چکیده

در این مقاله، گراف جهت دار $\Gamma(n)$ را با مجموعه رئوس $H = \{0,1,...,n-1\}$ مطالعه می کنیم بطوری که یک یال جهت دار از a به b وجود دارد اگر $a^5 \equiv b \pmod{n}$ به ازای $a,b \in \{0,1,...,n-1\}$. همچنین دو زیر گراف $\Gamma_1(n)$ و $\Gamma_2(n)$ را معرفی می کنیم. فرض کنید $\Gamma_1(n)$ توسط رئوسی که نسبت به n اولند و $\Gamma_2(n)$ توسط رئوسی که نسبت به n اول نیستند، القا شوند. شرایط منظم بودن و نیم منظم بودن $\Gamma_1(n)$ را ارائه می دهیم. همچنین نشان می دهیم هر مؤلفه گراف جهت دار $\Gamma(n)$ دور است اگر و فقط اگر $5 \nmid \varphi(n)$ و n فاقد مربع کامل باشد. ما در اینجا فرمولی برای تعداد نقاط ثابت $\Gamma(n)$ ارائه می دهیم.

فهرست مطالب

پیشگفتار

فرض کنید $n \geq ۱$ و $H = \{۰,۱,...,n-۱\}$. گراف جهت دار $\Gamma(n)$ را با رئوس متعلق به H در نظر بگیرید به طوری که یک یال جهت دار از a به b وجود داشته باشد اگر و فقط اگر $a^۵ \equiv b \pmod{n}$. همچنین برخی روابط بین نظریه اعداد، نظریه گراف و نظریه گروه را که توسط [۶]، [۱۱]، [۱۴]، [۱۶]، [۱۸]، [۲۰] و [۲۱] بصورت گراف متناظر با رابطه همنهشتی $a^۲ \equiv b \pmod{n}$ و $a^۳ \equiv b \pmod{n}$ در نظر گرفته شده است، نشان می دهیم.

اگر $a_۱, a_۲, \ldots, a_t \in H$ دو بدو مجزا باشند و

$$a_۱^۵ \equiv a_۲ \pmod{n}, \quad a_۲^۵ \equiv a_۳ \pmod{n}, \ldots, a_t^۵ \equiv a_۱ \pmod{n}.$$

در این صورت $a_۱, a_۲, \ldots, a_t$ یک دور به طول t تشکیل می دهند. دوری به طول یک را نقطه ثابت گوییم. یک مؤلفه از گراف جهت دار $\Gamma(n)$، زیر گرافی است که در بین گراف های همبند گراف غیر جهت دار وابسته به $\Gamma(n)$ ماکزیمال باشد.

فرض کنید $a \in H$. تعداد یال های جهت دار وارد شده به رأس a را درجه ورودی رأس a گوئیم و با $indeg(a)$ نمایش می دهیم و تعداد یال های جهت دار خارج شده از رأس a را درجه خروجی رأس a گوئیم و با $outdeg(a)$ نمایش می دهیم. درجه خروجی هر رأس $\Gamma(n)$ برابر با یک است. لذا تعداد مؤلفه های $\Gamma(n)$ با تعداد دورها برابر است.

دو زیر گراف برای $\Gamma(n)$ معرفی می کنیم. فرض کنید $\Gamma_۱(n)$ توسط رئوسی که نسبت به n اولند و $\Gamma_۲(n)$ توسط رئوسی که نسبت به n اول نیستند، القا می شوند. واضح است که $\Gamma_۱(n)$ و $\Gamma_۲(n)$ مجزا هستند و $\Gamma(n) = \Gamma_۱(n) \cup \Gamma_۲(n)$. گراف جهت دار را منظم گوییم اگر درجه ورودی هر رأس یک باشد. یک گراف جهت دار را نیم منظم گوییم اگر عدد صحیح مثبت d وجود داشته باشد به طوری که درجه ورودی هر رأس یا d یا 0 باشد. شرایط منظم بودن و نیم منظم بودن زیر گراف $\Gamma_۱(n)$ داده شده اند. همچنین نشان داده شده است که هر مؤلفه گراف جهت دار $\Gamma(n)$ دور است اگر و فقط اگر $۵ \nmid \varphi(n)$ و n فاقد مربع کامل باشد. در آخر فرمولی برای تعداد نقاط ثابت $\Gamma(n)$ ارائه می دهیم.

فصل اول

مقدمات و پیشنیازها

1-1 مقدمه‌ای بر نظریه گراف

در این فصل به بیان تعاریف ونتایج مقدماتی می‌پردازیم که در فصل‌های بعد مورد استفاده قرار خواهند گرفت.

مطالبی چند بر گراف ها

تعریف 1-1-1 گراف (یا **گراف بدون جهت**) G از دو مجموعه زیر تشکیل می شود: مجموعه V متشکل از **رأس ها** (یا **گره ها**) و مجموعه E متشکل از **یال ها** (یا **قوس ها**) به طوری که هر یال $e \in E$ متناظر با زوج نامرتبی از رأس هاست. اگر متناظر با رأس های v و w، یال منحصر بفرد e وجود داشته باشد می نویسیم $e = (v,w)$. در این مقاله، منظور از (v,w) یال بین v و w در یک گراف بدون جهت است و نه زوج مرتب.

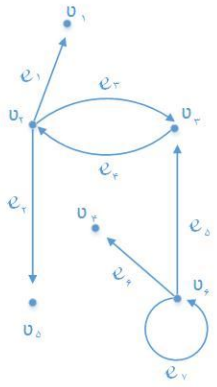
تعریف 1-1-2 گراف جهت دار (یا **دایگراف**) از دو مجموعه زیر تشکیل می شود: مجموعه V متشکل از **رأس ها** (یا **گره ها**) و مجموعه E متشکل از **یال ها** (یا **قوس ها**) به طوری که هر یال $e \in E$ متناظر با زوج مرتبی از رأس هاست. اگر متناظر با زوج مرتب (v,w) از رأس های v و w، یال منحصر بفرد e وجود داشته باشد می نویسیم $e = (v,w)$ که یالی از v به w را نمایش می دهد.

یال e در یک گراف (بدون جهت یا جهت دار) که متناظر با زوج رأس های v و w باشد، روی v و w بنا شده است و گفته می شود رأس های v و w روی یال e قرار دارند و **رأس های مجاور** نام دارند.

اگر گراف (بدون جهت یا جهت دار) G با مجموعه رأس های V و مجموعه یال های E باشد می نویسیم $G = (V, E)$.

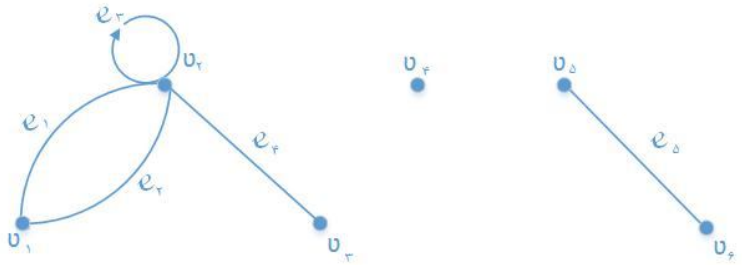
بنا به قرارداد، مجموعه های E و V متناهی هستند و V نیز ناتهی است مگر آن که خلاف آن به صراحت بیان شده باشد.

مثال 1-1-3 یک گراف جهت دار در شکل 1-1-1 نشان داده شده است. یال های جهت دار با پیکان مشخص شده اند. یال e_1 متناظر با زوج مرتب (v_2,v_1) و یال e_7 متناظر با زوج مرتب (v_4,v_4) از رأس هاست. یال e_1 با (v_2,v_1) و یال e_7 با (v_4,v_4) نمایش داده می شود.



شکل 1-1-1

تعریف 1-1-1 اجازه می دهد یال های متمایز، متناظر با زوج های یکسانی از رئوس باشند. برای مثال در شکل 1-1-2 یال های e_1 و e_2 هر دو متناظر با زوج رأس $\{v_1,v_2\}$ هستند. به این یال ها، **یال های موازی** می گویند. یالی که تنها از یک رأس ایجاد شده باشد **حلقه** نام دارد. برای مثال، در شکل 1-1-2 یال $e_3=(v_2,v_2)$ یک حلقه است. یک رأس نظیر رأس v_4 در شکل 1-1-2 که متعلق به هیچ یالی نباشد **رأس تنها** یا **رأس منفرد** نامیده می شود.



شکل 1-1-2

تعریف 1-1-4 گراف ساده، گرافی است که حلقه یا یال های موازی نداشته باشد.

تعریف 1-1-5 فرض کنید v_0 و n دو رأس یک گراف هستند. یک مسیر از v_0 به v_n به طول

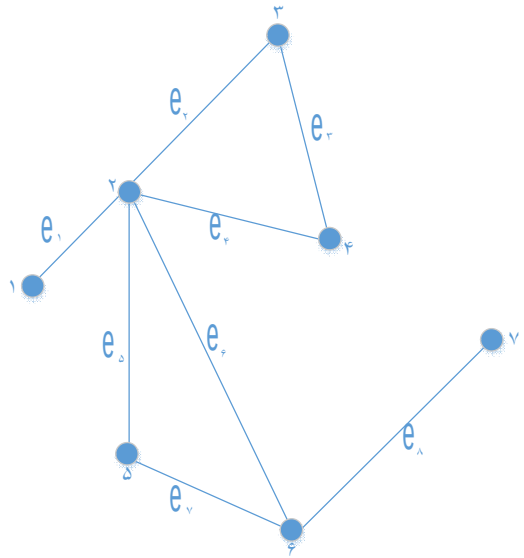
$n+1$، دنباله ای از $n+1$ رأس دو به دو متفاوت و n یال است که از رأس v_0 شروع و با رأس v_n پایان می رسد:

$$(v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n),$$

که در آن، یال e_i به ازای $i = 1, \ldots, n$، روی رأس های v_{i-1} و v_i بنا شده است.

صورت گرایی تعریف 1-1-5 به این معنی است که: از رأس v_0 شروع کنید، در امتداد یال e_1 به v_1 حرکت کنید، در امتداد یال e_2 به v_2 بروید و همین طور تا آخر.

مثال 1-1-6 در گراف شکل 1-1-3، $(1, e_1, 2, e_2, 3, e_3, 4, e_4, 2)$ مسیری از رأس 1 به رأس 2 به طول 4 است.



شکل 1-1-3

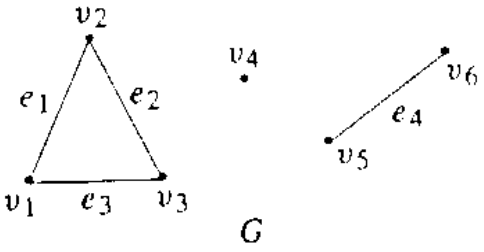
گراف همبند، گرافی است که در آن، در یک مسیر از هر رأس می توانیم به هر رأس دیگر برویم. تعریف رسمی آن بصورت زیر است:

تعریف 1-1-7 گراف G، **همبند** است اگر برای هر دو رأس v و w در G یک مسیر از v به w وجود داشته باشد.

مثال 1-1-8 گراف شکل 1-1-3 همبند است زیرا برای هر دو رأس v و w در G، یک مسیر از v به w وجود دارد.

مثال 1-1-9 گراف شکل 1-1-4 همبند نیست زیرا برای مثال، هیچ مسیری از رأس v_2 به رأس v_5

وجود ندارد.



شکل 1-1-4

گراف همبند از یک "قطعه" تشکیل شده است حال آن که گرافی که همبند نیست از دو یا چند قطعه تشکیل شده است. این "قطعه" ها ، **زیر گراف های** مسیر اصلی هستند که **مؤلفه ها** یا **اجزای گراف** نامیده می شوند.

تعاریف رسمی را با زیر گراف شروع می کنیم.

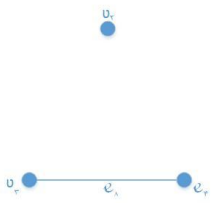
زیر گراف G' از گراف G با انتخاب یال ها و رأس های معینی از G به دست می آید با این شرط که اگر یال e در G را انتخاب کنیم که روی رأس های v و w بنا شده باشد باید v و w را در G' قرار دهیم. این شرط تضمین می کند که G' واقعاً یک گراف است. تعریف رسمی آن بصورت زیر است:

تعریف 1-1-10 فرض کنید $G=(V,E)$ یک گراف باشد. (V',E') یک **زیر گراف** از G است اگر:

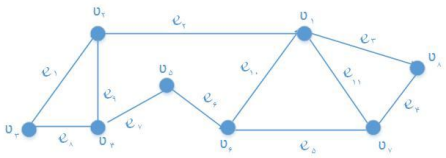
(الف) $V'\subseteq V$ و $E'\subseteq E$ باشند.

(ب) برای هر یال $e'\in E'$، اگر e' روی v' و w' بنا شده باشد آنگاه $v',w'\in V'$ خواهند بود.

مثال 1-1-11 گراف $G'=(V',E')$ از شکل 1-1-5، زیر گرافِ گراف $G=(V,E)$ از شکل 1-1-6 است زیرا $V'\subseteq V$ و $E'\subseteq E$ هستند.



شکل 1-1-5



شکل 1-1-6

تعریف 1-1-12 فرض کنید G یک گراف و v یک رأس آن باشد. زیر گراف G' از G متشکل از تمام یال ها و رأس های موجود در G است که در یک مسیر با شروع از v قرار دارد و **مؤلفه** حاوی v نام دارد.

مثال 1-1-13 گراف G از شکل 1-1-3 یک مؤلفه دارد که خودش است. در واقع یک گراف همبند است اگر و فقط اگر تنها یک مؤلفه داشته باشد.

