فرهنگ و اندیشهٔ ریاضی
شماره ۳۹ (پاییز ۱۳۸٦) صص. ۴۵ تا ۵۴

اعداد اول در حلقهٔ اعداد صحیح گاوس

منوچهر میثاقیان

چکیده

حلقهٔ اعداد صحیح گاوسی به تعبیری نخستین گسترش حلقهٔ اعداد صحیح معمولی $\mathbb{Z}$ است. حلقهٔ اعداد صحیح گاوسی $\mathbb{Z}[i]$ شباهت‌هایی به $\mathbb{Z}$ دارد، از جمله یک حلقهٔ اقلیدسی و در نتیجه یک حوزهٔ تجزیهٔ یکتا[1] است. با توجه به اهمیت اعداد اول، بررسی اعداد اول در $\mathbb{Z}[i]$ نیز از اهمیت ویژه‌یی برخوردار است.

در این مقاله به دو پرسش زیر پاسخ می‌دهیم:

- کدام یک از اعضای $\mathbb{Z}[i]$ اول هستند؟
- شرط لازم و کافی برای آن که عدد اول $y \in \mathbb{Z}$ در $\mathbb{Z}[i]$ نیز اول باشد چیست؟

۱. مقدمه

اعداد اوّل در مجموعهٔ اعداد صحیح، $\mathbb{Z}$، مهمترین مجموعهٔ عددی را تشکیل می‌دهند که همواره مورد توجه ریاضیدانان بوده‌اند و هستند. در واقع این اعداد اساسی‌ترین مصالح ساختمانی در نظریه اعداد و بلکه تمامی ریاضیات هستند. یک خاصیت بنیادین حلقهٔ اعداد صحیح این است که حلقهٔ اقلیدسی است. اوّلین گسترش این حلقه، $\mathbb{Z}[i]$، باز هم یک حلقهٔ اقلیدسی و بنابراین یک حوزهٔ تجزیهٔ یکتا(UFD) است. این حلقه به حلقهٔ اعداد صحیح گاوسی معروف است. طبیعی است که بپرسیم اعداد اول در $\mathbb{Z}[i]$ چه اعدادی هستند؟ به عبارت دیگر چگونه می‌توانیم مشخص کنیم که عدد $z \in \mathbb{Z}[i]$ اوّل است یا نه؟ آیا عدد اوّل $p \in \mathbb{Z}$ باز هم در $\mathbb{Z}[i]$ اوّل است؟ در این نوشتار به این پرسش‌ها پاسخ می‌دهیم.

۲. پیش‌نیازها و یادآوری‌ها

در سرتاسر این نوشتار $\mathbb{Z}$ حلقهٔ اعداد صحیح را نمایش می‌دهد. عدد صحیح $p > ۱$ را یک عدد اوّل

1) Unique factorization domain (UFD)

در $\mathbb{Z}$ می‌گوییم هرگاه تنها مقسوم‌علیه‌های مثبت آن ۱ و p باشند.

تعریف ۲.۱. عدد صحیح m را یک مقسوم علیه عدد صحیح n می‌گوییم و می‌نویسیم $m|n$ اگر و تنها اگر عدد صحیح k وجود داشته باشد به گونه‌یی که $n = km$

تعریف ۲.۲. فرض می‌کنیم m یک عدد صحیح مثبت است. دو عدد صحیح a و b را هم ارز به پیمانهٔ m می‌گوییم هرگاه m یک مقسوم علیه عدد $a - b$ باشد. این مفهوم را به صورت $a \equiv b(m)$ می‌نویسیم. این رابطه یک رابطهٔ هم‌ارزی در $\mathbb{Z}$ تعریف می‌کند. با مسامحه رده‌های هم‌ارزی این رابطه را به صورت $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$ نشان می‌دهیم. این مجموعه با جمع و ضرب به پیمانهٔ m یک حلقهٔ جابجایی یکدار تعریف می‌کند. اگر $m = p$ یک عدد اوّل باشد در این صورت هر ردهٔ هم‌ارزی غیرصفر وارون‌پذیر است. یعنی $\mathbb{Z}/p\,\mathbb{Z}$ یک هیأت می‌شود. تعداد عناصر غیرصفر $\mathbb{Z}/p\,\mathbb{Z}$ برابر است با $p - 1$. از این رو داریم:

قضیهٔ کوچک فرما. برای عدد صحیح a که بر p بخش پذیر نباشد،

$$a^{p-1} \equiv 1(p)$$

به نتایج سادهٔ زیر هم نیاز داریم:

لم ۲.۱. اگر برای اعداد صحیح و مثبت a و b داشته باشیم $ab = 1$، در این صورت $a = b = 1$.
اثبات ساده است و به عنوان تمرین مقدماتی واگذار می‌شود.

