Zakon kvadratne recipročnosti

Nino Cajnkar, Klara Drofenik
Mentor: Rok Havlas

Povzetek

V članku smo se ukvarjali s kvadratnimi ostanki. Najprej smo si ogledali nekaj teorije in dokazali izreke, ki so nam kasneje služili kot orodje za dokaz enega najpomembnejših izrekov v teoriji števil - Gaussovega zakona kvadratne recipročnosti.

1 Uvod

Zakon kvadratne recipročnosti velja za enega izmed najpomembnejših izrekov v teoriji števil. Prvi ga je dokazal Gauss leta 1795 pri svojih osemnajstih letih, imenoval pa ga je kar "aureum theorema"(zlati izrek). Od tedaj je bil dokazan še na več kot 100 načinov - 7 izmed dokazov je dal Gauss sam, prispevali pa so jih tudi znani matematiki kot npr. Cauchy, Dirichlet, Dedekind, Eisenstein, Jacobi... Izrek zaznamuje tudi znameniti spor med Legendrom in Gaussom. Legendre je sicer podal svoj dokaz izreka 10 let pred Gaussom, vendar je bil njegov dokaz nepopoln, saj je privzel, da je v vsakem aritmetičnem zaporedju oblike $a + kb$ (za tuja a in b) neskončno preštevil - dejstvo, ki ga je dokazal

komaj Dirichlet 50 let kasneje. Ko je Gauss izrek dokazal in ga pripisal sebi, je Legendre to smatral kot veliko krajo.

Glavni namen našega članka bo dokazati zakon kvadratne recipročnosti. Najprej bomo pogledali, kako je z rešljivostjo kvadratnih kongruenc in dokazali kriterij, kdaj je dano število kvadratni ostanek po modulu p. Nato bomo definirali Legendrov simbol in dokazali nekaj njegovih lastnosti. Pokazali bomo še Gaussovo lemo in se tako opremljeni lotili dokaza zakona kvadratne recipročnosti.

2 Rešljivost kvadratnih kongruenc

Naprej si poglejmo, kaj lahko povemo o rešljivosti kvadratne kongruence

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

kjer je p liho praštevilo in $\gcd(a, p) = 1$. Ker je $\gcd(a, p) = 1$, je tudi $\gcd(4a, p) = 1$, torej je ekvivalentno iskati rešitve kongruence

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

Kongruenco lahko preuredimo v obliko

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

in z uvedbo nove spremenljivke $y = 2ax+b$ ter združitvijo konstant $b^2-4ac = d$ dobimo kongruenco

$$y^2 \equiv d \pmod{p}.$$

Naj bo $x \equiv x_0 \pmod{p}$ rešitev naše začetne kongruence $ax^2 + bx + c \equiv 0 \pmod{p}$. Potem $2ax_0 + b = y$ reši kongruenco $y^2 \equiv d \pmod{p}$. Velja tudi obratno; naj bo $y \equiv y_0 \pmod{p}$ rešitev kongruence $y^2 \equiv d \pmod{p}$, potem je rešitev kongruence $ax^2 + bx + c \equiv 0 \pmod{p}$ ravno rešitev linearne kongruence $2ax + b \equiv y_0 \pmod{p}$. Torej lahko reševanje kongruence $ax^2+bx+c \equiv 0 \pmod{p}$ prevedemo na reševanje kongruence $y^2 \equiv d \pmod{p}$.

Zanima nas, kdaj ima kongruenca

$$x^2 \equiv a \pmod{p}$$

rešitve, če je p liho praštevilo.

V primeru, ko velja $p|x$ imamo kongruenco $x^2 \equiv 0 \pmod{p}$, ki pa ima samo eno rešitev $x \equiv 0 \pmod{p}$.

Privzamimo torej, da p ne deli x. Če ima kongruenca rešitev x_0, ima tudi rešitev $p-x_0$. Preveriti moramo, da ti dve rešitvi nista kongruentni. Recimo, da sta kongruentni. Potem velja

$$p - x_0 \equiv x_0 \pmod{p},$$

torej

$$0 \equiv p \equiv 2x_0 \pmod{p}$$

in zato

$$p|x_0,$$

kar pa ni mogoče, saj p ne deli x_0. Zato sta x_0 in $p - x_0$ res dve različni nekongruentni rešitvi, ne vemo pa še, ali sta tudi edini rešitvi.