تعریف 1-1-14 یک **مؤلفه** از گراف جهت دار G، زیر گرافی است که در بین گراف های همبند گراف غیر جهت دار وابسته به G ماکزیمال باشد.

تعریف 1-1-15 فرض کنید v و w دو رأس گراف G باشند. **مسیر ساده** از v به w، مسیری است که هیچ رأس تکراری نداشته باشد.

تعریف 1-1-16 دور (مدار)، مسیری با طول ناصفر از v به v است که هیچ یال تکراری نداشته باشد.

تعریف 1-1-17 دور ساده، دوری از v به v است که در آن، صرف نظر از رأس های شروع و پایان که هر دو برابر v هستند هیچ رأس تکراری وجود نداشته باشد.

تعریف 1-1-18 دوری به طول 1 را **نقطه ثابت** گوئیم.

تعریف 1-1-19 دوری در گراف G که شامل تمام یال ها و تمام رأس های گراف G باشد **دور اویلری** نامیده می شود.

تعریف 1-1-20 درجه رأس v را که با $\delta(v)$ نشان می دهیم برابر است با تعداد یال هایی است که با v تلاقی دارند (بنا به تعریف، درجه v که به صورت یک حلقه باشد برابر 2 است).

تعریف 1-1-21 فرض کنید $v \in V$. تعداد یال های جهت دار وارد شده به رأس v را **درجه ورودی** رأس v گوئیم و با $indeg(v)$ نمایش می دهیم و تعداد یال های جهت دار خارج شده از رأس v را **درجه خروجی** رأس v گوئیم و با $outdeg(v)$ نمایش می دهیم.

قضیه 1-1-22 اگر گراف G دور اویلری داشته باشد آن گاه G همبند است و درجه هر رأس آن، زوج است.

اثبات. ر.ک. [1، قضیه 6-2-17].□

قضیه 1-1-23 اگر G گراف همبند و درجه هر رأس آن، زوج باشد آن گاه G دور اویلری دارد.

اثبات. ر.ک. [1، قضیه 6-2-18].□

قضیه 1-1-24 اگر G گرافی با m یال و رأس های $\{v_1, v_2, ..., v_n\}$ باشد آن گاه:

$$\sum_{i=1}^{n} \delta(v_i) = 2m$$

در حالت خاص، مجموع درجهٔ تمام رأس های یک گراف، زوج است.

اثبات. ر.ک. [1، قضیه 6-2-21].□

نتیجه 1-1-25 در هر گراف، تعداد رأس هایی که درجه فرد دارند زوج است.

اثبات. ر.ک. [1، نتیجه 6-2-22].□

قضیه 1-1-26 گرافی مسیری از v به w ($v \neq w$) بدون یال های تکراری، حاوی تمام یال ها و رأس هاست اگر و فقط اگر همبند و v و w تنها رأس های با درجهٔ فرد باشند.

اثبات. ر.ک. [1، قضیه 6-2-23].□

مطالبی چند بر درخت ها

تعریف 1-1-27 درخت (آزاد) T، گراف ساده ای است که در شرط زیر صدق کند:

اگر v و w دو رأس T باشند آن گاه مسیر سادهٔ منحصر به فردی از v به w در آن وجود داشته باشد.

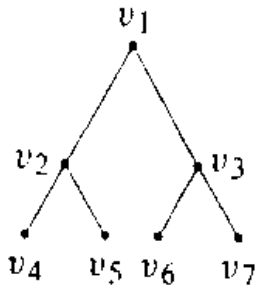
تعریف 1-1-28 درخت ریشه دار، درختی است که دارای رأس خاصی به نام ریشه باشد.

از آنجا که مسیر ساده از ریشه به هر رأس مفروض، منحصر به فرد است از این رو هر رأس دارای رتبه ای است که به صورت منحصر به فردی تعیین می شود. رتبه ریشه را **رتبه صفر** می نامیم. رأس هایی که زیر ریشه قرار دارند در رتبه یک قرار دارند و همین طور تا آخر.

تعریف 1-1-29 رتبه رأس v، طول مسیر ساده ای از ریشه به v است.

تعریف 1-1-30 ارتفاع درخت ریشه دار، بزرگترین شماره رتبه موجود درخت است.

مثال 1-1-31 رأس های $v_7, v_6, v_5, v_4, v_3, v_2, v_1$ در درخت ریشه دار شکل 1-1-7 به ترتیب در رتبه های ۲،۲،۲،۲،۱،۱،۰ قرار دارند. ارتفاع این درخت، 2 است.



شکل 1-1-7

تعریف 1-1-32 گرافی که هیچ دوری نداشته باشد **گراف بدون دور** نام دارد.

قضیه 1-1-33 فرض کنید T گرافی با n رأس است. گزاره های زیر هم ارزند.

(i) T یک درخت است.

(ii) T همبند است و بدون دور است.

(iii) T همبند است و $n-1$ یال دارد.

(iv) T بدون دور است و $n-1$ یال دارد.

اثبات. ر.ک. [1، قضیه 7-2-3].□

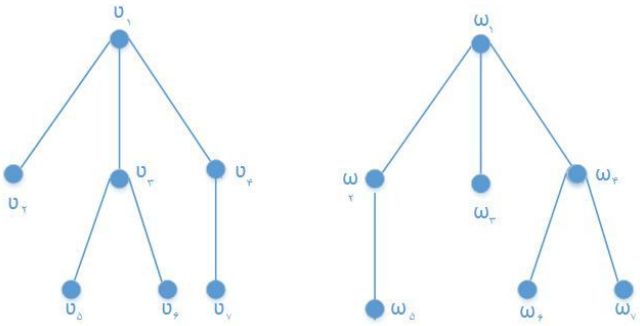
تعریف 1-1-34 فرض کنید T_1 درختی ریشه دار با ریشه r_1 و T_2 درختی ریشه دار با ریشه r_2 باشد، درخت های ریشه دار T_1 و T_2 یک ریخت هستند اگر تابع یک به یک و پوشای f از مجموعهٔ رئوس T_1 به مجموعهٔ رئوس T_2 وجود داشته باشد که در شرایط زیر صدق می کند:

(i) رأس های v_i و v_j در T_1 مجاور هستند اگر و فقط اگر رأس های $f(v_i)$ و $f(v_j)$ در T_2 مجاور باشند.

(ii) $f(r_1)=r_2$.

تابع f، **یک ریختی** نامیده می شود.

مثال درخت های ریشه دار T_1 و T_2 شکل 1-1-8 یک ریخت هستند.



شکل 1-1-8

یک ریختی این درخت ها به صورت زیر است:

$$f(v_1)=w_1,\quad f(v_2)=w_3,\quad f(v_3)=w_4,\quad f(v_4)=w_2,$$
$$f(v_5)=w_7,\quad f(v_6)=w_6,\quad f(v_7)=w_5.$$

2-1 مقدمه‌ای بر نظریه اعداد

تعریف 1-2-1 m عددی طبیعی است. اگر a و b دو عدد صحیح باشند به طوری که $m \mid a-b$، می گوییم a **همنهشت** b **به هنگ** m است و می نویسیم $a \equiv b \pmod m$. همچنین وقتی $m \nmid a-b$ گوییم a ناهمنهشت b به هنگ m است و می نویسیم $a \not\equiv b \pmod m$.

عبارت $a \equiv b \pmod m$ را همنهشتی یا همنهشتی به هنگ m می گویند و m را هنگ این همنهشتی می نامند.

قضیه 1-2-2 اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$ آنگاه

$$a+c \equiv b+d \pmod m, \qquad ac \equiv bd \pmod m.$$

اثبات. ر.ک. [2، قضیه 2-5].□

قضیه 1-2-3 اگر $a \equiv b \pmod{m}$ آنگاه به ازای هر عدد صحیح c،

$$a+c \equiv b+c \pmod{m}, \qquad ac \equiv bc \pmod{m}.$$

اثبات. ر.ک. [2، قضیه 2-6].□

قضیه 1-2-4 k عددی طبیعی دلخواه است. اگر به ازای هر k و $i = ۱،۲,\cdots$، $a_i \equiv b_i \pmod{m}$ آنگاه

الف) $$\sum_{i=۱}^{k} a_i \equiv \sum_{i=۱}^{k} b_i \pmod{m}$$

ب) $$\prod_{i=۱}^{k} a_i \equiv \prod_{i=۱}^{k} b_i \pmod{m}$$

اثبات. ر.ک. [2، قضیه 2-7].□

قضیه 1-2-5 اگر $a \equiv b \pmod{m}$ آنگاه به ازای هر عدد طبیعی k، $a^k \equiv b^k \pmod{m}$.

اثبات. ر.ک. [2، قضیه 2-8].□

قضیه 1-2-6 اگر $d > ۰$، $a \equiv b \pmod{m}$ اگرو تنها اگر $ad \equiv bd \pmod{m}$.

اثبات. ر.ک. [2، قضیه 2-10].□

قضیه 1-2-7 اگر $a+c \equiv b+c \pmod{m}$ آنگاه $a \equiv b \pmod{m}$.

اثبات. ر.ک. [2، قضیه 2-11].□

قضیه 1-2-8 اگر $ab \equiv ac \pmod{m}$ و $d = (a,m)$ آنگاه $b \equiv c \pmod{m/d}$.

اثبات. ر.ک. [2، قضیه 2-12].□

قضیه 1-2-9 اگر $ab \equiv ac \pmod{m}$ و $(a,m) = ۱$، آنگاه $b \equiv c \pmod{m}$.

اثبات. ر.ک. [2، قضیه 2-13].□

قضیه 1-2-10 فرض کنیم m_i $(i = ۱،۲،\cdots,k)$ عددی طبیعی باشد، شرط لازم و کافی برای اینکه $a \equiv b \pmod{m_i}$ آن است که $a \equiv b \pmod{[m_۱,...,m_k]}$.

اثبات. ر.ک. [2، قضیه 2-14].□

قضیه 1-2-11 (قضیه اویلر) اگر $(a,m) = ۱$، آنگاه $a^{\varphi(m)} \equiv ۱ \pmod{m}$.

اثبات. ر.ک. [2، قضیه 2-35].□

قضیه 1-2-12 (قضیه فرما) اگر p عددی اول باشد و $p \nmid a$، آنگاه $a^{\varphi(p-۱)} \equiv ۱ \pmod{p}$.

اثبات. ر.ک. [2، قضیه 2-36].□

قضیه 1-2-13 اگر p عددی اول باشد، آنگاه به ازای هر عدد صحیح a، $a^p \equiv a \pmod{p}$.

اثبات. ر.ک. [2، قضیه 2-37].□

تعریف 1-2-14 اگر $(a,m) = ۱$، در این صورت کوچکترین عدد طبیعی r که $a^r \equiv ۱ \pmod{m}$، را مرتبه a به هنگ m می گویند.

به ازای هر عدد صحیح a که $(a,m) = ۱$، مرتبه a به هنگ m مقسوم علیه $\varphi(m)$ است.

قضیه 1-2-15 (قضیه باقیمانده چینی) فرض کنید $n_1, n_2, ..., n_k$ اعداد صحیح مثبت باشند به طوری که دو به دو نسبت به هم اولند. در این صورت برای هر دنباله از اعداد صحیح $a_1, a_2, ..., a_k$، عدد صحیح x وجود دارد به طوری که همزمان جواب همنهشتی های زیر است:

$$x \equiv a_1 \pmod{n_1},$$

$$x \equiv a_2 \pmod{n_2},$$

$$\vdots$$

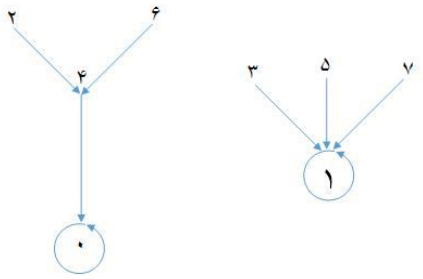
$$x \equiv a_k \pmod{n_k}.$$

علاوه بر این، تمام جواب های x از این سیستم به پیمانه $N = n_1 n_2 \dots n_k$ همنهشت هستند.
لذا $x \equiv y \pmod{n_i}$ به ازای $1 \le i \le k$، اگر و تنها اگر $x \equiv y \pmod{N}$.
اثبات. **ر.ک.** [3، قضیه 4-5]. □

فصل دوم

2-1 گراف جهت دار مکرر

تعریف 2-1-1 گراف جهت دار $\Gamma(n)$ را با رئوس متعلق به مجموعه $H = \{0,1,...,n-1\}$ **گراف جهت دار مکرر** می نامیم به طوری که دقیقاً یک یال جهت دار از $a \in H$ به $b \in H$ وجود دارد اگر و فقط اگر $a^2 \equiv b \pmod{n}$.



شکل 2-2-1 (گراف $\Gamma(8)$)

فرض کنید $a_1, a_2, \ldots, a_t \in H$ دو بدو مجزا باشند و

$$a_1^2 \equiv a_2 \pmod{n},$$

$$a_2^2 \equiv a_3 \pmod{n},$$

$$\vdots$$

$$a_t^2 \equiv a_1 \pmod{n}.$$

در این صورت $a_1, a_2, \ldots, a_t$ یک دور به طول t تشکیل می دهند. دوری به طول t را یک **t- دور** گوئیم که بر خلاف جهت حرکت ساعت می باشد.

فرض کنید $a \in H = \{0,1,...,n-1\}$ رأس دلخواه باشد. در این صورت همواره $\text{indeg}(a) \geq 0$ و $\text{outdeg}(a) = 1$. همچنین برای هر نقطه ثابت مجزا، درجه ورودی و خروجی هر دو برابر 1 است.

از آنجا که درجه خروجی هر رأس گراف $\Gamma(n)$، یک می باشد لذا تعداد مؤلفه های $\Gamma(n)$ با تعداد

دورها برابر است. دورها ممکن است مجزا باشند یا نباشند.