لم ۲.۲. برای اعداد صحیح و نامنفی a و b اگر $a + b = 1$ آنگاه $b = 0$ و $a = 1$ یا $b = 1$ و $a = 0$. اثبات ساده است و به عنوان تمرین مقدماتی واگذار می‌شود.

قضیه ۲.۱. فرض کنیم p یک عدد اوّل است. اگر $p|ab$ دراین صورت $p|a$ یا $p|b$.
این قضیه در هر حلقهٔ اقلیدسی معتبر است. مطالعهٔ مقدماتی حلقهٔ $\mathbb{Z}$ که تعریف حلقه‌های اقلیدسی و اثبات قضیهٔ فوق را در بردارد جزٔ مطالب آشنادر سطح دبیرستان است. به عنوان مثال، رجوع شود به بند ۲ از فصل ۳ صفحات ۱۶۴ تا ۲۰۳ کتاب شرح ریاضیات جدید [۳].

تعریف ۲.۳. فرض کنیم p یک عدد اوّل است. عدد z را یک ریشهٔ اوّلیه به پیمانهٔ p گوییم. هرگاه $z^{(p-1)} \equiv 1(p)$ و $p - 1$ کوچکترین عدد مثبت با این خاصیت باشد. مثلاً عدد ۳ یک ریشهٔ اوّلیه به پیمانهٔ ۵ است امّا ۴ یک ریشهٔ اوّلیه به پیمانهٔ ۵ نیست زیرا $4^2 \equiv 1(5)$ و $4 = 1 - 5 < 2$. فرض کنیم برای عدد اوّل p، z یک ریشهٔ اوّلیه به پیمانهٔ p باشد. در این صورت برای هر عدد صحیح $1 \le a < p$ یک و تنها یک عدد صحیح $1 \le i \le p - 1$ وجود دارد به گونه‌یی که $a \equiv z^i(p)$.

۳. قانون تقابل درجه دوم

قانون تقابل درجه دوم یکی از زیباترین و در عین حال قویترین مفاهیم در نظریه اعداد است که صورت‌های مختلف و متفاوتی دارد. یکی از ساده‌ترین و معمولی‌ترین اشکال آن را که در این جا نیاز داریم بیان می‌کنیم.

تعریف ۳.۱. فرض کنیم p یک عدد اوّل در حلقهٔ $\mathbb{Z}$ است. عدد صحیح $a \in \mathbb{Z}$ را یک **ماندهٔ درجه**

دوم به پیمانهٔ p می‌گوییم هرگاه عدد صحیح $x \in \mathbb{Z}$ وجود داشته باشد که

$$x^۲ \equiv a(\mathrm{mod}P)$$

یعنی $x^۲ - a$ بر p بخش‌پذیر باشد.
مثلاً برای $p = ۷$، عدد ۲ یک ماندهٔ درجه دوم به پیمانهٔ ۷ است زیرا

$$۳^۲ = ۹ \equiv ۲(۷)$$

امّا ۳ یک ماندهٔ درجه دوم به پیمانهٔ ۷ نیست، همچنان که می‌توان نشان داد که معادلهٔ $x^۲ \equiv ۳(۷)$ جواب ندارد. (کافی است که همهٔ اعداد ۰، ۱، ۲، ۳، ۴، ۵ و ۶ را در معادلهٔ بالا قرار داد و ملاحظه کرد که هیچکدام صدق نمی‌کند.)

