بسم اللّه الرّحمن الرّحيم

دانشگاه فردوسی مشهد

دانشکده ریاضی

پایان‌نامه کارشناسی ارشد

رشته ریاضی کاربردی

موضوع

همنهشتی فازی و کاربردهای آن

استاد راهنما

دکتر علی وحیدیان کامیاد

استاد مشاور

دکتر جعفر صابری نجفی

تدوین

مینا لگزیان

شهریور ماه ۱۳۸۸

فهرست مندرجات

پیشگفتار

بسیاری از سوالات مربوط به علم نظریه اعداد به سوالاتی در مورد باقیمانده ها تحویل می شود که می توان به روشی نظام مند به آنها پاسخ داد. برای هر عدد صحیح $n > ۱$، حسابی موسوم به پیمانه n وجود دارد که بازتابی از حساب معمولی است اما به شکل متناهی، چون فقط با n باقیمانده $۱، ۲، ...، n-۱$ که در تقسیم بر n ظاهر می شوند سروکار دارد، آن را حساب به پیمانه n یا حساب همنهشتی می نامند. این مفهوم یکی از مباحث مطرح شده در نظریه اعداد کلاسیک می باشد. به سبب اینکه با استفاده از مفهوم همنهشتی به جای یک عدد، مجموعه ای از اعداد در نظر گرفته می شود، حل بسیاری از مسائل آسان تر می گردد. از جمله کاربردهای مفهوم همنهشتی در دسته بندی یا کلاس بندی اعداد و تعیین خواص آنها می باشد که می توان از آن در حل ساده تر مسائل نظریه اعداد کمک گرفت. در این پایان نامه مفهوم جدیدی به نام همنهشتی فازی در اعداد فازی را ارائه می دهیم و برخی از کاربردهای آن را بیان می نماییم و از آن در کاهش قواعد فازی که در کنترل فازی نقش بسیارباهمیتی دارد به وسیله دسته بندی کردن[۱] قواعد فازی استفاده می کنیم. از جمله کاربردهای دیگر مفهوم همنهشتی فازی برای حل معادله $f(x)=۰$ با تقریب خواسته شده می باشد.مزیت روش همنهشتی فازی در حل معادله $f(x)=۰$ کاهش تکرار محاسبات می باشد. به بیان دیگر در تعداد کمتری به جواب معادله با تقریب خواسته شده دست می یابیم. همچنین از این روش در بدست آوردن نقاط ایستای دستگاه معادلات دیفرانسیل معمولی استفاده می شود که در تعیین پایداری سیستم نقش بسزایی را ایفا می نماید. حل دستگاه معادلات غیر خطی از دیگر کاربردهای همنهشتی فازی می باشد که آن را نیز مورد بررسی قرار می دهیم. این پایان نامه شامل ۷ فصل می باشد. فصل اول شامل تاریخچه ای از نظریه اعداد و مفاهیم و تعاریف مقدماتی مربوط به مفهوم همنهشتی کلاسیک می باشد. همچنین در این فصل قضایا و لم هایی را که مورد نیاز است بیان نموده ایم. در فصل دوم تاریخچه

[۱] Clustering

مختصر و مقدمه ای از منطق فازی و تعاریف مربوط به آن را شامل می شود. همچنین مفاهیم مختصر و مقدماتی از کنترل فازی را بیان نموده ایم. در فصل سوم مفهوم جدید همنهشتی فازی ارائه گردیده است. فصل چهارم شامل کاربرد همنهشتی در دسته بندی اعداد می باشد. در این فصل الگوریتم هایی برای دسته بندی اعداد صحیح، حقیقی و فازی ارائه گردیده است. همانطور که بیان نمودیم بحث دسته بندی، در کنترل فازی دارای اهمیت بسزایی می باشد، بدین جهت این کاربرد همنهشتی را متذکر شده ایم. در فصل پنجم به بیان کاربرد همنهشتی در حل معادلات جبری پرداخته ایم. در ابتدای این فصل مقدمه ای از روش های کلاسیک حل معادلات جبری را بیان نموده ایم. در فصل ششم کاربرد همنهشتی را در حل دستگاه معادلات معمولی و همچنین در محاسبه نقاط ایستای دستگاه معادلات دیفرانسیل معمولی ارائه نموده ایم. فصل پایانی یا فصل هفتم پایان نامه شامل کاربرد همنهشتی در برنامه ریزی خطی می باشد. در این فصل روش حل معادله سیاله خطی به کمک همنهشتی بیان و سپس روش به حل یک دستگاه معادلات سیاله خطی تعمیم داده می شود.

