.

دانشگاه تبریز

دانشکده علوم ریاضی و کامپیوتر

جزوه درسی

نظریه اعداد

مولف:

دکتر محمد شهریاری

۱۳۸۷

فهرست مطالب

مقدمه

هدف این درس مطالعه خواص دستگاه اعداد صحیح، یعنی

$$(\mathbb{Z}, +, \times, \leq)$$

می‌باشد. یکی از مهم‌ترین ویژگیهای مجموعه اعداد صحیح خاصیت خوش‌ترتیبی آن است.

خوش ترتیب بودن $\mathbb{Z}$—

اگر $S \subseteq \mathbb{Z}$ ناتهی و از پایین (از بالا) کراندار باشد آنگاه S عضو ابتدا (عضو انتها) دارد.

اصل استقرای ریاضی معادل ویژگی خوش ترتیب بودن $\mathbb{Z}$ است.

جزوهٔ حاضر خلاصه درسی است که تحت عنوان **نظریه اعداد** در نیمسال اول سال تحصیلی ۸۷—۸۶ در دانشکدهٔ ریاضی دانشگاه تبریز توسط مولف ارائه شده است.

فصل ۱

تقسیم‌پذیری

در این فصل یک رابطه دوتایی بسیار مهم را در مجموعه اعدد صحیح معرفی می‌کنیم و به بررسی خواص آن می‌پردازیم.

۱.۱ تعریف— فرض کنید a و b دو عدد صحیح باشند و $a \neq 0$. می‌گوییم a، b را عاد می‌کند (و یاa شمارنده b است و یا b بر a تقسیم‌پذیر (بخش‌پذیر) است) هرگاه

$$\exists x \in \mathbb{Z} : b = ax$$

در این حالت می‌نویسیم $a|b$. اگر a شمارنده b نباشد، می‌نویسیم $a \nmid b$.

۲.۱ گزاره— احکام زیر درست می‌باشند:

الف) اگر $a|b$ آنگاه بازای هر عدد صحیح c داریم

$$a|bc\ .$$

ب) اگر$a|b$ و $b|c$ آنگاه $a|c$.

ج) اگر$a|b$ و $a|c$ آنگاه

$$\forall x, y \in \mathbb{Z} : a|(bx + cy)\ .$$

د) اگر$a|b$ و $b|a$ آنگاه $a = \pm b$.

ه) اگر$a|b$ و a و b هر دو مثبت باشند آنگاه $a \leq b$.

۳.۱ تبصره— اگر

$$a|b_1, a|b_2, \ldots, a|b_n$$

آنگاه بازای هر $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ داریم:

$$a|\sum_{i=1}^{n} b_i x_i\ .$$

۴.۱ قضیه (الگوریتم تقسیم)— فرض کنیم a و b دو عدد صحیح باشند و $0 < a$. آنگاه اعداد صحیح منحصر بفرد q و r وجود دارند که

$$b = aq + r \quad , \quad 0 \leq r < a \; .$$

اثبات— مجموعه S را چنین تعریف می‌کنیم

$$S = \{b - ax \quad : \quad x \in \mathbb{Z} \quad , \quad b - ax \geq 0\}$$

این مجموعه ناتهی است، چون بازای اعداد صحیح $b/a \geq x$ مقدار $b - ax$ در داخل S قرار می‌گیرد. در ضمن S از پایین کراندار است. پس S یک عضو ابتدا مانند r دارد. چون $r \in S$ پس

$$\exists q \in \mathbb{Z} \quad : \quad r = b - aq$$

بنابراین $b = aq + r$. بدیهی است که $0 \leq r$. نشان میدهیم که $r < a$. فرض کنیم چنین نباشد. پس $a \leq r$. پس می‌توان نوشت

$$\begin{aligned} b &= aq + r \\ &= aq + a + (r - a) \\ &= a(q + 1) + (r - a) \end{aligned}$$

بنابراین

$$b - a(q+1) = r - a \geq 0$$

پس $r - a \in S$ و این با عضو ابتدا بودن r در مجموعه S متناقض است. پس ثابت کردیم که $r < a$.

حال نشان میدهیم که r و q با خاصیت بالا منحصربفرد است. فرض کنیم r' و q' اعداد صحیح دیگری باشند که $0 \leq r' < a$ و $b = aq' + r'$. باید نشان دهیم که $r' = r$ و $q' = q$. داریم

$$aq + r = b = aq' + r' .$$

بنابراین با تفریق طرفین دو عبارت خواهیم داشت

$$a(q - q') = r' - r .$$

پس $a|(r' - r)$. اما $0 \leq r, r' < a$. پس باید داشته باشیم $r' - r = 0$. پس $r' = r$. بلافاصله $q' = q$ هم نتیجه می‌شود.

■

۵.۱ تبصره— در الگوریتم تقسیم می‌توانستیم a را منفی نیز فرض کنیم. در این صورت عدد r باید در نامساوی $0 \leq r < |a|$ صدق می‌کرد.

۶.۱ تبصره— در الگوریتم تقسیم، q را خارج قسمت و r را باقیمانده می‌نامیم.

۷.۱ تعریف— فرض کنیم $b_1, b_2, \ldots, b_n \neq 0$

اعداد صحیح باشند. بازای هر $1 \leq i \leq n$ تعریف می‌کنیم

$$D_i = \{a \in \mathbb{Z} \quad : \quad a|b_i\}.$$

حال قرار می‌دهیم $S = \bigcap_{i=1}^{n} D_i$. بدیهی است که S ناتهی است. هر عضو S را یک مقسوم علیه مشترک b_i ها می‌نامیم. چون S متناهی است، پس عضو انتها دارد. این عضو را بزرگترین مقسوم علیه مشترک b_i ها نامیده و با نماد $(b_1, b_2, \ldots, b_n)$ و یا گاهی با $gcd(b_1, b_2, \ldots, b_n)$ نشان می‌دهیم. بزرگترین مقسوم‌علیه مشترک دو عدد صحیح a و b را با (a, b) یا گاهی $gcd(a, b)$ نشان می‌دهیم.

۸.۱ تبصره— تعریف می‌کنیم

$$(a, 0) = |a| \ .$$

۹.۱ قضیه— فرض کنید $g=(b,c)$. آنگاه

$$\exists x_0, y_0 \in \mathbb{Z} \quad : \quad g = bx_0 + cy_0$$

اثبات— اگر $c=0$ آنگاه $g=|b|$ و در نتیجه می‌توان از یکی از دو حالت زیر x_0 و y_0 را بدست آورد:

الف) $b>0 \quad \Rightarrow \quad x_0=1 \quad , \quad y_0=$دلخواه

ب) $b<0 \quad \Rightarrow \quad x_0=-1 \quad , \quad y_0=$دلخواه

پس فرض کنیم b و c هر دو غیرصفر باشند. مجموعه S را چنین تعریف می‌کنیم

$$S = \{bx+cy \quad : \quad x,y \in \mathbb{Z} \ , \ bx+cy>0\}$$

این مجموعه ناتهی و از پایین کراندار است. پس عضو ابتدایی مانند l دارد. چون $l \in S$ پس

$$\exists x_0, y_0 \in \mathbb{Z} \ : \ l = bx_0 + cy_0 > 0 \ .$$

ادعا می‌کنیم که $l|b$. فرض کنیم چنین نباشد. پس طبق الگوریتم تقسیم اعداد صحیح r و q وجود دارند که

$$b = lq + r \quad , \quad 0 < r < l \ .$$

بنابراین

$$\begin{aligned} 0 < r \quad &= b - lq \\ &= b - (bx_0 + cy_0)q \\ &= b(1 - qx_0) + cy_0(-q) \ . \end{aligned}$$

این نشان میدهد که r بفرم اعضای S است. پس $r \in S$. اما r از عضو ابتدای S هم کوچکتر است. این تناقض است و در نتیجه باید داشته باشیم $l|b$.

به شکل مشابه ثابت می‌شود که $l|c$. بنابراین $l \leq g$. از سوی دیگر چون g بزرگترین مقسوم‌علیه مشترک b و c است پس

$$\exists \alpha \in \mathbb{Z} \quad : \quad b = g\alpha \ ,$$

$$\exists \beta \in \mathbb{Z} \quad : \quad c = g\beta \ .$$

پس داریم

$$\begin{aligned} l \quad &= bx_0 + cy_0 \\ &= g(\alpha x_0 + \beta y_0) \ . \end{aligned}$$

درنتیجه $g|l$. پس $g \leq l$. حال همزمان داریم

$$g \leq l \quad , \quad l \leq g \ ,$$

پس $l = g$. بنابراین $g = bx_0 + cy_0$.

■

۱۰.۱ نتیجه — کوچکترین عدد صحیح مثبت به شکل $bx + cy$ همان بزرگترین مقسوم‌علیه مشترک b و c است.

۱۱.۱ نتیجه — اگر $a|b$ و $a|c$ آنگاه $a|(b, c)$.

۱۲.۱ تبصره — فرض کنیم

$$g = gcd(b_1, b_2, \ldots, b_n)$$

آنگاه اعداد صحیح $x_1, x_2, \ldots, x_n$ وجود دارند که

$$g = \sum_{i=1}^{n} b_i x_i$$

ضمنا دو نتیجه ۱۰.۱ و ۱۱.۱ را می‌توان به این حالت هم تعمیم داد.

۱۳.۱ گزاره— فرض کنید m یک عدد صحیح مثبت باشد. آنگاه

$$(ma, mb) = m(a, b)$$

اثبات— می‌دانیم که (ma, mb) کمترین مقدار مثبت اعداد زیر است:

$$max + mby \quad ; \quad x, y \in \mathbb{Z}$$

اما کمترین مقدار موردنظر با ضرب کردن m به کمترین مقدار مثبت اعداد زیر حاصل می‌شود:

$$ax + by \quad ; \quad x, y \in \mathbb{Z}$$

■

۱۴.۱ گزاره— اگر $d|a$ و $d|b$ آنگاه

$$(\frac{a}{d}, \frac{b}{d}) = \frac{(a, b)}{d}$$

اثبات— مثل ۱۳.۱.

■

۱۵.۱ تعریف— دو عدد a و b را متباین یا نسبت به هم اول می‌نامیم هرگاه $(a,b)=1$. اگر $(b_1,b_2,\ldots,b_n)=1$ آنگاه b_i ها را کلاً متباین می‌نامیم. اگر

$$\forall\, i,j \quad : \quad i\neq j \quad \Rightarrow \quad (b_i,b_j)=1$$

آنگاه b_i ها را دوبه‌دو متباین می‌گوییم.

۱۶.۱ تبصره— اگر $g=(a,b)$ آنگاه a/g و b/g متباین هستند.

۱۷.۱ گزاره— اگر m نسبت به a و b اول باشد آنگاه نسبت به ab نیز اول است.

