PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **20** (1992/1993)
Številka 2
Strani 120–123

Borut Zalar:

UPORABA OSTANKOV PRI PROBLEMIH IZ TEORIJE ŠTEVIL

Ključne besede: matematika, teorija števil, praštevila, ostanek, deljivost.

Elektronska verzija: http://www.presek.si/20/1127-Zalar.pdf

UPORABA OSTANKOV PRI PROBLEMIH IZ TEORIJE ŠTEVIL

Ogledali si bomo uporabo ostankov pri nekaterih problemih iz teorije naravnih števil, ki navidez nimajo z ostanki nobene direktne zveze. Včasih se namreč izkaže, da različni algebraični izrazi ne morejo biti povsem poljubni, ampak imajo pri deljenju z nekaterimi števili povsem določene ostanke. Oglejmo si najprej preprost zgled.

Zgled 1. *Dokaži, da enačba* $x^2 - 3y = 14$ *nima rešitve v naravnih številih.*

Pri deljenju s 3 ima število x lahko tri različne ostanke:

1. možnost. Število x je oblike $3k$.

Tedaj je število $x^2 - 3y$ deljivo s 3 (z drugimi besedami $x^2 - 3y$ ima pri deljenju s 3 ostanek 0) in zato ne more biti enako 14, ki ima pri deljenju s 3 ostanek 2.

2. možnost. Število x je oblike $3k + 1$.

Tedaj je

$$x^2 - 3y = 9k^2 + 6k + 1 - 3y = 3(3k^2 + 2k - y) + 1,$$

torej ima število $x^2 - 3y$ pri deljenju s 3 ostanek 1 in zato ne more biti enako 14.

3. možnost. Število x je oblike $3k + 2$.

Tedaj je

$$x^2 - 3y = 9k^2 + 12k + 4 - 3y = 3(3k^2 + 4k + 1 - y) + 1,$$

torej število $x^2 - 3y$ ne more biti enako 14.

Ker smo upoštevali vse možnosti in rešitve nismo dobili, enačba pač ni rešljiva v naravnih številih.

S podobnim prijemom bomo ugnali malce drugačen problem.

Zgled 2. *Poišči vsa tista naravna števila* n*, za katera je število* $2^n - 1$ *popolni kvadrat.*

Napišimo nekaj prvih členov zaporedja:

$$2^1 - 1 = 1$$
$$2^2 - 1 = 3$$
$$2^3 - 1 = 7$$
$$2^4 - 1 = 15$$
$$2^5 - 1 = 31.$$

Vidimo, da dajo vsi členi, razen prvega, pri deljenju s 4 ostanek 3. Tudi v splošnem to z lahkoto dokažemo, saj je za vsak $n \geq 2$ število 2^n deljivo s 4. Od tod sledi:

Če bi veljalo $2^n - 1 = m^2$, potem bi moralo biti število m liho.

1. možnost. Število m je oblike $4k + 1$.

Tedaj je

$$m^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1$$

in da pri deljenju s 4 ostanek 1, zato ne more biti enako številu $2^n - 1$ za $n \geq 2$.

2. možnost. Število m je oblike $4k + 3$.

Tedaj je

$$m^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$$

in podobno kot prej ne more biti enako številu $2^n - 1$ za $n \geq 2$. Ostane nam še možnost $n = 1$, ki nam da edino rešitev $2^1 - 1 = 1^2$.

Zgled 3. *Dokaži, da obstaja neskončno mnogo naravnih števil, ki jih ni mogoče zapisati kot vsoto treh kubov naravnih števil.*

Če vzamemo naravno število n, moramo rešiti enačbo $n = x^3 + y^3 + z^3$ v naravnih številih ali pa pokazati, da rešitev te enačbe ne obstaja. Takoj se vidi, da za števila 2, 4, 5, 6, 7, 9, 11 enačba ni rešljiva. Na prvi pogled pa ni jasno, kaj je z rešljivostjo te enačbe za velike n. Na pomoč bomo tokrat poklicali ostanke pri deljenju z 9. Vzemimo poljubno naravno število x.

1. možnost. Število x je oblike $3k$.

Tedaj je x^3 očitno deljiv z 9.

2. možnost. Število x je oblike $3k + 1$.

Tedaj

$$x^3 = 27k^3 + 27k^2 + 9k + 1 = 9(3k^3 + 3k^2 + k) + 1$$

da pri deljenju z 9 ostanek 1.

3. možnost. Število x je oblike $3k + 2$.

Tedaj

$$x^3 = 27k^3 + 54k^2 + 36k + 8 = 9(3k^3 + 6k^2 + 4k) + 8$$

da pri deljenju z 9 ostanek 8.

To pomeni, da lahko dajo števila x^3, y^3 in z^3 pri deljenju z 9 ostanke 0, 1 ali 8. Zdaj imamo 27 možnih kombinacij glede na ostanke posameznih števil x^3, y^3 in z^3. Če preverimo vse, dobimo, da ima število $x^3 + y^3 + z^3$ lahko pri deljenju z 9 ostanek 0, 1, 2, 3, 6, 7 ali 8. To pomeni, da tistih števil, ki dajo pri deljenju z 9 ostanek 4 ali 5, ni mogoče izraziti kot vsoto treh kubov. Seveda je takih števil neskončno.

Še več informacij o ostankih dobimo takrat, ko imamo opravka s praštevili. Pri deljenju s 6 lahko liho število daje ostanek 1, 3 ali 5. Če pa imamo praštevilo različno od 3, potem pri deljenju s 6 tudi ostanek 3 ni možen. Če bi namreč imeli $p = 6k + 3 = 3(2k + 1)$, bi število p ne bilo praštevilo. Ta razmislek nam bo prišel prav v naslednjem zgledu.

Zgled 4. *Dokaži, da je število $p^2 - 1$ deljivo s 24 za vsako praštevilo p, ki je večje od 4:*

1. možnost Število p je oblike $6k + 1$. Tedaj je

$$p^2 - 1 = 36k^2 + 12k = 12k(3k + 1).$$

Torej je število $p^2 - 1$ deljivo z 12. Hitro se lahko prepričate, da je eno od števil k in $3k + 1$ sodo, drugo pa liho, kar pomeni, da je število $k(3k + 1)$ deljivo z 2, število $p^2 - 1$ pa s 24.

2. možnost. Število p je oblike $6k + 5$.

Tedaj je

$$p^2 - 1 = 36k^2 + 60k + 24 = 12(3k^2 + 5k + 2).$$

Hitro se lahko prepričate, da je število $3k^2 + 5k + 2$ vedno sodo, zato je število $p^2 - 1$ deljivo s 24.

Za konec pa še en zgled s praštevili.

Zgled 5. *Poišči vsa taka praštevila p, da je $14p^2 + 1$ praštevilo.*

Naj bo $p \neq 3$. Ker je p praštevilo, ni deljivo s 3, zato daje pri deljenju s 3 ostanek bodisi 1 bodisi 2.

1. možnost. Število p je oblike $3k + 1$.

Tedaj je število

$$14p^2 + 1 = 9 \cdot 14k^2 + 6 \cdot 14k + 15 = 3(42k^2 + 28k + 5)$$

in zato ni praštevilo.

2. možnost. Število p je oblike $3k + 2$.

Tedaj je število

$$14p^2 + 1 = 9 \cdot 14k^2 + 12 \cdot 14k + 57 = 3(42k^2 + 56k + 19)$$

in zato ni praštevilo. Če je $p = 3$, je $14p^2 + 1 = 127$. Z malce vztrajnosti se lahko sami prepričate, da je 127 praštevilo.

Borut Zalar