فصل اول: مفاهیم و تعاریف مقدماتی

۱-۱تاریخچه نظریه اعداد

بعد از دوران یونان باستان، نظریه اعداد در سده شانزدهم و هفدهم با زحمات ویت[۱]، باشه[۲] دو مزیریاک، و بخصوص فرما دوباره مورد توجه قرار گرفت. در قرن هجدهم اویلر و لاگرانژ به قضیه پرداختند و در همین مواقع لژاندر وگاوس به آن تعبیر علمی بخشیدند. در ۱۸۰۱ گاوس در مرجع [۷] حساب نظریه اعداد مدرن را پایه گذاری کرد.

چبیشف کران هایی برای تعداد اعداد اول بین یک بازه ارائه داد. ریمان اظهار کرد که حد تعداد اعداد اول از یک عدد داده شده تجاوز نمی کند. قضیه عدد اول و آنالیز مختلط را در تئوری تابع زتای ریمان گنجاند. و فرمول صحیح تئوری اعداد اول را از صفرهای آن نتیجه گرفت. تئوری همنهشتی[۳] از مرجع [۷] شروع شد. او علامت گذاری زیر را پیشنهاد کرد:

$$mod\ \ c$$

چبیشف در سال ۱۸۴۷ به زبان روسی کاری را در این زمینه (تئوری همنهشتی) منتشر کرد و سره[۴] آن را در فرانسه عمومی کرد. بجای خلاصه کردن کارهای قبلی، لژاندر قانون تقابل درجه دوم را گذاشت. این قانون از استقراء کشف شد و قبلا اویلر آن را مطرح کرده بود. لژاندر در کتاب تئوری اعداد[۵] در سال ۱۷۸۹ برای حالت های خاص آن (قانون تقابل درجه دوم) را ثابت کرد. جدا از کارهای اویلر و لژاندر، گاوس این قانون را در سال ۱۷۹۵ کشف کردو اولین کسی بود که یک اثبات کلی ارائه داد.

---

[۱] Viete

[۲] Bachet de Meziriac

[۳] Congruence theory

[۴] Serret

[۵] NumberTheory

کوشی؛ دیریشله در مرجع [۵] که او یک مقاله کلاسیک است؛ جکوبی که علامت جکوبی[۱] را معرفی کرد؛ لیوویل؛ زلر[۲]؛ آیزنشتین؛کومر و کرونکر نیز در این زمینه کارهایی کرده اند. این تئوری تقابل درجه دوم و سوم راشامل می شود (گاوس؛ جکوبی اولین بار قانون تقابل درجه سوم را ثابت کرد؛ و کومر).

نمایش اعداد با صورت درجه دوم دوتایی[۳] مدیون گاوس است. کوشی، پوانسو ۱۸۴۵، لوبک ۱۸۶۸-۱۸۵۹و بخصوص هرمیت به موضوع، چیزهایی افزوده اند. آیزنشتاین در تئوری صورت های سه گانه پیشتاز است و تئوری فرم ها[۴] به طور کلی مدیون او و اچ.اسمیت است. اسمیت دسته بندی کاملی از صورتهای سه گانه انجام داد و تحقیقات گاوس در مورد صورت های درجه دوم حقیقی به فرمهای مختلط افزود. جستجو هایی در مورد نمایش اعداد به صورت جمع مربعات ۷،۶،۵،۴ و یا ۸ عدد توسط آیزنشتاین ادامه یافت و اسمیت آن را کامل کرد. دیریشله اولین کسی بود که در یک دانشگاه آلمانی در این مورد سخنرانی کرد.

بین نویسندگان فرانسوی، بورل و پوانکاره ذهن قوی داشتند و همچنین تانری و استلیجز. کرونکر،کومر، شرینگ، باخمن و ددکیند آلمانی های پیشتاز در زمینه نظریه اعداد هستند. در اتریش مقاله استلز در فاصله سالهای ۸۶-۱۸۸۵ و در انگلستان تئوری اعداد ماتیو (قسمت اول، ۱۸۹۲) جزو کارهای عمومی دانشگاهی هستند. جنوچی، سیلوستر، و جی.گلیشر[۵] به این تئوری چیزهایی افزوده اند [۴].

---

[۱] Jacobi Symbol

[۲] Zeller

[۳] Binary Quadratic Forms

[۴] Forms Theory

[۵] J.W.L.

۱-۲ همنهشتی کلاسیک

حساب باقیمانده ها یا نظریه همنهشتی ها ابزاری است که در اثبات بسیاری از قضیه های نظریه اعداد به کار گرفته می شود. به سبب اینکه با استفاده از مفهوم همنهشتی ، به جای یک عدد مجموعه ای از اعداد در نظر گرفته می شود ، حل بسیاری از مسائل از این طریق ساده تر می گردد. در این فصل ابتدا با مفاهیم اساسی نظریه همنهشتی ها و نمادهای آن آشنا می شویم. سپس معادله های همنهشتی خطی و نیز دستگاه معادله های همنهشتی خطی را بیان می نماییم. همچنین به بیان قضیه باقیمانده چینی و تعمیم آن می پردازیم. در انتها نیز معادله سیاله خطی و روش حل آن به کمک همنهشتی کلاسیک را بیان می نماییم[۱].