Pri odgovru na to vprašanje nam bo v pomoč naslednji izrek o številu rešitev polinoma po modulu p.

Izrek 1 (Lagrange)**.** *Naj bo* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *in* $\gcd(p, a_n) = 1$; $n \geq 1$, $a_i \in \mathbb{Z}$ $\forall i \in \{1, \ldots, n\}$. *Potem ima kongruenca* $f(x) \equiv 0 \pmod{p}$ *največ* n *nekongruentnih rešitev.*

Dokaz. Izrek bomo dokazali z uporabo načela popolne indukcije.

- Za $n = 1$ dobimo
$$a_1 x + a_0 \equiv 0 \pmod{p}$$
in ker je $\gcd(a_1, p) = 1$, velja
$$x \equiv -\frac{a_0}{a_1} \pmod{p}.$$
Z a_1 lahko delimo, ker sta a_1 in n tuja. Torej dobimo 1 rešitev.

- Sedaj predpostavimo, da trditev velja za $n - 1$.
Naj bo $f(x)$ polinom stopnje n. Iščemo rešitve enačbe $f(x) \equiv 0 \pmod{p}$. Če ta enačba nima rešitve, smo končali, saj imamo res manj kot n nekongruentnih rešitev. Sicer imamo vsaj eno rešitev, ki jo označimo z a. Osnovni izrek o deljenju polinomov nam da
$$f(x) = (x - a)q(x) + r(x),$$
pri čemer je $q(x)$ polinom stopnje $n - 1$ s celoštevilskimi koeficienti, $r(x) = r$ pa celoštevilska konstanta (saj je stopnja $r(x)$ manjša od stopnje linearnega polinoma $(x - a)$). Če vstavimo $x = a$ dobimo
$$f(a) \equiv 0 + r \equiv r \pmod{p}$$

in ker je a rešitev $f(x) \equiv 0 \pmod{p}$, sledi, da je $r = 0$. Torej imamo

$$f(x) = (x - a)q(x).$$

Predpostavimo, da je b še ena rešitev $f(x) \equiv 0 \pmod{p}$ in $b \not\equiv a \pmod{p}$. Velja:

$$0 = f(b) \equiv (b - a)q(b) \pmod{p}.$$

Ker $b - a \not\equiv 0 \pmod{p}$ sledi, da mora veljati $q(b) \equiv 0 \pmod{p}$. Vsaka rešitev $f(x) \equiv 0 \pmod{p}$, ki ni kongruentna a, mora rešiti $q(x) \equiv 0 \pmod{p}$. Po indukcijski predpostavki vemo, da ima $q(x) \equiv 0 \pmod{p}$ največ $n - 1$ nekongruentnih rešitev, saj je stopnja $q(x)$ ravno $n - 1$. Iz tega sledi, da ima enačba

$$f(x) \equiv 0 \pmod{p}$$

največ n nekongruentnih rešitev.

□

Izrek nam tako pove, da ima kongruenca

$$x^2 \equiv a \pmod{p}$$

največ 2 nekongruentni rešitvi, ker pa smo že našli 2 taki rešitvi, sledi, da ima natanko 2 rešitvi.

3 Kvadratni ostanki

Definicija 1. *Naj bo p liho praštevilo in a takšno število, da velja* $\gcd(a, p) = 1$. *Če ima kongruenca*

$$x^2 \equiv a \pmod{p}$$

rešitev, potem rečemo, da je a **kvadratni ostanek** *po modulu p. Če rešitve ni, potem a* **ni kvadratni ostanek** *po modulu p.*

Poglejmo si primer za $p = 13$. Iskali bomo, katera števila so kvadratni ostanki. Torej rešujemo enačbo

$$x^2 \equiv a \pmod{p}.$$

Pomagajmo si s tabelo vseh možnosti za x:

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	16	25	36	49	64	81	100	121	144
a	1	4	9	3	12	10	10	12	3	9	4	1

Tabela 1: Kvadratni ostanki po modulu 13

Sledi torej, da so kvadratni ostanki po modulu 13 ravno števila $1, 3, 4, 9, 10, 12$.

