Vsota štirih kvadratov in Waringov problem

Nik Globočnik

Seminar, FMF

20. maj 2020

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$

$$2 = 1^2 + 1^2$$

$$3 = ?$$

$$4 = 2^2 + 0^2$$

$$5 = 2^2 + 1^2$$

$$6 = ?$$

$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ?$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ?$$
$$7 = ?$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko število zapišemo kot vsoto dveh kvadratov celih števil?

$$
\begin{aligned}
1 &= 1^2 + 0^2 \\
2 &= 1^2 + 1^2 \\
3 &= ? \\
4 &= 2^2 + 0^2 \\
5 &= 2^2 + 1^2 \\
6 &= ? \\
7 &= ?
\end{aligned}
$$

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko praštevilo p zapišemo kot vsoto dveh kvadratov celih števil?

$p = 2$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$2 = 1^2 + 1^2$	$5 = 2^2 + 1^2$	$3 = ?$
	$13 = 3^2 + 2^2$	$7 = ?$
	$17 = 4^2 + 1^2$	$11 = ?$
	$29 = 5^2 + 2^2$	$19 = ?$
	$\vdots$	$\vdots$

Izrek (Fermat)

Naravno število n lahko zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko ima vsak prafaktor p števila n, ki zadošča $p \equiv 3 \pmod 4$, v praštevilskem razcepu sod eksponent.

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko praštevilo p zapišemo kot vsoto dveh kvadratov celih števil?

$p = 2$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$2 = 1^2 + 1^2$	$5 = 2^2 + 1^2$	$3 = ?$
	$13 = 3^2 + 2^2$	$7 = ?$
	$17 = 4^2 + 1^2$	$11 = ?$
	$29 = 5^2 + 2^2$	$19 = ?$
	$\vdots$	$\vdots$

Izrek (Fermat)

Naravno število n lahko zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko ima vsak prafaktor p števila n, ki zadošča $p \equiv 3 \pmod 4$, v praštevilskem razcepu sod eksponent.

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko praštevilo p zapišemo kot vsoto dveh kvadratov celih števil?

$p = 2$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$2 = 1^2 + 1^2$	$5 = 2^2 + 1^2$	$3 = ?$
	$13 = 3^2 + 2^2$	$7 = ?$
	$17 = 4^2 + 1^2$	$11 = ?$
	$29 = 5^2 + 2^2$	$19 = ?$
	$\vdots$	$\vdots$

Izrek (Fermat)

Naravno število n lahko zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko ima vsak prafaktor p števila n, ki zadošča $p \equiv 3 \pmod 4$, v praštevilskem razcepu sod eksponent.

Fermatov izrek o vsotah dveh kvadratov

Kdaj lahko praštevilo p zapišemo kot vsoto dveh kvadratov celih števil?

$p = 2$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$2 = 1^2 + 1^2$	$5 = 2^2 + 1^2$	$3 = ?$
	$13 = 3^2 + 2^2$	$7 = ?$
	$17 = 4^2 + 1^2$	$11 = ?$
	$29 = 5^2 + 2^2$	$19 = ?$
	$\vdots$	$\vdots$

Izrek (Fermat)

Naravno število n lahko zapišemo kot vsoto dveh kvadratov celih števil natanko tedaj, ko ima vsak prafaktor p števila n, ki zadošča $p \equiv 3 \pmod 4$, v praštevilskem razcepu sod eksponent.

Nekaj izrekov

Izrek (Legendre)

Naravno število n lahko zapišemo kot vsoto treh kvadratov celih števil natanko tedaj, ko n ni oblike $4k(8\ell + 7)$.

Lema

Naj bo p liho praštevilo. Potem obstajajo cela števila x, y in m, da je

$$1 + x^2 + y^2 = mp, \quad 0 < m < p.$$

Primer

Za $p = 3$ imamo $1 + 1^2 + 2^2 = 2 \cdot 3$, za $p = 7$ pa $1 + 2^2 + 4^2 = 3 \cdot 7$.

Lema

Naj bo p liho praštevilo. Potem obstajajo cela števila x, y in m, da je

$$1 + x^2 + y^2 = mp, \quad 0 < m < p.$$

Primer

Za $p = 3$ *imamo* $1 + 1^2 + 2^2 = 2 \cdot 3$, *za* $p = 7$ *pa* $1 + 2^2 + 4^2 = 3 \cdot 7$.

- Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p.
  Premislek: Če bi bilo $x_1^2 \equiv x_2^2 \pmod{p}$, bi to pomenilo $p \mid (x_1 - x_2)(x_1 + x_2)$. Od tod pa bi sledilo
  $$x_1 \equiv \pm x_2 \pmod{p},$$
  kar pa je protislovje.
- Podobno sklepamo, da dajo za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, števila $-1 - y^2$ različne ostanke pri deljenju z p.
- V teh dveh množicah imamo skupno $p + 1$ števil, ampak samo p možnih ostankov pri deljenju s p.

- Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p.
  Premislek: Če bi bilo $x_1^2 \equiv x_2^2 \pmod p$, bi to pomenilo $p \mid (x_1 - x_2)(x_1 + x_2)$. Od tod pa bi sledilo
  $$x_1 \equiv \pm x_2 \pmod p,$$
  kar pa je protislovje.
- Podobno sklepamo, da dajo za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, števila $-1 - y^2$ različne ostanke pri deljenju z p.
- V teh dveh množicah imamo skupno $p + 1$ števil, ampak samo p možnih ostankov pri deljenju s p.

