"Višje" metode v teoriji števil

Luka Urbanc, 6. november 2024

1 "Karakterizacijske" oz. "diofantske" naloge

Zanima nas, za katere n nekaj velja. Hočemo torej izločiti čim več n, da nam ostane le neka obvladljiva podmnožica (pogosto končna). Kako to doseči? *Omejimo* n po "velikosti". Če je $n \in \mathbb{Z}$ ali $\mathbb{Q}$, so najpogostejše "velikosti" absolutna vrednost in p-adična valuacija (za polinome pa lahko uporabimo npr. stopnjo). Glavno je torej ugotoviti, kakšno velikost in velikost česa nam pogoj naloge omogoči omejiti. Pridevnika "aditivna" in "multiplikativna" naloga se nanašata na to, ali se moramo pri nalogi bolj osredotočiti na absolutno vrednost ali p-adično valuacijo. Pri aditivnih je ponavadi ključna pametna uporaba neenakosti, Evklidovega algoritma in dejstva, da je najmanjše naravno število 1. Pri multiplikativnih pa nam prav pridejo redi in vseh nešteto lemic, povezanih z njimi (primitivni koreni, LTE, kvadratna recipročnost, ciklotomični polinomi in Zsigmondyjev izrek...). Da jih lahko kreativno uporabimo, pa jih je dobro razumeti *heuristično*. To pomeni, da izrek razumemo abstraktneje kot le enačbo.

Evklidov algoritem	Z njim preoblikujemo pogoje z deljivostmi, da dobimo lepše (krajše, manjše) izraze.
Kitajski izrek o ostankih	Modulo $n \cong$ modulo $p^{\nu_p(n)}$ $\forall p \in \mathbb{P}$.
Henselova lema	V kombinaciji s kitajskim izrekom o ostankih pove, da so rešitve polinoma modulo n skoraj popolnoma odvisne le od rešitev modulo p za $p \in \mathbb{P}$.
Lema o dvigu eksponenta	Če poznamo $\nu_p(a \pm b)$, lahko izračunamo $\nu_p(a^n \pm b^n)$.
Obstoj primitivnih korenov	Multiplikativne probleme modulo n lahko pretvorimo v aditivne modulo $\varphi(n)$.
Kvadratna recipročnost	Znamo rešiti kvadratne enačbe modulo p. Dobimo malo dodatnih informacij o redih števil. Imamo dodatne "simetrije" modulo p.
Lastnosti ciklotomičnih polinomov	Elementi reda n so natanko ničle n-tega ciklotomičnega polinoma. To velja v $\mathbb{C}$, poleg tega pa še npr. modulo p.
Zsigmondyjev izrek	Za skoraj vsak racionalen r in naraven n obstaja praštevilo p, da je $\mathrm{ord}_p(r) = n$.
Dirichletov izrek	Če za "kongruenčni pogoj" ni očitno, da ga izpolnjuje največ končno mnogo praštevil, jih ga mora izpolnjevati neskončno mnogo.
Neskončni spust (Vieta, Fermat)	Če lahko iz neke rešitve generiramo manjšo, lahko vse rešitve povežemo s končno mnogimi (pogosto 0).

1.1 Aditivne

Naloga 1.1. Najdi vse pare celih števil (x, y), da $x^2 + y^2$ deli $x^3 + y$ in $x + y^3$.

Naloga 1.2. Najdi vse pare $(a, b) \in \mathbb{N}^2$, za katere velja, da $a^2b - 1$ deli $ab^3 - 1$.

Naloga 1.3. Najdi vse trojice $x, y \in \mathbb{N}, p \in \mathbb{P}$, za katere velja $x^3 + y^3 = p(xy + p)$.

Naloga 1.4. Določi vse pare $(a, p) \in \mathbb{N} \times \mathbb{P}$, da je $p^a + a^4$ popoln kvadrat.

Naloga 1.5. Najdi vse pare naravnih števil (a, b), za katere velja $a \mid b^2 + 1$ in $b \mid a^2 + 1$.

Naloga 1.6. Določi vse pare praštevil (p, q), za katere $pq \mid p^3 + q^3 + 1$.

1.2 Multiplikativne

Naloga 1.7. Če za $a, b, c \in \mathbb{Z}$ velja $a^2c + b^2a + c^2b = 0$, dokaži, da mora veljati $a^2b + b^2c + c^2a = 0$.