۱۸.۱ گزاره— اگر $c|ab$ و $(b,c)=1$ آنگاه $c|a$.

اثبات—چون $(b,c)=1$ پس

$$\exists x,y\in\mathbb{Z} \quad : \quad bx+cy=1\ .$$

با ضرب طرفین رابطه بالا به a خواهیم داشت:

$$abx+acy=a\ .$$

حال چون c سمت چپ تساوی بالا را عاد می‌کند پس $c|a$.

■

۱۹.۱ الگوریتم اقلیدس— فرض کنیم a و b دو عدد صحیح مثبت باشند و هدف محاسبه (a,b) باشد. با بکار بردن الگوریتم تقسیم، معادلات متوالی زیر را تا جایی ادامه می‌دهیم که به باقیمانده صفر برسیم:

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b \\
b &= r_1q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

آنگاه $(a,b) = r_n$، یعنی آخرین باقیمانده غیرصفر در تقسیمات متوالی بالا عبارت است از بزرگترین مقسوم علیه مشترک a و b.

۲۰.۱ مثال — فرض کنیم $a = 963$ و $b = 657$. داریم

$$963 = 657 \times 1 + 306$$

$$657 = 306 \times 2 + 45$$

$$306 = 45 \times 6 + 36$$

$$45 = 36 \times 1 + 9$$

$$36 = 9 \times 4$$

پس نتیجه می‌گیریم $(963, 657) = 9$.

۲۱.۱ تعریف — فرض کنیم $a_1, a_2, \ldots, a_n$ اعداد صحیح غیرصفر باشند. اگر

$$\forall i \quad : \quad a_i | b$$

آنگاه b را یک مضرب مشترک a_i ها می‌نامیم. کوچکترین مضرب مشترک a_i ها را با نماد $[a_1, a_2, \ldots, a_n]$ نشان می‌دهیم.

۲۲.۱ گزاره— فرض کنیم b یک مضرب مشترک a_i ها باشد و $h = [a_1, a_2, \ldots, a_n]$. آنگاه $h|b$.

اثبات— طبق قضیه تقسیم اعداد صحیح q و r وجود دارند که

$$b = hq + r \quad , \quad 0 \leq r < h \; .$$

فرض کنیم $r \neq 0$. چون

$$\forall i \quad : \quad a_i|b \;\; \& \;\; a_i|h$$

پس تمام a_i ها باید r را عاد کنند. پس r هم یک مضرب مشترک a_i هااست. طبق تعریف h باید داشته باشیم $h \leq r$. این یک تناقض است.

■

۲۳.۱ گزاره— داریم

$$[a, b] = \frac{|ab|}{(a, b)} \; .$$

فصل ۲

اعداد اول

هدف این فصل معرفی مفهوم اول بودن در مجموعه اعداد صحیح است. اعداد اول، بلوکهای سازنده بقیه اعداد صحیح محسوب می‌شوند.

۱.۲ تعریف— عدد صحیح و مثبت p را اول می‌نامیم هرگاه $p \neq 1$ و p جز خودش و 1 شمارنده مثبت دیگر نداشته باشد. هر عدد صحیح غیر اول که مساوی یک یا صفر نباشد مرکب نامیده می‌شود.

۲.۲ گزاره— اگر $1 < n$ یک عدد صحیح باشد آنگاه عددی اول مانند p وجود دارد که $p|n$.

اثبات— اگر n اول باشد قرار می‌دهیم $p = n$. پس فرض کنیم n مرکب باشد. بنابراین

$$\exists n_1, n_2 \quad : \quad n = n_1 n_2$$

و ضمنا $1 < n_1, n_2 < n$. حال بنا به فرض استقراء قوی عدد اول p وجود دارد که $p|n_1$. پس $p|n$.

■

۳.۲ قضیه— اگر $1 < n$ یک عدد صحیح باشد آنگاه n به حاصلضربی از اعداد اول تجزیه می‌شود.

اثبات— اگر n اول باشد چیزی برای اثبات نداریم. پس فرض کنیم n مرکب باشد. طبق گزاره ۲.۲ عدد اولی مانند p وجود دارد که $p|n$. پس می‌توان نوشت $n = pm$. که در آن $1 < m < n$. حال طبق فرض استقراء m به حاصلضربی از اعداد اول تجزیه می‌شود؛ پس n نیز تجزیه می‌شود.

■

۴.۲ گزاره— فرض کنیم p یک عدد اول باشد. اگر $p|ab$ آنگاه $p|a$ یا $p|b$.

اثبات— فرض کنیم $p \nmid a$. چون عاملهای مثبت p عبارتند از ۱ و p، پس $(p, a) = 1$. حال طبق

۱۸.۱ باید داشته باشیم $p|b$.

■

۵.۲ قضیه (قضیه بنیادی حساب)— فرض کنیم $1 < n$ یک عدد صحیح باشد. فرض کنیم

$$n = p_1 p_2 \dots p_r \;=\; q_1 q_2 \dots q_s$$

که در آن تمام p_i ها و q_j ها اولند. آنگاه $r = s$ و

$$\{p_1, \dots, p_r\} = \{q_1, \dots, q_s\}$$

اثبات— در تساوی

$$p_1 p_2 \dots p_r \;=\; q_1 q_2 \dots q_s$$

تمام عاملهای مساوی از طرفین را حذف می‌کنیم. فرض کنیم بعد از این عمل هنوز عاملهایی در دو طرف تساوی باقی مانده باشند. مثلا

$$a_1 a_2 \dots a_l \;=\; b_1 b_2 \dots b_t$$

که در آن

$$\forall i \;:\; a_i \in \{p_1, \dots, p_r\}$$

$$\forall j \ : \ b_j \in \{q_1, \ldots, q_s\}$$

و ضمنا

$$\forall i, j \ : \ a_i \neq b_j \ .$$

حال داریم

$$a_1 \mid b_1 b_2 \ldots b_t$$

و طبق ۴.۲ باید

$$\exists j \ : \ a_1 \mid b_j$$

اما چون a_1 و b_j اول می‌باشند پس $a_1 = b_j$ که تناقض است.

■

۶.۲ تبصره— فرض کنیم $1 < n$ یک عدد صحیح مثبت باشد. با توجه به ۳.۲ می‌توان n را بصورت

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l}$$

نوشت که در آن p_i ها اعداد اول و α_i ها اعداد صحیح مثبت می‌باشند. بعلاوه طبق قضیه بنیادی حساب این تجزیه منحصر بفرد است.

۷.۲ الگوریتم محاسبه بزرگترین مقسوم علیه مشترک و کوچکترین مضرب مشترک با استفاده از تجزیه

— فرض کنیم a و b دو عدد صحیح مثبت و بزرگتر از یک باشند. فرض کنیم تجزیه ایندو عدد به شکل زیر باشد:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \quad , \quad \alpha_i \geq 0$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \quad , \quad \beta_i \geq 0$$

آنگاه داریم

$$(a,b) = \prod_{i=1}^{n} p_i^{min(\alpha_i,\beta_i)} \ ,$$

$$[a,b] = \prod_{i=1}^{n} p_i^{max(\alpha_i,\beta_i)} \ .$$

۸.۲ قضیه (اقلیدس)

— مجموعه اعداد اول نامتناهی است.

اثبات— فرض کنیم چنین نباشد. پس می‌توان نوشت

$$\text{مجموعه اعداد اول} = \{p_1, \dots, p_n\}$$

حال عدد صحیح مثبت N را چنین تعریف می‌کنیم

$$N = 1 + p_1 p_2 \dots p_n$$

چون $1 < N$، پس باید لااقل یک عامل اول داشته باشد یعنی

$$\exists i \ : \ p_i \mid N$$

اما این یعنی $p_i \mid 1$ که تناقض است.

■

۹.۲ قضیه— بازای هر عدد صحیح مثبت n، دنباله‌ای از n عدد صحیح مثبت متوالی وجود دارد که هیچکدام از عناصر آن اول نیست.

اثبات— کافی است به دنباله اعداد زیر توجه کنیم که تعداد آنها n است و هیچکدام اول نیست:

$$(n+1)! + 2 \ , \ (n+1)! + 3 \ , \ \dots \ , \ (n+1)! + (n+1) \ .$$

■

فصل ۳

هم‌نهشتی

هم‌نهشتی یا هم‌باقیمانده بودن نسبت به یک پیمانه، یک رابطه هم‌ارزی بسیار مفید در مجموعه اعداد صحیح است و هدف این فصل معرفی و مطالعه خواص مقدماتی چنین رابطه‌ای می‌باشد.

۱.۳ تعریف— فرض کنیم $0 < m$ یک عدد صحیح باشد. دو عدد صحیح a و b را به پیمانه m هم‌نهشت می‌نامیم هرگاه $m \mid (a-b)$. در این حالت می‌نویسیم $a \equiv b(mod\ m)$. عدد m را پیمانه یا مدول هم‌نهشتی می‌نامیم.

۲.۳ تبصره— داریم $a \equiv b(mod\ m)$ اگر و تنها اگر هنگام تقسیم a بر m و نیز تقسیم b بر m باقیمانده برابر حاصل شود.

۳.۳ گزاره— رابطه هم‌نهشتی به پیمانه m یک رابطه هم‌ارزی روی $\mathbb{Z}$ است. یعنی داریم

الف) $\forall a \ : \ a \equiv a \pmod{m}$,

ب) $\forall a, b \ : \ a \equiv b \pmod{m} \ \Rightarrow \ b \equiv a \pmod{m}$,

ج) $\forall a, b, c \ : \ a \equiv b \pmod{m} \ \& \ b \equiv c \pmod{m} \ \Rightarrow \ a \equiv c \pmod{m}$.

۴.۳ تعریف— فرض کنیم $a \in \mathbb{Z}$. کلاس هم‌ارزی شامل a را نسبت به رابطه هم‌نهشتی به پیمانه m، کلاس مانده‌های شامل a می‌نامیم و آن را با $[a]_m$ نشان می‌دهیم. برخی مواقع که احتمال اشتباه کم باشد از نماد $[a]$ استفاده می‌کنیم. پس داریم

$$[a]_m = \{b \in \mathbb{Z} \ : \ a \equiv b \pmod{m}\}$$

۵.۳ تبصره— می‌دانیم که

$$a \equiv b \pmod{m} \Leftrightarrow \exists q \in \mathbb{Z} \ : \ a - b = mq$$

پس داریم

$$[a]_m = \{a + mq \ : \ q \in \mathbb{Z}\} \ .$$

۶.۳ گزاره— کلاسهای هم‌نهشتی دارای خواص زیر می‌باشند:

الف) هر کلاس هم‌نهشتی ناتهی است.

ب) $[a]_m \cap [b]_m \neq \emptyset$ اگر و تنها اگر $a \equiv b \pmod m$.