Vsota štirih kvadratov
Dokaz leme

- Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p.
  Premislek: Če bi bilo $x_1^2 \equiv x_2^2 \pmod{p}$, bi to pomenilo $p \mid (x_1 - x_2)(x_1 + x_2)$. Od tod pa bi sledilo
  $$x_1 \equiv \pm x_2 \pmod{p},$$
  kar pa je protislovje.
- Podobno sklepamo, da dajo za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, števila $-1 - y^2$ različne ostanke pri deljenju z p.
- V teh dveh množicah imamo skupno $p + 1$ števil, ampak samo p možnih ostankov pri deljenju s p.

- Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p.
  Premislek: Če bi bilo $x_1^2 \equiv x_2^2 \pmod p$, bi to pomenilo $p \mid (x_1 - x_2)(x_1 + x_2)$. Od tod pa bi sledilo
  $$x_1 \equiv \pm x_2 \pmod p,$$
  kar pa je protislovje.
- Podobno sklepamo, da dajo za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, števila $-1 - y^2$ različne ostanke pri deljenju z p.
- V teh dveh množicah imamo skupno $p + 1$ števil, ampak samo p možnih ostankov pri deljenju s p.

- Za $x \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$ imajo števila x^2 same različne ostanke pri deljenju s p.
  Premislek: Če bi bilo $x_1^2 \equiv x_2^2 \pmod{p}$, bi to pomenilo $p \mid (x_1 - x_2)(x_1 + x_2)$. Od tod pa bi sledilo
  $$x_1 \equiv \pm x_2 \pmod{p},$$
  kar pa je protislovje.

- Podobno sklepamo, da dajo za $y \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, števila $-1 - y^2$ različne ostanke pri deljenju z p.

- V teh dveh množicah imamo skupno $p + 1$ števil, ampak samo p možnih ostankov pri deljenju s p.

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod p \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod p$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \Rightarrow 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1-y^2 \pmod p \;\Rightarrow\; 1+x^2+y^2 \equiv 0 \pmod p$$

$$\Rightarrow\; 1+x^2+y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1+x^2+y^2 < 1+2\cdot\left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$.

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$.

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1 - y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

Vsota štirih kvadratov

Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1-y^2 \pmod{p} \;\Rightarrow\; 1+x^2+y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1+x^2+y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1+x^2+y^2 < 1+2\cdot\left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$.

□

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1 - y^2 \pmod{p} \;\Rightarrow\; 1 + x^2 + y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow\; 1 + x^2 + y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. □

Vsota štirih kvadratov
Dokaz leme

- Potem je vsaj eno število x^2 kongruentno $-1-y^2$ po modulu p. Torej

$$x^2 \equiv -1-y^2 \pmod p \ \Rightarrow\ 1+x^2+y^2 \equiv 0 \pmod p$$

$$\Rightarrow\ 1+x^2+y^2 = mp.$$

- Rabimo še oceno za m. Ker velja $x^2 < \left(\frac{p}{2}\right)^2$ in $y^2 < \left(\frac{p}{2}\right)^2$, je

$$mp = 1+x^2+y^2 < 1+2\cdot\left(\frac{p}{2}\right)^2 < p^2.$$

- In zato $m < p$. $\square$

Vsota štirih kvadratov

Izrek

Izrek (Lagrange)

Vsako naravno število lahko zapišemo kot vsoto štirih kvadratov celih števil.

Primer

$5 = 2^2 + 1^2 + 0^2 + 0^2$, $21 = 4^2 + 2^2 + 1^1 + 0^2$, $127 = 11^2 + 2^2 + 1^2 + 1^2$.

Izrek (Lagrange)

Vsako naravno število lahko zapišemo kot vsoto štirih kvadratov celih števil.

Primer

$5 = 2^2 + 1^2 + 0^2 + 0^2$, $21 = 4^2 + 2^2 + 1^1 + 0^2$, $127 = 11^2 + 2^2 + 1^2 + 1^2$.

- Najprej si oglejmo t. i. *Eulerjevo identiteto*:

$$
\begin{aligned}
(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\
&(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\
&+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
&+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\
&+ (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.
\end{aligned}
$$

- Vidimo, da je produkt dveh števil, ki sta vsoti štirih kvadratov, tudi vsota štirih kvadratov.

- Za število 1 je izrek trivialen. Vemo, da lahko vsako naravno število > 1 zapišemo kot produkt praštevil, zato je dovolj pokazati izrek za vsa praštevila.

- Najprej si oglejmo t. i. *Eulerjevo identiteto*:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=$$
$$\begin{aligned}&(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\+&(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\+&(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2\\+&(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2.\end{aligned}$$

- Vidimo, da je produkt dveh števil, ki sta vsoti štirih kvadratov, tudi vsota štirih kvadratov.

- Za število 1 je izrek trivialen. Vemo, da lahko vsako naravno število > 1 zapišemo kot produkt praštevil, zato je dovolj pokazati izrek za vsa praštevila.

Vsota štirih kvadratov

Dokaz izreka

- Najprej si oglejmo t. i. *Eulerjevo identiteto*:

$$
\begin{aligned}
(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = {} & \\
& (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\
& + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
& + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\
& + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.
\end{aligned}
$$

- Vidimo, da je produkt dveh števil, ki sta vsoti štirih kvadratov, tudi vsota štirih kvadratov.

- Za število 1 je izrek trivialen. Vemo, da lahko vsako naravno število > 1 zapišemo kot produkt praštevil, zato je dovolj pokazati izrek za vsa praštevila.

- Najprej si oglejmo t. i. *Eulerjevo identiteto*:

$$
\begin{aligned}
(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\
&(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\
&+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
&+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\
&+ (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.
\end{aligned}
$$

- Vidimo, da je produkt dveh števil, ki sta vsoti štirih kvadratov, tudi vsota štirih kvadratov.
- Za število 1 je izrek trivialen. Vemo, da lahko vsako naravno število > 1 zapišemo kot produkt praštevil, zato je dovolj pokazati izrek za vsa praštevila.