Naloga 1.8. Najdi vsak $n \in \mathbb{N}$, da je za vsak tuji par njegovih deliteljev a, b tudi $a + b - 1$ delitelj n.

Naloga 1.9. Racionalno število je *pogenčno*, če ga lahko zapišemo kot $\frac{m^k}{n}$ za $k, m, n \in \mathbb{N}$, kjer sta m in n tuja in $k > 1$. Naj bodo a, b, c pozitivna racionalna števila, za katera velja $abc = 1$ in za neke naravne x, y, z velja, da je $a^x + b^y + c^z$ naravno število. Dokaži, da so a, b in c pogenčna števila.

Naloga 1.10. Dokaži, da $3(ab + bc + ca) \nmid a^2 + b^2 + c^2$ za vse $a, b, c \in \mathbb{Z}\backslash\{0\}$.

Naloga 1.11. Za katere naravne n obstaja natanko eno celo število a, da $0 \leq a < n!$ in $n! \mid a^n + 1$?

Naloga 1.12. Če za naravni števili m, n velja $\varphi(5^m - 1) = 5^n - 1$, dokaži, da si nista tuji.

Naloga 1.13. Najdi vse polinome s celoštevilskimi koeficienti $f \in \mathbb{Z}[x]$, za katere velja $f(p) \mid 2^p - 2\ \forall p \in \mathbb{P}$.

2 Konstrukcijske naloge

Medtem ko karakterizacijske naloge rešimo z implikacijami iz danega pogoja v $n \in \mathcal{M}$, tu iščemo ravno obratno implikacijo. Ker nam množica $\mathcal{M}$ ni vnaprej znana, je potrebno na neki točki izvesti miselni preskok in "uganiti," katera števila bi lahko zadoščala pogoju.

V teoriji števil je ogromno odprtih problemov, ki se jih je dobro zavedati, da na olimpijadi ne zapravljamo časa. Beri https://en.wikipedia.org/wiki/Category:Unsolved_problems_in_number_theory.

Naloga 2.1. Ali obstajajo naravna števila a, b in N, da je $ap + bq$ praštevilo za vsa različna praštevila $p, q > N$?

Naloga 2.2. Najdi vse pare $(p, k) \in \mathbb{P}\times\mathbb{N}$, za katere obstajata naravni števili $x, y \in \mathbb{N}$, da velja $p^k \mid x^2+y^2+1$.

Naloga 2.3. Dokaži, da za vsa naravna števila a, b in c obstaja naravno število x, da je $a^x + x \equiv b \pmod{c}$.

Naloga 2.4. Dokaži, da $\forall a, b, c \in \mathbb{N}$ obstaja naravno število k, da je $\gcd(a^k + bc, b^k + ca, c^k + ab) > 1$.

Naloga 2.5. Dokaži, da za vsak $n \in \mathbb{N}$ obstaja neskončno $k \in \mathbb{N}$, za katere je $\left\lfloor \frac{n^k}{k} \right\rfloor$ lih.

Naloga 2.6. Dokaži, da za vsa praštevila p obstaja praštevilo q, da $q \nmid n^p - p\ \forall n \in \mathbb{N}$. (Posplošitev: dokaži, da enako velja, če je p katerokoli naravno število, različno od 1).

Naloga 2.7. Dokaži, da obstaja $k \in \mathbb{N}$, za katerega je $\forall n \in \mathbb{N}$ število $k \cdot 2^n + 1$ sestavljeno.

3 Nekaj tretjega

Naloga 3.1. Dokaži, da $\forall n \in \mathbb{N}$ število $(1^4 + 1^2 + 1)(2^4 + 2^2 + 1) \cdots (n^4 + n^2 + 1)$ ni popolni kvadrat.

Naloga 3.2. Naj bo $n \in \mathbb{N}$. Če je $p = 4n + 1$ praštevilo, dokaži, da $p \mid n^n - 1$.

Naloga 3.3. Izračunaj izraz

$$\sum_{k=0}^{2001} \left\lfloor \frac{2^k}{2003} \right\rfloor.$$

Naloga 3.4. Dokaži, da ima za $3 \leq n \in \mathbb{N}$ število $2^{2^n} + 1$ prafaktor, večji od $2^{n+4}(n + 2)$.