فرض کنید $N_n(a)$ تعداد جواب های ناسازگار همنهشتی $x^2 \equiv a \pmod n$ باشد. در این صورت واضح است که $N_n(a)=\text{indeg}(a)$.

تعریف 2-1-2 فرض کنید $x^2 \equiv y \pmod n$. در این صورت گوییم x به y توسط $f(x) \equiv x^2 \pmod n$ نگاشته می شود.

تعریف 2-1-3 فرض کنید تجزیه n به حاصل ضرب عوامل اول را به فرم

$$n = \prod_{i=1}^{s} p_i^{k_i} \qquad (1,2)$$

نمایش دهیم که در آن $p_1 < p_2 < ... < p_s$ اعداد اول و $k_i > 0$. اگر $\omega(n)$ تعداد اعداد اول مجزای موجود در تجزیه n باشد آن گاه $s = \omega(n)$.

د و قضیه زیر در {23} توسط شالای ثابت شده اند.

قضیه 2-1-4 (szalay) تعداد نقاط ثابت گراف $\Gamma(n)$ برابر است با $2^{\omega(n)}$.

تعریف 2-1-5 گراف $\Gamma(n)$ را **متقارن** گوییم اگر مجموعه مؤلفه های آن به دو مجموعه افراز شود به طوری که بین این دو مجموعه یک تابع دوسویی وجود داشته باشد و گراف های متناظرشان یکریخت باشند.

قضیه 2-1-6 (szalay) گراف مکرر $\Gamma(n)$، متقارن است اگر $n \equiv 2 \pmod 4$ یا $n \equiv 4 \pmod 8$.

توجه کنید که قضیه بالا شرط کافی برای تقارن گراف $\Gamma(n)$ را ارائه می دهد و نه شرط لازم را.

2-2 ساختار گراف های مکرر

قضیه 2-2-1 عدد 0 نقطه ثابت مجزای $\Gamma(n)$ است اگر و فقط اگر n فاقد مربع کامل باشد.

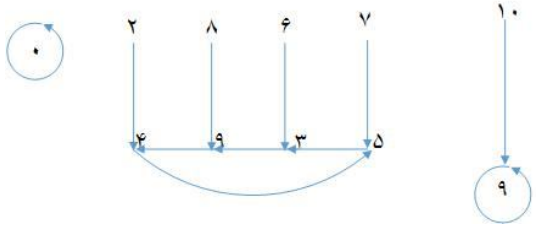
اثبات. اگر $p^2 \mid n$ به ازای عدد اول p، آنگاه

$$\left(\frac{n}{p}\right)^2 = n.\frac{n}{p^2} \equiv 0 \pmod n,$$

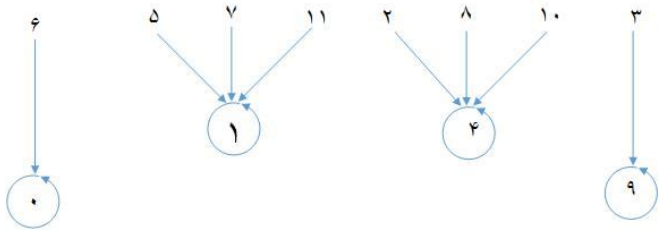
چون $\frac{n}{p}$ به 0 نگاشته می شود، 0 نقطه ثابت مجزا نمی باشد.

برعکس، فرض کنید n فاقد مربع کامل باشد. در این صورت بدیهی است که $x \equiv 0 \pmod{n}$ تنها جواب همنهشتی $x^2 \equiv 0 \pmod{n}$ می باشد. بنابراین 0 نقطه ثابت مجزای $\Gamma(n)$ است. □

همانطور که در شکل زیر نشان داده شده، 0 نقطه ثابت مجزای گراف $\Gamma(11)$ و نقطه ثابت غیرمجزای گراف $\Gamma(12)$ می باشد.



شکل 2-2-2



شکل 2-2-3

قضیه 2-2-2 در گراف $\Gamma(n)$ دور مجزا با طول بیشتر از 1 وجود ندارد. گراف $\Gamma(n)$ نقطه ثابت مجزای $a \neq 0$ دارد اگر و فقط اگر $2 \mid n$ و n فاقد مربع کامل باشد. در این حالت $a = \frac{n}{2}$.

اثبات. فرض کنید $a \neq 0$ قسمتی از دور مجزای $\Gamma(n)$ باشد. ابتدا نشان می دهیم n عدد صحیح زوجی است که فاقد مربع کامل باشد. سپس ثابت می کنیم $a = \frac{n}{2}$ و a نقطه ثابت است. فرض کنید $b^2 \equiv a \pmod{n}$. از آنجا که $(-b)^2 \equiv b^2 \pmod{n}$ و $N_n(a) = \text{indeg}(a) = 1$، لذا $-b \equiv b \pmod{n}$. در نتیجه $2b \equiv 0 \pmod{n}$. چون $a \neq 0 \pmod{n}$، لذا $2 \mid n$ و $b \equiv \frac{n}{2} \pmod{n}$.

حال فرض کنید $p^2 \mid n$ به ازای عدد اول p. اگر $p = 2$، آنگاه $a \equiv (\frac{n}{2})^2 \equiv 0 \pmod{n}$ که تناقض است. سپس فرض کنید p عدد اول فرد و $2 \| n$. توجه کنید اگر m عدد صحیح فرد باشد، آنگاه

$$\frac{n}{2}m \equiv \frac{n}{2} \pmod{n}. \qquad (2,1)$$

چون $\frac{n}{2}$ فرد است، نتیجه می شود که

$$a \equiv \frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \equiv \frac{n}{2}\frac{n}{2p^2} \equiv \frac{n}{(2p)^2} \pmod{n},$$

که در تضاد با فرض $N_n(a) = 1$ است. بنابراین n فاقد مربع کامل می باشد. بنا به رابطه (2,1) مشاهده می کنیم که

$$a \equiv b^2 \equiv \frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \pmod{n}. \qquad (2,2)$$

در نتیجه $a \equiv \frac{n}{2} \pmod{n}$ و a نقطه ثابت گراف $\Gamma(n)$ است.

اکنون فرض کنید $2|n$ و n فاقد مربع کامل باشد. در این صورت $\frac{n}{2}$ فرد است و $\frac{n}{2} \not\equiv 0 \pmod{n}$. با توجه به (2,1) و (2,2) می توان نتیجه گرفت که

$$\frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \pmod{n}, \qquad (2,3)$$

و $\frac{n}{2}$ نقطه ثابت گراف $\Gamma(n)$ است. فرض کنید $b^2 \equiv \frac{n}{2} \pmod{n}$. چون $\frac{n}{2}$ فرد و n زوج است، لذا $b \equiv 1 \pmod{2}$. از آنجا که $\frac{n}{2}$ فاقد مربع کامل است و $\frac{n}{2}|n$، براحتی می توان نتیجه گرفت $b \equiv 0 \pmod{\frac{n}{2}}$. توجه کنید $\gcd(2, \frac{n}{2}) = 1$. از اینرو بنا به قضیه باقیمانده چینی، b به پیمانه n منحصر به فرد است و با توجه به (2,3)، $b \equiv \frac{n}{2} \pmod{n}$. لذا $\frac{n}{2}$ نقطه ثابت مجزای گراف $\Gamma(n)$ و اثبات کامل است. □

تنیجه زیر از قضایای 2-2-1 و 2-2-2 پیروی می کند.

نتیجه 2-2-3 هر گراف $\Gamma(n)$، حداکثر دو نقطه ثابت مجزا دارد. همچنین $\Gamma(n)$ دقیقاً دو نقطه ثابت مجزا دارد اگر و فقط اگر $2|n$ و n فاقد مربع کامل باشد. در این حالت 0 و $\frac{n}{2}$ تنها نقاط ثابت مجزا هستند.

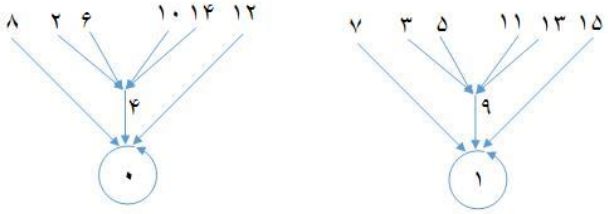
اثبات. با توجه به دو قضیه قبل، اثبات واضح است. □

تعریف 2-2-4 گراف جهت دار را **منظم** گوییم اگر درجه ورودی هر رأس یک باشد. (یا درجه همه رئوس برابر باشد)

هر مؤلفه گراف جهت دار یک دور است.

تعریف 2-2-5 گراف جهت دار را **نیم منظم** گوییم اگر عدد صحیح مثبت d وجود داشته باشد به طوری که درجه ورودی هر رأس یا d یا 0 باشد.

مثال 2-2-6 گراف $\Gamma(۱۶)$ را به ازای $d = ۴$ در شکل زیر ببینید.



شکل 2-2-4

برای عدد صحیح n، $\varepsilon(n)$ را بصورت زیر را تعریف می کنیم:

$$\varepsilon(n)=\begin{cases} -۱ & ۲\| n \\ 0 & ۲\nmid n \text{ یا } ۴\| n \\ ۱ & ۸\mid n. \end{cases} \qquad (2,4)$$

قضیه 2-2-7 گراف جهت دار $\Gamma_{۱}(n)$ به ازای هر عدد صحیح مثبت n، نیم منظم است. علاوه بر این، درجه ورودی هر رأس $\Gamma_{۱}(n)$ یا برابر 0 یا $۲^{\omega(n)+\varepsilon(n)}$ می باشد.

اگر $n \geq ۲$، آن گاه $\Gamma_{۲}(n)$ نیم منظم است اگر و فقط اگر $n = p^k$ به ازای عدد اول فرد p و $k \in \{۱،۲\}$ یا $n = ۲^k$ به ازای $k \in \{۱،۲،۳،۴،۶\}$.

گراف $\Gamma(n)$ نیم منظم است اگر و فقط اگر $n = ۲^k$ به ازای $k \in \{۰،۱،۲،۴\}$.

قبل از اثبات قضیه، لم زیر را ثابت می کنیم.

لم 2-2-8 اگر $\gcd(a,n) = ۱$ و $N_n(a) > 0$، آن گاه $N_n(a) = ۲^{\omega(n)+\varepsilon(n)}$.

اثبات در حالتی که $n = ۱$، نتیجه واضح است. بنابراین فرض می کنیم $n > ۱$. از آن جایی که عناصری که نسبت به n اولند، یک گروه ضربی به پیمانه n تشکیل می دهند، به راحتی می توان دید اگر

$\gcd(a,n)=1$ و $N_n(a)>0$، $N_n(a)=N_n(1)$. لذا کافی است $N_n(1)$ را مشخص کنیم.

ابتدا $N_{p^k}(1)$ را به ازای عدد اول p و $k \geq 1$ پیدا می کنیم. توجه کنید

$$a^2 \equiv 1 \pmod{p^k} \qquad (2,5)$$

اگر و فقط اگر

$$a^2 - 1 \equiv (a+1)(a-1) \equiv 0 \pmod{p^k}. \qquad (2,6)$$

فرض کنید p عدد اول فرد باشد. چون $\gcd(a+1,a-1) \mid 2$، رابطه (2,5) برقرار است اگر و فقط اگر $a \equiv \pm 1 \pmod{p^k}$. بنابراین $N_{p^k}(1)=2$.

فرض کنید $p=2$. توجه کنید اگر (2,6) برقرار باشد، آن گاه 4 دقیقاً یکی از جملات $a+1$ و $a-1$ را عاد می کند و 2 جمله دیگر را عاد می کند. از این رو (2,5) برقرار است اگر و فقط اگر $a \equiv 1 \pmod{2}$ به ازای $1 \leq k \leq 3$ و $a \equiv \pm 1 \pmod{2^{k-1}}$ به ازای $k \geq 4$. بنابراین $N_{2^k}(1)=2^{1+\varepsilon(2^k)}$. نتیجه بنا به رابطه (2,4) و قضیه باقیمانده چینی بدست می آید. □

اثبات قضیه 2-2-7 از لم قبل نتیجه می شود اگر $a \in \Gamma_1(n)$ و $N_n(a)>0$، آن گاه

$$\text{indeg}(a) = N_n(a) = 2^{\omega(n)+\varepsilon(n)}. \qquad (2,7)$$

لذا به ازای هر a، $\Gamma_1(n)$ نیم منظم است.