Vsota štirih kvadratov

Dokaz izreka

- Za $p = 2$ imamo $2 = 1^2 + 1^2 + 0^2 + 0^2$.
- V primeru, ko je p lih, si pomagamo s prej dokazano lemo.
- Iz leme direktno sledi, da za liho praštevilo p obstaja m, $0 < m < p$, da je
$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$
- Dokazali bomo, da je najmanjši tak m kar $m = 1$.

Vsota štirih kvadratov
Dokaz izreka

- Za $p = 2$ imamo $2 = 1^2 + 1^2 + 0^2 + 0^2$.
- V primeru, ko je p lih, si pomagamo s prej dokazano lemo.
- Iz leme direktno sledi, da za liho praštevilo p obstaja m, $0 < m < p$, da je
$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$
- Dokazali bomo, da je najmanjši tak m kar $m = 1$.

- Za $p = 2$ imamo $2 = 1^2 + 1^2 + 0^2 + 0^2$.
- V primeru, ko je p lih, si pomagamo s prej dokazano lemo.
- Iz leme direktno sledi, da za liho praštevilo p obstaja m, $0 < m < p$, da je
$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$
- Dokazali bomo, da je najmanjši tak m kar $m = 1$.

- Za $p = 2$ imamo $2 = 1^2 + 1^2 + 0^2 + 0^2$.
- V primeru, ko je p lih, si pomagamo s prej dokazano lemo.
- Iz leme direktno sledi, da za liho praštevilo p obstaja m, $0 < m < p$, da je
$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$
- Dokazali bomo, da je najmanjši tak m kar $m = 1$.

- Označimo z m_0 najmanjši tak m, da je

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

- Če je $m_0 = 1$ smo končali.
- Predpostavimo sedaj, da je $1 < m_0 < p$.

- Označimo z m_0 najmanjši tak m, da je

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

- Če je $m_0 = 1$ smo končali.
- Predpostavimo sedaj, da je $1 < m_0 < p$.

- Označimo z m_0 najmanjši tak m, da je

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

- Če je $m_0 = 1$ smo končali.
- Predpostavimo sedaj, da je $1 < m_0 < p$.

- Če je m_0 sod, so vsi x_i sodi ali lihi, ali pa sta po dva soda in po dva liha.
- Recimo, da sta x_1 in x_2 soda. Potem so v vsakem od zgornjih treh primerov $x_1 \pm x_2$ in $x_3 \pm x_4$ sodi.
- Zato lahko zapišemo

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

kar je v protislovju z minimalnostjo m_0.

- Če je m_0 sod, so vsi x_i sodi ali lihi, ali pa sta po dva soda in po dva liha.
- Recimo, da sta x_1 in x_2 soda. Potem so v vsakem od zgornjih treh primerov $x_1 \pm x_2$ in $x_3 \pm x_4$ sodi.
- Zato lahko zapišemo

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

kar je v protislovju z minimalnostjo m_0.

- Če je m_0 sod, so vsi x_i sodi ali lihi, ali pa sta po dva soda in po dva liha.
- Recimo, da sta x_1 in x_2 soda. Potem so v vsakem od zgornjih treh primerov $x_1 \pm x_2$ in $x_3 \pm x_4$ sodi.
- Zato lahko zapišemo

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

kar je v protislovju z minimalnostjo m_0.

- Če je m_0 sod, so vsi x_i sodi ali lihi, ali pa sta po dva soda in po dva liha.
- Recimo, da sta x_1 in x_2 soda. Potem so v vsakem od zgornjih treh primerov $x_1 \pm x_2$ in $x_3 \pm x_4$ sodi.
- Zato lahko zapišemo

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2,$$

kar je v protislovju z minimalnostjo m_0.

- Izberimo sedaj tak y_i, da je

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \frac{m_0}{2}.$$

(To lahko storimo, saj je $\{y \mid -\frac{m_0-1}{2} \leqslant y \leqslant \frac{m_0-1}{2}\}$ popoln sistem ostankov modulo m_0.)

- Opazimo, da ne morajo biti vsi x_i deljivi z m_0, saj bi potem imeli

$$m_0^2 \mid m_0 p \Rightarrow m_0 \mid p,$$

kar je protislovje.

- Izberimo sedaj tak y_i, da je

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \frac{m_0}{2}.$$

(To lahko storimo, saj je $\{y \mid -\frac{m_0-1}{2} \leqslant y \leqslant \frac{m_0-1}{2}\}$ popoln sistem ostankov modulo m_0.)

- Opazimo, da ne morajo biti vsi x_i deljivi z m_0, saj bi potem imeli

$$m_0^2 \mid m_0 p \Rightarrow m_0 \mid p,$$

kar je protislovje.

- Izberimo sedaj tak y_i, da je

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \frac{m_0}{2}.$$

(To lahko storimo, saj je $\{y \mid -\frac{m_0-1}{2} \leqslant y \leqslant \frac{m_0-1}{2}\}$ popoln sistem ostankov modulo m_0.)

- Opazimo, da ne morajo biti vsi x_i deljivi z m_0, saj bi potem imeli

$$m_0^2 \mid m_0 p \Rightarrow m_0 \mid p,$$

kar je protislovje.

- Izberimo sedaj tak y_i, da je

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \frac{m_0}{2}.$$

(To lahko storimo, saj je $\{y \mid -\frac{m_0-1}{2} \leqslant y \leqslant \frac{m_0-1}{2}\}$ popoln sistem ostankov modulo m_0.)

- Opazimo, da ne morajo biti vsi x_i deljivi z m_0, saj bi potem imeli

$$m_0^2 \mid m_0 p \Rightarrow m_0 \mid p,$$

kar je protislovje.