تعریف ۳.۲. فرض کنیم p یک عدد اوّل در $\mathbb{Z}$ است. نماد(تابع) لژاندر که به صورت $(\frac{\circ}{P})$ نشان داده می‌شود، برای هر عدد صحیح $a \in \mathbb{Z}$ چنین تعریف می‌شود:

$$\left(\frac{a}{p}\right) = \begin{cases} ۱ & \text{اگر } a \text{ یک ماندهٔ درجه دوم به پیمانهٔ } p \text{ است} \\ ۰ & \text{اگر } a \text{ بر } p \text{ بخش‌پذیر است} \\ -۱ & \text{اگر } a \text{ ماندهٔ درجه دوم به پیمانهٔ } p \text{ نیست} \end{cases}$$

مثلاً $(\frac{۲}{۷}) = ۱$، $(\frac{۳۵}{۷}) = ۰$ و $(\frac{۳}{۷}) = -۱$.

قضیه اویلر. فرض کنیم p یک عدد اوّل فرد است. دراین صورت برای عدد صحیح a داریم:

$$a^{(\frac{p-۱}{۲})} \equiv (\frac{a}{p})(\mathrm{mod}p)$$

اثبات. فرض کنیم z یک ریشهٔ اوّلیه به پیمانهٔ p است. هر عدد صحیح a هم‌ارز یک توان z است، بخصوص a یک ماندهٔ درجه دوم به پیمانهٔ p است اگر هم‌ارز یک توان زوج z باشد. فرض کنیم a یک ماندهٔ درجه دوم (به پیمانهٔ p) است یعنی $(\frac{a}{p}) = ۱$. بنابراین داریم:

$$a \equiv z^{۲k}(\mathrm{mod}p)$$

برای هر عدد صحیح و مثبت k بنابر قضیهٔ کوچک فرما داریم:

$$a^{(\frac{p-۱}{۲})} \equiv (g^{۲k})^{(\frac{p-۱}{۲})} \equiv (g^{p-۱})^k \equiv ۱^k \equiv ۱(\mathrm{mod}p) \equiv (\frac{a}{P})(\mathrm{mod}p).$$

حالا فرض کنیم a ماندهٔ درجه دوم نیست یعنی $(\frac{a}{P}) = -۱$. این واقعیت که a یک ماندهٔ درجه دوم به پیمانهٔ p نیست به این معنی است که a هم‌ارز یک توان فرد z به پیمانهٔ p است. بنابراین داریم:

$$a \equiv \xi^{۲k+۱}(\mathrm{mod}p)$$

برای یک عدد صحیح و مثبت k. با استفاده از قضیهٔ کوچک فرما داریم:

$$a^{(\frac{p-1}{2})} \equiv (z^{2k+1})^{(\frac{p-1}{2})} \equiv (z^{p-1})^k . z^{(\frac{p-1}{2})} \equiv z^{(\frac{p-1}{2})} (\mathrm{mod} p)$$

واضح است که $z^{(\frac{p-1}{2})}$ هم‌ارز ۱ و ۱− است امّا چون $p-1 > \frac{p-1}{2}$ و z یک ریشهٔ اوّلیه است پس $z^{(\frac{p-1}{2})}$ نمی‌تواند هم‌ارز ۱ باشد در نتیجه:

$$a^{(\frac{p-1}{2})} \equiv z^{(\frac{p-1}{2})} \equiv -1 (\mathrm{mod} p) \equiv (\frac{a}{p}) (\mathrm{mod} p)$$

و اثبات تمام است.

نماد لژاندر یک تابع ضربی است. دقیقتر این تابع دارای خواص زیراست.

قضیه ۳.۱. فرض کنیم p یک عدد اوّل باشد. برای هر دو عدد صحیح $a, b \in \mathbb{Z}$ داریم:

الف) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

ب) $a \equiv b (\mathrm{mod} p) \Longrightarrow (\frac{a}{p}) = (\frac{b}{p})$

اثبات. اگر p یکی از اعداد a یا b را بشمارد، قضیه بدیهی است. بنابراین فرض کنیم p هیچکدام از اعداد a یا b را نشمارد. در این صورت:

الف) بنابر قضیهٔ اویلر داریم:

$$\begin{aligned}
(\frac{ab}{p}) \equiv & \quad (ab)^{(\frac{p-1}{2})} (\mathrm{mod} p) \\
\equiv & \quad (a)^{(\frac{p-1}{2})} (b)^{(\frac{p-1}{2})} (\mathrm{mod} p) \\
\equiv & \quad ((a)^{\frac{p-1}{2}} (\mathrm{mod} p))((b)^{\frac{p-1}{2}} (\mathrm{mod} p)) \\
= & \quad (\frac{a}{p})(\frac{b}{p})
\end{aligned}$$

ب) بی‌درنگ از تعریف نتیجه می‌شود. اثبات تمام است.