Izrek 2 (Eulerjev kriterij)**.** *Naj bo p liho praštevilo in a število, ki je tuje p. Če je a kvadratni ostanek po modulu p, potem velja*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Še več, velja tudi, da če a ni kvadratni ostanek, je potem

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Za dokaz tega izreka bomo potrebovali Wilsonov izrek, ki pravi, da je

$$(p-1)! \equiv -1 \pmod{p}$$

in ga v članku ne bomo dokazali.

Dokaz. Predpostavimo, da a ni kvadratni ostanek po modulu p. Naj bo $c \in \{1, 2, 3, \ldots, p-1\}$. Za enačbo

$$cx \equiv a \pmod{p}$$

obstaja natanko 1 rešitev, naj bo to c'; $c' \in \{1, 2, 3, \ldots, p-1\}$.

Velja $c' \neq c$, sicer bi a bil kvadratni ostanek. V ostalih primerih dobimo za c' linerano kongruenco, za katero obstaja natanko 1 rešitev. Števila med 1 in $p-1$ razelimo v pare $\{c_i, d_i\}$, tako da velja

$$c_i d_i \equiv a (\mathrm{mod}\, p).$$

Takih parov je $\frac{p-1}{2}$:

$$\begin{aligned} c_1 d_1 &\equiv a \pmod{p} \\ c_2 d_2 &\equiv a \pmod{p} \\ &\cdots \\ c_{\frac{p-1}{2}} d_{\frac{p-1}{2}} &\equiv a \pmod{p}. \end{aligned}$$

Če zmnožimo te kongruence dobimo

$$c_1 d_1 \cdots c_{\frac{p-1}{2}} d_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Leva stran enačbe je enaka $(p-1)!$, saj so števila c_i in d_j, $1 \leq i, j \leq \frac{p-1}{2}$, permutacija števil od 1 do $p-1$. Torej po Wilosonovem izreku velja

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Če je a kvadratni ostanek, to pomeni, da ima enačba

$$x^2 \equiv a \pmod{p}$$

dve rešitvi $x \equiv x_1 \pmod{p}$ in $x \equiv p - x_1 \pmod{p}$, za kateri velja $1 \leq x_1 \leq p-1$. Vsa ostala števila med 1 in $p-1$ razen x_1 in $p - x_1$ damo v pare $\{c_i, d_i\}$; $c_i \neq d_i$ tako, da velja $c_i d_i \equiv a \pmod{p}$. Torej imamo

$$\begin{aligned} c_1 d_1 &\equiv a \pmod{p} \\ c_2 d_2 &\equiv a \pmod{p} \\ &\cdots \\ c_{\frac{p-3}{2}} d_{\frac{p-3}{2}} &\equiv a \pmod{p}. \end{aligned}$$

Za x_1 in $p - x_1$ velja:

$$x_1(p - x_1) \equiv p x_1 - x_1^2 \equiv -x_1^2 \equiv -a \pmod{p}.$$

Vse na desni streni zgornjih kongruenc zmnožimo skupaj in vse na levi strani zmnožimo skupaj in dobimo

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}.$$

Po Wilsonovem izreku je $(p-1)! \equiv -1 \pmod{p}$, iz česar sledi

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

□

Definicija 2. *Naj bo p liho praštevilo in a celo število, da velja* $\gcd(a, p) = 1$. ***Legendrov simbol*** *definiramo kot*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{če je } a \text{ kvadratni ostanek } \pmod{p} \\ -1, & \text{če } a \text{ ni kvadratni ostanek } \pmod{p}. \end{cases}$$