- Od tod sledi
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

- Imamo tudi
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \text{ in } y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

- Zato je
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \quad (m_0 < p)$$
in
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1 \quad (0 < m_1 < m_0).$$

- Od tod sledi

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

- Imamo tudi

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \text{ in } y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

- Zato je

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \quad (m_0 < p)$$

in

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1 \quad (0 < m_1 < m_0).$$

- Od tod sledi
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

- Imamo tudi
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \text{ in } y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

- Zato je
$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \quad (m_0 < p)$$
in
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1 \quad (0 < m_1 < m_0).$$

- Dobimo
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^4,$$
kjer so z_i primerni členi iz *Eulerjeve identitete*.

- Oglejmo si $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$:
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

- Torej je $z_1 \equiv 0 \pmod{m_0}$, podobmo pa pokažemo še za ostale z_i.

- Dobimo
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^4,$$
kjer so z_i primerni členi iz *Eulerjeve identitete*.

- Oglejmo si $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$:
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

- Torej je $z_1 \equiv 0 \pmod{m_0}$, podobmo pa pokažemo še za ostale z_i.

- Dobimo
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^4,$$
kjer so z_i primerni členi iz *Eulerjeve identitete*.

- Oglejmo si $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$:
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

- Torej je $z_1 \equiv 0 \pmod{m_0}$, podobmo pa pokažemo še za ostale z_i.

- Dobimo
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^4,$$
kjer so z_i primerni členi iz *Eulerjeve identitete*.

- Oglejmo si $z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$:
$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}.$$

- Torej je $z_1 \equiv 0 \pmod{m_0}$, podobmo pa pokažemo še za ostale z_i.

- Torej lahko pišemo
$$z_i = m_0 w_i,$$
za nek $w_i \in \mathbb{Z}$.

- Če enakost
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$$
delimo z m_0^2 dobimo
$$m_1 p = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$
kar pa je spet protislovje z minimalnostjo m_0.

- Zato je $m_0 = 1$. $\square$

- Torej lahko pišemo
$$z_i = m_0 w_i,$$
za nek $w_i \in \mathbb{Z}$.

- Če enakost
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$$
delimo z m_0^2 dobimo
$$m_1 p = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$
kar pa je spet protislovje z minimalnostjo m_0.

- Zato je $m_0 = 1$. $\square$

- Torej lahko pišemo
$$z_i = m_0 w_i,$$
za nek $w_i \in \mathbb{Z}$.

- Če enakost
$$m_1 m_0^2 p = z_1^2 + z_2^2 + z_3^2 + z_4^2$$
delimo z m_0^2 dobimo
$$m_1 p = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$
kar pa je spet protislovje z minimalnostjo m_0.

- Zato je $m_0 = 1$. $\square$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$
\begin{aligned}
1 &= 1^2 + 0^2 + 0^2 + 0^2 \\
2 &= 1^2 + 1^2 + 0^2 + 0^2 \\
3 &= 1^2 + 1^2 + 1^2 + 0^2 \\
4 &= 2^2 + 0^2 + 0^2 + 0^2 \\
5 &= 2^2 + 1^2 + 0^2 + 0^2 \\
6 &= 2^2 + 1^2 + 1^2 + 0^2 \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 \\
8 &= 2^2 + 2^2 + 0^2 + 0^2 \\
9 &= 3^2 + 0^2 + 0^2 + 0^2 \\
10 &= 3^2 + 1^2 + 0^2 + 0^2
\end{aligned}
$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$1 = 1^2 + 0^2 + 0^2 + 0^2$$
$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2$$
$$4 = 2^2 + 0^2 + 0^2 + 0^2$$
$$5 = 2^2 + 1^2 + 0^2 + 0^2$$
$$6 = 2^2 + 1^2 + 1^2 + 0^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2 + 0^2 + 0^2$$
$$9 = 3^2 + 0^2 + 0^2 + 0^2$$
$$10 = 3^2 + 1^2 + 0^2 + 0^2$$

Vsota štirih kvadratov

$$
\begin{aligned}
1 &= 1^2 + 0^2 + 0^2 + 0^2 \\
2 &= 1^2 + 1^2 + 0^2 + 0^2 \\
3 &= 1^2 + 1^2 + 1^2 + 0^2 \\
4 &= 2^2 + 0^2 + 0^2 + 0^2 \\
5 &= 2^2 + 1^2 + 0^2 + 0^2 \\
6 &= 2^2 + 1^2 + 1^2 + 0^2 \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 \\
8 &= 2^2 + 2^2 + 0^2 + 0^2 \\
9 &= 3^2 + 0^2 + 0^2 + 0^2 \\
10 &= 3^2 + 1^2 + 0^2 + 0^2
\end{aligned}
$$

Vsota štirih kvadratov

$$
\begin{aligned}
1 &= 1^2 + 0^2 + 0^2 + 0^2 \\
2 &= 1^2 + 1^2 + 0^2 + 0^2 \\
3 &= 1^2 + 1^2 + 1^2 + 0^2 \\
4 &= 2^2 + 0^2 + 0^2 + 0^2 \\
5 &= 2^2 + 1^2 + 0^2 + 0^2 \\
6 &= 2^2 + 1^2 + 1^2 + 0^2 \\
7 &= 2^2 + 1^2 + 1^2 + 1^2 \\
8 &= 2^2 + 2^2 + 0^2 + 0^2 \\
9 &= 3^2 + 0^2 + 0^2 + 0^2 \\
10 &= 3^2 + 1^2 + 0^2 + 0^2
\end{aligned}
$$

Vsota štirih kvadratov

Obstaja tudi izrek, ki pove, koliko rešitev ima enačba

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

v celih številih, za $n \in \mathbb{N}$.