قضیه (قانون تقابل درجه دوم). اکنون صورتی از قانون تقابل درجه دوم گاوس را می‌آوریم که نیازمان را برطرف خواهد کرد.

فرض کنیم p یک عدد اوّل فرد است. دراین صورت

$$(\frac{-1}{p}) = \begin{cases} 1 & p \equiv 1 (\mathrm{mod} 4) \\ -1 & p \equiv 3 (\mathrm{mod} 4) \end{cases}$$

اثبات. فرض کنیم $p \equiv 1 (\mathrm{mod} 4)$، در این صورت $p = 4k+1$ برای یک عدد صحیح k. از این جا خواهیم داشت $\frac{p-1}{2} = 2k$ و بنابر قضیه اویلر داریم:

$$(-1)^{\frac{p-1}{2}} \equiv (\frac{-1}{p}) (\mathrm{mod} p)$$

$$۱ = (-۱)^{۲k} \equiv (\frac{-۱}{p})(\mathrm{mod}p) \Longrightarrow (\frac{-۱}{p}) = ۱$$

یعنی ۱− یک ماندهٔ درجه دوم به پیمانهٔ p است.
اگر $p \equiv ۳(\mathrm{mod}۴)$ در این صورت برای یک عدد صحیح k داریم:

$$p = ۳ + ۴k$$

یعنی $\frac{p-۱}{۲} = ۲k + ۱$ و مجدداً بنابر قضیه اویلر داریم

$$(\frac{-۱}{p}) \equiv (-۱)^{(\frac{p-۱}{۲})}(\mathrm{mod}p) \equiv -۱(\mathrm{mod}p)$$

بنابراین $(\frac{-۱}{p}) = -۱$

قضیه ۳.۲. عدد اوّل $p \in \mathbb{Z}$ را می‌توان به صورت مجموع مربع‌های دو عدد صحیح نوشت اگر و تنها اگر $p = ۲$ یا $p \equiv ۱(\mathrm{mod}۴)$.

اثبات. اگر $p = ۲$ در این صورت $p = ۱ + ۱ = ۱^۲ + ۱^۲$. اگر $p = x^۲ + y^۲$ در این صورت x و y هر دو نمی‌توانند زوج باشند و چون p اوّل است هر دو می‌توانند فرد باشند اگر $x^۲ = y^۲ = ۱$ و بنابراین $p = ۲$.
فرض کنیم p عدد اوّل فردی است. اگر $p = x^۲ + y^۲$ در این صورت یکی از اعداد x یا y فرد و دیگری زوج است. فرض کنیم $x = ۲k$ و $y = ۲l - ۱$ است.
در این صورت داریم:

$$\begin{aligned} p &= (۲k)^۲ + (۲l - ۱)^۲ \\ &= ۴k^۲ + ۴l^۲ - ۴l + ۱ \\ &= ۴(k^۲ + l^۲ - l) + ۱ \end{aligned}$$

یعنی $p \equiv ۱(\mathrm{mod}۴)$.
برعکس فرض کنیم $p \equiv ۱(\mathrm{mod}۴)$. بنابر قضیه تقابل درجه دوم اعداد صحیح x و t وجود دارند به گونه‌یی که $pt = x^۲ + ۱$ و $۱ \leq t < p$.
اگر $t = ۱$ حکم تمام است و اگر $t \geq ۲$، عدد صحیح $y \in \mathbb{Z}$ را می‌توان یافت به طوری که $y \equiv x(\mathrm{mod}\ t)$ و $\frac{-t}{۲} < y < \frac{t}{۲}$. بنابراین خواهیم داشت:

$$y^۲ \equiv x^۲(\mathrm{mod}\ t)$$

$$۱ \equiv ۱(\mathrm{mod}\ t)$$

از این جا خواهیم داشت:

$$y^۲ + ۱ \equiv x^۲ + ۱ \equiv ۰(mod\ t)$$

یعنی $y^۲ + ۱ = rt$ برای عدد صحیح $۱ \leq r < t$. و چون داریم $x^۲ + ۱ = pt$، از ضرب پهلو به پهلوی این دو هم‌ارزی خواهیم داشت:

$$(y^۲ + ۱)(x^۲ + ۱) = prt^۲$$

حاصلضرب سمت چپ این رابطه برابر است با

$$(y^۲ + ۱)(x^۲ + ۱) = (x - y)^۲ + (xy + ۱)^۲$$

یعنی

$$(x - y)^۲ + (xy + ۱)^۲ = prt^۲$$

با توجه به روابط بین x و y واضح است که هر دو عامل $(x - y)^۲$ و $(xy + ۱)^۲$ بر $t^۲$ بخش‌پذیرند. بنابراین داریم.

$$(\frac{x - y}{t})^۲ + (\frac{xy + ۱}{t})^۲ = rp$$

رابطهٔ اخیر نشان می‌دهد که ضریب کوچکتری از $p(r < t)$ را می‌توان به صورت حاصل جمع دو مربع نوشت. اگر $r = ۱$ حکم تمام است و اگر $r \geq ۲$ روش بالا را می‌توان تکرار کرد تا ضریب کوچکتری از p را به صورت حاصل جمع دو مربع بتوان نوشت. واضح است که پس از تکرار با پایانی به ضریب ۱ می‌رسیم و برهان تمام است.

۴. حلقهٔ اعداد صحیح گاوسی

فرض کنیم i واحد انگاری است، یعنی در رابطهٔ اساسی $i^۲ = -۱$ صدق می‌کند. قرار می‌دهیم

$$\mathbb{Z}[i] = \{m + ni | m, n \in \mathbb{Z}\}.$$

این مجموعه با جمع و ضرب برگرفته از هیأت اعداد مختلط یک حلقهٔ جابجایی یکدار است. این حلقه که $\mathbb{Z}$ را به صورت یک زیرحلقه در بر دارد به حلقهٔ اعداد صحیح گاوسی معروف است. تابع ν، نرم، را به صورت زیر درنظر بگیرید:

$$\nu : \mathbb{Z}[i] \longrightarrow \{۰, ۱, ۲, \ldots, n, \ldots\}$$
$$\nu(m + ni) = m^۲ + n^۲$$

این تابع دارای خواص زیر است:
(۱) برای هر عدد صحیح گاوسی $z = m + ni \neq ۰$ داریم $\nu(z) \geq ۰$ و برعکس اگر $\nu(z) \neq ۰$

آنگاه $z \neq 0$.
(۲) برای همهٔ اعداد صحیح گاوسی z_1 و z_2 داریم:

$$\nu(z_1 z_2) = \nu(z_1)\nu(z_2)$$

به کمک این نرم می‌توان نشان داد که $\mathbb{Z}[i]$ یک حلقهٔ اقلیدسی و بنابراین یک حوزهٔ تجزیهٔ یکتا است.

تعریف ۴.۱. عدد $z = m + ni \in \mathbb{Z}[i]$ را وارون پذیر(یا یکان) می‌گوییم هرگاه عدد $z^{-1} = a + bi \in \mathbb{Z}[i]$ وجود داشته باشد که

$$zz^{-1} = 1$$

لم ۴.۱. مجموعهٔ یکان‌ها (وارون پذیر) در حلقهٔ $\mathbb{Z}[i]$ برابر است با

$$U = \{-1, 1, -i, i\}$$

اثبات . فرض کنیم $z = a + bi \in \mathbb{Z}[i]$ یکان است. بنابراین $z^{-1} = c + di \in \mathbb{Z}[i]$ وجود دارد به طوری که

$$zz^{-1} = 1$$

از این جا داریم:

$$\nu(zz^{-1}) = \nu(z)\nu(z^{-1}) = \nu(1)$$
$$(a^2 + b^2)(c^2 + d^2) = 1$$

از این رابطه بنابر لم ۲.۱ خواهیم داشت $a^2 + b^2 = c^2 + d^2 = 1$ و بنابر لم ۲.۲ نتیجه می‌گیریم که $a = \pm 1$ یا $b = \pm 1$ یعنی $z = \pm 1$ یا $z = \pm i$.