حال شرط کافی برای نیم منظم بودن $\Gamma_2(n)$ را بررسی می کنیم. ابتدا فرض کنید $n=p^k$ به ازای عدد اول فرد p و $k \in \{1,2\}$. در این صورت به ازای هر $a \in \Gamma_2(n)$، $\text{indeg}(a)>0$ اگروفقط اگر $a=0$. بنابراین در این حالت $\Gamma_2(n)$ نیم منظم است. به طور خاص

$$\text{indeg}(0) = N_n(0) = p^{[k/2]}. \qquad (2,8)$$

براحتی می توان بررسی کرد $\Gamma_2(n)$ به ازای $n=2^k$ و $k \in \{1,2,3,4,6\}$ برقرار است. علاوه بر این اگر $a \in \Gamma_2(2^k)$ به ازای $k \in \{1,2,3,4,6\}$ و $\text{indeg}(a)>0$، آن گاه

$$\text{indeg}(a) = 2^{[k/2]}. \qquad (2,9)$$

حال شرط لازم نیم منظم بودن $\Gamma_2(n)$ را بررسی می کنیم. فرض کنید $n \geq 2$ و $\Gamma_2(n)$ نیم منظم است. ابتدا حالتی را در نظر می گیریم که $\omega(n) \geq 2$ و $p^2 \mid n$ به ازای عدد اول فرد p. فرض کنید به ازای $k \geq 2$، $p^k \| n$. اگر $q \neq p$ اول باشد به طوری که $q^l \| n$ و $l \geq 1$. فرض کنید $n = p^k n_1 = q^l n_2$. بنا به

قضیه باقیمانده چینی رئوس a_1 و a_2 از $\Gamma_2(n)$ وجود دارد به طوری که

$$a_1 \equiv 0 \pmod{p^k},\ a_1 \equiv 1 \pmod{n_1},\ a_2 \equiv 0 \pmod{q^l},\ a_2 \equiv 1 \pmod{n_2}.$$

با توجه به (۲،۸) و قضیه باقیمانده چینی و لم 2-2-8 داریم

$$\begin{aligned} \operatorname{indeg}(a_1) = N_n(a_1) &= N_{p^k}(a_1)N_{n_1}(a_1) = N_{p^k}(0)N_{n_1}(1) \\ &= \frac{p^k}{p^{[k/2]}}2^{\omega(n_1)+\varepsilon(n_1)} = p^{[k/2]}2^{\omega(n_1)+\varepsilon(n_1)} \end{aligned} \qquad (2,10)$$

و

$$\begin{aligned} \operatorname{indeg}(a_2) = N_n(a_2) &= N_{q^l}(a_2)N_{n_2}(a_2) = N_{q^l}(0)N_{n_2}(1) \\ &= q^{[l/2]}2^{\omega(n_2)+\varepsilon(n_2)}. \end{aligned} \qquad (2,11)$$

از (۲،۱۰) و (۲،۱۱) نتیجه می شود $p \mid \operatorname{indeg}(a_1)$ در حالیکه $p \nmid \operatorname{indeg}(a_2)$. لذا در این حالت $\Gamma_2(n)$ نیم منظم نیست.

فرض کنید $\omega(n) \geq 2$ و $2^i \| n$ که $i \geq 1$ و $\frac{n}{2^i}$ فاقد مربع کامل باشد. اگر $n = 2^i n_3$. آن گاه با توجه به قضیه باقیمانده چینی، رئوس a_3 و a_4 از $\Gamma_2(n)$ وجود دارد به طوری که

$$a_3 \equiv 0 \pmod{2^i},\ a_3 \equiv 0 \pmod{n_3},\ a_4 \equiv 0 \pmod{2^i},\ a_4 \equiv 1 \pmod{n_3}.$$

لذا با توجه به اثبات قضیه2-2-1 و لم 2-2-8

$$\operatorname{indeg}(a_3) = N_n(a_3) = N_{2^i}(a_3)N_{n_3}(a_3) = N_{2^i}(0)N_{n_3}(0) = 2^{[i/2]} \qquad (2,12)$$

و

$$\operatorname{indeg}(a_4) = N_n(a_4) = N_{2^i}(0)N_{n_3}(1) = 2^{[i/2]}2^{\omega(n_3)+\varepsilon(n_3)}. \qquad (2,13)$$

چون $n_3 > 1$ و $2 \nmid n_3$، $2^{[i/2]}2^{\omega(n_3)+\varepsilon(n_3)} \geq 2$. حال از (2,12) و (2,13) نتیجه می گیریم که $\Gamma_2(n)$ نیم منظم نیست.

اکنون فرض کنید $\omega(n) \geq 2$، n فرد و فاقد مربع کامل باشد. در این صورت $\operatorname{indeg}(0) = 1$. اگر p کوچکترین عدد اولی باشد که n را عاد می کند. آن گاه $p^2 < n$ و $p^2 \equiv (n-p)^2 \pmod n$. در نتیجه $\operatorname{indeg}(p^2) > 1$ و $\Gamma_2(n)$ نیم منظم نیست.

از مطالب بالا نتیجه می شود که اگر $\Gamma_2(n)$ نیم منظم باشد، آن گاه $\omega(n)=1$.

اکنون حالتی را بررسی می کنیم که $n=p^k$ به ازای عدد اول فرد p و $k \geq 3$. در این حالت

$$\text{indeg}(0) = N_{p^k}(0) = p^{[k/2]}. \qquad (2,14)$$

جواب های همنهشتی

$$x^2 \equiv p^2 \pmod{p^k} \qquad (2,15)$$

را در نظر بگیرید. واضح است که p جوابی از رابطه (2,15) است. اگر c جواب (2,15) باشد، چون 0 جواب (2,15) نمی باشد، آن گاه $n-c$ نیز جوابی از (2,15) است و $n-c \not\equiv c \pmod{p^k}$. لذا $N_{p^k}(p^2)$ زوج می باشد. بنابراین از (2,14) نتیجه می گیریم که $\text{indeg}(0) \neq \text{indeg}(p^2)$ و $\Gamma_2(p^k)$ نیم منظم نیست.

حال قضیه را برای حالتی که $n=2^k$ به ازای $k=5$ یا $k \geq 7$ بررسی می کنیم. برای اثبات، کافی است نشان دهیم $\Gamma_2(2^k)$ نیم منظم نیست با وجود رأس $2^{2t} \in \Gamma_2(2^k)$ به ازای $2 \leq 2t < k$، $\text{indeg}(2^{2t}) > 0$ و $\text{indeg}(2^{2t}) \neq \text{indeg}(0) = 2^{\lfloor k/2 \rfloor}$. فرض کنید $2 \leq 2t < k$. در این صورت واضح است که $b^2 \equiv 2^{2t} \pmod{2^k}$ اگر و فقط اگر

$$b \equiv 2^t c \pmod{2^k} \qquad (2,16)$$

به ازای عدد صحیح c به طوری که

$$c^2 \equiv 1 \pmod{2^{k-2t}}. \qquad (2,17)$$

با توجه به اثبات لم 2-2-8. (۲،۱۷) برقرار است اگر و فقط اگر

$$\begin{aligned} &c \equiv 1 \pmod{2} && 1 \leq k-2t \leq 3 \\ &c \equiv \pm 1 \pmod{2^{k-2t-1}} && k-2t \geq 4. \end{aligned}$$

علاوه بر این $2^t c_1 \equiv 2^t c_2 \pmod{2^k}$ اگر و فقط اگر

$$c_1 \equiv c_2 \pmod{2^{k-t}}. \qquad (2,18)$$

با توجه به روابط (۲،۱۶) ، (۲،۱۷) و (۲،۱۸) ، اگر $2 \leq 2t < k$، آن گاه

$$N_{2^k}(2^{2t}) = \begin{cases} 2^{k-t-1} & 1 \leq k-2t \leq 3 \\ 2^{t+2} & k-2t \geq 4. \end{cases} \qquad (2,19)$$

اگر $k \neq ۷$، آن گاه از (۲،۱۹) نتیجه می شود که $\text{indeg}(0) = ۲^{\lfloor k/۲ \rfloor} \neq ۸$ و $\text{indeg}(۲^{۲}) = ۸$ و در نتیجه $\Gamma_{۲}(۲^{k})$ نیم منظم نیست.

اگر $k = ۷$، آن گاه با توجه به (۲،۱۹) نتیجه می شود که $\text{indeg}(0) = ۲^{\lfloor ۷/۲ \rfloor} = ۸$ و $\text{indeg}(۲^{۴}) = ۲^{۷-۲-۱} = ۱۶$ و لذا $\Gamma_{۲}(۲^{۷})$ نیم منظم نیست.

در نهایت حالتی را بررسی می کنیم که $\Gamma(n)$ نیم منظم است. فرض کنید a رأسی از $\Gamma_{۱}(n)$ باشد به طوری که $\text{indeg}(a) > 0$ و b رأسی از $\Gamma_{۲}(n)$ باشد به طوری که $\text{indeg}(b) > 0$. همچنین فرض کنید $n > ۱$. در این صورت $\Gamma(n)$ نیم منظم است اگر و فقط اگر $\Gamma_{۱}(n)$ و $\Gamma_{۲}(n)$ هر دو نیم منظم باشند و $\text{indeg}(a) = \text{indeg}(b)$. با توجه به (۲،۷) ، (۲،۸) و (۲،۹) نتیجه می شود که $\Gamma(n)$ نیم منظم است اگر و فقط اگر $n = ۲^{k}$ به ازای $k \in \{۰،۱،۲،۴\}$. □

قضیه 2-2-9 فرض کنید d عدد صحیح مثبت باشد. در این صورت اعداد صحیح مثبت n و a وجود دارد به طوری که a رأسی از $\Gamma_{۲}(n)$ باشد و $\text{indeg}(a) = d$.

اثبات. اگر $d = ۱$، قرار می دهیم $n = ۲m$ که در آن m فرد و فاقد مربع کامل باشد و $a = \frac{n}{۲}$.

اکنون فرض کنید $d > ۱$. عدد $k_{۱}$ را طوری انتخاب می کنیم که $d = ۲^{k_{۱}} d_{۱}$، $d_{۱}$ فرد باشد. عدد صحیح مثبت $d_{۲}$ را طوری انتخاب می کنیم که $\omega(d_{۲}) = k_{۱}$ و $\gcd(۲d_{۱}, d_{۲}) = ۱$ (اگر $k_{۱} = 0$، $d_{۲} = ۱$).

حال فرض کنید

$$n = d_{۱}^{۲} d_{۲}, \qquad a = d_{۱}^{۲}.$$

با توجه به لم 2-2-8 و قضیه باقیمانده چینی:

$$\text{indeg}(a) = N_{n}(a) = N_{d_{۱}^{۲}}(d_{۱}^{۲}) N_{d_{۲}}(d_{۱}^{۲}) = d_{۱} ۲^{k_{۱}} = d.$$

□

گوییم رأس a از $\Gamma(n)$ دارای رتبه i، $i \geq ۱$ است، اگر یک مسیر جهت دار با طول ماکسیمم i وجود داشته باشد به طوری که به رأس a ختم شود و شامل هیچ یال جهت دار متعلق به یک دور نباشد. اگر چنین مسیری وجود نداشته باشد، گوییم رأس دارای رتبه 0 است.

همچنین گوییم یک مؤلفه از $\Gamma(n)$ دارای رتبه l است اگر بالاترین رتبه یک رأس از این مؤلفه، $l-۱$ باشد. برای مثال، اگر $n=۱۶$ آن گاه رئوس ۲ و ۸ در رتبه 0، رأس ۴ در رتبه ۱، رأس 0 در رتبه ۲ و هر دو مؤلفه اش دارای رتبه ۳ هستند.

فرض کنید مؤلفه C از گراف $\Gamma(n)$ دقیقاً l رتبه داشته باشد. واضح است که هر رأس با رتبه $l-۱$ قسمتی از یک دوراست، چون درجه خروجی هر رأس ۱ است. علاوه بر این، اگر a و b دو رأس مجزا با رتبه i، از مؤلفه C باشند، که $0 \le i < l$، آن گاه مسیر جهت دار از a به b وجود ندارد. گزاره زیر همواره برقرار است.

گزاره 2-2-10 هر مؤلفه دقیقاً یک دور دارد یعنی تعداد مؤلفه های $\Gamma(n)$ با تعداد دورهای آن برابر است.

یادآوری 2-2-11 گزاره قبل یک ویژگی عمومی از گراف مکرر با نگاشت $f: H \to H$ می باشد.

3-2 کاربرد λ-تابع کارمایکل

اکنون می خواهیم λ-تابع کارمایکل $\lambda(n)$ و برخی از ویژگی های آن را یادآوری کنیم که اولین بار در سال 1912 توسط رابرت دنیل [۴] تعریف شد.

تعریف 2-3-1 فرض کنید n عدد صحیح مثبت باشد. λ-تابع کارمایکل $\lambda(n)$ به صورت زیر تعریف می شود:

$$\begin{aligned}
&\lambda(۱) = ۱ = \varphi(۱),\\
&\lambda(۲) = ۱ = \varphi(۲),\\
&\lambda(۴) = ۲ = \varphi(۴),\\
&\lambda(۲^k) = ۲^{k-۲} = \frac{۱}{۲}\varphi(۲^k) \quad k \ge ۳,\\
&\lambda(p^k) = (p-۱)p^{k-۱} = \varphi(p^k)
\end{aligned}$$

به ازای عدد اول فرد p و $k \ge ۱$،

$$\lambda(p_۱^{k_۱} p_۲^{k_۲} \dots p_s^{k_s}) = \operatorname{lcm}\,[\lambda(p_۱^{k_۱}), \lambda(p_۲^{k_۲}), \dots, \lambda(p_s^{k_s})],$$

که به ازای $k_i \ge ۱$ و $i \in \{۱,\dots,s\}$، $p_۱, p_۲, \dots, p_s$ اعداد اول مجزا هستند. همچنین کوچکترین مضرب مشترک اعداد a و b را با $\operatorname{lcm}(a,b)$ نشان می دهیم.

بنا به تعریف بالا به ازای هر n، $\lambda(n)|\varphi(n)$ و $\lambda(n)=\varphi(n)$ اگر و فقط اگر $n \in \{۱،۲،۴,q^k,۲q^k\}$ که q عدد اول فرد و $k \geq ۱$.

فرض کنید رتبه ضربی g به پیمانه n را به صورت $t = \mathrm{ord}_n g$ نشان می دهیم (یعنی t کوچکترین عدد طبیعی است به طوری که $g^t \equiv ۱ \pmod n$).

قضیه زیر ، قضیه اویلر را که بیان می کند $a^{\varphi(n)} \equiv ۱ \pmod n$ اگر و فقط اگر $\gcd(a,n)=۱$، تعمیم می دهد.