Izrek

Označimo z $r_4(n)$ število celoštevilskih rešitev enačbe

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

za $n \in \mathbb{N}$. Imamo

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$

Vsota štirih kvadratov

Obstaja tudi izrek, ki pove, koliko rešitev ima enačba

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

v celih številih, za $n \in \mathbb{N}$.

Izrek

Označimo z $r_4(n)$ število celoštevilskih rešitev enačbe

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

za $n \in \mathbb{N}$. Imamo

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$

Vsota štirih kvadratov

Zgled

Za $n = 1$ *imamo*

$$r_4(1) = 8,$$

za $n = 2$ *imamo*

$$r_4(2) = 8(1 + 2) = 24$$

in za $n = 3$

$$r_4(3) = 8(1 + 3) = 48.$$

Vsota štirih kvadratov

Zgled

Za $n = 1$ *imamo*

$$r_4(1) = 8,$$

za $n = 2$ *imamo*

$$r_4(2) = 8(1 + 2) = 24$$

in za $n = 3$

$$r_4(3) = 8(1 + 3) = 48.$$

Vsota štirih kvadratov

Zgled

Za $n = 1$ *imamo*

$$r_4(1) = 8,$$

za $n = 2$ *imamo*

$$r_4(2) = 8(1 + 2) = 24$$

in za $n = 3$

$$r_4(3) = 8(1 + 3) = 48.$$

Waringov problem

Z $n \in \mathbb{N}$ si oglejmo enačbo

$$n = x_1^k + x_2^k + \cdots + x_s^k, \quad x_i \in \mathbb{N}_0,\ k > 1.$$

Če fiksiramo k in je s premajhen, zgornja enačba nima rešitve za vsak $n \in \mathbb{N}$.

Porodi se vprašanje, če za dan k obstaja tak $s = s(k)$, da ima zgornja enačba rešitev za vsak $n \in \mathbb{N}$.

Waringov problem

Z $n \in \mathbb{N}$ si oglejmo enačbo

$$n = x_1^k + x_2^k + \cdots + x_s^k, \quad x_i \in \mathbb{N}_0,\ k > 1.$$

Če fiksiramo k in je s premajhen, zgornja enačba nima rešitve za vsak $n \in \mathbb{N}$.

Porodi se vprašanje, če za dan k obstaja tak $s = s(k)$, da ima zgornja enačba rešitev za vsak $n \in \mathbb{N}$.

Waringov problem

Z $n \in \mathbb{N}$ si oglejmo enačbo

$$n = x_1^k + x_2^k + \cdots + x_s^k, \quad x_i \in \mathbb{N}_0,\ k > 1.$$

Če fiksiramo k in je s premajhen, zgornja enačba nima rešitve za vsak $n \in \mathbb{N}$.
Porodi se vprašanje, če za dan k obstaja tak $s = s(k)$, da ima zgornja enačba rešitev za vsak $n \in \mathbb{N}$.

Waringov problem, število $g(k)$

- Če obstaja tak s, da ima enačba $n = x_1^k + \cdots + x_s^k$ za fiksen k vedno rešitev, potem to velja tudi za vsak $s' > s$.
- Torej mora obstajati najmanjši tak s.

Definicija

Naj bo $k \geqslant 2$. Število $g = g(k)$ je najmanjše naravno število, za katero je mogoče vsako naravno število zapisati kot vsoto g k-tih potenc nenegativnih celih števil.

Waringov problem, število $g(k)$

- Če obstaja tak s, da ima enačba $n = x_1^k + \cdots + x_s^k$ za fiksen k vedno rešitev, potem to velja tudi za vsak $s' > s$.
- Torej mora obstajati najmanjši tak s.

Definicija

Naj bo $k \geqslant 2$. Število $g = g(k)$ je najmanjše naravno število, za katero je mogoče vsako naravno število zapisati kot vsoto g k-tih potenc nenegativnih celih števil.

Waringov problem, število $g(k)$

- Če obstaja tak s, da ima enačba $n = x_1^k + \cdots + x_s^k$ za fiksen k vedno rešitev, potem to velja tudi za vsak $s' > s$.
- Torej mora obstajati najmanjši tak s.

Definicija

Naj bo $k \geqslant 2$. Število $g = g(k)$ je najmanjše naravno število, za katero je mogoče vsako naravno število zapisati kot vsoto g k-tih potenc nenegativnih celih števil.

Waringov problem, število $g(k)$

- Če obstaja tak s, da ima enačba $n = x_1^k + \cdots + x_s^k$ za fiksen k vedno rešitev, potem to velja tudi za vsak $s' > s$.
- Torej mora obstajati najmanjši tak s.

Definicija

Naj bo $k \geqslant 2$. Število $g = g(k)$ je najmanjše naravno število, za katero je mogoče vsako naravno število zapisati kot vsoto g k-tih potenc nenegativnih celih števil.

Waringov problem, število $g(k)$

$$
\begin{aligned}
454 &= 3^2 + 11^2 + 18^2 \\
&= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\
&= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\
&= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\
&\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5
\end{aligned}
$$

Lahko sklepamo, da je $g(2) \geqslant 3$, $g(4) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Waringov problem, število $g(k)$

$$
\begin{aligned}
454 &= 3^2 + 11^2 + 18^2 \\
&= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\
&= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\
&= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\
&\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5
\end{aligned}
$$

Lahko sklepamo, da je $g(2) \geqslant 3$, $g(4) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Waringov problem, število $g(k)$

$$
\begin{aligned}
454 &= 3^2 + 11^2 + 18^2 \\
&= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\
&= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\
&= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\
&\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5
\end{aligned}
$$

Lahko sklepamo, da je $g(2) \geqslant 3$, $g(4) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Waringov problem, število $g(k)$

$$
\begin{aligned}
454 &= 3^2 + 11^2 + 18^2 \\
&= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\
&= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\
&= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\
&\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5
\end{aligned}
$$

Lahko sklepamo, da je $g(2) \geqslant 3$, $g(4) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Waringov problem, število $g(k)$

$$
\begin{aligned}
454 &= 3^2 + 11^2 + 18^2 \\
&= 1^3 + 1^3 + 1^3 + 3^3 + 3^3 + 3^3 + 3^3 + 7^3 \\
&= 1^4 + 2^4 + 2^4 + 2^4 + 3^4 + 3^4 + 3^4 + 3^4 + 3^4 \\
&= 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 1^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 \\
&\quad + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5 + 2^5
\end{aligned}
$$

Lahko sklepamo, da je $g(2) \geqslant 3$, $g(4) \geqslant 8$, $g(4) \geqslant 9$ in $g(5) \geqslant 20$.