تعریف ۴.۲. عدد $z = m + ni \in \mathbb{Z}[i]$ را اوّل می‌گوییم هرگاه از برابری زیر

$$m + ni = (a + bi)(c + di)$$

نتیجه بگیریم یکی از عامل‌های سمت راست یکان است. به عنوان مثال، ۵ در $\mathbb{Z}[i]$ اوّل نیست زیرا می‌توان آن را به صورت زیر تجزیه کرد

$$5 = (1 + 2i)(1 - 2i)$$

همین طور $z = 3 + 4i$ اوّل نیست زیرا

$$3 + 4i = (2 + i)^2$$

امّا $z = ۲ + i$ و $z = ۲ + i$ اوّل هستند. مثلاً برای $z = ۲ + i$ اگر داشته باشیم

$$z = ۲ + i = (a + bi)(c + di)$$

آنگاه باید داشته باشیم

$$\nu(۲ + i) = \nu(a + bi)\nu(c + di)$$
$$۵ = (a^۲ + b^۲)(c^۲ + d^۲)$$

از این جا با توجه به این که ۵ در $\mathbb{Z}$ عددی اوّل است نتیجه می‌گیریم که $a^۲ + b^۲ = ۱$ یا $c^۲ + d^۲ = ۱$ یعنی $a + bi$ یا $c + di$ باید یکان باشد.

قضیهٔ ۴.۱. عدد اوّل $p \in \mathbb{Z}$ در حلقهٔ $\mathbb{Z}[i]$ اوّل است اگر و تنها اگر $p \equiv ۳ (\mathrm{mod} ۴)$

اثبات. فرض کنیم p در $\mathbb{Z}[i]$ اوّل است. اگر $p \not\equiv ۳ (\mathrm{mod} ۴)$ در این صورت $p = ۲$ یا $p = ۱ (\mathrm{mod} ۴)$. بنابراین براساس قضیه ۳.۲، p را می‌توان بصورت مجموع دو مربع کامل نوشت یعنی $p = m^۲ + n^۲$ و از این جا خواهیم داشت:

$$p = m^۲ + n^۲ = (m + ni)(m - ni)$$

یعنی p در $\mathbb{Z}[i]$ اوّل نیست که خلاف فرض ماست. برعکس فرض کنیم $p \equiv ۳ (\mathrm{mod} ۴)$. اگر p در $\mathbb{Z}[i]$ اوّل نباشد در این صورت p را می‌توان در $\mathbb{Z}[i]$ به صورت زیر تجزیه کرد:

$$p = (a + bi)(c + di)$$

این رابطه نتیجه می‌دهد که

$$\nu(p) = \nu(a + bi)\nu(c + di)$$
$$p^۲ = (a^۲ + b^۲)(c^۲ + d^۲)$$

چون p در $\mathbb{Z}$ اوّل است بنابراین مطابق قضیه ۲.۱ باید داشته باشیم

$$p|(c^۲ + d^۲) \quad \text{یا} \quad p|(a^۲ + b^۲)$$

فرض کنیم $p|a^۲ + b^۲$ یعنی $pt = a^۲ + b^۲$ برای یک عدد صحیح t. از این جا خواهیم داشت:

$$a^۲ + b^۲ \equiv ۰ (\mathrm{mod} p)$$

یا

$$a^۲ \equiv -b^۲ (\mathrm{mod}\ p)$$

و بنابر قضیه ۳.۱(ب) خواهیم داشت:

$$(\frac{a^۲}{p}) = (\frac{-b^۲}{p})$$

اگر بند الف قضیه ۳.۱ را در مورد رابطهٔ اخیر به کار بگیریم خواهیم داشت:

$$(\frac{a^2}{p}) = (\frac{a}{p})^2 = (\frac{-1}{p})(\frac{b}{p})^2$$

چون همواره $(\frac{a}{p}) = \pm 1$ و $(\frac{b}{p}) = \pm 1$ (حالت پیش پا افتادهٔ $(\frac{a}{p}) = 0$ یا $(\frac{b}{p}) = 0$ نمی‌تواند این جا پیش بیاید). بنابراین

$$(\frac{a}{p})^2 = (\frac{b}{p})^2 = 1$$

یعنی $(\frac{-1}{p}) = 1$ و بنابر قضیهٔ تقابل درجه دوم خواهیم داشت $p \equiv 1 \pmod 4$ که خلاف فرض است. بنابراین p در $\mathbb{Z}[i]$ اوّل است.