Naloga 3.5. Naj bo p fiksno praštevilo, k pa naravno število, za katerega so si vsa števila $a_i = i^k + i$ za $i = 0, 1, \ldots, p - 1$ paroma različna modulo p. Določi vse možne ostanke $a_2 \pmod{p}$.

Naloga 3.6. Naravno število je *sveže*, če se ga da zapisati v obliki $a^2 + 5b^2$ za neki tuji si naravni števili a in b. Naj bo $p \equiv 3 \pmod 4$ praštevilo. Dokaži: če p deli neko sveže število, je $2p$ svež.

Naloga 3.7. Najdi vse pare naravnih števil (a, b), za katere obstaja neskončno $n \in \mathbb{N}$, da $n^2 \mid a^n + b^n$.

4 Namigi

Dešifriraj z ROT-13 (https://www.dcode.fr/rot-13-cipher).

Naloga 1.1. Namig 1: rixyvq va bzrwrinawr. Namig 2: m tpqkl wr ran qbxnmv k an xinqeng cyhf l an xinqeng qryv kl zvahf ran.
Naloga 1.2. Namig 1: rixyvq va bzrwrinawr. Namig 2: cbgerohwrf qrywvibfgv m n xeng o an gev zvahf ran, o an qin zvahf n, n an gev zvahf o, n an crg zvahf ran.
Naloga 1.3. Namig 1: bzrwrinawr abir fcerzraywvixr. Namig 2: qbxnmv k cyhf l znaw xbg qinxeng c.
Naloga 1.4. Namig 1: tebmab bzrwrinawr. Namig 2: rxfcbaragar shaxpvwr wr qboeb bzrwvgv f cbyvabzfxvzv, anwynmwr m vaqhxpvwb.
Naloga 1.5. Namig 1: ivrgn whzcvat. Namig 2: anwcerw mqehmv qrywvibfgv i rab rxivinyragab.
Naloga 1.6. Namig 1: znyb pnfrjbexn va ivrgn. Namig 2: anwcerw ybpv an qir qrywvibfgv va boenianinw ifnxb cbfrorw, angb fcrg mqehmv.
Naloga 1.7. Namig 1: cnqvpabfg. Namig 2: pr wr ifbgn geru fgrivy avp fgn anwznawfn qin icwn ranxn.
Naloga 1.8. Namig 1: sbxhf an anwznawfrz censnxgbewh. Namig 2: imrzv n zva censnxgbe a, o cn a qrywrab m znxfvznyab cbgrapb n. xngrev censnxgbewv a ynuxb qryvwb n cyhf o zvahf ran?
Naloga 1.9. Namig 1: onfu cnqvpabfgv fgripri va vzrabinypri.
Naloga 1.10. Namig 1: xinqengav bfgnaxv. Namig 2: cbfxhfv vm geru xinqengbi arxnxb hfginevgv rartn, angb tyrw cenfgrivyn zbqhyb gev.
Naloga 1.11. Namig 1: mn a cenfgrivyn qbxnmv, qn vzn n rqvafgira bfgnarx zbqhyb c an e mn ifr c an e, xv fb znxfvznyar cbgrapr c, xv qryvwb a snxhygrgn.
Naloga 1.12. Namig 1: f xinqengab erpvcebpabfgwb va qehtvzv bebqwv qbxnmv, qn fb yvuv censnxgbewv crg an z zvahf ran ifv fgvev zbqhyb crg. Namig 2: cebgvfybiwr cb cneabfgv fgrivyn censnxgbewri crg an z zvahf ran.
Naloga 1.13. Namig 1: m qvevpuyrgbz anwqv cenfgrivyn c, d, qn fgn s bq c va s bq d bon qrywvin m arxvz cenfgrivybz e.
Naloga 2.1. Namig 1: qvevpuyrgbi vmerx. Namig 2: svxfvenw d va fr arxb cenfgrivyb e, m qvevpuyrgbz vmorev c cbywhoab iryvx, qn wr nc cyhf od qrywvi m e
Naloga 2.2. Namig 1: vaqhxpvwn an x, urafry. Namig 2: onmb qbxnmv m anprybz tbyboawnxn.
Naloga 2.3. Namig 1: vaqhxpvwn an p. Namig 2: mn vaqhxpvwfxv xbenx hcbenov xvgnwfxv vmerx b bfgnaxvu va qrwfgib, qn wr tpq bq p va rhyrewrir cuv shaxpvwr p znawfr bq p.