Waringov problem, število $g(k)$

Iz zgodovine:

- Leta 1770 je Waring izjavil, da se da vsako naravno število zapisati kot vsoto 4 kvadratov, 9 kubov in 19 bikvadratov (četrtih potenc)
- Hilbert je leta 1909 dokazal, da se da to storiti za vsak k.

Dokazali smo že, da je $g(2) = 4$.

Waringov problem, število $g(k)$

Iz zgodovine:

- Leta 1770 je Waring izjavil, da se da vsako naravno število zapisati kot vsoto 4 kvadratov, 9 kubov in 19 bikvadratov (četrtih potenc)
- Hilbert je leta 1909 dokazal, da se da to storiti za vsak k.

Dokazali smo že, da je $g(2) = 4$.

Waringov problem, število $g(k)$

Iz zgodovine:

- Leta 1770 je Waring izjavil, da se da vsako naravno število zapisati kot vsoto 4 kvadratov, 9 kubov in 19 bikvadratov (četrtih potenc)
- Hilbert je leta 1909 dokazal, da se da to storiti za vsak k.

Dokazali smo že, da je $g(2) = 4$.

Waringov problem, število $g(k)$

Iz zgodovine:

- Leta 1770 je Waring izjavil, da se da vsako naravno število zapisati kot vsoto 4 kvadratov, 9 kubov in 19 bikvadratov (četrtih potenc)
- Hilbert je leta 1909 dokazal, da se da to storiti za vsak k.

Dokazali smo že, da je $g(2) = 4$.

Waringov problem, število $g(k)$

Izrek (Hilbert-Waring)

Za vsa naravna števila $n \geqslant 2$ obstaja tako končno število $g = g(k)$, da je možno n zapisati kot vsoto najmanj g k-tih potenc nenegativnih celih števil.

Waringov problem, število $g(k)$

Izrek

$g(4)$ *obstaja in je* $\leqslant 53$.

- Označimo z B_s število, ki je vsota s četrtih potenc.

- Velja identiteta

$$
\begin{aligned}
6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4 \\
&+ (a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4 \\
&+ (a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4.
\end{aligned}
$$

- Od tod je $6(a^2+b^2+c^2+d^2)^2 = B_{12}$

- Iz Lagrangeovega izreka o štirih kvadratih potem sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$.

- Označimo z B_s število, ki je vsota s četrtih potenc.

- Velja identiteta

$$\begin{aligned}6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\ &\quad+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\ &\quad+(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4.\end{aligned}$$

- Od tod je $6(a^2+b^2+c^2+d^2)^2 = B_{12}$

- Iz Lagrangeovega izreka o štirih kvadratih potem sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$.

- Označimo z B_s število, ki je vsota s četrtih potenc.

- Velja identiteta

$$\begin{aligned}6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\ &\quad+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\ &\quad+(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4.\end{aligned}$$

- Od tod je $6(a^2+b^2+c^2+d^2)^2 = B_{12}$

- Iz Lagrangeovega izreka o štirih kvadratih potem sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$.

- Označimo z B_s število, ki je vsota s četrtih potenc.
- Velja identiteta

$$\begin{aligned}6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\ &+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\ &+(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4.\end{aligned}$$

- Od tod je $6(a^2+b^2+c^2+d^2)^2 = B_{12}$
- Iz Lagrangeovega izreka o štirih kvadratih potem sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$.

- Označimo z B_s število, ki je vsota s četrtih potenc.

- Velja identiteta

$$\begin{aligned}6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\ &\quad+(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\ &\quad+(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4.\end{aligned}$$

- Od tod je $6(a^2+b^2+c^2+d^2)^2 = B_{12}$

- Iz Lagrangeovega izreka o štirih kvadratih potem sledi

$$6x^2 = B_{12},$$

za vsak $x \in \mathbb{N}$.

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo
$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$
- In od tod
$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$
saj lahko r zapišemo kot vstot največ petih četrtih potenc
$(r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4)$.
- Zato $g(4)$ obstaja in je največ 53. $\square$

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.

- Če še enkrat uporabimo izrek o štirih kvadratih dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

- In od tod

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

  saj lahko r zapišemo kot vstot največ petih četrtih potenc
  $(r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4)$.

- Zato $g(4)$ obstaja in je največ 53. □

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

- In od tod

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

saj lahko r zapišemo kot vstot največ petih četrtih potenc ($r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4$).

- Zato $g(4)$ obstaja in je največ 53. $\square$

Waringov problem, število $g(k)$

Dokaz izreka

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo
$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$
- In od tod
$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$
saj lahko r zapišemo kot vstot največ petih četrtih potenc $(r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4)$.
- Zato $g(4)$ obstaja in je največ 53. □

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

- In od tod

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

saj lahko r zapišemo kot vstot največ petih četrtih potenc $(r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4)$.