Poglejmo si še nekaj lastnosti Legendrovega simbola:

a)

$$\left(\frac{a^2}{p}\right) = 1.$$

Dokaz. Kongruenca

$$x^2 \equiv a^2 \pmod{p},$$

je očitno vedno rešljiva, zato lastnost drži. □

Posledično je tudi

$$\left(\frac{1}{p}\right) = 1.$$

b)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{če je } p = 4k+1 \\ -1, & \text{če je } p = 4k+3 \end{cases}$$

Dokaz.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1, & \text{če je } p = 4k+1 \\ -1, & \text{če je } p = 4k+3 \end{cases}$$

V enačbah smo dokazli kongruentnost, nas pa zanima, če velja tudi enakost. Poglejmo primer, kjer je $p = 4k+1$. Po definiciji je Legendrov simbol enak 1 ali -1. Vemo, da je $\left(\frac{-1}{p}\right) \equiv 1 \pmod{p}$, saj smo kongruenco že dokazali. Zdaj želimo ugotoviti, ali iz kongruence sledi tudi enakost. Če je Legndrov simbol tudi enak 1 za naš primer, potem smo lasnost dokazali. Če bi pa bil enak -1, bi iz kongruenc sledilo

$$-1 \equiv 1 \pmod{p}$$

oziroma

$$2 \equiv 0 \pmod{p},$$

kar pa je protislovje, ker je p liho praštevilo. Torej smo dokazali, da iz kongruence sledi tudi enakost. Podobno naredimo tudi za primer, ko je $p = 4k+3$.

□

c)

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Dokaz.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) (\mathrm{mod}\, p)$$

S podobnimi argumenti kot v primeru b) pokažemo, da imamo tudi tukaj enakost. □

Sedaj si bomo pogledali zelo močno lemo, ki nam bo pomagala pri dokazu našega glavnega izreka o kvadratni recipročnosti.

Izrek 3 (Gaussova lema)**.** *Naj bo p liho praštevilo ter a tako celo število, da velja* $\gcd(a, p) = 1$. *Če z n ozaničimo število celih števil v množici $S = \{a, 2a, \ldots, (\frac{p-1}{2})a\}$, ki so po modulu p večja od $\frac{p}{2}$, potem je*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Dokaz. Ker je $\gcd(a, p) = 1$, ni nobeno število v S deljivo s p in nobeni dve števili nista med seboj kongruentni. Naj bodo $\{r_1, \ldots, r_m\}$ tisti ostanki števil iz S po $\mathrm{mod}\, p$, ki so manjši od $\frac{p}{2}$ in $\{s_1, \ldots, s_n\}$ tisti ostanki, ki so večji od $\frac{p}{2}$. Očitno je $m+n = \frac{p-1}{2}$. Torej so števila $\{r_1, \ldots, r_m, \ldots, p-s_1, \ldots, p-s_n\}$ pozitivna in manjša od $\frac{p}{2}$. Pokazali bomo, da so vsa med seboj različna. Predpostavili bomo nasprotno in želeli priti do protislovja. Naj bo torej

$$p - s_i = r_j$$

za neka i, j; $1 \leq i \leq m$ in $1 \leq j \leq n$. Potem $\exists\, u, v \in \mathbb{Z}$, kjer je $1 \leq u, v \leq \frac{p-1}{2}$, da velja

$$s_i \equiv ua\ (\mathrm{mod}\, p)$$

in

$$r_j \equiv va\ (\mathrm{mod}\, p).$$

Iz tega sledi, da je

$$(u+v)a \equiv s_i + r_j \equiv p \equiv 0\ (\mathrm{mod}\, p)$$

in ker je $\gcd(a, p) = 1$, je

$$u + v \equiv 0\ (\mathrm{mod}\, p).$$

Torej so števila $\{r_1, \ldots, r_m, \ldots, p - s_1, \ldots, p - s_n\}$ ravno permutacija števil $1, \ldots, \frac{p-1}{2}$. Ko ta števila zmnožimo, dobimo