۱-۲-۱ مفاهیم و تعاریف اصلی

قبل از شروع این بخش ذکر این نکته ضروری اس که تعریف و قضایای این بخش از مرجع [۱] و [۳] استخراج گردیده است.

تعریف ۱-۲-۱-۱ فرض می کنیم m یک عدد طبیعی باشد،گوییم عدد صحیح a با عدد صحیح b به پیمانه m همنهشت است، هرگاه m، $a-b$ را بشمارد(عاد کند). در این صورت می نویسیم $a\equiv b(\mathrm{mod}\, m)$. اگر a با b همنهشت نباشد می نویسیم، $a\not\equiv b(\mathrm{mod}\, m)$. به علت اینکه هر عدد صحیح بر یک بخش پذیر است، برای هر دو عدد صحیح a و b، $a\equiv b(\mathrm{mod}\, ۱)$ یعنی هر دو عدد صحیح به پیمانه یک، همنهشت هستند. همچنین توجه می کنیم که $a\equiv b(\mathrm{mod}\, m)$ اگر و تنها اگر عدد صحیحی مانند k وجود داشته باشد که $a=b+km$.

لم ۱-۲-۱-۱ برای هر عدد صحیح و مثبت m

الف) $a\equiv a(\mathrm{mod}\, m)$

ب) اگر $a\equiv b(\mathrm{mod}\, m)$، آنگاه $b\equiv a(\mathrm{mod}\, m)$

پ) اگر $a \equiv b \pmod{m}$ و $b \equiv c \pmod{m}$، آنگاه $a \equiv c \pmod{m}$

از لم قبل چنین نتیجه می شود که رابطه همنهشتی در $\mathbb{Z}$، که $\mathbb{Z}$ مجموعه اعداد صحیح است، یک رابطه هم ارزی در $\mathbb{Z}$ است. هر رده هم ارزی را یک رده همنهشتی می نامیم. رده همنهشتی شامل a را با $\bar{a}$ نشان می دهیم، بنابراین:

$$\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{b : b = a + km, k \in \mathbb{Z}\}$$

لم ۱-۲-۱-۲ $a \equiv b \pmod{m}$؛ اگر و تنها اگر باقیمانده های a و b بر m، برابر باشند.

لم ۱-۲-۱-۳ هر عدد صحیح a با یکی و تنها یکی از اعداد مجموعه $\{۰.۱.۲,\ldots,m-۱\}$ همنهشت است.

با توجه به دو لم قبل، نتیجه می گیریم، نتیجه می گیریم که m مجموعه زیر، تنها رده های همنهشتی به پیمانه m هستند.

$$\bar{۰} = \{\ldots, -۲m, -m, ۰, m, ۲m, \ldots\}$$
$$\bar{۱} = \{\ldots, -۲m-۱, -m-۱, ۱, m+۱, ۲m+۱, \ldots\}$$
$$\vdots$$
$$\overline{m-۱} = \{\ldots, m-۳, -m-۱, m, m+۱, m+۳, \ldots\}$$

تعریف ۱-۲-۱-۲ مجموعه رده های همنهشتی به پیمانه m را مجموعه اعداد صحیح به پیمانه m و آن را با $\mathbb{Z}_m$ نشان می دهیم، پس :

$$\overline{\mathbb{Z}_m} = \{\bar{۰}, \bar{۱}, \ldots, \overline{m-۱}\}$$

تعریف ۱-۲-۱-۳ مجموعه ای را که هر عضو آن به یکی از رده های همنهشتی، به پیمانه m تعلق داشته باشد، یک دستگاه کامل مانده می نامیم.

قضیه ۱-۲-۱-۱ برای هر پیمانه m و هر عدد صحیح a، b، c و d

الف) اگر $a \equiv b \pmod{m}$ و $c \equiv d \pmod{m}$، آنگاه $a + c \equiv b + d \pmod{m}$

ب) $ac \equiv bd \pmod{m}$

پ) اگر $a\equiv b(\mathrm{mod}\, m)$، آنگاه $a+c\equiv b+c\,(\mathrm{mod}\, m)$ و $ac\equiv bc\,(\mathrm{mod}\, m)$

ت) اگر $a\equiv b(\mathrm{mod}\, m)$، برای هر عدد طبیعی k، $a^k\equiv b^k(\mathrm{mod}\, m)$

نتیجه ۱-۲-۱-۱ فرض کنیم

$$p(x)=\sum_{k=0}^{n}c_k x^k$$

یک چند جمله ای با ضرایب صحیح باشد، در این صورت اگر $a\equiv b(\mathrm{mod}\, m)$، آنگاه $p(a)\equiv p(b)(\mathrm{mod}\, m)$.