- Zato $g(4)$ obstaja in je največ 53. □

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo
$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$
- In od tod
$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$
saj lahko r zapišemo kot vstot največ petih četrtih potenc $(r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4)$.
- Zato $g(4)$ obstaja in je največ 53. □

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

- In od tod

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

saj lahko r zapišemo kot vstot največ petih četrtih potenc ($r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4$).

- Zato $g(4)$ obstaja in je največ 53. □

- Vemo že, da je vsako naravno število n oblike $6t + r$ za $0 \leqslant r \leqslant 5$.
- Če še enkrat uporabimo izrek o štirih kvadratih dobimo

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r.$$

- In od tod

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r \leqslant B_{53},$$

saj lahko r zapišemo kot vstot največ petih četrtih potenc ($r = 5 = 1^4 + 1^4 + 1^4 + 1^4 + 1^4$).

- Zato $g(4)$ obstaja in je največ 53. $\square$

Waringov problem, število $g(k)$

Izrek (Euler)

Za $k \geqslant 2$ *je*

$$g(k) \geqslant \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2.$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število

$$n = 2^k q - 1 < 3^k.$$

- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v

$$n = (q-1)2^k + (2^k - 1)1^k.$$

- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi

$$g(k) \geqslant q + 2^k - 2. \quad \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k - 1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k-1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \ \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število

$$n = 2^k q - 1 < 3^k.$$

- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v

$$n = (q-1)2^k + (2^k - 1)1^k.$$

- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi

$$g(k) \geqslant q + 2^k - 2. \ \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k - 1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k - 1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \square$$

Waringov problem, število $g(k)$

Dokaz izreka

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k - 1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \ \square$$

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število

$$n = 2^k q - 1 < 3^k.$$

- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v

$$n = (q-1)2^k + (2^k - 1)1^k.$$

- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi

$$g(k) \geqslant q + 2^k - 2. \square$$

- Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$.
- Oglejmo si število
$$n = 2^k q - 1 < 3^k.$$
- Od tod sledi, da lahko le s seštevanjem potenc 1^k in 2^k pridemo do števila n.
- Da minimiziramo število potrebnih sumandov, uporabimo karseda veliko potenc 2^k. Najmanjše število sumandov je dano v
$$n = (q-1)2^k + (2^k - 1)1^k.$$
- Zato za število n potrebujemo najmanj $q + 2^k - 2$ sumandov. Od tod sledi
$$g(k) \geqslant q + 2^k - 2. \ \square$$

Waringov problem, število $g(k)$

- Ne potrebujejo pa vsa števila natančno $g(k)$ potenc števila k.
- Vemo, da je $g(3) = 9$,a le števili 23 in 239 potrebujeta 9 kubov, samo 15 števil potrebuje 8 kubov in samo 121 števil potrebuje 7 kubov (Jacobi, preveril do 12 000.)
- Linnik je leta 1942 pokazal, da za dovolj veliko naravno število potrebujemo 7 ali manj kubov.

Waringov problem, število $g(k)$

- Ne potrebujejo pa vsa števila natančno $g(k)$ potenc števila k.
- Vemo, da je $g(3) = 9$, a le števili 23 in 239 potrebujeta 9 kubov, samo 15 števil potrebuje 8 kubov in samo 121 števil potrebuje 7 kubov (Jacobi, preveril do 12 000.)
- Linnik je leta 1942 pokazal, da za dovolj veliko naravno število potrebujemo 7 ali manj kubov.

Waringov problem, število $g(k)$

- Ne potrebujejo pa vsa števila natančno $g(k)$ potenc števila k.
- Vemo, da je $g(3) = 9$,a le števili 23 in 239 potrebujeta 9 kubov, samo 15 števil potrebuje 8 kubov in samo 121 števil potrebuje 7 kubov (Jacobi, preveril do 12 000.)
- Linnik je leta 1942 pokazal, da za dovolj veliko naravno število potrebujemo 7 ali manj kubov.

Waringov problem, število $g(k)$

- Ne potrebujejo pa vsa števila natančno $g(k)$ potenc števila k.
- Vemo, da je $g(3) = 9$,a le števili 23 in 239 potrebujeta 9 kubov, samo 15 števil potrebuje 8 kubov in samo 121 števil potrebuje 7 kubov (Jacobi, preveril do $12\,000$.)
- Linnik je leta 1942 pokazal, da za dovolj veliko naravno število potrebujemo 7 ali manj kubov.

Waringov problem, število $g(k)$

- Ne potrebujejo pa vsa števila natančno $g(k)$ potenc števila k.
- Vemo, da je $g(3) = 9$,a le števili 23 in 239 potrebujeta 9 kubov, samo 15 števil potrebuje 8 kubov in samo 121 števil potrebuje 7 kubov (Jacobi, preveril do $12\,000$.)
- Linnik je leta 1942 pokazal, da za dovolj veliko naravno število potrebujemo 7 ali manj kubov.

Idealni Waringov problem

Izrek

Označimo $q := \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$ *in* $p := \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor$*. Za* $k \geqslant 2$ *je*

$$g(k) = \begin{cases} q + 2^k - 2, & \textit{če } \ 2^k \left(\left(\frac{3}{2}\right)^k - q \right) + q \leqslant 2^k, \\ 2^k + p + q - \theta, & \textit{sicer}, \end{cases}$$

kjer je

$$\theta := \begin{cases} 2, & \textit{če } \ pq + p + q = 2^k, \\ 3, & \textit{če } \ pq + p + q > 2^k. \end{cases}$$

Idealni Waringov problem

- Kubina in Wunderlich sta leta 1990 dokazala,da prvi pogoj iz zgornjega izreka velja za vse $k \leqslant 471\,600\,000$.
- Leta 1957 je Mahler dokazal, da je izjem v zgornjem izreku največ končno mnogo (če sploh so).
- Zato je najbolj verjetno, da je Eulerjeva ocena za število $g(k)$ kar njegova natančna vrednost.