ج) $[a]_m = [b]_m$ اگر و تنها اگر $a \equiv b \pmod m$.

د) کلاسهای هم‌نهشتی به پیمانه m مجموعه $\mathbb{Z}$ را افراز می‌کنند.

ه) فقط m کلاس هم‌نهشتی به پیمانه m وجود دارند که عبارتند از

$$[0]_m, [1]_m, \ldots, [m-1]_m$$

اثبات— تمام خواص بالا بلافاصله از این واقعیت که هم‌نهشتی یک رابطه هم‌ارزی است نتیجه می‌شوند. فقط برای اثبات (ه) توجه می‌کنیم که هنگام تقسیم عدد صحیح a بر m تنها یکی از اعداد زیر به عنوان باقیمانده ظاهر می‌شود

$$0, 1, 2, \ldots, m-1$$

پس هر عدد صحیح مانند a با یکی از اعداد فوق به پیمانه m هم‌نهشت است، یعنی

$$\forall a \;\; \exists b \;:\; 0 \leq b \leq m-1 \;\; \& \;\; [a]_m = [b]_m$$

ضمنا توجه کنید که هیچکدام از اعداد لیست بالا با عنصر دیگری از همین لیست به پیمانه m هم‌نهشت نیست.

■

۷.۳ تعریف— مجموعه کلاسهای هم‌نهشتی به پیمانه m را با نماد $\mathbb{Z}_m$ نشان می‌دهیم. پس

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} .$$

۸.۳ گزاره— هم‌نهشتی به پیمانه m دارای خواص جبری زیر است:

الف) اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$ آنگاه

$$\forall x, y \ : \ ax + cy \equiv bx + dy \pmod m .$$

ب) اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$ آنگاه

$$ac \equiv bd \pmod m .$$

۹.۳ تبصره— طبق گزاره فوق طرفین دو هم‌نهشتی به پیمانه m را می‌توان با هم جمع و یا بهم ضرب کرد. به (از) طرفین یک هم‌نهشتی به پیمانه m می‌توان مقدار ثابتی را اضافه (کم) کرد.

طرفین یک هم‌نهشتی را می‌توان به هر مقدار ثابتی ضرب کرد. با این وجود همواره نمی‌توان طرفین یک هم‌نهشتی را به مقدار ثابتی (حتی غیرصفر) تقسیم کرد.

۱۰.۳ قضیه — اگر $ax \equiv ay \pmod{m}$ آنگاه

$$x \equiv y \pmod{\frac{m}{(a,m)}}$$

بخصوص اگر $(a,m)=1$ آنگاه $x \equiv y \pmod{m}$.

اثبات— فرض کنیم $ax \equiv ay \pmod{m}$. پس

$$\exists q \quad : \quad ax - ay = mq$$

در نتیجه

$$\frac{a}{(a,m)}(x-y) = \frac{m}{(a,m)}q \ .$$

پس داریم

$$\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x-y)$$

اما می‌دانیم که $(\frac{m}{(a,m)}, \frac{a}{(a,m)}) = 1$. پس باید داشته باشیم

$$\frac{m}{(a,m)} \mid (x-y)$$

و این اثبات را کامل می‌کند.

■

۱۱.۳ قضیه— فرض کنیم $m_r, \ldots, m_1$ اعداد صحیح مثبت باشند. فرض کنیم

$$\forall i \ : \quad x \equiv y \pmod{m_i}$$

آنگاه

$$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]} .$$

عکس این هم درست است.

اثبات— فرض کنیم

$$\forall i \ : \quad x \equiv y \pmod{m_i}$$

پس

$$m_1, m_2, \ldots, m_r \mid (x - y)$$

یعنی $x - y$ یک مضرب مشترک m_i ها است. پس

$$[m_1, m_2, \ldots, m_r] \mid (x - y) ,$$

در نتیجه

$$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]} .$$

برای اثبات عکس این گزاره کافی است به رابطه زیر توجه کنیم:

$$\forall i \ : \ m_i \mid [m_1, m_2, \ldots, m_r] .$$

■

۱۲.۳ **تعریف**— مجموعه‌ای از اعداد صحیح مانند

$$x_1, x_2, \ldots, x_m$$

را به پیمانه m کامل می‌نامیم هرگاه

$$\forall a \in \mathbb{Z} \ \ \exists i \ : \ a \equiv x_i \pmod{m} .$$

مثلا مجموعه

$$0, 1, 2, \ldots, m-1$$

کامل است.

۱۳.۳ تبصره— برای بدست آوردن یک مجموعه کامل به پیمانه m لازم و کافی است از هر کدام از کلاسهای هم‌نهشتی

$$[0]_m, [1]_m, \ldots, [m-1]_m$$

یک عضو انتخاب کنیم.

۱۴.۳ گزاره— اگر $x \equiv y \pmod m$ آنگاه

$$(x, m) = (y, m) .$$

اثبات— چون $m \mid (x-y)$ پس $\exists q \ : \ x - y = mq .$

حال داریم $(x, m) \mid x - mq = y$

پس $(x, m) \mid (y, m)$. به طریق مشابه داریم

$$(y, m) \mid (x, m) .$$

■

۱۵.۳ تعریف— یک مجموعه کامل تحویل یافته به پیمانه m عبارت است از مجموعه‌ای از اعداد صحیح مانند

$$x_1, x_2, \ldots, x_r$$

بطوریکه:

الف) هر x_i نسبت به m اول باشد.

ب) اگر $i \neq j$ آنگاه $x_i \not\equiv x_j \pmod m$.

ج) اگر $(a, m) = 1$ آنگاه

$$\exists i \ : \ a \equiv x_i \pmod m$$

۱۶.۳ تبصره— برای بدست آوردن یک مجموعه کامل تحویل یافته به پیمانه m کافی است از هر کدام از کلاسهای

$$[0]_m, [1]_m, \ldots, [m-1]_m$$

که نماینده آنها نسبت به m اول باشد یک عضو انتخاب می‌کنیم. هر مجموعه کامل تحویل یافته به این طریق حاصل می‌شود.

۱۷.۳ گزاره— فرض کنیم

$$x_1, x_2, \ldots, x_r$$

یک مجموعه کامل تحویل یافته به پیمانه m باشد. فرض کنیم $(a, m) = 1$. آنگاه

$$ax_1, ax_2, \ldots, ax_r$$

نیز یک مجموعه کامل تحویل یافته به پیمانه m است.

اثبات— باید سه شرط تعریف ۱۵.۳ را بررسی کنیم.

الف)چون $(x_i, m) = (a, m) = 1$ پس

$$\forall i \ : \ (ax_i, m) = 1 \ .$$

ب) فرض کنیم

$$ax_i \equiv ax_j \pmod{m} \ .$$

چون $(a, m) = 1$ پس طبق ۱۰.۳ داریم

$$x_i \equiv x_j \pmod{m} \ .$$

و این بنا به تعریف ۱۵.۳ نتیجه می‌دهد $i = j$.

ج) چون $(ax_j, m) = 1$ پس داریم

$$\forall i \ \ \exists i \ : \ ax_j \equiv x_i \pmod{m}$$

چون تعداد ax_j ها با تعداد x_i ها برابر است پس داریم

$$\forall i \ \ \exists j \ : \ ax_j \equiv x_i \pmod{m}$$

این یعنی هر عدد صحیح که نسبت به m اول باشد با یکی از ax_j ها به پیمانه m هم‌نهشت است.

■

۱۸.۳ تعریف— فرض کنید m یک عدد صحیح مثبت باشد. تعریف می‌کنیم

$$\varphi(m) = |\{a \in \mathbb{Z} \ : \ 1 \leq a \leq m \ , \ (a,m) = 1\}|$$

بعبارت دیگر $\varphi(m)$ تعداد عناصر متباین با m از مجموعه

$$1, 2, \ldots, m$$

است. $\varphi(m)$ را تابع اویلر می‌نامند. بدیهی است که اگر $m = p$ یک عدد اول باشد آنگاه $\varphi(p) = p - 1$.

۱۹.۳ قضیه (اویلر)— فرض کنیم $(a,m) = 1$. آنگاه

$$a^{\varphi(m)} \equiv 1 \pmod{m} \ .$$

اثبات— فرض کنیم

$$x_1, x_2, \ldots, x_r \ ; \ (r = \varphi(m))$$

مجموعه تمام آن عناصر از مجموعه

$$1, 2, \ldots, m$$

باشد که هر x_i نسبت به m اول است. پس x_i ها یک مجموعه کامل تحویل یافته به پیمانه m تشکیل می‌دهند. حال طبق ۱۷.۳ مجموعه

$$ax_1, ax_2, \ldots, ax_r$$

هم کامل تحویل یافته است. پس داریم

$$\forall i \ \ \exists j \ : \ x_i \equiv ax_j \pmod{m} ,$$

$$\forall j \ \ \exists i \ : \ x_i \equiv ax_j \pmod{m} .$$

با ضرب کردن طرفین هم‌نهشتی‌های بالا خواهیم داشت

$$(ax_1)(ax_2)\ldots(ax_r) \equiv x_1x_2\ldots x_r \pmod{m} ,$$

یعنی

$$a^r(x_1x_2\ldots x_r) \equiv (x_1x_2\ldots x_r) \pmod{m} .$$

اما چون $(x_1x_2\dots x_r, m) = 1$، پس

$$a^r \equiv 1 \pmod{m} .$$

پس

$$a^{\varphi(m)} \equiv 1 \pmod{m} .$$

■

۲۰.۳ قضیه (فرما)— اگر p یک عدد اول باشد و $p \nmid a$ آنگاه $a^{p-1} \equiv 1 \pmod{p}$.

اثبات— کافی است در قضیه اویلر قرار دهیم $m = p$.

■

۲۱.۳ تبصره— می‌توان قضیه فرما را بصورت زیر هم نوشت:

$$\forall a \in \mathbb{Z} \ : \ a^p \equiv a \pmod{p} .$$

۲۲.۳ گزاره— فرض کنیم $(a,m)=1$. آنگاه معادله

$$ax \equiv b \pmod{m}$$

دارای جواب است. اگر x_0 یکی از جوابها باشد سایر جوابها عبارتند از

$$x_0 + mq \;\; ; \;\; q \in \mathbb{Z}$$

اثبات— می‌دانیم که $\varphi(m) \geq 1$. قرار می‌دهیم

$$x_0 = a^{\varphi(m)-1}b$$

داریم

$$\begin{aligned} ax_0 &= a^{\varphi(m)}b \\ &\equiv b \pmod{m}\ . \end{aligned}$$

پس معادله جواب دارد و x_0 یک جواب آن است. فرض کنیم x یک جواب دیگر باشد. پس

$$ax - ax_0 \equiv b - b \pmod{m}$$

بنابراین $m \mid (x - x_0)$ و حکم حاصل می‌شود.

