دانشگاه تهران

دانشکده علوم

(رشته ریاضی)

پایان‌نامه

برای دریافت درجه فوق لیسانس

موضوع :

" نظریه اعداد "

استاد راهنما :

جناب آقای دکتر وحدتی

تهیه کننده :

مهدی بدیعی

ازراهنمائیهای جناب‌آقای دکتر وحدتی
کمال تشکـــر را دارم.

۶۲۱۶

فهرست مطالب

خلاصه

برای تهیه رساله مطالب و قضایای زیر ثابت گردیده است

الف- برای ساختن اعداد صحیح ومثبت از اصول موضوعه پئانو استفاده شده است.

قضیه ۱- هر مجموعه غیر تهی S از اعداد صحیح و مثبت شامل یک کوچکترین عدد است.

ب- روابط هم ارزی

ج- ساختمان اصل موضوعی اعداد صحیح

قضیه ۱- فرض میکنیم a عدد صحیح طبیعی باشد و A مجموعه اعداد $\leq a$ باشد در آنصورت هر زیر مجموعه غیر تهی A شامل یک کوچکترین جزء است.

د- ساختمان اصل موضوعی اعداد کسری

ه- ساختمانهای جبری نیم گروه جابجائی، گروه آبلی، حلقه، میدان، انتگرال دامنه

۱- قضیه ۲- اگر a و b اعداد صحیح و b مخالف صفر باشد در آنصورت اعداد صحیح منحصر بفردی مانند q و r وجود دارند بطوریکه

$$0 \leq r < |b| \quad , \quad a = qb + r$$

قضیه ۳- اگر a و b اعداد صحیح باشند و b مخالف صفر باشد در آنصورت اعداد صحیح منحصر بفردی مانند r و q وجود دارند بطوریکه $-\frac{1}{2}|b| \leq r < \frac{1}{2}|b| \; , \; a = qb + r$

را کوچکترین مضرب مشترک a و b گویند مثلاً کوچکترین مضرب مشترک ۷۸ است و ۷ ...

... است.

الف- بزرگترین مقسوم علیه اعداد غیر صفر $a_1, \dots, a_n$ را با $(a_1, a_2, \dots, a_n)$ نشان میدهیم.

قضیه هـ- اگر $d = (a_1, a_2, \dots, a_n)$ در اینصورت اعداد صحیح $x_1, x_2, \dots, x_n$ وجود دارند بطوریکه

$$d = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$$

قضیه ۱- اگر a, b, k اعداد صحیح باشند در اینصورت $(a + kb, b) = (a, b)$

هـ- اعداد اول.

لم ۱- اگر p یک عدد اول باشد و $p|mn$ در اینصورت یا $p|m$ و یا اینکه $p|n$

لم ۲- اگر $a|mn$ و اگر $(a,m)=1$ در اینصورت $a|n$

و- اعداد اول نسبی، تابع اویلر

لم ۳- اگر r و m ، n اعداد صحیحی باشند در اینصورت r نسبت به mn اول خواهد بود اگر و فقط اگر r نسبت به m و r نسبت به n اول باشد.

لم ۴- اگر اعداد مثبت m و n نسبت بهم اول باشند در اینصورت

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

قضیه ۲- $\sum_{d|n} \varphi(d) = n$ که در آن حاصل جمع نسبت به تمام مقسوم علیه های مثبت عدد n گرفته شده است.

فصـــــل اول

هم نهشتـــــی هـا

۱.۱ـ تعریف هم نهشتی ـ عملیات روی هم نهشتی‌ها ـ اگر m عدد صحیح مثبت ثابتی باشد ، هر عدد در تقسیم بر m یک باقیمانده اصلی دارد برابر یکی از اعداد $0, 1, 2, \ldots, m-1$ بنابراین برای هر عدد طبیعی و مثبت m ، مجموعه اعداد را میتوان برحسب باقیمانده اصلی آنها به m زیر مجموعه تقسیم کرد . ازآنجائیکه تمام اعداد متعلق بیکی ازاین زیرمجموعه هـا خواص حسابی مشترک و متعددی دارند ، بهتراست که یک نوع علامتگذاری ساده داشته باشیم تا توسط آن بتوانیم درمورد تمام اعداد متعلق بیک زیرمجموعه بحث کنیم . این کار توسط علامت هم نهشتی که بوسیله گوس معرفی شده است، انجام میگیرد . اگر a و b دو عدد صحیح باشند مینویسیم $a \equiv b \pmod{m}$ (۱.۱.۱) برای اینکه بیان کنیم تفاضل a و b بر m قابل قسمت است، یعنی عددی مانند k وجود دارد بطوریکه $a-b=km$. رابطه (۱.۱.۱) چنین خوانده میشود ؛ a نسبت به مدول m با b هم نهشت است، m مدول هم نهشتی (۱.۱.۱) نامیده میشود .