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv r_1 \cdot \cdots \cdot r_m \cdot (p - s_1) \cdot \cdots \cdot (p - s_n) \\ &\equiv r_1 \cdot \cdots \cdot r_m \cdot (-s_1) \cdot \cdots \cdot (-s_n) \\ &\equiv (-1)^n \cdot r_1 \cdot \ldots \cdot r_m \cdot s_1 \cdot \ldots \cdot s_n \\ &\equiv (-1)^n \cdot a \cdot 2a \cdot \ldots \cdot \left(\frac{p-1}{2}\right) a \\ &\equiv (-1)^n \cdot \left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \pmod{p}.\end{aligned}$$

Iz $\gcd((\frac{p-1}{2})!, p) = 1$ sledi

$$1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \pmod{p}.$$

Kongruenco pomnožimo z $(-1)^n$ in dobimo

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p},$$

torej

$$\left(\frac{a}{p}\right) = (-1)^n.$$

□

Uporabo leme si poglejmo na primeru.
Vzemimo $p = 13$ in $a = 5$. Potem je $S = \{5, 10, 15, 20, 25, 30\}$, torej so ostanki teh števil po modulu 13 ravno $\{5, 10, 2, 7, 12, 4\}$. Od števila $\frac{p-1}{2} = 6$ so večji natanko trije ostanki, torej je $n = 3$. Po Gaussovi lemi zato sledi

$$\left(\frac{5}{13}\right) = (-1)^n = (-1)^3 = -1.$$

Lema 1. *Naj bo p liho praštevilo in a tako celo število, da velja* $\gcd(a, p) = 1$. *Potem je*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}$$

Dokaz. Poglejmo množico

$$S = \left\{a, \ldots, \left(\frac{p-1}{2}\right) a\right\}.$$

Za vsak $k;\ 1 \leq k \leq \frac{p-1}{2}$ obstajata taka q_k in $c_k;\ 1 \leq c_k \leq p-1,$ da je

$$ka = q_k p + c_k.$$

Ko enačbo delimo s p, dobimo

$$\frac{ka}{p} = q_k + \frac{c_k}{p},$$

torej je

$$q_k = \lfloor \frac{ka}{p} \rfloor.$$

Prvotno enačbo lahko tako zapišemo kot

$$ka = \lfloor \frac{ka}{p} \rfloor p + c_k.$$

Če je $c_k < \frac{p}{2}$, je c_k eden izmed $\{r_1, ..., r_m\}$ iz dokaza Gaussove leme, če pa je $c_k > \frac{p}{2}$ pa je c_k eden izmed $\{s_1, ..., s_n\}$. Nadalje

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}} ka &= \sum_{k=1}^{\frac{p-1}{2}} (\lfloor \frac{ka}{p} \rfloor p + c_k) = \sum_{k=1}^{\frac{p-1}{2}} (\lfloor \frac{ka}{p} \rfloor p) + \sum_{k=1}^{\frac{p-1}{2}} c_k \\ &= \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k. \end{aligned} \tag{1}$$

Iz dokaza Gaussove leme se spomnimo tudi, da so $\{r_1, \ldots, r_m, \ldots, p - s_1, \ldots, p - s_n\}$ ravno permutacija števil $1, \ldots, \frac{p-1}{2}$. Torej je

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = np + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \tag{2}$$

Sedaj od enačbe (1) odštejemo enačbo (2):

$$\sum_{k=1}^{\frac{p-1}{2}} ka - \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k - np - \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k,$$

torej je

$$\sum_{k=1}^{\frac{p-1}{2}} k(a-1) = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor p + 2\sum_{k=1}^{n} s_k - np.$$

Dobimo

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p\left[\left(\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor\right) - n\right] + 2\sum_{k=1}^{n} s_k.$$

Če enačbo pogledamo po modulu 2 vidimo, da je

$$0 \equiv \left[\left(\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor\right) - n\right] \pmod 2,$$

in torej

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor \pmod 2 \ (\heartsuit).$$

Gaussova lema nam pove, da je

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Iz enačbe ($\heartsuit$) sledi

$$n = 2l + \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor$$

in tako dobimo

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{2l+\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor} = (-1)^{2l} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor} =$$

$$= (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}.$$

□

Poglejmo si spet primer, ko je $p = 13$, $a = 5$ in $S = \{5, 10, 15, 20, 25, 30\}$. Izračunamo naslednje vrednosti:

$$\lfloor \frac{5}{13} \rfloor = 0, \lfloor \frac{10}{13} \rfloor = 0, \lfloor \frac{15}{13} \rfloor = 1, \lfloor \frac{20}{13} \rfloor = 1, \lfloor \frac{25}{13} \rfloor = 1 \lfloor \frac{30}{13} \rfloor = 2.$$