■

۲۳.۳ تبصره— اگر $(a, m) = 1$ آنگاه معادله

$$ax \equiv 1 \pmod{m}$$

یک جواب منحصر به فرد در فاصله 1 تا $m - 1$ دارد. چون فقط و فقط یک q وجود دارد که

$$1 \leq x_0 + mq < m$$

۲۴.۳ تبصره— اگر p یک عدد اول باشد و $x^2 \equiv 1 \pmod{p}$ آنگاه

$$x \equiv 1 \text{ یا } p - 1 \pmod{p}$$

برای اثبات این ادعا فرض کنیم $0 \leq x \leq p - 1$. داریم

$$p \mid x^2 - 1 = (x - 1)(x + 1)$$

پس داریم

$$p \mid (x-1) \text{ یا } p \mid (x+1)$$

اگر $p \mid (x-1)$ آنگاه $x = np+1$ بازای برخی n. پس $n = 0$ و در نتیجه $x = 1$. حال اگر $p \mid (x+1)$ آنگاه $x = np-1$ بازای برخی n. پس $n = 1$ و $x = p-1$.

۲۵.۳ قضیه (ویلسون)— فرض کنیم p یک عدد اول باشد. آنگاه

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

اثبات— بازای هر $2 \leq a \leq p-2$ یک $2 \leq b \leq p-2$ وجود دارد که $a \neq b$ و داریم

$$ab \equiv 1 \pmod{m} ,$$

ضمنا b با این خاصیت منحصر بفرد است. پس داریم

$$\begin{aligned} 1 \times 2 \times \ldots \times (p-2) \times (p-1) &\equiv 1 \times (p-1) \pmod{p} \\ &\equiv -1 \pmod{p} . \end{aligned}$$

■

۲۶.۳ قضیه— فرض کنید p یک عدد اول باشد. معادله

$$x^2 \equiv -1 \pmod{p}$$

دارای جواب است اگر و تنها اگر $p = 2$ یا $p \equiv 1 \pmod{4}$.

اثبات— فرض کنیم $p = 2$. آنگاه $x = 1$ جواب معادله است. حال فرض کنیم $p \neq 2$ اما $p \equiv 1 \pmod{4}$. این یعنی p فرد است ولی $\frac{p-1}{2}$ زوج می‌باشد. طبق قضیه ویلسون داریم

$$(1 \times 2 \times \ldots \times \frac{p-1}{2})(\frac{p+1}{2} \times \ldots \times (p-2) \times (p-1)) \equiv -1 \pmod{p}$$

بعبارت فشرده‌تر

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \pmod{p} .$$

اما می‌دانیم که

$$j(p-j) \equiv -j^2 \pmod{p} ,$$

پس داریم

$$-1 \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \pmod{p}$$

$$= (-1)^{p-1/2} \prod_{j=1}^{(p-1)/2} j^2 \pmod p$$
$$\equiv (\prod_{j=1}^{(p-1)/2} j)^2 \pmod p$$

پس در واقع

$$x = \prod_{j=1}^{(p-1)/2} j$$

یک جواب معادله است.

حال فرض کنیم $p \neq 2$ و $p \not\equiv 1 \pmod 4$. آنگاه

$$p \equiv 3 \pmod 4 .$$

چون اگر $p \equiv 2 \pmod 4$ آنگاه p باید زوج باشد. فرض کنیم معادله $x^2 \equiv -1 \pmod p$ دارای جواب باشد. داریم

$$x^{p-1} = (x^2)^{p-1/2}$$
$$\equiv (-1)^{p-1/2} \pmod p$$
$$\equiv -1 \pmod p .$$

از طرف دیگر طبق قضیه فرما $x^{p-1} \equiv 1 \pmod p$. پس $1 \equiv -1 \pmod p$. یعنی $p = 2$ که تناقض است.

■

در پایان این فصل، معادلات هم‌نهشتی خطی را بطور مختصر مورد بررسی قرار می‌دهیم.

۲۷.۳ گزاره— فرض کنیم $d = (a, m)$. اگر $d \nmid b$ آنگاه معادله $ax \equiv b \pmod m$ جواب ندارد.

اثبات— فرض کنیم چنین نباشد و u را یک جواب معادله فوق فرض می‌کنیم. چون $d \mid m$ پس داریم

$$au \equiv b \pmod d .$$

اما $d \mid a$. پس $b \equiv 0 \pmod d$. این یعنی $d \mid b$ که با فرض در تناقض است.

■

۲۸.۳ قضیه— فرض کنیم $d = (a, m)$ و $d \mid b$. فرض کنیم u یک جواب معادله $\frac{a}{d}\, x \equiv 1 \pmod{\frac{m}{d}}$ باشد.

آنگاه جوابهای معادله $ax \equiv b \pmod{m}$ تماما به فرم

$$x \equiv \frac{b}{d}u + q\frac{m}{d} \pmod{m}$$

می‌باشند که در آن $0 \leq q \leq d-1$.

اثبات— در معادله هم‌نهشتی

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

داریم $(\frac{a}{d}, \frac{m}{d}) = 1$. پس این معادله جواب منحصر به فردی مانند $x \equiv x_1 \pmod{\frac{m}{d}}$ دارد. در نتیجه جوابهای معادله $ax \equiv b \pmod{m}$ تماما به شکل

$$x \equiv x_1 + q\frac{m}{d} \pmod{m}$$

می‌باشند که در آن $0 \leq q \leq d-1$. حال اگر فرض کنیم u جواب $\frac{a}{d}x \equiv 1 \pmod{\frac{m}{d}}$ باشد آنگاه خواهیم داشت

$$x_1 = \frac{b}{d}u$$

و اثبات تکمیل می‌شود.

■

۲۹.۳ قضیه (باقیمانده‌های چینی) — فرض کنیم

$$m_1, m_2, \ldots, m_r$$

اعداد صحیح مثبت دوبدو متباین باشند. فرض کنیم

$$a_1, a_2, \ldots, a_r$$

اعداد صحیح دلخواه باشند. آنگاه دستگاه هم‌نهشتی

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

دارای جواب است.

اثبات— قرار می‌دهیم $m = m_1 m_2 \dots m_r$. بازای هر $1 \leq j \leq r$ داریم

$$(\frac{m}{m_j}, m_j) = 1$$

پس عدد صحیح b_j وجود دارد که

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$$

ضمنا اگر $i \neq j$ آنگاه چون $m_i \mid \frac{m}{m_j}$، پس

$$\frac{m}{m_j} b_j \equiv 0 \pmod{m_i} .$$

حال تعریف می‌کنیم

$$x = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$$

داریم

$$\begin{aligned} x &\equiv \frac{m}{m_i} b_i a_i \pmod{m_i} \\ &\equiv a_i \pmod{m_i} . \end{aligned}$$

■

۳۰.۳ مساله— عدد صحیحی مانند x بیابید که

الف) اگر x بر 5 تقسیم شود باقیمانده 4 شود.

ب) اگر x بر 7 تقسیم شود باقیمانده 1 شود.

ج) اگر x بر 11 تقسیم شود باقیمانده 3 شود.

فصل ۴

توابع حسابی

در این فصل با چند تابع حسابی مهم آشنا خواهیم شد. هر تابع مانند $f : \mathbb{Z} \to \mathbb{C}$ یک تابع حسابی نامیده می‌شود. ممکن است دامنه f کل $\mathbb{Z}$ نباشد. اولین نمونه از توابع حسابی مهم تابع اویلر است که پیش از این در فصل ۳ معرفی شد. اما بعنوان یادآوری بار دیگر آنرا تعریف می‌کنیم.

۱.۴ تعریف — بازای هر عدد طبیعی $n > 1$، تعداد اعداد صحیح مثبت کمتر از n که نسبت به آن اول می‌باشند با نماد $\varphi(n)$ نشان داده می‌شود. ضمنا تعریف می‌کنیم $\varphi(1) = 1$.

در جدول زیر برخی مقادیر $\varphi(n)$ ارائه شده است:

n	1	2	3	4	10	16	20	23	48
$\varphi(n)$	1	1	2	2	4	8	8	22	16

۲.۴ تبصره— توجه کنید که اگر p یک عدد اول باشد آنگاه

$$\varphi(p) = p - 1 \ .$$

۳.۴ گزاره— فرض کنیم p یک عدد اول باشد و $1 \leq \alpha$. آنگاه $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

اثبات— از میان اعداد

$$1, 2, 3, \ldots, p^\alpha$$

آنهایی نسبت به p متباین نیستند که مضرب p باشند، یعنی به شکل kp که در آن $1 \leq k \leq p^{\alpha-1}$. پس تعداد عناصر متباین با p در فهرست بالا $p^\alpha - p^{\alpha-1}$ می‌باشد.

■

۴.۴ تعریف— تابع حسابی f را ضربی می‌نامیم هرگاه $(m, n) = 1$ ایجاب کند $f(mn) = f(m)f(n)$. تابع f را کاملا ضربی می‌نامیم هرگاه بازای هر m و n داشته باشیم

$$f(mn) = f(m)f(n)$$

۵.۴ قضیه— تابع φ ضربی است.

اثبات— فرض کنیم $(m,n)=1$. مجموعه اعداد از 1 تا mn را در جدول زیر مرتب می‌کنیم

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
r & m+r & 2m+r & \dots & (n-1)m+r \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
m & 2m & 3m & \dots & mn
\end{array}$$

فرض کنیم $1 \le r \le m$ و $(m,r)=d>1$. آنگاهd تمام عناصر واقع در سطر r—ام را عاد می‌کند. پس هیچکدام از عناصر این سطر نسبت به mn متباین نیستند. پس برای بدست آوردن اعداد متباین باmn در جدول فوق، باید به سطرهایی توجه کنیم که در آن $(m,r)=1$. بدیهی است که تعداد این سطرها $\varphi(m)$ تا است. فرض کنیم در حال بررسی چنین سطری هستیم. هر عضو این سطر به شکل $km+r$ است که $0 \le k \le n-1$. پس

$$(km+r,m)=(r,m)=1$$

یعنی تمام اعضای این سطر نسبت به m اولند. یعنی $km+r$ نسبت به mn اول است اگر و تنها اگر نسبت به n اول باشد. اما اعداد

$$r, m+r, 2m+r, \ldots, (n-1)m+r$$

بوضوح یک مجموعه کامل مانده به پیمانه n تشکیل می‌دهند. پس از میان این اعداد دقیقا $\varphi(n)$ تا نسبت به n (و در نتیجه نسبت به mn) اولند. حال داریم

$$\varphi(mn) = \varphi(m)\varphi(n)$$

■

۶.۴ نتیجه— فرض کنیم $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ تجزیه به عوامل اول عدد n باشد. آنگاه

$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

اثبات—

$$\begin{aligned} \varphi(n) &= \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_{i-1}}) \\ &= \prod_{i=1}^{r} p_i^{\alpha_i} (1 - \frac{1}{p_i}) \end{aligned}$$

$$= n\prod_{i=1}^{r}(1-\frac{1}{p_i})\ .$$

■

۷.۴ تعریف— فرض کنیم $0 \leq k$. تابع حسابی σ_k را چنین تعریف می‌کنیم

$$\sigma_k(n) = \sum_{d|n} d^k$$

معمولا σ_0 را با نماد τ نشان می‌دهیم. در واقع $\tau(n)$ نشان‌دهنده تعداد شمارنده‌های مثبت n است. همچنین σ_1 را با نماد σ نشان می‌دهیم. در این حالت $\sigma(n)$ مساوی مجموع شمارنده‌های مثبت n است.