اگر $a-b$ بر m قابل قسمت نباشد ، مینویسیم $a \not\equiv b \pmod{m}$ و میگوئیم

a و b غیرهم‌نهشت هستند.

مثلاً $13 \equiv -2 \pmod{5}$ بعلت اینکه $13-(-2)=3\times 5$ و $4 \not\equiv -2 \pmod{5}$ بعلت اینکه $4-(-2)=6$ و $5 \nmid 6$ قضیه زیر نشان میدهد که هم‌نهشتی یک رابطه هم ارزی روی مجموعه اعداد است، و کلاسهای هم ارزی مربوطه را — مشخص میکند.

قضیه ۸ — اگر هم نهشتی وجود داشته باشد $(\mathrm{mod}\ m)$ درآنصورت.

(۱) $a \equiv a$

(۲) $a \equiv b$ معادل آنست که $b \equiv a$ است.

(۳) اگر $a \equiv b$ و $b \equiv c$ باشد درآنصورت $a \equiv c$ است.

(۴) $a \equiv b$ اگروفقط اگر a و b درتقسیم بر m دارای یک باقیمانده اصلی باشند.

اثبات — قسمتهای (۱) و (۲) و (۳) را میتوان از روی تعریف هم نهشتی در روابط $a-a=0$ و $b-a=-(a-b)$ و $a-c=(a-b)+(b-c)$ ثابت نمود.

اکنون فرض میکنیم که a و b درتقسیم بر m دارای باقیمانده های اصلی r و s باشند. درآنصورت $0 \leq r < m$ و $0 \leq s < m$ واعداد صحیح q و h وجود دارند بطوریکه $a = qm + r$ و $b = hm + s$ نتیجه میگیریم که $a-b=(q-h)m+(r-s)$

پس $a \equiv b \pmod{m}$ اگروفقط اگر $m \mid r-s$ ولی $0 \leq |r-s| \leq m-1$

بنابراین $a \equiv b \pmod{m}$ اگر وفقط اگر $r = s$ و خاصیت (۴) ثابت میشود .
خاصیتهای (۱) و (۲) و (۳) نشان میدهند که روابط هم نهشتی روی مجموعه
اعداد روابط هم ارزی میباشند . ونتیجه عدد وکلاس هم ارزی راسیتوان از روی
(۴) مشخص نمود . تعداد کلاسهای هم ارزی برابر m است که عبارتند از کلاسهای

$$C_0 , C_1 , C_2 , \ldots , C_{m-1}$$

عدد a متعلق به C_r است اگر وفقط اگر باقیمانده اصلی آن در تقسیم بر m
برابر r باشد . در حقیقت C_r برای هر $r = 0, 1, \ldots, m-1$ شامل تمام
اعداد بشکل $km + r$ است که بوسیله $k = 0, \pm 1, \pm 2, \ldots$ بدست میآیند
مجموعه های $C_0 , C_1 , C_2 , \ldots$ کلاسهای هم نهشتی ($\bmod\ m$)
نامیده میشوند . این مجموعه ها درست همان m مجموعه ای هستند که در اول
این فصل شرح داده شدند . در قضیه بعد درباره جمع وتفریق و ضرب وتقسیم
(برای عدد) هم نهشتی ها بحث خواهیم کرد .

قضیه ۹ — اگر $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$ درآنصورت

$$a \pm c \equiv b \pm d \pmod{m} \qquad (۱)$$

همچنین

$$ac \equiv bd \pmod{m} \qquad (۲)$$

(۳) $an \equiv bn \pmod{m}$ اگر وفقط اگر $a \equiv b \left(\bmod \frac{m}{(m,n)}\right)$

(۴) و اگر $a \equiv b \pmod{m}$ و اگر $f(x)$ یک کثیرالجمله انتگرالی از x با ضرایب صحیح باشد در آنصورت $f(a) \equiv f(b) \pmod{m}$