قضیه 2-3-2 (قضیه کارمایکل) فرض کنید $a,n \in \mathbb{N}$. در این صورت

$$a^{\lambda(n)} \equiv ۱ \pmod n$$

اگر و فقط اگر $\gcd(a,n)=۱$. علاوه بر این عدد صحیح g وجود دارد به طوری که

$$\mathrm{ord}_n g = \lambda(n).$$

اثبات. ر.ج به [۲] یا [۸،گزاره 21] . □

حال فرض کنید تجزیه $\lambda(n)$ به حاصل ضرب عوامل اول بصورت زیر باشد:

$$\lambda(n) = \prod_{j=۱}^{s} q_j^{l_j} \qquad (۳،۱)$$

که در آن $q_۱ < q_۲ < ... < q_s$ اعداد اول و $l_j > 0$. از تعریف λ نتیجه می شود که به ازای $n > ۲$، $q_۱ = ۲$.

قضیه 2-3-3 دوری به طول t در گراف $\Gamma(n)$ وجود دارد اگر و فقط اگر $t = \mathrm{ord}_d ۲$ به ازای مقسوم علیه مثبت فرد d از $\lambda(n)$.

اثبات. فرض کنید a رأسی از یک t-دور در $\Gamma(n)$ باشد. در این صورت

$$a^{۲^t} \equiv a \pmod n. \qquad (۳،۲)$$

ثابت می کنیم t کوچکترین عدد صحیح مثبتی است که در رابطه بالا صدق می کند. کافی است ثابت کنیم در $\Gamma(n)$ دورها مجزایند. اگر فرض کنید دو دور به طول $t_۱$ و $t_۲$ در $\Gamma(n)$ وجود دارد که حداقل در یک رأس اشتراک داشته باشند، از این رأس 2 یال خارج می شود که یکی متعلق به دور $t_۱$ و دیگری متعلق به دور $t_۲$ است و با این مطلب که درجه خروجی هر رأس برابر 1 است در تناقض است. لذا در

$\Gamma(n)$ دورها مجزایند.

t کوچکترین عدد صحیح مثبتی است که

$$a^{۲^t} - a \equiv a(a^{۲^t-۱} - ۱) \equiv ۰ \pmod{n}. \qquad (۳,۳)$$

چون $\gcd(a, a^{۲^t-۱} - ۱) = ۱$، لذا از رابطه (3,3) نتیجه می شود اگر $n_۱ = \gcd(a,n)$ و $n_۲ = \frac{n}{n_۱}$، آنگاه ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که

$$a \equiv ۰ \pmod{n_۱}, \qquad a^{۲^t-۱} \equiv ۱ \pmod{n_۲} \qquad (۳,۴)$$

و $\gcd(n_۱, n_۲) = ۱$. فرض کنید $t_۱ < t$ به طوری که

$$\left.\begin{aligned} a^{۲^{t_۱}-۱} &\equiv ۱ \pmod{n_۲} \\ a^{۲^{t_۱}-۱} &\equiv ۱ \pmod{n_۱} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} a^{۲^{t_۱}} &\equiv a \pmod{n_۲} \\ a^{۲^{t_۱}} &\equiv a \equiv ۰ \pmod{n_۱} \end{aligned}\right\} \Rightarrow a^{۲^{t_۱}} \equiv a \pmod{n}$$

که با رابطه (3,3) تناقض دارد. برعکس اگر فرض کنید $t_۱ < t$ به طوری که

$$a^{۲^{t_۱}} \equiv a \pmod{n} \Rightarrow \begin{cases} (a,n) = ۱ \Rightarrow a^{۲^{t_۱}} \equiv ۱ \pmod{n} \Rightarrow a^{۲^{t_۱}} \equiv ۱ \pmod{n_۲} \\ (a,n) \neq ۱ \Rightarrow a^{۲^{t_۱}} \equiv ۱ \pmod{n} \Rightarrow a^{۲^{t_۱}} \equiv ۱ \pmod{n_۲} \end{cases}$$

که با رابطه (3,4) تناقض دارد. بنا به قضیه باقیمانده چینی عدد صحیح b وجود دارد به طوری که

$$b \equiv ۱ \pmod{n_۱}, \qquad b \equiv a \pmod{n_۲}. \qquad (۳,۵)$$

با برهان خلف ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که

$$\left.\begin{aligned} b^{۲^t-۱} &\equiv ۱ \pmod{n_۱} \\ b^{۲^t-۱} &\equiv a^{۲^t-۱} \equiv ۱ \pmod{n_۲} \end{aligned}\right\} \Rightarrow b^{۲^t-۱} \equiv ۱ \pmod{n}. \qquad (۳,۶)$$

فرض کنید $t_۱ < t$ به قسمی که:

$$\left.\begin{aligned} a^{۲^{t_۱}} &\equiv a \pmod{n_۲} \\ a^{۲^{t_۱}} &\equiv a \equiv ۰ \pmod{n_۱} \end{aligned}\right\} \Rightarrow a^{۲^{t_۱}} \equiv a \pmod{n}$$

که تناقض است.

حال فرض کنید $d = \mathrm{ord}_n b$. در این صورت $d \mid ۲^t - ۱$. با توجه به رابطه (۳,۶)، t کوچکترین عدد صحیح مثبت است به طوری که $d \mid ۲^t - ۱$. لذا $t = \mathrm{ord}_d ۲$. واضح است که d فرد است. علاوه بر این

با توجه به قضیه کارمایکل، $d \mid \lambda(n)$.

بر عکس، فرض کنید $t = \mathrm{ord}_d 2$ و d مقسوم علیه مثبت فرد $\lambda(n)$ باشد. بنا به قضیه کارمایکل، باقیمانده g به پیمانه n وجود دارد به طوری که $\mathrm{ord}_n g = \lambda(n)$. قرار دهید $h = g^{\lambda(n)/d}$، لذا $\mathrm{ord}_n h = d$. چون $d \mid 2^t - 1$ و به ازای $1 \le k < t$ ، $d \nmid 2^k - 1$، بنابراین t کوچکترین عدد صحیح مثبتی است که

$$h^{2^t - 1} \equiv 1 \pmod n. \qquad (3,7)$$

$$h.h^{2^t - 1} \equiv h^{2^t} \equiv h \pmod n.$$

در نتیجه h رأسی از یک t-دور در $\Gamma(n)$ است و اثبات تمام است. □

تعداد دورهای بطول t در گراف $\Gamma(n)$ را با $A_t(\Gamma(n))$ نشان می دهیم. در [12]، شالای فرمول بازگشتی برای $A_t(\Gamma(n))$ ارائه داد که برای حالتی که $t = 1$ یا $2^t - 1$ عدد اول مرسن باشد بدون استفاده از زیرگراف های $\Gamma_1(n)$ و $\Gamma_2(n)$ به دست آمده است. در [11]، روگرز $A_t(\Gamma(n))$ را برای $t \ge 1$ و n های اول بطور کامل مشخص کرده است. او ثابت کرد که زیر گراف های متصل به هر رأس از همه دور ها، بجز نقطه ثابت 0، درخت های دوتایی با ساختار مشابه هستند.

در حالتی که n عدد صحیح مثبت می باشد، تعداد ریشه های مربعی از هر باقیمانده درجه دو در $\Gamma_1(n)$ با تعداد ریشه های مربعی 1 به پیمانه n برابر است. نتیجه می شود به ازای $n \ge 2$، زیر گراف های متصل به هر رأس از هر دور از $\Gamma_1(n)$ شبیه هستند (شکل 2 و 5 را ببینید). اثبات این ویژگی بلافاصله از قضیه 2-2-7 و قضیه 4,4 که در بخش بعد مطرح می گردند، نتیجه می شود.

قضیه 2-3-4 اگر n عدد صحیح مثبت باشد، آن گاه $A_1(\Gamma_1(n)) = 1$ و $A_1(\Gamma_2(n)) = 2^{\omega(n)-1}$. علاوه بر این اگر $t > 1$، آن گاه $A_t(\Gamma_1(n)) \ge 1$ و $A_t(\Gamma_2(n)) \ge 1$.

اثبات. ابتدا فرض کنید $t = 1$. با توجه به قضیه شالای، $A_1(\Gamma(n)) = 2^{\omega(n)}$. فرض کنید a نقطه ثابت $\Gamma_1(n)$ باشد. در این صورت

$$a^2 - a \equiv a(a-1) \equiv 0 \pmod n \qquad (3,8)$$

چون $\gcd(a,n) = 1$، از (3,8) نتیجه می شود $a \equiv 1 \pmod n$. بنابراین $A_1(\Gamma(n)) = 1$ و $A_1(\Gamma_2(n)) = 2^{\omega(n)-1}$.

حال فرض کنید $t > 1$ و $a \in \Gamma_2(n)$ قسمتی از یک t-دور باشد. با توجه به (3,4) اعداد صحیح n_1 و

$n_۲$ وجود دارد به طوری که $n_۱, n_۲ > ۱$ ، $\gcd(n_۱, n_۲) = ۱$ ، $n_۱ n_۲ = n$ و t کوچکترین عدد صحیح مثبتی است که

$$\begin{aligned} a &\equiv 0 \pmod{n_۱}, \\ a^{۲^t - ۱} &\equiv ۱ \pmod{n_۲}. \end{aligned} \qquad (۳,۹)$$

بنا به قضیه باقیمانده چینی و اثبات قضیه 2-3-3، رأس $b \in \Gamma_۱(n)$ وجود دارد به طوری که b قسمتی از یک t-دور باشد و

$$\begin{aligned} b &\equiv ۱ \pmod{n_۱}, \\ b &\equiv a \pmod{n_۲}. \end{aligned} \qquad (۳,۱۰)$$

□

یادآوری 2-3-5 با توجه به [9، گزاره ٥٤٤]، تعداد نامانده های درجه دوم $\Gamma_۱(n)$ به ازای $n \geq ۳$، بزرگتر یا مساوی با تعداد مانده های درجه دوم می باشد. بنابراین تعداد رئوس $\Gamma_۱(n)$ با درجه ورودی صفر، بزرگتر یا مساوی با رئوس با درجه ورودی مثبت است. بویژه تعداد رئوس $\Gamma_۱(n)$ که روی یک دور قرار نگرفته، بزرگتر یا مساوی با تعداد رئوس $\Gamma_۱(n)$ قرار گرفته روی دور است.

2-4 کاربرد تابع φ اویلر

مجموعه

$$S = \{n \geq ۱ \mid \text{توانی از } 2 \text{ است } \varphi(n)\}$$

را که در آن $\varphi(n)$ تابع اویلر می باشد، در نظر بگیرید.

روشن است که عدد صحیح مثبت n متعلق به S است اگر و فقط اگر $n = ۲^{\alpha} F_{m_۱} \dots F_{m_j}$ به ازای $\alpha \geq 0$، $j \geq 0$ ، که $F_{m_i} = ۲^{۲^{m_i}} + ۱$ اعداد اول مجزای فرما هستند.

قضیه 2-4-1 دوری با طول بزرگتر از 1 در $\Gamma_۱(n)$ وجود ندارد اگر و فقط اگر $n \in S$. علاوه بر این، دوری با طول بزرگتر از 1 در $\Gamma_۲(n)$ وجود ندارد اگر و فقط اگر $n \in S$ یا n، به ازای $k \geq 0$، kامین توان اول باشد.

اثبات. با توجه به تعریف تابع کارمایکل، $\lambda(n) = ۲^i$ برای عدد صحیح $i \geq 0$ اگر و فقط اگر $\varphi(n) = ۲^j$ برای عدد صحیح $j \geq i$.

فرض کنید d عدد صحیح مثبت فرد باشد. در این صورت مشاهده می کنیم که $\operatorname{ord}_d ۲ = ۱$ اگر و فقط

اگر $d = ۱$. بنا به قضیه 2-3-4، $A_t(\Gamma(n)) = 0$ به ازای $t \geq ۲$ اگر و فقط اگر $A_t(\Gamma_۱(n)) = 0$ به ازای $t \geq ۲$.

ابتدا فرض کنید $n \in S$. در این صورت 1 مقسوم علیه مثبت فرد $\lambda(n)$ است و از قضیه 2-3-3 نتیجه می شود که به ازای $t \geq ۲$:

$$A_t(\Gamma(n)) = A_t(\Gamma_۱(n)) = A_t(\Gamma_۲(n)) = 0.$$

اگر $n \notin S$، آن گاه $\lambda(n)$ مقسوم علیه فردی مانند $d > ۱$ دارد. با توجه به قضیه 2-3-3 و 2-3-4 نتیجه می شود که برای $t = \mathrm{ord}_d ۲ > ۱$، $A_t(\Gamma_۱(n)) \geq ۱$.

مشاهده می کنیم اگر n توانی از اعداد اول باشد، آن گاه نقطه ثابت 0، تنها دور گراف $\Gamma_۲(n)$ می باشد. حال فرض کنید n توانی از اعداد اول نباشد و $n \notin S$. نشان می دهیم به ازای $t \geq ۲$ $A_t(\Gamma_۲(n)) > 0$. توجه کنید وجود دارد $p^k \notin S$ به طوری که $p^k \| n$به ازای $k \geq ۱$. علاوه بر این، $\lambda(p^k)$ مقسوم علیه فردی مانند $d > ۱$ دارد. علاوه بر این $d \mid \lambda(n)$ چون $\lambda(p^k) \mid \lambda(n)$. فرض کنید $t = \mathrm{ord}_d ۲$. با توجه به یادآوری 2-3-5، باقیمانده a وجود دارد به طوری که t کوچکترین عدد صحیح مثبتی است که

$$a^{۲^t - ۱} \equiv ۱ \pmod{p^k}. \qquad (۴,۱)$$

قرار دهید $n = p^k n_۱$، که $n_۱ > ۱$. با استفاده از قضیه چینی رأس $b \in \Gamma_۲(n)$ وجود دارد به طوری که

$$\begin{aligned} b &\equiv a \pmod{p^k}, \\ b &\equiv 0 \pmod{n_۱}. \end{aligned} \qquad (۴,۲)$$

توجه کنید که بنا به (۴,۱) و (۴,۲)، $\gcd(a, p^k) = ۱$، $\gcd(b, p^k)$. همچنین t کوچکترین عدد صحیح مثبتی است که

$$b^{۲^t} - b = b(b^{۲^t - ۱} - ۱) \equiv 0 \pmod{n}.$$

در نتیجه t کوچکترین عدد صحیح مثبتی است که

$$b^{۲^t} \equiv b \pmod{n}.$$

و b قسمتی از یک t-دور در $\Gamma_۲(n)$ است. □

نتیجه 2-4-2 دوری با طول بزرگتر از 1 در $\Gamma(n)$ وجود ندارد اگر و فقط اگر $n \in S$.