۸.۴ گزاره— اگر $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ آنگاه

$$\tau(n) = \prod_{i=1}^{r}(\alpha_i+1)\ .$$

اثبات— فرض کنیم $d \mid n$. پس می‌توان نوشت

$$d = p_1^{\beta_1}p_2^{\beta_2}\dots p_r^{\beta_r}$$

که در آن بازای هر i داریم $0 \leq \beta_i \leq \alpha_i$. پس برای هر β_i تعداد $\alpha_i + 1$ حالت امکان دارد. این نشان می‌دهد که تعداد d ها مساوی

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$$

است.

■

۹.۴ قضیه— فرض کنیم f یک تابع ضربی باشد. تعریف می‌کنیم

$$F(n) = \sum_{d|n} f(d) \ .$$

آنگاه F نیز ضربی است.

اثبات— فرض کنیم $(m, n) = 1$ و

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad , \quad n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

تجزیه به عوامل اول m و n باشد. اگر $d \mid mn$ آنگاه

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} q_1^{\delta_1} q_2^{\delta_2} \dots q_s^{\delta_s}$$

که در آن بازای هر i داریم

$$0 \leq \gamma_i \leq \alpha_i \quad , \quad 0 \leq \delta_i \leq \beta_i$$

فرض کنیم

$$d_1 = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} \quad , \quad d_2 = q_1^{\delta_1} q_2^{\delta_2} \dots q_s^{\delta_s}$$

پس $d = d_1 d_2$ و $d_1 \mid m$ و $d_2 \mid n$. ضمنا تناظر

$$d \mapsto (d_1, d_2)$$

یک به یک است. علاوه بر این $(d_1, d_2) = 1$. حال داریم

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) \\ &= \sum_{d_1 \mid m, d_2 \mid n} f(d_1 d_2) \\ &= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) f(d_2) \\ &= (\sum_{d_1 \mid m} f(d_1))(\sum_{d_2 \mid n} f(d_2)) \\ &= F(m) F(n) \end{aligned}$$

■

۱۰.۴ نتیجه — بازای هر k تابع σ_k ضربی است. بخصوص τ و σ ضربی است.

اثبات— فرض کنیم $f(n) = n^k$. بدیهی است که f ضربی است. حال چون

$$\sigma_k(n) = \sum_{d|n} f(d)$$

پس σ_k ضربی است.

■

۱۱.۴ گزاره— فرض کنیم p یک عدد اول باشد و $1 \leq \alpha$. آنگاه

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}$$

اثبات— شمارنده‌های p^α عبارتند از

$$1, p, p^2, \ldots, p^\alpha$$

پس داریم

$$\begin{aligned} \sigma(p^\alpha) &= 1 + p + p^2 + p^3 + \ldots + p^\alpha \\ &= \frac{p^{\alpha+1} - 1}{p - 1} \ . \end{aligned}$$

■

۱۲.۴ نتیجه— فرض کنیم $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ تجزیه به عوامل اول n باشد. آنگاه

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} .$$

۱۳.۴ تعریف— عدد صحیح مثبت n را فارغ از مربع می‌نامند هرگاه $1 < n$ و n بر مربع هیچ عدد صحیح بزرگتر از یک بخش‌پذیر نباشد. در این حالت عاملهای اول n متمایزند. این تعداد را با نماد p_n نشان می‌دهیم.

۱۴.۴ تعریف— تابع موبیوس را به صورت زیر تعریف می‌کنیم:

الف) $\mu(1) = 1$

ب) $\mu(n) = 0$ اگر n فارغ از مربع نباشد

ج) $\mu(n) = (-1)^{p_n}$ اگر n فارغ از مربع باشد

۱۵.۴ گزاره— تابع موبیوس ضربی است.

اثبات— فرض کنیم $(m,n)=1$. اگر m و n فارغ از مربع باشند آنگاه mn نیز چنین است و ضمنا داریم

$$p_{mn}=p_m+p_n\ ,$$

پس $\mu(mn)=\mu(m)\mu(n)$. اگر یکی از اعداد m یا n فارغ از مربع نباشد mn نیز چنین است پس

$$0=\mu(mn)=\mu(m)\mu(n)=0\ .$$

■

۱۶.۴ گزاره— اگر $n>1$ آنگاه

$$\sum_{d|n}\mu(d)=0\ .$$

اثبات— فرض کنیم

$$F(n)=\sum_{d|n}\mu(d)$$

پس F یک تابع ضربی است. فرض کنیم p یک عدد اول باشد و $\alpha\geq 1$. آنگاه

$$\begin{aligned} F(p^\alpha) &= \sum_{d|p^\alpha} \mu(d) \\ &= \sum_{k=0}^{\alpha} \mu(p^k) \\ &= 1 + (-1) + 0 + \ldots + 0 \\ &= 0 \end{aligned}$$

پس اگر $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ آنگاه

$$\begin{aligned} F(n) &= \prod_{i=1}^{r} F(p_i^{\alpha_i}) \\ &= 0 \end{aligned}$$

■

۱۷.۴ قضیه (عکس موبیوس) — فرض کنید $F(n) = \sum_{d|n} f(d)$. آنگاه

$$f(n) = \sum_{d|n} \mu(d) F(n/d)$$

اثبات — داریم

$$\begin{aligned}\sum_{d|n}\mu(d)F(\frac{n}{d}) &= \sum_{d|n}\mu(d)\sum_{d'|\frac{n}{d}}f(d')\\ &= \sum_{d'|n}\sum_{d|\frac{n}{d'}}\mu(d)f(d')\\ &= \sum_{d'|n}f(d')\sum_{d|\frac{n}{d'}}\mu(d)\\ &= f(n)\ .\end{aligned}$$

■

۱۸.۴ نتیجه— اگر $f(n)=\sum_{d|n}\mu(d)F(n/d)$ آنگاه $F(n)=\sum_{d|n}f(d)$.

اثبات— داریم

$$\begin{aligned}\sum_{d|n}f(d) &= \sum_{d|n}\sum_{d'|d}\mu(d')F(\frac{d}{d'})\\ &= \sum_{d|n}\sum_{d''|d}\mu(\frac{d}{d''})F(d'')\\ &= \sum_{d''|n}\sum_{d''q|n}\mu(\frac{d''q}{d''})F(d'')\\ &= \sum_{d''|n}F(d'')\sum_{q|\frac{n}{d''}}\mu(q)\\ &= F(n)\ .\end{aligned}$$

■

در پایان این بخش به بیان یکی از کاربردهای قضیه عکس موبیوس می‌پردازیم. برای این منظور لازم است نخست قضیه زیر را که منتسب به گاوس است ثابت می‌کنیم.

۱۹.۴ قضیه— داریم $\sum_{d|n} \varphi(d) = n$.

اثبات— فرض کنیم

$$X = \{1, 2, \ldots, n\}$$

اگر $d \mid n$ آنگاه مجموعه X_d را چنین تعریف می‌کنیم

$$X_d = \{a \in X \ : \ (a, n) = d\}$$

بدیهی است که X به اجتماع X_d ها افراز می‌شود. حال $a \in X_d$ اگر و تنها اگر $a = dq$ که در آن $1 \leq q \leq \frac{n}{d}$ و $(q, \frac{n}{d}) = 1$. پس $|X_d| = \varphi(\frac{n}{d})$. بنابراین

$$\begin{aligned} n &= |X| = \sum_{d|n} |X_d| \\ &= \sum_{d|n} \varphi(\frac{n}{d}) \\ &= \sum_{d|n} \varphi(d) \ . \end{aligned}$$

■

۲۰.۴ نتیجه — داریم

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} .$$

اثبات — کافی است قضیه بالا را به همراه قضیه عکس موبیوس بکار ببریم.

■

فصل ۵

تقابل درجه دوم

در این فصل اعداد صحیحی را مطالعه می‌کنیم که به پیمانه عدد اول فرد p مربع کامل می‌باشند.

۱.۵ تعریف— فرض کنیم p یک عدد اول فرد باشد و $p \nmid a$. اگر معادله همنهشتی $x^2 \equiv a \pmod{p}$ دارای جواب باشد آنگاه a را یک مانده درجه دوم به پیمانه p می‌نامیم. اگر چنین نباشد a را نامانده درجه دوم می‌گوییم.

۲.۵ گزاره— فرض کنیم p یک عدد اول فرد باشد و $p \nmid a$. آنگاه معادله $x^2 \equiv a \pmod{p}$ یا جواب ندارد و یا دارای دقیقاً دو جواب به پیمانه p است.

اثبات— فرض کنیم x_0 یک جواب این معادله باشد. چون p فرد است پس $x_0 \not\equiv -x_0 \pmod p$، اما بدیهی است که $-x_0$ هم یک جواب این معادله است. حال نشان می‌دهیم این معادله جواب دیگری ندارد. اگر

$$x_1^2 \equiv a \pmod p$$

آنگاه خواهیم داشت

$$x_1^2 \equiv x_0^2 \pmod p$$

پس $p \mid (x_1^2 - x_0^2)$ در نتیجه $p \mid (x_1 - x_0)(x_1 + x_0)$. چون p اول است پس خواهیم داشت

$$x_1 \equiv x_0 \pmod p \quad \text{یا} \quad x_1 \equiv -x_0 \pmod p$$

پس معادله مذکور دقیقا دو جواب به پیمانه p دارد.

■

۳.۵ نتیجه— در مجموعه $\mathbb{Z}_p$ دقیقا $\frac{p-1}{2}$ مانده درجه دوم موجود است به شرطی که p فرد باشد.

۴.۵ تعریف— فرض کنیم p یک عدد اول فرد باشد و $p \nmid a$. نماد لژاندر $(\frac{a}{p})$ را چنین تعریف می‌کنیم

$$(\frac{a}{p}) = \begin{cases} +1 & : \text{اگر } a \text{ یک مانده درجه دوم به پیمانه } p \text{ باشد} \\ -1 & : \text{در غیر اینصورت} \end{cases}$$

۵.۵ گزاره— نماد لژاندر دارای خواص زیر است

الف) اگر $a \equiv b \pmod p$ آنگاه $(\frac{a}{p}) = (\frac{b}{p})$.