اثبات ــ اگر $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$ در آنصورت

$a-b=hm$

$c-d=km$

بنابراین

$$(a \pm c)-(b \pm d)=(h \pm k)m$$

پس

$$a \pm c \equiv b \pm d \pmod{m}$$

همچنین

$$ac-bd=(a-b)c+b(c-d)=(hc+kb)m$$

پس

$$ac = bd \pmod{m}$$

برای اثبات نتیجه (۳) فرض میکنیم $d=(m,n)$ و $m=dm_1$ و $n=dn_1$

بنابراین $(m_1,n_1)=1$ اگر $an=bn \pmod{m}$ در آنصورت $dm_1 \mid (a-b)dn_1$

پس بنابه لم ۲ $m_1 \mid (a-b)$ یعنی $a \equiv b \left(\bmod\, m_1=\frac{m}{(m,n)}\right)$ عکس این قضیه را

میتوان با استفاده از اینکه اگر $m_1 \mid (a-b)$ در آنصورت $dm_1 \mid (a-b)dn_1$ ، ثابت کرد.

برای اثبات قسمت (۴) فرض میکنیم $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$

$$f(a)-f(b)=a_n(a^n-b^n)+a_{n-1}(a^{n-1}-b^{n-1})+\cdots+a_1(a-b)=N(a-b)$$

در آنصورت

بنابراین اگر $a-b$ بر m قابل قسمت باشد $f(a)-f(b)$ هم بر m قابل

قسمت است. یعنی $a \equiv b \pmod{m}$ مستلزم آنست که $f(a) \equiv f(b) \pmod{m}$

بدین ترتیب قضیه ۹ ثابت شده است. یادآوری میکنیم که اگر $(m,n)=1$ ، در

بصورت اول بنابقسمت (۲) قضیه ، میتوان گفت $an \equiv bn \pmod m$ آنوقت اگر $a \equiv b \pmod m$ نتیجه میگیریم که درهم نهشتی بین دو عدد صحیح میتوانیم طرفین رابریك عدد n تقسیم کنیم ، بدون اینکه نهشتی بهم بخورد ولی بشرط اینکه $(m,n)=1$ باشد .

۱۱ــ مجموعه های باقیمانده های $\pmod m$ ــ m کلاس همنهشتی $C_0, C_1, \ldots, C_{m-1}$ را درنظرمیگیریم . اگر x_i برای هر $i=0,1,\ldots,m-1$ یك عدد اختیاری از C_i باشد درانصورت میگویند مجموعه اعداد $x_0, x_1, \ldots, x_{m-1}$ یك مجموعه کامل ازباقیمانده های $\pmod m$ است . درانصورت هر عدد بایکی وفقط یکی از x_i ها هم نهشت است $\pmod m$.

ساده ترین این سیستمها مجموعه اعداد $0, 1, \ldots, m-1$ میباشد . اعداد مجموعه لزومی ندارد که باین ترتیب مخصوص باشند . سایرمجموعه های کامل ازباقیمانده های $\pmod m$ عبارتند از $1, 2, \ldots, m$ و $m, m+1, \ldots, 2m-1$ والی آخر . سیستم دیگری که درآن تمام اعداد غیرمنفی نمیباشند ، مجموعه اعداد x است که درنامساوی $-\frac{1}{2}m < x \le \frac{1}{2}m$ صدق میکنند . ازآنجائیکه کوچکترین باقیمانده مطلق یك عدد درتقسیم بر m دراین فاصله تغییرمیکند ، این مجموعه کامل باقیمانده های $\pmod m$ مجموعه ایست که درآن $\max(|r|)$ کوچکترین مقدار ممکن خود را دارد .

مثلا ۶ و ۵ و ۴ و ۳ و ۲ و ۱ و ۰ و $0, \pm 1, \pm 2, \pm 3$ مجموعه های کامل از باقیمانده های $(\mathrm{mod}\ 7)$ میباشند . یعنی از خواص مجموعه های کامل باقیمانده ها را میتوان از قضیه زیر نتیجه گرفت :

قضیه ۱۰ - (۱) اگر $x_0, x_1, \ldots, x_{m-1}$ یک مجموعه کامل باقیمانده های $(\mathrm{mod}\ m)$ باشد و اگر عدد a طوری باشد که $(a,m)=1$ و اگر عدد b اختیاری باشد در آنصورت (۱۰۱۱) $ax_0+b, ax_1+b, \ldots, ax_{m-1}+b$ یک مجموعه کامل از باقیمانده های $(\mathrm{mod}\ m)$ است .