قضیه ۱-۲-۱-۲ اگر $ca\equiv cb\,(\mathrm{mod}\, m)$ و $d=(c,m)$؛ که d بزرگترین مقسوم علیه c و m است؛ آنگاه $a\equiv b\,(\mathrm{mod}\,\frac{m}{d})$.

قضیه ۱-۲-۱-۳ هیچ چند جمله ای غیر ثابت $p(x)$ وجود ندارد، به طوری که برای تمام xهای صحیح $p(x)$ یک عدد اول باشد.

نتیجه ۱-۲-۱-۲ اگر $ca\equiv cb\,(\mathrm{mod}\, m)$و $(c,m)=1$؛ یعنی بزرگترین مقسوم علیه cو m، ۱ می باشد؛ آنگاه $a\equiv b(\mathrm{mod}\, m)$.

نتیجه ۱-۲-۱-۳ اگر $ca\equiv cb\,(\mathrm{mod}\, m)$، p عددی اول و $p|c$، آنگاه $a\equiv b\,(\mathrm{mod}\, p)$.

۱-۳ همنهشتی های چند جمله ای

تعریف ۱-۳-۱ اگر $f(x)$ یک چند جمله ای با ضرایب صحیح باشد، $f(x)\equiv 0(\mathrm{mod}\, m)$ را یک همنهشتی چند جمله ای و عدد صحیح a را یک جواب آن می نامیم، هر گاه $f(a)\equiv 0(\mathrm{mod}\, m)$.

بنا به نتیجه ۱-۲-۱-۱ اگر a یک جواب $f(x)\equiv 0(\mathrm{mod}\, m)$ و $a\equiv b(\mathrm{mod}\, m)$، آنگاه b نیز یک جواب همنهشتی $f(x)\equiv 0(\mathrm{mod}\, m)$ است. بنابراین طبیعی است که در معادله های همنهشتی به دنبال یافتن جواب های نا همنهشت (در صورت وجود) باشیم.

تعریف ۱-۳-۲ معادله همنهشتی $ax \equiv b \pmod{m}$ را یک معادله همنهشتی خطی می نامیم.

عدد صحیح $x_۰$ یک جواب معادله همنهشتی $ax \equiv b \pmod{m}$ است، اگر و تنها اگر $ax_۰ - b$ بر m بخشپذیر باشد، یا هم ارز آن، اگر وتنها اگر به ازای یک عدد صحیح $y_۰$، $ax_۰ - my_۰ = b$. پس مساله یافتن جواب های $ax \equiv b \pmod{m}$، هم ارز یافتن جواب های معادله سیاله $ax - my = b$ است.

قضیه ۱-۳-۱ همنهشتی $ax \equiv b \pmod{m}$ دارای جواب است، اگر و تنها اگر b بر d بخش پذیر باشد که در آن $d = (a,m)$. با برقراری این شرط، معادله دارای d جواب است که دو به دو به پیمانه m نا همنهشت هستند.

نتیجه ۱-۳-۱ اگر $(a,m) = ۱$، همنهشتی $ax \equiv b \pmod{m}$ دارای یک جواب منحصر به فرد به پیمانه m است.

مثال ۱-۳-۱ برای یافتن جواب های همنهشتی $۶x \equiv ۱۵ \pmod{۲۱}$، ابتدا توجه می کنیم که $(۶,۲۱) = ۳$ و ۱۵ بر ۳ بخش پذیر است. پس همنهشتی داده شده دارای جواب است و تعداد جواب های دو به دو نا هنمهشت آن برابر با ۳ است. اکنون کافی است جواب های معادله سیاله $۶x - ۲۱y = ۱۵$ را بیا بیم. به سادگی و با استفاده از الگوریتم تقسیم در می یابیم که $x_۰ = -۱۵$ و $y_۰ = -۵$ یک جواب معادله است. جواب های نا همنهشت عبارتند از:

$$-۱۵ ، -۱۵ + (\frac{۲۱}{۳}) ، -۱۵ + (\frac{۴۲}{۳}) \quad \text{یا} \quad -۱۵ ، -۸ ، -۱$$

پس از پرداختن به یک همنهشتی خطی، به حل یک دستگاه معادله های همنهشتی هم زمان زیر توجه می کنیم:

$$\begin{aligned} a_۱ x &\equiv b_۱ \pmod{m_۱} \\ a_۲ x &\equiv b_۲ \pmod{m_۲} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}$$