Naloga 2.4. Namig 1: mryvzb, qn c qryv ifr gev. mn xngreb vmoveb x fb ifr gev ranxr zbq c?
Naloga 2.5. Namig 1: vmorev gnxr x, qn wr bfgnarx a an x (zbq x) ran.
Naloga 2.6. Namig 1: ubprzb xbagebyvengv erq c zbq d, mngb pvxybgbzvpav cbyvabzv cevqrwb ceni. Namig 2: erq c zbq d ar fzr qryvgv (d zvahf ran) qrywrab m (tpq c va d zvahf ran), mnqbfpn gberw qn wr erq c zbq d ranx c va qn c an xinqeng ar qryv d zvahf ran.
Naloga 2.7. Namig 1: pr c qryv qin an o zvahf ran va wr x xbatehragra zvahf (qin an (o zvahf n)) zbqhyb c mn arx n, irpwv nyv ranx avp va znawfv bq o, cbgrz wr, xb wr a xbatehragra n zbq o, x xeng qin an a cyhf ran qrywvi f c. anwgv wr geron gnxr cner (n,o), qn gnxb cbxevwrzb ifr a. pr fb cevcnqnwbpv c enmyvpav, ynuxb f xvgnwfxvz vmerxbz b bfgnaxvu anwqrzb cbywhoab iryvx x, xv erfv anybtb. qn obqb xbatehrapr cbxevyr ifr a, ubprzb, qn wr ypz o-wri znwura, mngb vmorerzb gnx ypz, xv vzn iryvxb qryvgrywri. Namig 2: ypz fgvevvaqinwfrg m o wr qin, gev, fgvev, bfrz, qinanwfg, fgvevvaqinwfrg qryhwr.
Naloga 3.1. Namig 1: yrcn snxgbevmnpvwn k an fgvev cyhf k an qin cyhf ran, angb bzrwrinawr. Namig 2: snxgbewn ynuxb mncvfrf xbg c bq k va c bq (k cyhf ran). Namig 3: pr ov ovy cerbfgnyv pyra xinqeng, enmzvfywnw b awrtbivu fbfrqawvu xinqengvu.
Naloga 3.2. Namig 1: rhyrewri xevgrevw mn xinqengar bfgnaxr. Namig 2: vmenmv a vm c va cbyrcfnw cbtbw zbqhyb c. Namig 3: qin wr xinqengav bfgnarx zbq c pr va fnzb pr wr c ran nyv frqrz zbq bfrz.
Naloga 3.3. Namig 1: arpryv qryv enpvbanyartn fgrivyn fb rxivinyragav bfgnaxbz zbq vzrabinyrp. Namig 2: xnxb anwyrcfr cbcnepxngv bfgnaxr? vqrnyab ov ovyb x va qin gvfbp gev zvahf x, fnw ov fr arpryv qryv irqab frfgryv i ran. Namig 3: qin av xinqengav bfgnarx zbq qin gvfbp gev.
Naloga 3.4. Namig 1: bzrwv fgrivyb censnxgbewri vm boru fzrev. Namig 2: qbxnmv, qn mn censnxgbewr irywn, qn fb xbatehragav ran zbqhyb qin an (a cyhf qin). Namig 3: mncvfv c-wr xbg qin an (a cyhf qin) xeng n cyhf ran, awvubi cebqhxg bcnmhw zbqhyb cbgrapr qin.
Naloga 3.5. Namig 1: cebqhxg cbcbyartn fvfgrzn bfgnaxbi oerm avp wr zvahf ran. Namig 2: xngrev cbyvabz vzn avpyr eniab an (x zvahf ran)-gvu cbgrapnu bfgnaxbi?
Naloga 3.6. Namig 1: hcbenov vmerx zvaxbjfxrtn (mtyrq anw ob qbxnm vmerxn b ifbgnu qiru xinqengbi).
Naloga 3.7. Namig 1: pr bofgnwn yvu censnxgbe c bq n cyhf o va n cyhf o av gev, vaqhxpvwfxb xbafgehvenzb mncberqwr qryhwbpvu a. Namig 2: vaqhxpvwb vmirqrzb m qbqnwnawrz cenfgrivy, xv wvu qbovzb vm mfvtzbaqlwn, a-wh. Namig 3: ybpv an cevzrer: n va o avfgn ghwn, n cyhf o wr gev, n cyhf o wr cbgrapn qir va fgn ghwn, ifr bfgnyb.