Idealni Waringov problem

- Kubina in Wunderlich sta leta 1990 dokazala,da prvi pogoj iz zgornjega izreka velja za vse $k \leqslant 471\,600\,000$.
- Leta 1957 je Mahler dokazal, da je izjem v zgornjem izreku največ končno mnogo (če sploh so).
- Zato je najbolj verjetno, da je Eulerjeva ocena za število $g(k)$ kar njegova natančna vrednost.

Idealni Waringov problem

- Kubina in Wunderlich sta leta 1990 dokazala,da prvi pogoj iz zgornjega izreka velja za vse $k \leqslant 471\,600\,000$.
- Leta 1957 je Mahler dokazal, da je izjem v zgornjem izreku največ končno mnogo (če sploh so).
- Zato je najbolj verjetno, da je Eulerjeva ocena za število $g(k)$ kar njegova natančna vrednost.

Idealni Waringov problem

- Kaj manjka do dokaza *idealnega Waringovega problema*?

Waringov problem, število $G(k)$

- Oglejmo si še eno število, ki je povezano z Waringovim problemom.

Definicija

*Naj bo $k \geqslant 2$. Število $G = G(k)$ je najmanjše naravno število, za katero je mogoče vsako **dovolj veliko** naravno število zapisati kot vsoto G k-tih potenc nenegativnih celih števil.*

- Očitno je
$$G(k) \leqslant g(k).$$
- Za $k = 2$ imamo $G(k) = 4$, saj že vemo, da neskončno mnogo števil ni mogoče zapisati kot vsote dveh oz. treh kvadratov.

Waringov problem, število $G(k)$

- Oglejmo si še eno število, ki je povezano z Waringovim problemom.

Definicija

Naj bo $k \geqslant 2$. Število $G = G(k)$ je najmanjše naravno število, za katero je mogoče vsako ***dovolj veliko*** *naravno število zapisati kot vsoto G k-tih potenc nenegativnih celih števil.*

- Očitno je

$$G(k) \leqslant g(k).$$

- Za $k = 2$ imamo $G(k) = 4$, saj že vemo, da neskončno mnogo števil ni mogoče zapisati kot vsote dveh oz. treh kvadratov.

Waringov problem, število $G(k)$

- Oglejmo si še eno število, ki je povezano z Waringovim problemom.

Definicija

Naj bo $k \geqslant 2$. Število $G = G(k)$ je najmanjše naravno število, za katero je mogoče vsako ***dovolj veliko*** *naravno število zapisati kot vsoto G k-tih potenc nenegativnih celih števil.*

- Očitno je
$$G(k) \leqslant g(k).$$

- Za $k = 2$ imamo $G(k) = 4$, saj že vemo, da neskončno mnogo števil ni mogoče zapisati kot vsote dveh oz. treh kvadratov.

Waringov problem, število $G(k)$

- Oglejmo si še eno število, ki je povezano z Waringovim problemom.

Definicija

Naj bo $k \geqslant 2$. Število $G = G(k)$ je najmanjše naravno število, za katero je mogoče vsako ***dovolj veliko*** *naravno število zapisati kot vsoto G k-tih potenc nenegativnih celih števil.*

- Očitno je
$$G(k) \leqslant g(k).$$
- Za $k = 2$ imamo $G(k) = 4$, saj že vemo, da neskončno mnogo števil ni mogoče zapisati kot vsote dveh oz. treh kvadratov.

Waringov problem, število $G(k)$

Izrek

Za $k \geqslant 2$ je

$$G(k) \geqslant k + 1.$$

Imamo še tudi ocene za zgornjo mejo $G(k)$:

- $G(k) < ck \log k$, za neko konstanto c.
- Za velike k velja ocena

$$G(k) \leqslant k \left(\log k + \log \log k + 2 + \mathcal{O}\left(\frac{\log \log k}{\log k} \right) \right).$$

Waringov problem, število $G(k)$

Izrek

Za $k \geqslant 2$ je

$$G(k) \geqslant k + 1.$$

Imamo še tudi ocene za zgornjo mejo $G(k)$:

- $G(k) < ck \log k$, za neko konstanto c.
- Za velike k velja ocena

$$G(k) \leqslant k \left(\log k + \log \log k + 2 + \mathcal{O}\left(\frac{\log \log k}{\log k} \right) \right).$$

Waringov problem, število $G(k)$

Izrek

Za $k \geqslant 2$ je

$$G(k) \geqslant k + 1.$$

Imamo še tudi ocene za zgornjo mejo $G(k)$:

- $G(k) < ck \log k$, za neko konstanto c.
- Za velike k velja ocena

$$G(k) \leqslant k \left(\log k + \log \log k + 2 + \mathcal{O}\left(\frac{\log \log k}{\log k} \right) \right).$$

Waringov problem, število $G(k)$

Izrek

Za $k \geqslant 2$ je

$$G(k) \geqslant k + 1.$$

Imamo še tudi ocene za zgornjo mejo $G(k)$:

- $G(k) < ck \log k$, za neko konstanto c.
- Za velike k velja ocena

$$G(k) \leqslant k \left(\log k + \log \log k + 2 + \mathcal{O}\left(\frac{\log \log k}{\log k} \right) \right).$$

Waringov problem

k	$g(k)$	$G(k)$
2	4	4
3	9	$\leqslant 7$
4	19	16
5	37	$\leqslant 17$
6	73	$\leqslant 24$
7	143	$\leqslant 31$
8	279	$\leqslant 39$
9	548	$\leqslant 47$
10	1079	$\leqslant 55$
11	2132	$\leqslant 63$
12	4223	$\leqslant 72$
13	8384	$\leqslant 81$
14	16673	$\leqslant 90$