در ابتدا فرض می کنیم که پیمانه های m_n دو به دو متباین اند، بدیهی است که یک شرط لازم برای وجود جواب این دستگاه این است که هر معادله همنهشتی جواب داشته باشد. پس لازم است که برای هر n، اگر قرار دهیم $d_n=(a_n,m_n)$، b_n بر، d_n بخش پذیر باشد. اگر چنین شرطی برای هر n برقرار باشد، می توان d_n را از n امین همنهشتی حذف کرد تا این دستگاه جدید که با دستگاه داده شده جواب های یکسان دارد، بدست آید:

$$\begin{aligned} a'_1 &\equiv b'_1 \pmod{m'_1} \\ a'_2 &\equiv b'_2 \pmod{m'_2} \\ &\vdots \\ a'_n &\equiv b'_n \pmod{m'_n} \end{aligned}$$

در اینجا $m'_n=\frac{m_n}{d_n}$ و برای هر $i\neq j$، $(m'_i,m'_j)=1$. همچنین $(a'_i,m'_j)=1$.
در این صورت هر یک از معادله های همنهشتی داده شده به شکل زیر در می آید:

$$\begin{aligned} x &\equiv c_1 \pmod{m'_1} \\ x &\equiv c_2 \pmod{m'_2} \\ &\vdots \\ x &\equiv c_n \pmod{m'_n} \end{aligned}$$

بنابراین یافتن جواب های مساله به یافتن جواب های مشترک از نوع بالا منتهی می شود. برای مشاهده نکات بیشتر به مرجع [۳] مراجعه گردد.

قضیه۱-۳-۲ (قضیه باقیمانده چینی[۱]**)** فرض کنیم $n_1, n_2, \ldots, n_r$ عددهای صحیح مثبت دو به دو متباینی هستند یعنی به ازای $i\neq j$، $\gcd(n_i,n_j)=1$ در این صورت دستگاه همنهشتی های خطی $x\equiv a_1 \pmod{n_1}$، $x\equiv a_2 \pmod{n_2}$، ....، $x\equiv a_r \pmod{n_r}$ جوابی دارد که به پیمانه عدد صحیح $n_1 n_2 \cdots n_r$ یکتاست[۹].

مثال۱-۳-۲ دستگاه همنهشتی های خطی زیر را در نظر می گیریم:

$$x\equiv 1 \pmod 4,\ x\equiv 2 \pmod 3,\ \ldots,\ x\equiv 3 \pmod 5$$

۱

در ایـــــن حالـــــت، $m_1=4$، $m_2=3$، $m_3=5$. همچنـــــین $a_1=1$، $a_2=2$، $a_3=3$ پـــــس $m=4\times3\times5=60$ وازاین رو

$$M_1=\frac{60}{4}=15 ،M_2=\frac{60}{3}=20 ،M_3=\frac{60}{5}=12$$

اینک لازم است برای هر یک از همنهشتی های خطی زیر جوابی بیابیم:

$$15x\equiv1\pmod{m_1} ،20x\equiv1\pmod{m_2} ،12x\equiv1\pmod{m_3}$$

با استفاده ازالگوریتم تقسیم یا به هر روش دیگر، به ترتیب جواب های زیر بدست می آیند:

$$x_1=3 ،x_2=2 ،x_3=3$$

پس

$$\overline{x}=1\times15\times3+2\times20\times2+3\times12\times3=45+80+108=233$$

بنابراین با تقسیم ۲۳۳ بر ۶۰، کوچک ترین جواب دستگاه که ۵۳ است، بدست می آید. بقیه جواب ها به پیمانه ۶۰ با ۵۳ همنهشت اند؛ یعنی دستگاه به پیمانه ۶۰، دارای جواب یکتای ۵۳ است.

قضیه باقیمانده چینی، شرط کافی برای وجود جواب همزمان و همچنین روشی برای یافتن جـواب ارائه می دهد. می توان این قضیه را به شکلی تعمیم داد که به صورت اگر و تنها اگر باشـد. ابتـدا قضـیه زیر را بیان می نما ییم سپس تعمیم قضیه باقیمانده چینی را ارائه می دهیم.

قضیه۱-۳-۳ فرض کنیم

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$$

تجزیه متعارف m به حاصل ضرب اعداد اول باشد، در این صورت، $a\equiv b\pmod m$، اگر وتنهـا اگر برای هر $a=1,2,\dots,r$، $a\equiv b\pmod{p^{\alpha_r}}$.