ب) $(\frac{a^2}{p}) = +1$.

ج) $(\frac{1}{p}) = +1$.

اثبات— اگر $a \equiv b \pmod p$ آنگاه دو معادله

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

$$x^2 \equiv b \pmod p$$

معنی یکسانی دارند. پس $(\frac{b}{p}) = (\frac{a}{p})$. ضمنا چون a^2 همواره مربع کامل است پس $(\frac{a^2}{p}) = +1$.

بخش (ج) نتیجه‌ای از حالت اخیر است.

■

۶.۵ قضیه (اویلر)— فرض کنیم p یک عدد اول فرد باشد و $p \nmid a$. آنگاه

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

اثبات— اول فرض کنیم $(\frac{a}{p}) = 1$. پس معادله

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

دارای جواب می‌باشد. پس داریم

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (x^2)^{\frac{p-1}{2}} \\ &\equiv x^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p} . \end{aligned}$$

حال فرض کنیم $(\frac{a}{p}) = -1$. پس معادله

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

جواب ندارد. پس

$$\forall i \ \exists j \ : \ i \neq j \ \ \& \ \ ij \equiv a \pmod{p}$$

حال داریم

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

اما طبق قضیه ویلسون $(p-1)! \equiv -1 \pmod{p}$ و این اثبات را تکمیل می‌کند.

■

۷.۵ نتیجه — داریم

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

اثبات— طبق قضیه بالا داریم

$$\begin{aligned}(\frac{a}{p})(\frac{b}{p}) &\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p} \\ &\equiv (ab)^{\frac{p-1}{2}} \pmod{p} \\ &\equiv (\frac{ab}{p}) \pmod{p} .\end{aligned}$$

چون p فرد است نتیجه می‌گیریم که هم‌نهشتی فوق یک تساوی است یعنی

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

■

۸.۵ نتیجه— فرض کنیم p یک عدد اول فرد باشد. آنگاه

$$(\frac{-1}{p}) = \begin{cases} 1 & : \quad p \equiv 1 \pmod 4 \\ -1 & : \quad p \equiv 3 \pmod 4 \end{cases}$$

توضیح— نتیجه فوق شرط لازم و کافی برای جواب داشتن **معادله** $x^2 \equiv -1 \pmod p$ را بیان می‌کند.

اثبات— می‌دانیم که

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

حال اگر $p \equiv 1 \pmod 4$ آنگاه $\frac{p-1}{2}$ زوج است. پس

$$(\frac{-1}{p}) = 1$$

اما اگر $p \equiv 3 \pmod 4$ آنگاه $\frac{p-1}{2}$ فرد است و در نتیجه $(\frac{-1}{p}) = -1$.

■

۹.۵ قضیه (لم گاوس)— فرض کنیم p یک عدد اول فرد باشد و $p \nmid a$. اعداد

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

را به پیمانه p تبدیل کرده و فرض می‌کنیم s تعداد جوابهای بزرگتر از $p/2$ باشد. آنگاه

$$(\frac{a}{p}) = (-1)^s \ .$$

اثبات— فرض کنیم بعد از تبدیل اعداد داده شده به پیمانه p به اعداد

$$u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$$

برسیم که در آن

$$\forall i \ : \ u_i > p/2$$

$$\forall i \ : \ v_i < p/2$$

در نتیجه تمام اعداد

$$p - u_1, \ldots, p - u_s, v_1, \ldots, v_t$$

در فاصله 1 تا $\frac{p-1}{2}$ واقع می‌باشند. براحتی دیده می‌شود که هیچ زوجی از عناصر مجموعه اخیر به پیمانه p هم‌نهشت نمی‌باشند. پس این مجموعه در واقع همان مجموعه

$$1, 2, \ldots, \frac{p-1}{2}$$

است. در نتیجه

$$(p - u_1) \ldots (p - u_s) v_1 \ldots v_t \equiv (\frac{p-1}{2})! \pmod p$$

یعنی

$$(-1)^s u_1 u_2 \dots u_s v_1 v_2 \dots v_t \equiv (\frac{p-1}{2})! \pmod{p} .$$

از طرف دیگر می‌دانیم که

$$\begin{aligned} u_1 u_2 \dots u_s v_1 v_2 \dots v_t &\equiv a \cdot 2a \cdot \dots \cdot \frac{p-1}{2} a \pmod{p} \\ &\equiv a^{\frac{p-1}{2}} (\frac{p-1}{2})! \pmod{p} . \end{aligned}$$

پس داریم

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

اما بدیهی است که $p \nmid (\frac{p-1}{2})!$. پس

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

حال با توجه به قضیه ۶.۵ جواب نهایی حاصل می‌شود.

■

در قضیه زیر $[x]$ جزء صحیح عدد حقیقی x را نشان می‌دهد.

۱۰.۵ قضیه — فرض کنیم p یک عدد اول فرد باشد و a عدد فردی باشد که $p \nmid a$. آنگاه

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

که در آن

$$k = \sum_{j=1}^{\frac{(p-1)}{2}} [\frac{ja}{p}]$$

ضمناً

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} .$$

اثبات— ابتدا فرض کنیم a فرد یا زوج باشد و $p \nmid a$. فرض کنیم بعد از تبدیل اعداد

$$a, 2a, \ldots, \frac{p-1}{2}a$$

به پیمانه p جوابهای

$$u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$$

حاصل شوند که در آن v_i ها کمتر و u_i ها بیشتر از $\frac{p}{2}$ می‌باشند. در اثبات قضیه قبل دیدیم که مجموعه

$$p - u_1, \ldots, p - u_s, v_1, \ldots, v_t$$

با مجموعه

$$1, 2, \ldots, \frac{p-1}{2}$$

برابر است. پس داریم:

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = sp - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$$

از طرف دیگر فرض کنیم $1 \leq j \leq \frac{p-1}{2}$. وقتی ja را به پیمانه p تبدیل می‌کنیم در واقع آنرا بر p تقسیم می‌کنیم و بر اثر این عمل یک خارج قسمت بدست می‌آید که همان $[\frac{ja}{p}]$ است. باقیمانده این تقسیم هم یکی از u_i ها یا v_i ها است. پس داریم

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p[\frac{ja}{p}] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$$

با کم کردن طرفین دو رابطه خواهیم داشت

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p(\sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}] - s) + 2\sum_{j=1}^{s} u_j \ .$$

می‌دانیم که $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$. با قرار دادن این مقدار در رابطه فوق و تبدیل به پیمانه 2 خواهیم داشت

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}] - s \pmod 2$$

حال اگر a فرد باشد آنگاه سمت چپ رابطه فوق زوج خواهد شد. پس

$$s \equiv \sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}] \pmod 2$$

و حکم از ۹.۵ حاصل می‌شود. اگر $a = 2$ آنگاه

$$\forall\ 1 \leq j \leq \frac{p-1}{2} \quad : \quad [\frac{ja}{p}] = 0$$

و در نتیجه

$$s \equiv \frac{p^2-1}{8} \pmod 2$$

و باز هم حکم از ۹.۵ حاصل می‌شود.

■

۱۱.۵ نتیجه— فرض کنیم p یک عدد اول فرد باشد. آنگاه 2 یک مانده درجه دوم به پیمانه p است اگر و تنها اگر

$$p \equiv \pm 1 \pmod 8 .$$

حال به مهمترین قضیه این فصل، قضیه تقابل درجه دوم می‌رسیم.

۱۲.۵ قضیه (تقابل درجه دوم)— فرض کنیم p و q دو عدد اول فرد متمایز باشند. آنگاه

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

اثبات– فرض کنید S مجموعه تمام زوجهای صحیح مانند (x,y) باشد که $1 \leq x \leq \frac{p-1}{2}$ و $1 \leq y \leq \frac{q-1}{2}$. بدیهی است که

$$|S| = \frac{p-1}{2} \times \frac{q-1}{2}$$

مجموعه S را به دو زیر مجموعه S_1 و S_2 به شکل زیر افراز می‌کنیم

$$S_1 = \{(x,y) \ : \ qx > py\}$$

$$S_2 = \{(x,y) \ : \ qx < py\}$$

توجه کنید که تساوی $qx = py$ امکان ندارد. حال داریم

$$S_1 = \{(x,y) \ : \ 1 \leq x \leq \frac{p-1}{2}, 1 \leq y < qx/p\}$$

$$S_2 = \{(x,y) \ : \ 1 \leq y \leq \frac{q-1}{2}, 1 \leq x < py/q\}$$

پس داریم

$$|S_1| = \sum_{x=1}^{\frac{p-1}{2}} [\frac{qx}{p}] \ , \ |S_2| = \sum_{y=1}^{\frac{q-1}{2}} [\frac{py}{q}]$$

پس داریم

$$(\frac{p}{q}) = (-1)^{|S_2|} \ , \ (\frac{q}{q}) = (-1)^{|S_1|} \ .$$

پس نتیجه می‌گیریم

$$\begin{aligned} (\frac{p}{q}) &= (-1)^{|S_2|}(-1)^{|S_1|} \\ &= (-1)^{|S_1|+|S_2|} \\ &= (-1)^{|S|} \\ &= (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}} \ . \end{aligned}$$

■

فصل ٦

ریشه‌های اولیه

در فصل سوم دیدیم که اگر $(a, m) = 1$ آنگاه

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

بنابراین مجموعه

$$\{x \in \mathbb{Z}^+ : a^x \equiv 1 \pmod{m}\}$$

ناتهی است.

١.٦ تعریف— کوچکترین عضو مجموعه بالا را مرتبه a به پیمانه m می‌نامیم و با نماد $ord_m(a)$ نشان می‌دهیم. بدیهی است که $ord_m(a) \leq \varphi(m)$.

٢.٦ تعریف— a را یک ریشه اولیه به پیمانه m می‌نامیم هرگاه $(a,m) = 1$ و $ord_m(a) = \varphi(m)$.

٣.٦ تبصره— خواننده آشنا با مفهوم گروه متناهی براحتی تشخیص می‌دهد که یک ریشه اولیه به پیمانه m چیزی جز یک مولد برای گروه $\mathbb{Z}_m^*$ نیست. پس یک ریشه اولیه به پیمانه m وجود دارد اگر و تنها اگر گروه $\mathbb{Z}_m^*$ دوری باشد.

٤.٦ تبصره— هدف این فصل آن است که معین کنیم بازای کدام m ها ریشه اولیه موجود است.