نتیجه 2-4-3 عدد فرمای F_m مرکب است اگر و فقط اگر دوری با طول بزرگتر از 1 در $\Gamma(F_m)$

وجود داشته باشد.

در قضیه بعد نتیجه روگرز [۲۲] را از اعداد اول به اعداد طبیعی تعمیم می دهیم.

قضیه 2-4-4 هر مؤلفه $\Gamma_1(n)$ دقیقاً $v_2(\lambda(n))+1$ رتبه دارد که $v_2(c)$ نشان دهنده بیشترین توان ۲ است که c را عاد می کند.

اثبات. واضح است که قضیه برای $n \in \{1,2\}$ برقرار است. لذا فرض کنید $n > 2$. همچنین فرض کنید a یک رأس از مؤلفه C از گراف $\Gamma_1(n)$ باشد به طوری که $d = \mathrm{ord}_n a$. در این صورت با توجه به قضیه کارمایکل، $d \mid \lambda(n)$. بنا به اثبات قضیه 2-3-3، a قسمتی از یک t-دور در C است و بنابراین در بالاترین رتبه C است اگر و فقط اگر d فرد باشد.

فرض کنید $b^2 \equiv a \pmod n$. چون

$$d = \mathrm{ord}_n a = \frac{\mathrm{ord}_n b}{\gcd(2, \mathrm{ord}_n b)} \qquad (۴,۳)$$

نتیجه می شود که

$$\mathrm{ord}_n a \mid \mathrm{ord}_n b \mid 2\mathrm{ord}_n a$$

و اگر $2 \mid \mathrm{ord}_n a$، آن گاه $\mathrm{ord}_n b = 2\mathrm{ord}_n a$. همچنین از 2-4-3 نتیجه می شود که همه رئوس در همان دور از $\Gamma_1(n)$ دارای همان مرتبه به پیمانه n هستند، یعنی عدد صحیح فرد $d > 1$ وجود دارد به طوری که

$$d = \mathrm{ord}_n a \qquad (۴,۴)$$

برای همه رئوس a از t-دور در $\Gamma_1(n)$.

فرض کنید $l = v_2(\lambda(n))$ و $2^l \| \mathrm{ord}_n a$. توجه کنید $2 \mid \lambda(n)$ برای $n > 2$. اگر رأس $b \in \Gamma_1(n)$ وجود داشته باشد به طوری که $b^2 \equiv a \pmod n$، لذا $2^{l+1} \| \mathrm{ord}_n b$ که با $\mathrm{ord}_n b \mid \lambda(n)$ تناقض دارد. از این رو a رتبه 0 دارد. در نتیجه هر مؤلفه C از گراف $\Gamma_1(n)$ حداکثر دارای $l+1$ رتبه است.

فرض کنید a رأسی از $\Gamma_1(n)$ است به طوری که $d = \mathrm{ord}_n a$ فرد است. رأس b از گراف $\Gamma_1(n)$ را پیدا می کنیم به طوری که

$$b^{2^t} \equiv a \pmod n, \qquad \mathrm{ord}_n b^{2^{t-1}} = 2\mathrm{ord}_n a. \qquad (۴,۵)$$

با توجه به بحث بالا، $\mathrm{ord}_n b$ برابر با $2^l d$ است و b^{2^i} با رتبه i است به ازای $i \in \{0,1,\ldots,l\}$. لذا C دقیقاً $l+1$ رتبه دارد.

فرض کنید تجزیه n به عوامل اول بصورت (1,2) باشد. با توجه به تعریف $\lambda(n)$، عامل $p_j^{k_j}$ از n وجود دارد به طوری که $v_2(\lambda(p_j^{k_j})) = l$ به ازای $j \in \{1,2,\ldots,s\}$.

فرض کنید d_i برای $i = 1,2,\ldots,s$، مرتبه a به پیمانه $p_j^{k_j}$ باشد. در این صورت $d_i \mid d$، d_i فرد است و a قسمتی از یک دور بطول $t_i = \mathrm{ord}_{d_i}(p_i^{k_i})$ در $\Gamma_1(p_i^{k_i})$ است. ابتدا فرض کنید $v_2(\lambda(p_i^{k_i})) < l$. رأس $b_i \in \Gamma_1(p_i^{k_i})$ را در همان t_i-دور مانند رأس a به پیمانه $p_i^{k_i}$ انتخاب کنید که از رئوس l تا a در جهت عقربه های ساعت دور می زنند(احتمالا بیش از یک بار دور می زنند). بنابراین

$$b_i^{2^l} \equiv a \pmod{p_i^{k_i}}.$$

حال فرض کنید $2^l \parallel \lambda(p_i^{k_i})$ و $p_i^{k_i} = 2$ یا 4 یا p_i عدد فرد اول است. در این صورت رئوس $\Gamma_1(p_i^{k_i})$ یک گروه دوری به پیمانه $p_i^{k_i}$ با $\lambda(p_i^{k_i})$ عضو را تشکیل می دهند.

برعکس، ریشه اولیه $g_i \pmod{p_i^{k_i}}$ وجود دارد به طوری که

$$g_i^{\lambda(p_i^{k_i})/d_i} \equiv a \pmod{p_i^{k_i}}.$$

فرض کنید $c_i = \dfrac{\lambda(p_i^{k_i})}{2^l d_i}$ و $b_i \equiv g_i^{c_i} \pmod{p_i^{k_i}}$. در این صورت $b_i^{2^l} \equiv a \pmod{p_i^{k_i}}$ و مرتبه $b_i^{2^{l-1}}$ به پیمانه $p_i^{k_i}$ برابر است با $2d_i$.

در آخر، اگر $p_1 = 2$ و $k_1 = l$، $l \geq 3$ که در آن $2^{k_1} \parallel \lambda(n)$. آن گاه $a \equiv 1 \pmod{2^{k_1}}$، چون مرتبه a به پیمانه 2^{k_i} فرد است. علاوه بر این،

$$5^{2^l} \equiv 1 \equiv a \pmod{2^{k_1}}$$

و مرتبه $5^{2^{l-1}}$ به پیمانه 2^{k_1} برابر است با 2. فرض کنید $b_1 \equiv 5 \pmod{2^{k_1}}$. با توجه به قضیه چینی، رأس $b \in \Gamma_1(n)$ وجود دارد به طوری که به ازای $i = 1,\ldots,s$، $b \equiv b_i \pmod{p_i^{k_i}}$. دقت کنید اگر c_i مرتبه b_i به پیمانه $p_i^{k_i}$ باشد، آن گاه

$$\mathrm{ord}_n d = \mathrm{lcm}[c_1, c_2, \ldots, c_s].$$

لذا نتیجه می شود که b ویژگی مورد نیاز داده شده در (۴۰۵) را دارد. □

قضیه 5-4-2 فرض کنید a, b, c, d, e اعداد صحیح مثبت باشند به طوری که $b \geq a \geq 2$ و $d = 2^f$ به ازای $f \geq 2$. در این صورت عدد صحیح مثبت n وجود دارد به طوری که:

(i) هر مؤلفه $\Gamma_1(n)$ دقیقاً a رتبه دارد.

(ii) بعضی از مؤلفه های $\Gamma_2(n)$ حداقل b رتبه دارد.

(iii) $\Gamma_1(n)$ حداقل c مؤلفه دارد.

(iv) $\Gamma_2(n)$ حداقل c مؤلفه دارد.

(v) هر رأس $\Gamma_1(n)$ که رتبه 0 ندارد، دارای درجه ورودی d است.

(vi) تعدادی از رئوس $\Gamma_2(n)$ درجه ورودی بزرگتر یا مساوی با e دارند.

اثبات. با توجه به قضیه باقیمانده چینی و قضیه دیریکله برای نامتناهی بودن تصاعد حسابی اعداد اول، می توانیم عدد اول p را پیدا کنیم به طوری که $p \equiv 1 + 2^{a-1} \pmod{2^a}$ و $p-1$ توسط c عدد $2c-1, \ldots, 2^2-1, 2^1-1$ بخش پذیر است. عدد صحیح k را انتخاب کنید به طوری که $k \geq 2^{b-1}$ و $p^{[k/2]} \geq e$. بعد n را انتخاب کنید به طوری که $p^k \| n$، $\omega(n) = f$ و هر مقسوم علیه اول $q \neq p$ از n با 3 به پیمانه 4 همنهشت باشد. بنابراین

$$v_2(\lambda(n)) = v_2(\lambda(p^k)) = v_2(\lambda(p)) = a-1,$$

و با توجه به قضیه 2-4-4، $\Gamma_1(n)$ دقیقاً a رتبه دارد. لذا (i) برقرار است.

علاوه بر این اگر i رأسی از $\Gamma_1(n)$ باشد و $\mathrm{indeg}(i) > 0$، آن گاه

$$\mathrm{indeg}(i) = 2^{\omega(n)+\varepsilon(n)} = 2^f = d,$$

و (v) برقرار است. توجه کنید $p-1 \mid \lambda(n)$ و مرتبه 2 به پیمانه $2^t - 1$ برابر است با t. لذا بنا به گزاره 2-2-10، قضیه 2-3-3، (۳،۹)، (۳،۱۰) و (۴،۴)، $\Gamma_1(n)$ و $\Gamma_2(n)$ هر دو حداقل c مؤلفه دارند. بنابراین (iii) و (iv) نیز برقرار است. بدیهی است که در مؤلفه $\Gamma_2(n)$ شامل رأس p، تعداد رتبه ها حداقل $b \geq 1 + \lfloor \log_2 k \rfloor$ است، یعنی (ii) درست می باشد.

در آخر توجه کنید $0 \in \Gamma_2(n)$ و

$$\mathrm{indeg}(0) \geq \frac{p^k}{p^{[k/2]}} = p^{[k/2]} \geq e,$$

در نتیجه (vi) برقرار است. □

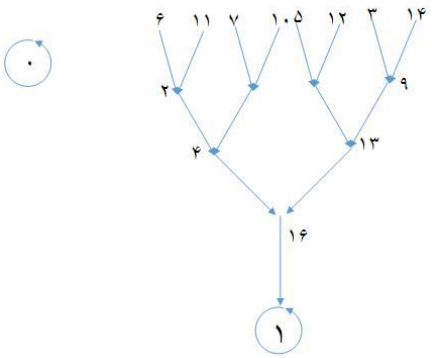
یادآوری 2-4-6 با توجه به قضایای 2-2-7، 2-2-9، 2-4-1، 2-4-4 و 2-4-5، $\Gamma_1(n)$ رفتار منظم تری نسبت به $\Gamma_2(n)$ نشان می دهد.

در قضیه زیر اعداد اول فرما را از سایر اعداد اول فرد جدا می کنیم.

قضیه 2-4-7 گراف $\Gamma(n)$ دقیقاً 2 مؤلفه دارد اگر و فقط اگر n عدد اول فرما یا n توانی از 2 باشد.

اثبات. حکم بلافاصله از گزاره 2-2-10، قضیه 2-1-4 و نتیجه 2-4-2 بدست می آید. □

در شکل 2-2-1، ساختار گراف $\Gamma(2^2)$ نشان داده شد. در شکل 2-2-5، گراف مکرر عدد اول فرمای $F_2 = 17$ نشان داده شده است.



شکل 2-2-5

نتیجه 2-4-8 عدد فرمای F_m مرکب است اگر و فقط اگر وجود داشته باشد $x \in \{2,3,\ldots,F_m - 1\}$ به طوری که $x^2 \equiv x \pmod{F_m}$.

یادآوری 2-4-9 با توجه به قضیه 2-1-1 عدد فرمای F_m فاقد مربع کامل است اگر و فقط اگر $x^2 \not\equiv 0 \pmod{F_m}$ به ازای $x \in \{1,\ldots,F_m - 1\}$.

برای قضایای 2-4-10 و 2-4-10 که بعد بیان می کنیم، فرض شده $\lambda(n)$ به عوامل اول رابطه (۳،۱) تجزیه می شود. قضیه 2-4-10 نتیجه روگزز [۱۱] را از عدد اول n به عدد طبیعی n تعمیم می دهد.

قضیه 2-4-10 گراف $\Gamma(n)$ دقیقاً ۳ مؤلفه دارد اگر و فقط اگر $n = 9$ یا $n = 25$ یا n اول و $q = (n-1)/2^k$ هم، اول باشد به طوری که ۲ ریشه اولیه به پیمانه q باشد.

اثبات. ابتدا فرض کنید $\Gamma(n)$ دقیقاً ۳ مؤلفه دارد. با توجه به گزاره 2-2-10 و قضیه 2-3-4، 2-4-1 و 2-4-7، این موضوع برقرار است اگر و فقط اگر $n = p^k$ به ازای عدد اول فرد p، $k \geq 1$ و $\Gamma_1(n)$ یک دور یکتا با طول بزرگتر از ۱ دارد. فرض کنید t طول این دور یکتا در $\Gamma_1(n)$ باشد. بنا به (۴،۴)، عدد صحیح فرد $d > 1$ وجود دارد به طوری که $d = \mathrm{ord}_n a$ اگر a رأسی از این t-دور در $\Gamma_1(n)$ باشد. علاوه بر این، بنا به قضیه 2-3-3، $t = \mathrm{ord}_d 2$ و $d \mid \lambda(n)$.