قضیه۱-۳-۴ (قضیه باقیمانده چینی تعمیم یافته) فرض کنـیم m_1، m_2، ...، m_r اعـداد صـحیح مثبتی باشند، در این صورت دستگاه

$$x\equiv a_1\pmod{m_1} ،x\equiv a_2\pmod{m_2} ،\dots ،x\equiv a_r\pmod{m_r}$$

دارای جواب است اگر وتنها اگر برای هر $i \neq j$، $(n_i, n_j) | (a_i - a_j)$. چنانچه این شرط برقرار باشد، جواب کلی به پیمانه کوچکترین مضرب مشترک m_1، m_2، ...، m_r یکتاست.

مثال۱-۳-۲ دستگاه همنهشتی های $x \equiv 7 \pmod{40}$، $x \equiv 11 \pmod{36}$ را در نظر می گیریم. در این مثال $m_1 = 36$، $m_2 = 40$ و $d_{12} = (40, 36)$ و چون $a_2 - a_1 = 4$، $4|4$ و بنا به قضیه قبل، دستگاه دارای جواب است. حل این دستگاه، هم ارز حل دستگاه های

$$x \equiv 11 \pmod{2^2},\ x \equiv 11 \pmod{3^2},\ x \equiv 7 \pmod{2^3},\ x \equiv 7 \pmod{5}$$

است. حال کافی است سه دستگاه همزمان زیر را در نظر بگیریم :

$$x \equiv 11 \pmod{3^2},\ x \equiv 7 \pmod{2^3},\ x \equiv 7 \pmod{5}$$

که پیمانه های آن دو به دو متباین اند. ادامه حل با استفاده از قضیه باقیمانده چینی میسر است.

قضیه۱-۳-۵ (قضیه لاگرانژ) فرض کنیم p یک عدد اول و $f(x) = a_n x^n + \cdots + a_1 x + a_0$ یک چند جمله ای با ضرایب صحیح باشد که در آن یکی از a_i بر p بخش پذیر نیست، در این صورت همنهشتی $f(x) \equiv 0 \pmod{p}$ حداکثر n جواب ناهمنهشت دارد.

۱-۴ همنهشتی های چند جمله ای به پیمانه توانی از یک عدد اول

در این بخش به اختصار روش کلی حل همنهشتی های چند جمله ای را بیان می نماییم. در قضیه زیر خواهیم دید که چگونه حل همنهشتی های چند جمله ای به حل همنهشتی های چند جمله ای با پیمانه توانی از یک عدد اول تبدیل می شود.

قضیه۱-۴-۱ فرض کنیم تجزیه m به صورت $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ باشد، اگر $x \equiv c \pmod{m}$ جوابی برای همنهشتی چند جمله ای $f(x) \equiv 0 \pmod{m}$ باشد، آنگاه برای هر $1 \le i \le r$، $x \equiv c \pmod{p_i^{\alpha_i}}$ جوابی برای همنهشتی $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ است. به عکس، اگر به ازای $1 \le i \le r$، $x \equiv c_i \pmod{p_i^{\alpha_i}}$ جوابی برای همنهشتی، $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$

باشد، آنگاه فقط یک جواب بـرای همنهشـتی، $f(x)\equiv ۰ \pmod m$ وجـود دارد، بطوریکـه بـرای هـر $۱\le i\le r$، $c\equiv c_i \pmod{p_i^{\alpha_i}}$.

مثال۱-۴-۱ فرض کنیم $f(x)=x^۲+x+۱$ و $p=۳$ ، در این صورت $f(۱)\equiv ۰\pmod ۳$. در واقع هر جواب $f(x)\equiv ۰\pmod ۳$ با ۱ به پیمانه ۳ همنهشت است. از آنجا که $f'(x)=۲x+۱$، نتیجـه می گیریم که $f'(۱)\equiv ۰\pmod ۳$ و $f(۱)\equiv ۳\pmod{۳^۲}$ ؛ پس $f'(۱)\equiv ۰\pmod{۳^۲}$.

۱-۵ قانون تقابل درجه دوم

هدف اصلی این فصل، بررسی همنهشتی در جه دوم است. ابتدا مفاهیم مهم و اولیه بیان می گردد. سپس قانون تقابل درجه دوم را که یکی از اساسی ترین قضیه ها در بـازه همنهشـتی هـای درجـه دوم است، بیان می کنیم. در انتها نیز همنهشتی های درجه دوم به پیمانه یـک عـدد مرکـب را ارائـه دهـیم (برای توضیح بیشتر مرجع [۳] را مطالعه کنید).

