \cdots m_1 m_0}$ i $\overline{n_k n_{k-1} \cdots n_1 n_0}$ njihovi zapisi u bazi p redom. Tada vrijedi

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Wolstenholmeov teorem. Za bilo koja dva nenegativna cijela broja a, b te prost broj $p > 3$ vrijedi

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

MEMO pripreme 2019., predavanje: Teorija brojeva

sastavio: Matko

4. 6. 2019.

1. zadatak: Riješi u prirodnima $3^a + 4^b = 5^c$.

2. zadatak: Riješi u prirodnima $x^2 = y^3 + 7$.

3. zadatak: Riješi u cijelima $x^2(y-1) + y^2(x-1) = 1$.

4. zadatak: Dokaži da je $n^4 + 4^n$ složen broj za sve prirodne $n > 1$.

5. zadatak: Dokaži da se ni za koji $n \in \mathbb{N}$ skup $\{n, n+1, \ldots, n+17\}$ ne može particionirati na dva skupa takva da imaju jednake umnoške elemenata.

6. zadatak: Riješi u prirodnima $n \mid 2m-1$, $m \mid 2n-1$.

7. zadatak: Dan je (beskonačan) niz $(a_n)_{n\geq 1}$, zadan s $a_n = NZV(1, 2, \ldots, n)$. Dokaži da postoji mjesto u nizu nakon kojeg se ista vrijednost ponavlja 2019 puta.

8. zadatak: Dokaži da postoji (beskonačan) niz $(b_n)_{n\geq 1}$ u kojem se svaki prirodan broj pojavljuje točno jednom te je suma prvih n elemenata dijeljiva s n, za svaki prirodan n.

9. zadatak: Iz skupa $\{1, 2, \ldots, 2n\}$ odabrano je $n+1$ brojeva. Dokaži da među njima postoje dva koji u sumi daju prost broj.

10. zadatak:

a) Dokaži da za svaki prirodan n postoje različiti prirodni x, y takvi da $y + j \mid x + j$, za sve $1 \leq j \leq n$.

b) Postoje li različiti prirodni x, y takvi da $y+j|x+j$ za sve $j \in mathbbN$?

MEMO pripreme 2019., tulum: Diofantske jednadžbe

sastavio: Matko

4. 6. 2019.

1. zadatak: Dani su relativno prosti prirodni brojevi a, b takvi da je $\frac{a+b}{a-b}$ prirodan broj. Dokaži da je tada točno jedan od brojeva $4ab+1, ab+1$ potpun kvadrat.

2. zadatak: Riješi u skupu prirodnih brojeva

$$x! + y! + z! = 2^{u!}.$$

3. zadatak: Nađi prirodne a, b, n i proste p takve da

$$a^{2013} + b^{2013} = p^n.$$

4. zadatak: Dokaži da jednadžba $x^2 + y^5 = z^3$ ima beskonačno mnogo rješenja u prirodnim brojevima.

5. zadatak: Dani su prirodni brojevi a, b takvi da su $\frac{b+1}{a}$ i $\frac{a^2-2}{b}$ cijeli. Dokaži da je $\frac{b+1}{2}$ kvadrat prirodnog broja.

6. zadatak: Nađi sve prirodne brojeve x, y, z takve da vrijedi

$$3^x - 5^y = z^2.$$

7. zadatak: Nađi sve prirodne a, b, c, n takve da vrijedi

$$(a^3 + b^2 + c^2)^2 = n^2 a^4 bc,$$

uz uvjet $a \geq b$, $a \geq c$.