چون رئوس $\Gamma_1(n)$ یک گروه دوری با ضرب به پیمانه n تشکیل می دهند، تعداد رئوس a در $\Gamma_1(n)$ به ازای $d = \mathrm{ord}_n a$ برابر است با $\varphi(d)$. بنابراین t-دور یکتایی در $\Gamma_1(n)$ وجود دارد اگر و فقط اگر به ازای d فرد،

$$\sum_{\substack{d \mid \lambda(n) \\ \mathrm{ord}_d 2 = t}} \frac{\varphi(d)}{t} = \frac{\varphi(d)}{\mathrm{ord}_d 2} = 1.$$

لذا لازم است که $\lambda(n)$ مقسوم علیه فرد یکتای $d>1$ داشته باشد و ۲ ریشه اولیه به پیمانه d باشد.
حال فرض کنید $k \geq 2$. در این صورت $\lambda(n)=p^{k-1}(p-1)$. بنابراین $\lambda(n)$ مقسوم علیه فرد یکتای $d>1$ دارد اگر و فقط اگر $k=2$ و $p-1$ توانی از ۲ است. لذا $d=p$ و d عدد اول فرما باشد. به هر حال ۲ ریشه اولیه به پیمانه عدد اول فرمای $F_m = 2^{2^m}+1$ است اگر و فقط اگر $m \in \{0,1\}$. در نتیجه $n=3^2=9$ یا $n=5^2=25$.

همچنین، فرض کنید $k=1$. در این صورت $\lambda(n)=p-1$ و $p-1$ مقسوم علیه اول فرد یکتای $q>1$ اگر و فقط اگر

$$n-1=\lambda(n)=2^h q,$$

که q عدد اول فرد است. بنابراین t -دور $\Gamma_1(n)$ یکتاست اگر و فقط اگر ۲ ریشه اولیه به پیمانه q باشد. لذا حکم ثابت شد. □

یادآوری 2-4-11 برای مثال، $\Gamma(n)$ دقیقاً ۳ مؤلفه دارد اگر(با شکل 2-2-2 مقایسه کنید)

$$n=7, 9, 11, 13, 23, 25, 41, 53.$$

قضیه زیر بدون اثبات داده شده که اثبات آن شبیه قضیه 2-4-7 و 2-4-10 می باشد.

قضیه 2-4-12 گراف $\Gamma(n)$ دقیقاً ۴ مؤلفه دارد اگر و فقط اگر یکی از شرایط زیر برقرار باشد:

(i) $n=27$ یا $n=125$.

(ii) n اول است و $p=(n-1)/2^h$ نیز اول است به ازای $\operatorname{ord}_p 2=(p-1)/2$.

(iii) n اول است به طوری که $p=(n-1)/2^h$ مربع عدد اول q و ۲ ریشه اولیه به پیمانه q^2 است.

(iv) n حاصل ضرب دو عدد صحیح نسبت به هم اول $q_1>1$ و $q_2>1$ است که هر کدام با عدد اول فرما یا توانی از ۲ برابر است.

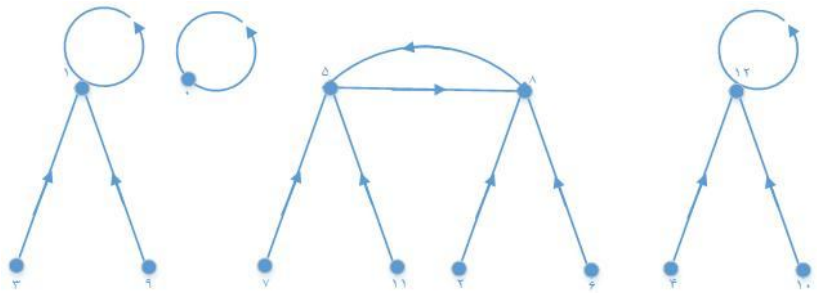
یادآوری 2-4-13 برای مثال، $\Gamma(n)$ دقیقاً ۴ مؤلفه دارد اگر(با شکل 2-2-3 مقایسه کنید)

$$n=6, 10, 12, 15, 19, 20, 24, 27, 29, 34, 37, 40, 47, 48, 51.$$

فصل سوم

3-1 ساختار گراف $\Gamma(n)$

تعریف 3-1-1 گراف جهت دار $\Gamma(n)$ را با رئوس متعلق به مجموعه $H = \{0,1,...,n-1\}$ گراف **جهت دار مکرر** می نامیم به طوری که دقیقاً یک یال جهت دار از $a \in H$ به $b \in H$ وجود دارد اگر و فقط اگر $a^3 \equiv b \pmod n$.



شکل 3-1-1

گراف $\Gamma(13)$ در شکل 3-1-1 داده شده است.

فرض کنید $a_1, a_2, \ldots, a_t \in H$ دو بدو مجزا باشند و

$$a_1^3 \equiv a_2 \pmod n,$$

$$a_2^3 \equiv a_3 \pmod n,$$

$$\vdots$$

$$a_t^3 \equiv a_1 \pmod n.$$

در این صورت $a_1, a_2, \ldots, a_t$ یک دور به طول t تشکیل می دهند. دوری به طول t را یک t- **دور** گوئیم که بر خلاف جهت حرکت ساعت می باشد. دوری به طول 1 را **نقطه ثابت** گوئیم.

تعریف 3-1-2 فرض کنید $x^3 \equiv y \pmod n$. در این صورت گوییم x به y توسط

$f(x) \equiv x^3 \pmod n$ نگاشته می شود.

حال زیر گراف های $\Gamma(n)$ را معرفی می کنیم.

تعریف 3-1-3 فرض کنید $\Gamma_1(n)$ توسط رئوسی که نسبت به n اول هستند و $\Gamma_2(n)$ توسط رئوسی که نسبت به n اول نیستند، تعیین شوند. مشاهده می کنیم که $\Gamma_1(n)$ و $\Gamma_2(n)$ مجزا هستند و $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$. واضح است که $0 \in \Gamma_2(n)$ و به ازای $n > 1$، اعداد 1 و $n-1$ متعلق به $\Gamma_1(n)$ می باشند.

مشاهدات ساده: فرض کنید $k, l \in \{1, \ldots, n-1\}$. در این صورت:

(i) k به 0 (یا به ازای هر n، به $\frac{n}{2}$) نگاشته می شود اگر و فقط اگر $(n-k)$ به 0 (یا به ازای هر n، به $\frac{n}{2}$) نگاشته شود.

(ii) k به l نگاشته می شود اگر و فقط اگر $(n-k)$ به $(n-l)$ نگاشته شود.

(iii) k نقطه ثابت مجزاست اگر و فقط اگر $(n-k)$ نقطه ثابت مجزا باشد.

(iv) k قسمتی از یک t- دور است اگر و فقط اگر $(n-k)$ قسمت دیگری از t- دور باشد. علاوه بر این مجزا بودن یکی از این t- دور، مستلزم مجزا بودن دیگری است.

گزاره 4-1-3 اعداد $0, 1, n-1$ نقاط ثابت $\Gamma(n)$ هستند. علاوه بر این، 0 نقطه ثابت مجزای $\Gamma(n)$ است اگر و فقط اگر n فاقد مربع باشد.

اثبات. واضح است که

$$0^3 \equiv 0 \pmod n,$$

$$1^3 \equiv 1 \pmod n$$

و

$$(n-1)^3 \equiv n-1 \pmod n.$$

حال فرض کنید n عامل مربع داشته باشد، در این صورت $p^2 \mid n$ به ازای عدد اول p. همچنین

$$\left(\frac{n}{p}\right)^3 = n.\frac{n}{p}.\frac{n}{p^2} \equiv 0 \pmod n.$$

لذا $\frac{n}{p}$ به 0 نگاشته می شود و 0 نقطه ثابت مجزا نیست.

برعکس، فرض کنید n فاقد مربع باشد. در این صورت وجود ندارد k, $2 \le k \le n-2$ بطوری که

$n \mid k^3$. بنابراین 0 مجزا است. □

تعریف 3-1-5 گراف جهت دار را **منظم** گوییم اگر درجه ورودی هر رأس یک باشد.

هر مؤلفه گراف جهت دار یک دور است.

تعریف 3-1-6 گراف جهت دار را **نیم منظم** گوییم اگر عدد صحیح مثبت d وجود داشته باشد به طوری که درجه ورودی هر رأس یا d یا 0 باشد.

تعریف 3-1-7 گراف جهت دار را **درخت جهت دار** m **- شاخه** با ریشه r گوییم اگر و فقط اگر $\text{indeg}(r) = m$، همچنین درجه ورودی هر رأس مجاور به ریشه برابر m است (دقیقاً m همسایه دارد). به طور مشابه درجه ورودی هر رأس از این m همسایه، m می باشد و به همین ترتیب.

فرض کنید

$$\omega(n) = \begin{cases} t+1 & 3^2 \mid n \\ t & 3^2 \nmid n \end{cases}$$

که در آن t تعداد اعداد اول مجزایی است که در همنهشتی $p \equiv 1 \pmod 3$ صدق می کند.

برای هر عدد طبیعی n، قضیه زیر برقرار است.

قضیه 3-1-8 گراف جهت دار $\Gamma_1(n)$ نیم منظم است اگر و فقط اگر $3 \mid \varphi(n)$. در این حالت درجه ورودی هر رأس $\Gamma_1(n)$ یا برابر $3^{\omega(n)}$ یا 0 می باشد.

اثبات. از آنجا که رئوس $\Gamma_1(n)$ یک گروه با مرتبه $\varphi(n)$ ($\varphi(n)$ تابع اویلر) نسبت به ضرب به پیمانه n تشکیل می دهند، ثابت می کنیم اگر $\text{indeg}(a) > 0$ و $\gcd(a,n) = 1$، آنگاه $\text{indeg}(a) = \text{indeg}(1)$، یعنی تعداد جواب های همنهشتی $x^3 \equiv a \pmod n$ و $x^3 \equiv 1 \pmod n$ برابر است. همچنین ادعا می کنیم اگر $x_1, x_2, \ldots, x_k$ تنها جواب های همنهشتی $x^3 \equiv 1 \pmod n$ و b جوابی از $x^3 \equiv a \pmod n$ باشند، آنگاه $x_1 b, x_2 b, \ldots, x_k b$ تنها جواب های همنهشتی $x^3 \equiv a \pmod n$ است. چون

$$(x_i b)^3 \equiv x_i^3 b^3 \equiv a \pmod n \qquad i = 1, \ldots, k$$

و

$$x_i b = x_j b \Rightarrow x_i = x_j \qquad i, j = 1, \ldots, k$$

همچنین اگر c جواب دیگری از همنهشتی $x^3 \equiv a \pmod n$ باشد داریم:

$$c^3 \equiv b^3 \pmod n \Rightarrow c^3 b^{-3} \equiv 1 \pmod n \Rightarrow (cb^{-1})^3 \equiv 1 \pmod n \Rightarrow cb^{-1} = x_i \Rightarrow c = x_i b.$$

ابتدا فرض کنید $n = p^\alpha$ به ازای عدد اول p و $\alpha \geq 1$. تعداد جواب های همنهشتی:

$$x^3 \equiv 1 \pmod n \quad \Leftrightarrow \quad (x-1)(x^2 + x + 1) \equiv 0 \pmod n$$

را تعیین می کنیم. اگر $3^2 \mid n$ یا $p \equiv 1 \pmod 3$، آن گاه $p-1=3k$، به ازای متغیر k. با انتخاب $x=3k, 3k-1, 3k+1$ به ازای متغیر k داریم:

$$x=3k \Rightarrow (x-1)(x^2+x+1)=(3k-1)(9k^2+3k+1)\neq 0$$
$$x=3k-1 \Rightarrow (x-1)(x^2+x+1)=(3k-2)(9k^2-3k+1)\neq 0$$
$$x=3k+1 \Rightarrow (x-1)(x^2+x+1)=(3k)(9k^2+9k+3)=0$$

بنابراین به ازای $x=3k+1$، (x^2+x+1) فقط شامل یک عامل 3 و $(x-1)$ شامل بقیه عوامل 3 است. از طرفی چون $x^3 \equiv 1 \pmod{p^\alpha}$ و $3^2 \mid p^\alpha$ ، $\alpha \geq 2$. بنابراین $x^3 \equiv 1 \pmod{3^\alpha}$.

اگر $x=3^{\alpha-1}t+1$ به ازای متغیر t، آنگاه

$$\begin{aligned}(x-1)(x^2+x+1) &= (3^{\alpha-1}t)((3^{\alpha-1}t+1)^2+3^{\alpha-1}t+1+1)\\ &= (3^{\alpha-1}t)(3^{2(\alpha-1)}t^2+2\cdot 3^{\alpha-1}t+1+3^{\alpha-1}t+1+1)\\ &= (3^{\alpha-1}t)(3^{2(\alpha-1)}t^2+2\cdot 3^{\alpha-1}t+3^{\alpha-1}t+3)\\ &= (3^{\alpha-1}t)(3k)\\ &= 3^\alpha tk\end{aligned}$$

در نتیجه $x^3-1\equiv 0 \pmod{3^\alpha}$. از این رو به ازای $t=0,1,2$، $x=1, 3^{\alpha-1}+1, 2\cdot 3^{\alpha-1}+1$ تنها جواب های همنهشتی $x^3 \equiv 1 \pmod n$ می باشند. فرض کنید $\rho(n)$ تعداد جواب های همنهشتی $x^3 \equiv 1 \pmod n$ باشد. در این صورت

$$\rho(n)=\begin{cases}3 & 3^2 \mid n,\ p \equiv 1 \pmod 3\\ 1 & \text{در غیر این صورت}\end{cases}$$

علاوه بر این، اگر n عدد طبیعی دلخواه و f چند جمله ای با ضرایب صحیح باشد، آنگاه تابع

$$\rho_f(n) = \left|\{0 \leq m \leq n-1 :\ f(m) \equiv 0 \pmod n\}\right|$$

ضربی است. لذا $\mathrm{indeg}(a)=1$ یا $\mathrm{indeg}(a)=3^{\omega(n)}$.