٥.٦ گزاره— فرض کنیم $(a,m) = 1$ و $a^x \equiv 1 \pmod m$. آنگاه

$$ord_m(a) \mid x\ .$$

اثبات— فرض کنیم $n = ord_m(a)$. طبق قضیه تقسیم q و r وجود دارند که

$$x = nq + r$$

و $0 \leq r < n$. اگر $r = 0$ حکم حاصل می‌شود. فرض کنیم $r \neq 0$. داریم

$$\begin{aligned} a^r &= a^r \cdot 1 \\ &\equiv a^r \cdot (a^n)^q \pmod{m} \\ &\equiv a^x \pmod{m} \\ &\equiv 1 \pmod{m} \end{aligned}$$

این با کوچکترین بودن n در تعریف ١.٦ متناقض است.

■

٦.٦ نتیجه— اگر $(a, m) = 1$ آنگاه

$$ord_m(a) \mid \varphi(m) .$$

می‌توان گزاره ٥.٦ را به شکل زیر هم بازنویسی کرد.

٧.٦ گزاره— فرض کنیم $(a, m) = 1$. داریم

$$a^x \equiv a^y \pmod{m}$$

اگر و تنها اگر $x \equiv y \pmod{n}$ که در آن $n = ord_m(a)$.

٨.٦ نتیجه— فرض کنیم a یک ریشه اولیه به پیمانه m باشد. آنگاه مجموعه

$$1, a, a^2, \ldots, a^{\varphi(m)-1}$$

یک مجموعه کامل تحویل یافته به پیمانه m است.

اثبات— بدیهی است که تمام اعداد فوق نسبت به m اولند. نشان می‌دهیم این اعداد دو به دو به پیمانه m متمایزند. فرض کنیم $0 \leq x, y \leq \varphi(m) - 1$ و $a^x \equiv a^y \pmod{m}$ طبق ٧.٦ خواهیم داشت

$$x \equiv y \pmod{n}$$

که در آن $n = ord_m(a) = \varphi(m)$. حال چون $0 \leq x, y \leq n - 1$ نتیجه می‌گیریم که $x = y$.

■

٩.٦ گزاره— فرض کنیم $ord_m(a) = n$. آنگاه

$$ord_m(a^x) = \frac{n}{(n, x)} .$$

اثبات— فرض کنیم $d = (n, x)$. داریم

$$\begin{aligned}(a^x)^{n/d} &= (a^n)^{x/d} \\ &\equiv 1 \pmod{m}\end{aligned}$$

(چون $a^n \equiv 1 \pmod{m}$ طبق تعریف مرتبه). پس مطابق ۵.٦ داریم

$$ord_m(a^x) \mid \frac{n}{d} .$$

از سوی دیگر

$$\begin{aligned}(a^x)^{ord_m(a^x)} &\equiv 1 \pmod{m} \\ &\Rightarrow a^x \cdot ord(a^x) \equiv 1 \pmod{m} \\ &\Rightarrow n \mid x \cdot ord(a^x) \\ &\Rightarrow \frac{n}{d} \mid x \cdot ord(a^x)\end{aligned}$$

و حکم حاصل می‌شود.

■

١٠.٦ نتیجه— فرض کنیم $(n,x)=1$ و $ord_m(a)=n$. آنگاه $ord_m(a^x)=n$.

١١.٦ نتیجه— اگر a یک ریشه اولیه به پیمانه m باشد و $(\varphi(m),x)=1$ آنگاه a^x هم یک ریشه اولیه به پیمانه m است. عکس این هم درست می‌باشد.

اثبات— داریم

$$\begin{aligned} ord_m(a^x) &= \frac{ord_m(a)}{(ord_m(a),x)} \\ &= \frac{\varphi(m)}{(\varphi(m),x)} \\ &= \varphi(m) \end{aligned}$$

و حکم نتیجه می‌شود.

■

١٢.٦ نتیجه— اگر m ریشه اولیه داشته باشد آنگاه دقیقا $\varphi(\varphi(m))$ ریشه اولیه دارد.

١٣.٦ تبصره— برای اینکه مشخص کنیم بازای کدام m ها ریشه اولیه موجود است به چند گزاره ساده در ارتباط با جوابهای معادلات چندجمله‌ای به پیمانه اعداد اول نیاز داریم.

١٤.٦ تعریف— فرض کنیم $f(x)$ یک چندجمله‌ای با ضرایب صحیح باشد. عدد صحیح x_0 را یک ریشه $f(x)$ به پیمانه m می‌نامیم هرگاه $f(x_0) \equiv 0 \pmod m$.

١٥.٦ گزاره (لاگرانژ)— فرض کنیم

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

یک چندجمله‌ای با ضرایب صحیح و p یک عدد اول باشد. فرض کنیم $p \nmid a_n$. آنگاه $f(x)$ حداکثر n ریشه دو به دو غیر هم‌نهشت به پیمانه p دارد.

اثبات— از استقراء روی n استفاده می‌کنیم. اگر $n = 1$ آنگاه به معادله هم‌نهشتی $a_1 x \equiv -a_0 \pmod p$ می‌رسیم و چون $p \nmid a_1$ پس این معادله فقط یک جواب

$$x \equiv a_1^{p-2}(-a_0) \pmod p$$

دارد. فرض کنیم حکم برای $n-1$ درست باشد اما اعداد صحیح

$$c_0, c_1, \ldots, c_n$$

موجود باشند که دو به دو به پیمانه p غیر هم‌نهشت‌اند و

$$\forall i \ : \ f(c_i) \equiv 0 \pmod{p}$$

داریم:

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \ldots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \ldots + c_0^{n-1}) \\ &+ a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \ldots + c_0^{n-2}) \\ &+ \ldots + a_1(x - c_0) \\ &= (x - c_0)g(x) \end{aligned}$$

که در آن

$$g(x) = a_n x^{n-1} + \ldots + (a_n c_0^{n-1} + \ldots + a_1)$$

چون $p \nmid a_n$ پس طبق فرض استقراء $g(x)$ حداکثر $n-1$ جواب دو به دو غیرهم‌نهشت به پیمانه p دارد. اما بازای هر $1 \leq i \leq n$ داریم

$$\begin{aligned} g(c_i)(c_i - c_0) &= f(c_i) - f(c_0) \\ &\equiv 0 \pmod{p} \end{aligned}$$

است و این امکان ندارد.

■

۱٦.٦ نتیجه— فرض کنیم p یک عدد اول باشد و $d \mid p-1$. آنگاه چندجمله‌ای $x^d - 1$ دقیقا d جواب دو به دو غیرهم‌نهشت به پیمانه p دارد.

اثبات— فرض کنیم $p - 1 = dq$. پس داریم

$$\begin{aligned} x^{p-1} - 1 &= (x^d - 1)(x^{d(q-1)} + \ldots + x^d + 1) \\ &= (x^d - 1)f(x) \end{aligned}$$

طبق قضیه کوچک فرما معادله

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

دقیقا $p-1$ جواب دو به دو غیرهم‌نهشت دارد. از طرفی تعداد جوابهای دو به دو غیرهم‌نهشت $f(x) \equiv 0 \pmod{p}$ حداکثر $d(q-1)$ است. اما داریم

$$\begin{aligned} d(q-1) &= dq - d \\ &= p - 1 - d \end{aligned}$$

پس از $p-1$ جواب معادله فوق حداقل

$$d = p - 1 - (p - 1 - d)$$

جواب به معادله $x^d - 1 \equiv 0 \pmod{p}$ تعلق دارد. اما باز هم مطابق ١٥.٦ معادله اخیر حداکثر d جواب دو به دو غیرهم‌نهشت به پیمانه p دارد. پس تعداد جوابهای آن دقیقا d می‌باشد.

■

١٧.٦ گزاره— فرض کنیم p یک عدد اول باشد و $d \mid p-1$. فرض کنیم

$$A_d = \{a \ : \ 1 \leq a \leq p, ord_p(a) = d\}$$

آنگاه $|A_d| \leq \varphi(d)$.

اثبات— اگر $|A_d| = \phi$ آنگاه حکم بدیهی است. پس فرض کنیم $a \in A_d$. چون $ord_p(a) = d$ پس اعداد

$$1, a, a^2, \ldots, a^{d-1}$$

دو به دو به پیمانه p غیرهم‌نهشت‌اند. از طرف دیگر هر کدام از این اعداد جواب $x^d \equiv 1 \pmod p$ می‌باشند. چون چندجمله‌ای $x^d - 1$ به پیمانه p دقیقا d جواب غیرهم‌نهشت دارد پس این d جواب دقیقا

$$1, a, a^2, \ldots, a^{d-1}$$

می‌باشند. حال می‌دانیم

$$ord_p(a^t) = d \quad \Leftrightarrow \quad (t, d) = 1$$

پس اگر یک عضو با مرتبه d موجود باشد آنگاه دقیقا $\varphi(d)$ عضو با این ویژگی موجود است. پس در حالت کلی

$$|A_d| \leq \varphi(d)$$

■

١٨.٦ قضیه— فرض کنیم p یک عدد اول باشد و $d \mid p-1$. آنگاه دقیقا $\varphi(d)$ عدد $1 \leq a \leq p-1$ وجود دارد که

$$ord_p(a) = d\ .$$

اثبات— فرض کنیم A_d مثل ١٧.٦ تعریف شود. چون بازای هر $1 \leq a \leq p-1$ داریم $ord_p(a) \mid p-1$ پس داریم

$$p-1 = \sum_{d|p-1} |A_d|\ .$$

از سوی دیگر می‌دانیم که

$$p-1 = \sum_{d|p-1} \varphi(d)$$

حال با توجه به نامساوی $|A_d| \leq \varphi(d)$ و با توجه به دو رابطه فوق حکم حاصل می‌شود.

■

١٩.٦ نتیجه— اگر p یک عدد اول باشد آنگاه یک ریشه اولیه به پیمانه p وجود دارد.

اثبات— می‌دانیم که $\varphi(p) = p-1$. حال طبق ١٨.٦ داریم

$$|A_{p-1}| = \varphi(p-1) \geq 1$$

پس لااقل یک عضو با مرتبه $p-1$ موجود است.

■

در پایان این فصل، بدون ارائه اثبات، تمام m هایی را که دارای ریشه اولیه می‌باشند توصیف می‌کنیم.

٦.٢٠ قضیه — فرض کنیم $1 < m$. شرط لازم و کافی برای آنکه یک ریشه اولیه به پیمانه m موجود باشد آن است که بتوان m را به یکی از اشکال زیر بیان کرد.

$$m = 2, 4, p^t, 2p^t$$

که در آن p یک عدد اول فرد است و $1 \leq t$.

فصل ۷

آزمونهای اول بودن

در بسیاری از کاربردهای نظریه اعداد، در اختیار داشتن عددهای اول بسیار بزرگ اهمیت دارد. در این فصل نشان می‌دهیم که چگونه می‌توان یک عدد اول بسیار بزرگ را در زمان معقول پیدا کرد.