قضیهٔ ۴.۲. عدد صحیح گاوسی $z = a + bi \in \mathbb{Z}[i]$ با $ab \neq 0$ اوّل است اگر و تنها اگر $\nu(z)$ در $\mathbb{Z}$ اوّل باشد.

اثبات. فرض کنیم $z = a + bi$ در $\mathbb{Z}[i]$ اوّل است. اگر $\nu(z) = a^2 + b^2$ در $\mathbb{Z}$ اوّل نباشد در این صورت عدد اوّل p در $\mathbb{Z}$ وجود دارد به طوری که $p|a^2 + b^2$ یعنی $a^2 + b^2 = pq$ که در آن q یک عدد صحیح در $\mathbb{Z}$ است و $q > 1$. در $\mathbb{Z}[i]$ رابطهٔ بالا برابر است با

$$(a + bi)(a - bi) = pq$$

چون $\mathbb{Z}[i]$ اقلیدسی است بنابر قضیه ۲.۱ نتیجه می‌شود که

$$(a + bi)|p \quad \text{یا} \quad (a + bi)|q$$

فرض کنیم $a + bi|p$ یعنی $p = z(a + bi)$ که در آن $z \in \mathbb{Z}[i]$، بنابراین اگر قرار دهیم $z = c + di$ آنگاه: $p = (c + di)(a + bi)$. از این جا خواهیم داشت:

$$\nu(p) = \nu(c + di)\nu(a + bi)$$

یا

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

نظر به این که $(a^2 + b^2) = pq$ رابطهٔ اخیر نتیجه می‌دهد که

$$p = q(c^2 + d^2)$$

بنابراین $p = q$ یا $p = c^2 + d^2$. اگر $p = q$ در این صورت $c^2 + d^2 = 1$ یعنی $z \in U$ که غیر ممکن است (زیرا p یک عدد صحیح در $\mathbb{Z}$ است نه در $\mathbb{Z}[i]$). و اگر $p = c^2 + d^2$ در این صورت $q = 1$ که خلاف $q > 1$ است. بنابراین $\nu(z)$ در $\mathbb{Z}$ اوّل است. اگر $a + bi|q$ در این صورت چنانچه q اوّل است، استدلال بالا را تکرار می‌کنیم و اگر q اوّل نیست در این صورت q یک فاکتور اوّل دارد و

استدلال بالا قابل تکرار است. بنابراین با تکرار تعدادی متناهی از استدلال بالا حکم ثابت می‌شود.
برعکس فرض کنیم برای $z = a + bi \in \mathbb{Z}[i]$، $\nu(z)$ در $\mathbb{Z}$ اوّل است. اگر z اوّل نباشد در این صورت

$$z = a + bi = (\alpha + \beta i)(\gamma + \delta i)$$

در این جا خواهیم داشت:

$$\nu(z) = \nu(\alpha + \beta i)\nu(\gamma + \delta i)$$

یا

$$\nu(z) = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)$$

چون $\nu(z)$ اوّل است، رابطهٔ بالا نتیجه می‌دهد که

$$\alpha^2 + \beta^2 = 1 \quad \text{یا} \quad \gamma^2 + \delta^2 = 1$$

و بنابر لم ۲.۲ نتیجه می‌شود که $\alpha + \beta i$ یا $\gamma + \delta i$ یکان است یعنی $z = a + bi$ اوّل است.

مراجع

[1] Ireland, K. and Rosen, M., "A Classical Introduction to Modern Number Theory", 2^{nd} Edition, Springer-Verlag, 1990.

[2] Silverman, J.H. , "A firendly Introduction to Number theory", 2^{nd} Edition, Prentice Hall, 2001.

[۳] شادمان، ا.، للهی، ک. و واحدی آملی، ع. ا. ،«شرح ریاضیات جدید» چاپ دوم، انتشارات علوی، تهران، ۱۳۶۹.

منوچهر میثاقیان

Manouchehr Misaghian
Mathematics Department
Johnson C. Smith Univ.
Charlotte, Nc 28216
USA
E-mail: mmisaghian@Jcsu.edu