S pomočjo prejšnje leme poračunamo še Legendrov simbol

$$\left(\frac{5}{13}\right) = (-1)^{\lfloor \frac{5}{13} \rfloor + \ldots + \lfloor \frac{30}{13} \rfloor} = (-1)^{0+0+1+1+1+2} = (-1)^5,$$

torej smo se še enkrat prepričali, da je

$$\left(\frac{5}{13}\right) = -1.$$

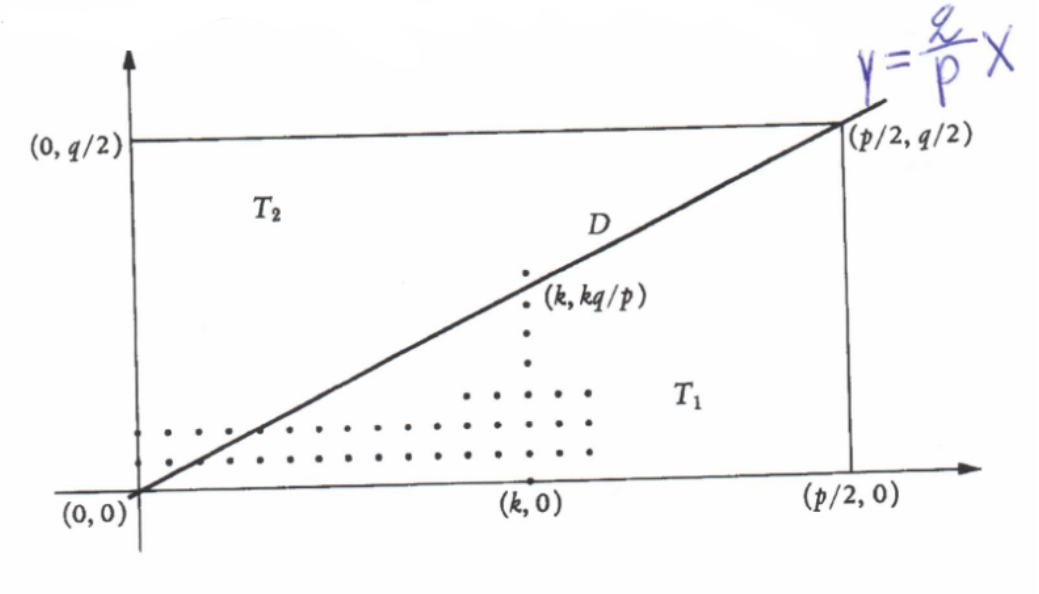
Sedaj imamo končno na voljo vsa orodja, da lahko formuliramo in dokažemo glavni izrek našega članka.

Izrek 4 (Gaussov zakon kvadratne recipročnosti)**.** *Naj bosta p in q različni lihi praštevili. Potem velja*

$$\boxed{\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.}$$

Dokaz. Poglejmo pravokotnik v ravnini xy z oglišči v točkah $(0,0)$, $(\frac{p}{2},0)$, $(\frac{p}{2},\frac{q}{2})$, $(0,\frac{q}{2})$. Naj bo R notranje območje pravokotnika brez robnih stranic. Cilj: Šteti celoštevilske točke v R na 2 načina. Celoštevilske točke v R so oblike (n,m); $1 \leq n \leq \frac{p-1}{2}$ in $1 \leq m \leq \frac{q-1}{2}$. Takšnih točk je $\frac{p-1}{2} \cdot \frac{q-1}{2}$, kjer je $\frac{p-1}{2}$ število možnosti za n in $\frac{q-1}{2}$ število možnosti za m.

Naj bo D diagonala pravokotnika ki poteka med točkama $(0,0)$ in $(\frac{p}{2},\frac{q}{2})$.