(۲) اگر $(m,n)=1$ و اگر $x_0, x_1, \ldots, x_{m-1}$ یک مجموعه کامل از باقیمانده های $(\mathrm{mod}\ m)$ باشد و اگر $y_0, y_1, \ldots, y_{n-1}$ یک مجموعه کامل از باقیمانده های $(\mathrm{mod}\ n)$ باشد . در آنصورت mn عدد nx_i+my_j $(i=0,1,\ldots,m-1)$ و $(j=0,1,\ldots,n-1)$ یک مجموعه کامل باقیمانده های $(\mathrm{mod}\ mn)$ را تشکیل میدهند .

اثبات (۱)- دو عدد متمایز (۱۰۱۱) غیر هم نهشت هستند $(\mathrm{mod}\ m)$. بعلت اینکه اگر $ax_i+b \equiv ax_j+b \pmod{m}$ در آنصورت $ax_i \equiv ax_j \pmod{m}$ پس بنابه نتیجه ۳ قضیه ۹ $x_i \equiv x_j \pmod{m}$ و در نتیجه $x_i = x_j$ از آنجائیکه در مجموعه (۱۰۱۱) m عدد موجود است، نتیجه میشود که این مجموعه

یک مجموعه کامل از باقیمانده های $(\bmod\ m)$ میباشد .

(۲) اگر $nx_i + my_j \equiv nx_k + my_l \pmod{mn}$ درآنصورت $nx_i \equiv nx_k \pmod m$ و $my_j \equiv my_l \pmod n$ بنابراین با استفاده از قسمت ۳ قضیه ۹ $x_i \equiv x_k \pmod m$ و $y_j \equiv y_l \pmod m$ بنابراین $x_i = x_k$ و $y_j = y_l$ است. پس mn عدد $nx_i + my_j$ یک مجموعه کامل باقیمانده های $(\bmod\ mn)$ را تشکیل میدهند .

از روی تعریف تابع اویلر $\phi(m)$ میتوان گفت که در مجموعه کامل باقیمانده های $(\bmod\ m)$ $0, 1, \ldots, m-1$ ، $\phi(m)$ عدد موجود است که نسبت به m اول هستند . برای اینکه ثابت کنیم این حکم برای هر مجموعه کامل از باقیمانده های $(\bmod\ m)$ برقرار است لم زیر را ثابت میکنیم :

لم ۵ــ اگر $a \equiv b \pmod m$ دراینصورت $(a,m) = (b,m)$

اثبات ــ اگر $a \equiv b \pmod m$ باشد $a - b = km$ است درنتیجه $(a,m) = (b+km, m)$ پس بنابه (۲۰۴) $(a,m) = (b,m)$ است .

عکس لم ۵ درست نیست . مثلا $1 = (2,4) = (1,4)$ ولی $1 \not\equiv 2 \pmod 4$

از لم ۵ نتیجه میشود که تمام اعداد صحیح یک کلاس هم نهشتی $(\bmod\ m)$ با m دارای یک بزرگترین مقسوم علیه مشترک میباشند . بخصوص اگر یکی از اعداد متعلق

یک کلاس نسبت به m اول باشد ، سایر اعداد کلاس هم با m اول هستند . ولی
در مجموعه کامل باقیمانده های $0, 1, \dots, m-1$ $(\bmod\ m)$ ، $\phi(m)$ عدد
موجود است که نسبت به m اول هستند . بنابراین $\phi(m)$ کلاس هم نهشتی
شامل اعداد اول نسبت به m وجود دارد . هر مجموعه $\phi(m)$ تائی از اعداد
که یک و تنها یکی از این $\phi(m)$ کلاس انتخاب شده اند یک مجموعه کاهش یافته
باقیمانده های $(\bmod\ m)$ نامیده میشوند . هر عدد که نسبت به m اول
باشد با یکی از این $\phi(m)$ عدد هم نهشت است $(\bmod\ m)$

مثال ــ مجموعه ۶ و ۵ و ۴ و ۳ و ۲ و ۱ و ۰ یک مجموعه کامل باقیمانده های
$(\bmod\ 7)$ و ۶ و ۵ و ۴ و ۳ و ۲ و ۱ یک مجموعه کاهش یافته باقیمانده های
$(\bmod\ 7)$ میباشند .

۹ و ۸ و ۷ و ۶ و ۵ و ۴ و ۳ و ۲ و ۱ و ۰ یک مجموعه کامل باقیمانده های
$(\bmod\ 10)$ و ۹ و ۷ و ۳ و ۱ یک مجموعه کاهش یافته باقیمانده های
$(\bmod\ 10)$ میباشند .