۱.۷ تعریف— فرض کنید x یک عدد حقیقی مثبت باشد. تعداد اعداد اول کمتر یا مساوی x را با نماد $\pi(x)$ نشان می‌دهیم. قضیه زیر که بنام قضیه اعداد اول معروف است در ابتدا توسط گاوس و لژاندر حدس زده شده است. اثبات آن توسط چبیشف، هادامار و پواسون با استفاده از تابع زتای ریمان تکمیل شده اما یک اثبات مقدماتی و در عین حال مشکل توسط سلبرگ و

اردیش ارائه شده است. در اینجا فقط صورت قضیه اعداد اول را بیان می‌کنیم.

۲.۷ قضیه اعداد اول— داریم

$$lim_{x\to\infty}(\frac{x/\ln x}{\pi(x)}) = 1 \ .$$

۳.۷ تبصره— طبق قضیه اعداد اول می‌توان برای x های بزرگ $\pi(x)$ را بوسیله $\frac{x}{\ln x}$ تقریب زد.

۴.۷ تبصره— فرض کنید بخواهیم یک عدد بیست رقمی را به تصادف انتخاب کنیم. احتمال اول بودن چنین عددی چقدر است؟ در زیر به محاسبه این احتمال می‌پردازیم. بدیهی است که تعداد کل اعداد 20—رقمی برابر است با

$$N = 10^{21} - 10^{20} = 10^{20} \times 9$$

طبق قضیه اعداد اول تعداد تقریبی اعداد اول ۲۰—رقمی نیز برابر است با

$$P = \frac{10^{21}}{\ln 10^{21}} - \frac{10^{20}}{\ln 10^{20}}$$

$$\simeq 10^{20}(\frac{10}{21 \times 2.302} - \frac{1}{20 \times 2.302})$$

$$\simeq 10^{20}(\frac{10}{48.342} - \frac{1}{46.040})$$

$$\simeq 10^{20} \times (\frac{412}{2208})$$

پس احتمال اول بودن عدد انتخاب شده برابر است با

$$A \simeq \frac{P}{N} \quad \simeq \frac{10^{20} \times \frac{412}{2208}}{10^{20} \times 9}$$

$$= \frac{412}{19872} \simeq \frac{1}{48}$$

یعنی از هر 48 عدد 20—رقمی انتخاب شده بطور متوسط یکی اول خواهد بود. با توجه به اینکه تقریبا 24 مورد از این اعداد زوج است کافی است اول بودن 24 مورد باقیمانده را بررسی کنیم. دقت کنید که بررسی اول بودن یک عدد 20—رقمی با استفاده از کامپیوتر و یکی از روشهای بیان شده در این فصل به زمان بسیار کم نیاز دارد.

اکثر این آزمونها بر اساس عکس قضیه کوچک فرما بوجود آمده‌اند.

۵.۷ قضیه (آزمون لوکاس)— فرض کنید m یک عدد صحیح مثبت باشد. فرض کنید عدد صحیح x موجود باشد که

الف) $x^{m-1} \equiv 1 \pmod{m}$،

ب) اگر q اول باشد و $q \mid m-1$ آنگاه

$$x^{\frac{m-1}{q}} \not\equiv 1 \pmod{m} .$$

آنگاه m اول است.

اثبات– چون $x^{m-1} \equiv 1 \pmod{m}$ پس $ord_m(x) \mid m-1$. ادعا می‌کنیم که

$ord_m(x) = m-1$.

اگر چنین نباشد آنگاه

$$\exists\, a > 1 \;:\; m-1 = a \cdot ord_m(x) .$$

فرض کنیم q یک عامل اول a باشد. پس در عین حال q عامل اولی از $m-1$ نیز است. داریم

$$\begin{aligned} x^{\frac{m-1}{q}} &= x^{\frac{a \cdot ord_m(x)}{q}} \\ &= (x^{ord_m(x)})^{\frac{a}{q}} \\ &\equiv 1 \pmod{m} . \end{aligned}$$

اما این با فرض (ب) متناقض است. پس داریم $ord_m(x) = m-1$. از طرف دیگر می‌دانیم که $ord_m(x) \leq \varphi(m)$. پس

$$m-1 \leq \varphi(m)$$

این نشان می‌دهد که $\varphi(m) = m-1$. یعنی m اول است.

■

۶.۷ تبصره— در عمل، استفاده از آزمون فوق مستلزم دانستن عاملهای اول $m-1$ است. این مساله بکاربردن آزمون فوق را مگر در حالات خاص مشکل می‌کند. یکی از مواردی که می‌توان آزمون لوکاس را بکار برد حالتی است که در آن $m = p^n + 1$ و p یک عدد اول است.

۷.۷ قضیه (آزمون پاک لینگ تون $Pocklington$)— فرض کنید m یک عدد صحیح مثبت باشد بطوریکه

$$m-1 = ab$$

و $(a,b) = 1$ و $a > b$. فرض کنید عدد صحیح x چنان یافت شود که $x^{m-1} \equiv 1 \pmod{m}$ و بازای هر عامل اول $q \mid a$ داشته باشیم

$$(x^{\frac{m-1}{q}} - 1, m) = 1 .$$

آنگاه m اول است.

اثبات— فرض کنید p یک عامل اول m باشد. چون

$$x^{m-1} \equiv 1 \pmod{m}$$

پس داریم

$$x^{m-1} \equiv 1 \pmod{p} .$$

بنابراین $ord_p(x) \mid m-1$. پس

$$\exists\, t \ : \ m-1 = t \cdot ord_p(x)$$

حال فرض کنیم q یک عامل اول a باشد. ادعا می‌کنیم $q \nmid t$. چون اگر $q \mid t$ آنگاه

$$\begin{aligned} x^{\frac{m-1}{q}} &= x^{(t \cdot ord_p(x))/q} \\ &\equiv 1 \pmod{p} . \end{aligned}$$

این ایجاب می‌کند که $p \mid x^{\frac{m-1}{q}} - 1$ و $p \mid m$. این نتیجه با فرض در تناقض است. پس $q \nmid t$.

یعنی هر عامل اول a باید $ord_p(x)$ را عاد کند. بعبارت دیگر باید داشته باشیم $a \mid ord_p(x)$. اما از

سوی دیگر $ord_p(x) \mid p-1$. پس $a \mid p-1$ و بخصوص $a < p$. حال چون $m-1 = ab$ و $a > b$

پس داریم

$$m-1 < a^2 < p^2$$

این یعنی $\sqrt{m} < p$. پس هر عامل اول m بزرگتر از $\sqrt{m} < p$ است. این یعنی m اول می‌باشد.

■

۸.۷ قضیه (آزمون پراث $-$ $Proth-$) فرض کنید m یک عدد صحیح مثبت باشد بطوریکه

$$m = 2^k \cdot a + 1$$

و در آن $a < 2^k$ فرد است. اگر x چنان یافت شود که

$$x^{\frac{m-1}{2}} \equiv -1 \pmod{m}$$

آنگاه m اول است.

اثبات— کافی است قرار دهیم $a = 2^k$ و $b = a$. با این a و b جدید تمام مفروضات آزمون پاک لینگ تون برقرارند و حکم از همان آزمون نتیجه می‌شود.

■

۹.۷ تبصره— آزمونهای فوق درباره اعداد خاصی قابل اجراء هستند. اما در ادامه این فصل یک آزمون تصادفی ارائه می‌کنیم که می‌توان آنرا درباره هر عدد صحیح مثبت بکار برد. نتیجه این آزمون قطعی نیست اما امکان خطا در آن بقدری کم است که بطور قریب به یقین می‌توانیم بگوییم عدد مورد نظر اول است.

۱۰.۷ تعریف— فرض کنید

$$m - 1 = 2^k \cdot a$$

که در آن $0 \leq k$ و a فرد است. فرض کنید x یک عدد صحیح باشد. فرض کنید یکی از احکام زیر درست باشد:

الف) $x^a \equiv 1 \pmod{m}$.

ب) $\exists\, j \;:\; 0 \leq j \leq k-1 \;\;\&\;\; x^{2^j a} \equiv -1 \pmod{m}$.

آنگاه می‌گوییم m از تست میلر به مبنای x عبور می‌کند و می‌نویسیم $Mill(m,x)^+$.

۱۱.۷ قضیه— فرض کنیم m اول و x عدد صحیح مثبتی باشد که $m \nmid x$. آنگاه $Mill(m,x)^+$.

اثبات— فرض کنیم $m-1=2^k\cdot a$ که در آن $0\leq k$ و a فرد است. بازای $0\leq i$ تعریف می‌کنیم

$$x_i=x^{(m-1)/2^i}=x^{2^{k-i}\cdot a}\ .$$

چون m اول است پس طبق قضیه کوچک فرما داریم

$$x_0=x^{m-1}\equiv 1\pmod m$$

حال چون

$$x_1^2=(x^{(m-1)/2})^2=x_0\equiv 1\pmod m$$

پس $x_1\equiv\pm 1\pmod m$. اگر -1 اتفاق بیافتد پس m از تست میلر به مبنای x عبور کرده است. فرض کنیم

$$x_1\equiv 1\pmod m$$

در اینصورت $x_2\equiv\pm 1\pmod m$. با تکرار این عمل به یکی از حالات زیر خواهیم رسید:

الف) $x_k\equiv 1\pmod m$

ب) $\exists\ i\ :\ x_i\equiv -1\pmod m$

در هر حالت نتیجه می‌گیریم که $Mill(m,x)^+$.

■

۱۲.۷ قضیه— اگر m فرد و مرکب باشد آنگاه تعداد x هایی که $1 \leq x \leq m-1$ و $Mill(m,x)^+$ حداکثر $\frac{m-1}{4}$ است.

قضیه فوق را اثبات نمی‌کنیم و به بیان آزمون تصادفی رابین می‌پردازیم که نتیجه قضیه فوق است.

۱۳.۷ قضیه (آزمون تصادفی رابین)— فرض کنید m یک عدد صحیح مثبت باشد. اگر

$$1 \leq x_1, x_2, \ldots x_k \leq m-1$$

k عدد صحیح متمایز باشند و

$$\forall\, i \quad : \quad Mill(m,x_i)^+$$

آنگاه به احتمال $\frac{4^k-1}{4^k}$ عدد m اول است.

۱۴.۷ تبصره— فرض کنید m یک عدد مرکب بزرگ باشد. اگر ۱۰۰ عدد

$$1 \leq x_1, x_2, \ldots x_{100} \leq m-1$$

انتخاب کنیم آنگاه احتمال اینکه

$$\forall\, i \quad : \quad Mill(m, x_i)^+$$

در حدود $\frac{1}{10^{60}}$ است. پس در عمل می‌توانیم از آزمون تصادفی رابین با خیال راحت استفاده کنیم.