ابتدا لازم است به دو مورد زیر توجه کنیم:

الف) فرض کنیم p یک عدداول فرد و $(a,p)=۱$، همنهشتی زیر را در نظر می گیریم:

$$ax^۲+bx+c\equiv ۰\pmod p \qquad (۱-۱)$$

از اینکه p فرداست، نتیجه می گیریم کـه $(۴a,p)=۱$؛ پـس همنهشـتی $(۱-۱)$ بـا همنهشـتی $۴a(ax^۲+bx+c)\equiv ۰\pmod p$ هم ارز است. با در نظر گرفتن برابری

$$۴a(ax^۲+bx+c)=(۲ax-b)^۲-(b^۲-۴ac)$$

همنهشتی زیر به دست می آید:

$$(۲ax-b)^۲\equiv (b^۲-۴ac)\pmod p$$

اینک قرار می دهیم $y=۲ax+b$ و $d=b^۲-۴ac$ همنهشتی زیر را خواهیم داشت:

$$y^۲\equiv d\pmod p \qquad (۲-۱)$$

چنانچه $x\equiv x_۰\pmod p$ یک جواب $(۱-۱)$ باشد،آنگاه

$$y \equiv 2ax_0 + b \pmod p$$

در (۱−۲) صدق می کند. به عکس، چنانچه $x \equiv x_0 \pmod p$ یک جواب (۱−۲) باشد، آنگاه با حل $2ax \equiv y_0 - b \pmod p$ یک جواب برای (۱−۱) به دست خواهد آمد. بدین ترتیب می توان نتیجه گرفت که حل همنهشتی (۱−۱) در نهایت به حل یک همنهشتی به شکل

$$y^2 \equiv A \pmod p$$

منتهی می شود.

ب) چنانچه m یک عدد طبیعی بزرگترازا و $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ تجزیه متعارف آن باشد، حل همنهشتی

$$ax^2 + bx + c \equiv 0 \pmod m$$

بنا به قضیه باقیمانده چینی، هم ارز حل دستگاه همنهشتی زیر است:

$$\begin{aligned} ax^2 + bx + c &\equiv 0 \pmod{p_1^{\alpha_1}} \\ ax^2 + bx + c &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ ax^2 + bx + c &\equiv 0 \pmod{p_k^{\alpha_k}} \end{aligned}$$

اما برای هر عدداول p برای حل همنهشتی

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

ابتدا لازم است که همنهشتی زیر حل شود:

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

از آنچه در (الف) و (ب) یاد آور شدیم، درمی یابیم که برای حل همنهشتی درجه دوم، نخست باید به همنهشتی هایی از نوع

$$x^2 \equiv a \pmod p \qquad (۱−۳)$$

که در آن p یک عدد فرد اول است، توجه کنیم. حالتی را که در آن $p = 2$، به سادگی می توان بررسی کرد و چنانچه $p \mid a$، تنها جواب همنهشتی $x^2 \equiv a \pmod p$ همان $x \equiv 0 \pmod p$ است. ازاین رو، پس ازاین فرض می کنیم که $p \nmid a$ و p یک عدداول فرد است. از طرفی، اگر x_0 یک جواب

(۱−۳) باشد، به سادگی دیده می شود که $p-x_{\cdot}$ نیز یک جواب آن است. اینک از قضیه لاگرانژ نتیجه می گیریم که همنهشتی (۱−۳) جواب ندارد یا این که دو جواب ناهمنهشت خواهد داشت.

۱-۶ همنهشتی های درجه دوم با پیمانه یک عدد مرکب

تا کنون همنهشتی های درجه دوم با پیمانه عدد اول فرد را مورد مطالعه قرار دادیم. در این بخش همنهشتی های به پیمانه هایی که لزوما یک عدداول نیستند، را ارائه می دهیم. در ابتدا حالتی را که پیمانه توانی از یک عدد اول فرداست، در نظر می گیریم.

قضیه۱-۶-۱ اگر n یک عدد طبیعی، p یک عدد فرد اول باشد و علاوه بر آن $(a,p)=۱$، آنگاه همنهشتی $x^{۲}\equiv a \pmod p$ دارای جواب است، اگر وتنها اگر $(\frac{a}{p})=۱$.

مثال۱-۶-۲ نخستین گام برای حل همنهشتی $x^{۲}\equiv ۲۳ \pmod{۷^{۲}}$ یافتن جوابی برای همنهشتی $x^{۲}\equiv ۲۳ \pmod ۷$ یا هم ارز آن $x^{۲}\equiv ۲ \pmod ۷$ است، $x_{\cdot}=۳$ یک جواب آشکاراین همنهشتی است. اما $x_{\cdot}^{۲}$ را می توان به صورت زیر نوشت:

$$۳^{۲}=۹=۲۳+(-۲)\times ۷$$

پس دراین حالت $a=۲۳, b=-۲$. در گام بعد y را چنان تعیین می کنیم که

$$۶y\equiv ۲ \pmod ۷$$

یعنی $۳y\equiv ۱ \pmod ۷$ یک جواب این همنهشتی $x_{\cdot}=۳$ است. جواب دیگر همنهشتی $x^{۲}\equiv ۲ \pmod ۷$ برابر ۴ است، که از طریق آن می توان جواب *11* را برای همنهشتی $x^{۲}\equiv ۲۳ \pmod ۷$ به دست آورد.