Slika 1: Pravokotnik z oglišči v $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$, $(\frac{p}{2},\frac{q}{2})$

Ta ima enačbo

$$y = \frac{q}{p}x \quad oz. \quad py = qx.$$

Ker vemo, da sta p in q različni praštevili, je $\gcd(p,q) = 1$ in torej $p|x$ ter $q|y$. Ampak $x \in \{0, 1, ..., \frac{p-1}{2}\}$, zato enačba nima celoštevilskih rešitev in tako na diagonali D ni celoštevilskih točk. Označimo del pod diagonalo z Z_1 in del nad diagonalo z Z_2. Ker na diagonali ni celoštevilskih točk, je dovolj prešteti vse celoštevilske točke v Z_1 in Z_2. Število celoštevilskih točk na intervalu $0 < y < \frac{kq}{p}$ je $\lfloor \frac{kq}{p} \rfloor$. Za interval $1 \leq k \leq \frac{p-1}{2}$ je točno $\lfloor \frac{kq}{p} \rfloor$ celoštevilskih točk nad točko $(k, 0)$ v Z_1. Torej je število celoštevilskih točk v Z_1 ravno

$$\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor.$$

V Z_2 delamo isto kot v Z_1, le z zamenjanima vlogama x in y, torej $0 < x < \frac{kp}{q}$. Število celoštevilskih točk v Z_2 je tako

$$\sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor.$$

Potem velja

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor,$$

torej je produkt Legendrovih simbolov

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor} \cdot (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor} =$$

$$= (-1)^{\sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor + \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{jq}{p} \rfloor} =$$

$$= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

Posledica 1. *Za različni lihi praštevili p in q velja*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ ali } q \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \text{ in } q \equiv 3 \pmod 4 \end{cases}.$$

Dokaz. Če je vsaj eno število izmed praštevil p in q oblike $4k + 1$, potem je vsaj eno izmed števil $\frac{p-1}{2}$ in $\frac{q-1}{2}$ sodo, torej je

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = ((-1)^2)^k = 1$$

Sicer sta števili $\frac{p-1}{2}$ in $\frac{q-1}{2}$ lihi in velja $(-1)^{2k-1} = -1$. □

Za konec si kot zanimivost poglejmo, kako bi s pomočjo znanja o kvadratnih ostnkih pokazali, da je praštevil oblike $4k+1$ neskončno.

Izrek 5. *Obstaja neskončno praštevil oblike* $4k+1$.

Dokaz. Dokaza se bomo lotili s protislovjem. Recimo torej, da je praštevil oblike $4k+1$ končno mnogo in naj bodo to števila $\{p_1, ..., p_n\}$. Označimo z $N = (2p_1 \cdot ... \cdot p_n)^2 + 1$. Po predpostavki to ni praštevilo, saj je oblike 4k+1 in večje od p_n, zato ima vsaj en praštevilski delitelj p. Iz tega sledi

$$(2p_1 \cdot ... \cdot p_n)^2 \equiv -1 \pmod{p}.$$

Z Legendrovim simbolom zapišemo to kot $\left(-\frac{1}{p}\right) = 1$, ampak vemo, da je $\left(-\frac{1}{p}\right) = 1$ za praštevila oblike $4k+1$. Iz tega sledi, da je $p = 4k+1$ in $p = p_i$ za nek $1 \leq i \leq n$, zaradi česar bi moralo veljati

$$p_i | N - (2p_1 \cdot ... \cdot p_n)^2$$

in

$$N - (2p_1 \cdot ... \cdot p_n)^2 = 1.$$

Sledi, da $p_i|1$, kar pa ni mogoče, torej smo prišli do protislovja. To pomeni, da je praštevil oblike $4k+1$ res neskončno. □

Literatura

[1] D. M. Burton, *Elementary number theory*, Revisited printing, Allyn and Bacon, Boston, 1976.

[2] *Quadratic Reciprocity*, v: Wikipedia: The Free Encyclopedia, [ogled 17. 8. 2017], dostopno na `https://en.wikipedia.org/wiki/Quadratic_reciprocity`.