نظیر قضیه ۱ که درمورد مجموعه های کامل باقیمانده ها بود ، قضیه دیگری در
مورد مجموعه های کاهش یافته باقیمانده ها داریم که چنین بیان میشود :

قضیه ۱۱ــ۱ . اگر $x_1, x_2, \dots, x_{\phi(m)}$ یک مجموعه کاهش یافته باقیمانده های

(mod m) باشد ، و اگر عدد a بطوری باشد که $(a,m)=1$ در اینصورت

$$ax_1, ax_2, \dots, ax_{\phi(m)} \qquad (۱۱۰۲)$$

یک مجموعه کاهش یافته باقیمانده های (mod m) است.

(۲) اگر $(m,n)=1$ و اگر $x_1, x_2, \dots, x_{\phi(m)}$ یک مجموعه کاهش یافته باقیمانده های (mod m) باشد و اگر $y_1, y_2, \dots, y_{\phi(n)}$ یک مجموعه کاهش یافته باقیمانده های (mod n) باشد، در اینصورت $\phi(m)\phi(n)=\phi(mn)$ عدد (nx_i+my_j) ؛ $\begin{pmatrix} i=1,2,\dots,\phi(m) \\ j=1,2,\dots,\phi(n) \end{pmatrix}$ یک مجموعه کامل کاهش یافته باقیمانده ها را تشکیل میدهند.

اثبات (۱) — $\phi(m)$ عدد مجموعه (۱۱۰۲) نسبت به m اول هستند. — همچنین با استدلالی شبیه استدلال قسمت (۱) قضیه ۱ میتوان گفت دو عدد متمایز مجموعه (۱۱۰۲) غیرهمنهشت هستند (mod m) بنابراین مجموعه (۱۱۰۲) یک مجموعه کاهش یافته باقیمانده ها است.

(۲) — برای تمام i و j ها (۱۱۰۳) $(nx_i+my_j, mn)=1$

بعلت اینکه $(nx_i+my_j, n)=(my_j, n)=1, (nx_i+my_j, m)=(nx_i, m)=1$

بنابراین ، طبق لم ۲ ، رابطه (۱۱۰۳) درست است.

بقیه قسمت (۲) با راهی شبیه قسمت (۲) قضیه ۱ با توجه باینکه $\phi(mn)=\phi(m)\phi(n)$ است.

ثابت میشود . باید دریافت که اگر $x_1, x_2, \dots, x_{\phi(m)}$ یک مجموعه کاهش یافته باقیمانده های $(\bmod m)$ باشد . و اگر b یک عدد صحیح باشد . درانصورت درحالت کلی نمیتوان ادعا کرد که $x_1+b, x_2+b, \dots, x_{\phi(m)}+b$ هم یک مجموعه کامل باقیمانده هاست

۱۲ــ قضیه اولر ، رتبه $a \pmod m$. قضیه مهم زیر منسوب به اولر است .

قضیه ۱۲ــ اگر $(a,m)=1$ درانصورت $a^{P(m)} \equiv 1 \pmod m$

اثبات ــ فرض میکنیم $n = P(m)$ و $x_1, x_2, \dots, x_n$ یک مجموعه کاهش یافته از باقیمانده های $(\bmod m)$ باشد . پس بنابه قسمت (۱) قضیه ۱۱ $ax_1, \dots, ax_n$ یک مجموعه کاهش یافته باقیمانده های $(\bmod m)$ است . نتیجه میگیریم که $ax_1, ax_2, \dots$ و ax_n با $x_1, x_2, \dots, x_n$ هم نهشت هستند $(\bmod m)$ ولی لزومی ندارد که ترتیب شان یکی باشد . بنابراین بموجب این هم نهشتی ها داریم .

$$ax_1 \times ax_2 \times \cdots \times ax_n \equiv x_1 x_2 \cdots x_n \pmod m$$

یعنی

$$a^{P(m)} x_1 x_2 \cdots x_n \equiv x_1 x_2 \cdots x_n \pmod m$$

ولی $(x_1 x_2 \cdots x_n, m) = 1$ است . پس بنابه قسمت ۳ قضیه ۹ نتیجه مطلوب حاصل میشود . یعنی

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

حالت خاص این قضیه که برای عدد اول p توسط فرما بیان شده است چنین است :