قضیه بعد در مورد حالتی است که پیمانه توانی از ۲ باشد.

قضیه۱-۶-۲ فرض کنیم a یک عدداول فرداست، دراین صورت:

الف) همنهشتی $x^۲ \equiv a \pmod{۲}$ همواره جواب دارد.

ب) همنهشتی $x^۲ \equiv a \pmod{۴}$ دارای جواب است، اگروتنها اگر $a \equiv ۱ \pmod{۴}$.

پ) برای $n \geq ۴$، همنهشتی $x^۲ \equiv a \pmod{۲^n}$ دارای جواب است، اگروتنها اگر $a \equiv ۱ \pmod{۸}$.

قضیه ۱-۶-۳ فرض کنیم n یک عدد طبیعی بزرگتراز۱ و $n = ۲^{k_۰} p_۱^{k_۱} p_۲^{k_۲} \ldots p_r^{k_r}$ تجزیه آن به حاصل ضرب اعداد اول متمایز باشد، اگر $(a, p) = ۱$، دراین صورت $x^۲ \equiv a \pmod{n}$ حل پذیر است، اگر و تنها اگر

الف) برای $l = ۱, ۲, \ldots, r$، $(\frac{a}{p_l}) = ۱$.

ب) اگر $۴ | n$، $a \equiv ۱ \pmod{۴}$ و اگر $۴ \nmid n$، $a \equiv ۱ \pmod{۸}$.

۱-۷ معادله های سیاله خطی

معادله های سیاله، معادله هایی با یک یا بیشتراز یک متغیر هستند که در جستجوی جواب های صحیح یا گویای آن هستیم. این معادله ها را معادله های دیوفانتی نیز می نامند. ساده ترین این معادله ها، معادله دیوفانتی خطی $ax + by = c$ است که می توان به کمک مفاهیم قبل، تمام جواب های آن را، در صورت وجود به دست آورد.

قضیه۱-۷-۱ معادله سیاله $ax + by = c$ که در آن دست کم یکی ازدو عدد صحیح a،b ناصفر است، دارای جواب است، اگروتنها اگر $(a,b) = ۱$. اگر $x_۰$،$y_۰$ در معادله صدق کنند تمام جواب ها از برابری زیر به دست می آیند:

$$x = x_۰ + \frac{b}{(a,b)} \times t, \quad y = y_۰ - \frac{a}{(a,b)} \times t$$

که درآن t یک عدد صحیح است.

نتیجه۱-۷-۱ اگر a،b اعداد طبیعی متباین باشند، آنگاه اعداد طبیعی u،v وجود دارند، بطوریکه $au-bv=1$.

نتیجه۱-۷-۲ اگر a،b عددهای طبیعی و متباین باشند و $n>ab$، آنگاه عددهای طبیعی x،y وجود دارند که $ax+by=n$.

مثال۱-۷-۱ برای حل معادله سیاله خطی $12x+5y=4$، ابتدا توجه می کنیم که $(12,5)=1$ و $1|4$، پس معادله داده شده دارای جواب است. به منظور یاقتن جوابی برای آن از الگوریتم اقلیدسی استفاده می کنیم:

$$12=2\times5+2 ، 5=2\times2+1$$

پس $1=5-2\times2=5-2(12-2\times5)=2\times12+5\times5$ ،

ازاین قرار، $12(-8)+5(20)=4$، یعنی $x_0=-8$ ،$y_0=20$ جوابی برای معادله $12x+5y=4$ است. تمام جواب ها، از برابری های زیر حاصل می گردند:

$$x=-8+5t ، y=20-12t$$

قضیه۱-۷-۲ اگر a_1، a_2، ...، a_n اعدادصحیح باشند و $(a_1,a_2,...,a_n)=1$، معادله سیاله

$$a_1x_1+a_2x_2+...+a_nx_n=b$$

دارای جواب است. مجموعه جواب ها نامتناهی است و می توان هر کدام را بر حسب $n-1$ متغیر بیان نمود.

نتیجه۱-۷-۳ معادله سیاله $a_1x_1+a_2x_2+...+a_nx_n=b$ دارای جواب است، اگروتنها اگر $(a_1,a_2,...,a_n)|b$ دراین صورت تعدادجواب ها نامتناهی است و هرکدام بر حسب $n-1$ متغیر بیان می شوند.