فرض کنید $\Gamma_1(n)$ نیم منظم است و $a \in \Gamma_1(n)$ به طوری که $\mathrm{indeg}(a)=3^{\omega(n)}$. اگر

$$H=\{0 \leq m \leq n-1 \mid (n,m)=1,\ m^3 \equiv 1 \pmod n\}.$$

آن گاه زیر گروهی از $\Gamma_1(n)$ است. در نتیجه مرتبه H مرتبه $\Gamma_1(n)$ را عاد می کند یعنی

$$3^{\omega(n)} \mid \varphi(n) \Rightarrow 3 \mid \varphi(n).$$

بر عکس فرض کنید $3 \nmid \varphi(n)$. در این صورت درجه ورودی هر رأس $\Gamma_1(n)$ برابر 1 است و در نتیجه

هر مؤلفه $\Gamma_1(n)$ دور است. □

نتیجه زیر به آسانی از قضیه بالا به دست می آید.

نتیجه 3-1-9 گراف جهت دار $\Gamma_1(n)$ منظم (هر مؤلفه $\Gamma_1(n)$ دور است) است اگر و فقط اگر $3 \nmid \varphi(n)$.

اثبات. با توجه به قضیه، قبل اثبات واضح است.

قضیه3-1-10 هر مؤلفه گراف جهت دار $\Gamma(n)$ دور است اگر و فقط اگر $3 \nmid \varphi(n)$ و n فاقد مربع کامل باشد.

اثبات. فرض کنید $3 \nmid \varphi(n)$ و n فاقد مربع کامل باشد. نشان می دهیم $\Gamma_2(n)$ منظم است. فرض کنید $a \neq 0$ یک رأس دلخواه $\Gamma_2(n)$ باشد و $d = \gcd(a,n)$ که در آن $\gcd(a,n)$ بزرگترین مقسوم علیه مشترک a و n است.

ابتدا فرض کنید $p \mid d$ به ازای عدد اول p. اگر b جواب همنهشتی $b^3 \equiv a \pmod{n}$ باشد، آنگاه

$$\left.\begin{matrix} d \mid b^3 - a \\ p \mid d \end{matrix}\right\} \Rightarrow p \mid b^3 \Rightarrow p \mid b \Rightarrow b \equiv 0 \pmod{p}$$

به ازای اعداد اول p که $p \mid d$. همچنین $b^3 \equiv a \equiv 0 \pmod{p}$، به ازای تمام اعداد اول p که $p \mid d$. با توجه به گزاره 3-1-4 جواب b یکتاست یعنی اگر $b^3 \equiv a \pmod{n}$ و $p \mid d$، آن گاه $p \mid a$ و $b^3 \equiv a \equiv 0 \pmod{p}$. لذا $p \mid b^3$ و در نتیجه $p \mid b$، به ازای تمام اعداد اول p که $p \mid d$.

حال فرض کنید $p \mid \frac{n}{d}$ به ازای اعداد اول p. در گروه دوری U_{p-1}□، چون $3 \nmid (p-1)$، لذا 3 مولد گروه است و معکوس ضربی دارد. در نتیجه وجود دارد x به طوری که $3x \equiv 1 \pmod{(p-1)}$. قرار دهید $b \equiv a^x \pmod{p}$. با ضرب طرفین همنهشتی در b^2 داریم:

$$b^3 \equiv b^2 a^x \equiv (a^x)^3 \pmod{p} \Rightarrow b^3 \equiv a^{3x} \pmod{p} \qquad (1,1)$$

از آن جایی که

$$\begin{matrix} 3x \equiv 1 \pmod{(p-1)} \Rightarrow 3x - 1 = k(p-1) \Rightarrow 3x = k(p-1) + 1 \\ \Rightarrow a^{3x} \equiv a^{k(p-1)+1} \equiv a^{k(p-1)}.a \equiv a \pmod{p}. \end{matrix} \qquad (1,2)$$

در رابطه بالا، با توجه به $a \in \Gamma_2(n)$، $(a,n) \neq 1$، $p \nmid a$ و بنا به قضیه کوچک فرما، $a^{(p-1)} \equiv 1 \pmod{p}$ برقرار است. همچنین بنا به رابطه های (1,1) و (1,2)، $b^3 \equiv a \pmod{p}$.

با توجه به قضیه چینی، نتیجه می شود که $b^3 \equiv a \pmod{n}$. چون 3 به پیمانه $p-1$ وارون پذیر است و بنا به قضیه کوچک فرما، جواب b یکتا است. فرض کنید

$$\left.\begin{matrix} b_{۱}^{۳} \equiv a \pmod{n} \\ b_{۲}^{۳} \equiv a \pmod{n} \end{matrix}\right\} \Rightarrow b_{۱}^{۳} \equiv b_{۲}^{۳} \pmod{n} \Rightarrow b_{۱}^{۳} \equiv b_{۲}^{۳} \pmod{p}$$
$$\Rightarrow b_{۱}^{۳x} \equiv b_{۲}^{۳x} \pmod{p} \Rightarrow b_{۱}^{k(p-۱)+۱} \equiv b_{۲}^{k(p-۱)+۱} \pmod{p}$$
$$\Rightarrow b_{۱}^{k(p-۱)}.b_{۱} \equiv b_{۲}^{k(p-۱)}.b_{۲} \pmod{p} \Rightarrow b_{۱} \equiv b_{۲} \pmod{p} \Rightarrow b_{۱} \equiv b_{۲} \pmod{n}.$$

با توجه به نتیجه قبل، $\Gamma_{۱}(n)$ منظم و لذا $\Gamma(n)$ منظم است. □

فرض کنید $n = ۲^{m} p_{۱}^{\alpha_{۱}} p_{۲}^{\alpha_{۲}} \ldots p_{s}^{\alpha_{s}}$ تجزیه n به عوامل اول باشد که در آن $p_{۱} < p_{۲} < \ldots < p_{s}$ اعداد اول فرد مجزا هستند و $\alpha_{i} \geq ۱$، $m \geq 0$ و $s \geq 0$.

قضیه زیر فرمولی برای تعداد نقاط ثابت گراف جهت دار $\Gamma(n)$ ارائه می دهد.

قضیه 3-1-11 تعداد $L(n)$ از نقاط ثابت گراف $\Gamma(n)$ برابر است با:

$$L(n) = \begin{cases} ۳^{s} & m = 0 \\ ۲.۳^{s} & m = ۱ \\ ۳.۳^{s} & m = ۲ \\ ۵.۳^{s} & m \geq ۳. \end{cases}$$

اثبات. عنصر a، که $0 \leq a \leq n-۱$ نقطه ثابت $\Gamma(n)$ است اگر و فقط اگر a صفر چند جمله ای $f_{۰}(x) \equiv x^{۳} - x \pmod{n}$ باشد. همچنین $\rho_{f_{۰}}(۲) = ۲$ و $\rho_{f_{۰}}(۲^{۲}) = ۳$. به ازای $n = ۲^{m}$، $m \geq ۳$، صفر های $f_{۰}$ متعلق به مجموعه $\{۰, ۱, ۲^{m-۱}-۱, ۲^{m-۱}+۱, n-۱\}$ هستند. در نتیجه $\rho_{f_{۰}}(۲^{m}) = ۵$.

فرض کنید $n = p^{\alpha}$ که در آن عدد اول $p \geq ۳$ و $\alpha \geq ۱$. در این صورت صفر های $f_{۰}$ متعلق به مجموعه $\{۰,۱, n-۱\}$ هستند. در نتیجه $\rho_{f_{۰}}(p^{\alpha}) = ۳$. چون تابع $\rho_{f_{۰}}(n)$ ضربی است، لذا اثبات تمام است. □

قضیه 3-1-12 فرض کنید $n > ۲$. در این صورت دوری به طول t در گراف $\Gamma(n)$ وجود دارد اگر و فقط اگر $t = \mathrm{ord}_{d} ۳$ به ازای مقسوم علیه مثبت زوج d از $\lambda(n)$.

اثبات. فرض کنید a رأسی از یک t-دور در $\Gamma(n)$ باشد. در این صورت

$$a^{۳^{t}} \equiv a \pmod{n}. \qquad (1,3)$$

ثابت می کنیم t کوچکترین عدد صحیح مثبتی است که در رابطه بالا صدق می کند. کافی است ثابت کنیم در $\Gamma(n)$ دورها مجزایند. اگر فرض کنید دو دور به طول $t_{۱}$ و $t_{۲}$ در $\Gamma(n)$ وجود دارد که حداقل در یک رأس اشتراک داشته باشند، از این رأس 2 یال خارج می شود که یکی متعلق به دور $t_{۱}$ و دیگری متعلق به دور $t_{۲}$ است و با این مطلب که درجه خروجی هر رأس برابر 1 است در تناقض است. لذا در

$\Gamma(n)$ دورها مجزایند.

t کوچکترین عدد صحیح مثبتی است که

$$a^{۳^t} - a \equiv a(a^{۳^t-۱}-۱) \equiv 0 \pmod{n}.$$

چون $\gcd(a, a^{۳^t-۱}-۱) = ۱$، لذا اگر $n_۱ = \gcd(a,n)$ و $n_۲ = n/n_۱$، آنگاه ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که

$$a \equiv 0 \pmod{n_۱}, \qquad a^{۳^t-۱} \equiv ۱ \pmod{n_۲} \qquad (1,4)$$

و $\gcd(n_۱, n_۲) = ۱$. فرض کنید $t_۱ < t$ به طوری که

$$\left.\begin{array}{l} a^{۳^{t_۱}-۱} \equiv ۱ \pmod{n_۲} \\ a^{۳^{t_۱}-۱} \equiv ۱ \pmod{n_۱} \end{array}\right\} \Rightarrow \left.\begin{array}{l} a^{۳^{t_۱}} \equiv a \pmod{n_۲} \\ a^{۳^{t_۱}} \equiv a \equiv 0 \pmod{n_۱} \end{array}\right\} \Rightarrow a^{۳^{t_۱}} \equiv a \pmod{n}$$

که با رابطه (1,3) تناقض دارد. برعکس اگر فرض کنید $t_۱ < t$ به طوری که

$$a^{۳^{t_۱}} \equiv a \pmod{n} \Rightarrow \begin{cases} (a,n) = ۱ \Rightarrow a^{۳^{t_۱}} \equiv ۱ \pmod{n} \Rightarrow a^{۳^{t_۱}} \equiv ۱ \pmod{n_۲} \\ (a,n) \neq ۱ \Rightarrow a^{۳^{t_۱}} \equiv ۱ \pmod{n} \Rightarrow a^{۳^{t_۱}} \equiv ۱ \pmod{n_۲} \end{cases}$$

که با رابطه (1,4) تناقض دارد. بنا به قضیه باقیمانده چینی عدد صحیح b وجود دارد به طوری که

$$b \equiv ۱ \pmod{n_۱}, \qquad b \equiv a \pmod{n_۲}.$$

با برهان خلف ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که

$$\left.\begin{array}{l} b^{۳^t-۱} \equiv ۱ \pmod{n_۱} \\ b^{۳^t-۱} \equiv a^{۳^t-۱} \equiv ۱ \pmod{n_۲} \end{array}\right\} \Rightarrow b^{۳^t-۱} \equiv ۱ \pmod{n}.$$

فرض کنید $t_۱ < t$ به قسمی که:

$$\left.\begin{array}{l} a^{۳^{t_۱}} \equiv a \pmod{n_۲} \\ a^{۳^{t_۱}} \equiv a \equiv 0 \pmod{n_۱} \end{array}\right\} \Rightarrow a^{۳^{t_۱}} \equiv a \pmod{n}$$

که تناقض است.

حال فرض کنید $c = \mathrm{ord}_n b$. در این صورت بنا به تعریف مرتبه، $۳^t \equiv ۱ \pmod{c}$. اگر c فرد باشد آنگاه بنا به $۳^t \equiv ۱ \pmod{۲}$، با برهان خلف ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که $۳^t \equiv ۱ \pmod{۲c}$. فرض کنید $t_۱ < t$ به قسمی که

$$۳^{t_۱} \equiv ۱ \pmod{۲c} \Rightarrow ۲c \mid ۳^{t_۱} - ۱ \begin{cases} ۲ \mid ۳^{t_۱} - ۱ \\ c \mid ۳^{t_۱} - ۱ \Rightarrow ۳^{t_۱} - ۱ = cx. \end{cases}$$

$$, b^{c} \equiv ۱ \pmod n \Rightarrow b^{cx} \equiv ۱ \pmod n \Rightarrow b^{۳^{n}-۱} \equiv ۱ \pmod n \Rightarrow \begin{cases} b^{۳^{n}-۱} \equiv ۱ \pmod{n_۱} \\ b^{۳^{n}-۱} \equiv ۱ \pmod{n_۲} \end{cases}$$

که تناقض است.

اگر

$$d = \begin{cases} ۲c & c \text{ فرد} \\ c & c \text{ زوج} \end{cases}$$

آنگاه با استفاده از قضیه کارمایکل می توان نتیجه گرفت $t = \mathrm{ord}_d ۳$ و $d \mid \lambda(n)$.

بر عکس، فرض کنید $t = \mathrm{ord}_d ۳$ و d مقسوم علیه مثبت زوج $\lambda(n)$ باشد. بنا به قضیه کارمایکل، باقیمانده g به پیمانه n وجود دارد به طوری که $\mathrm{ord}_n g = \lambda(n)$. قرار دهید $h = g^{\lambda(n)/d}$، لذا $\mathrm{ord}_n h = d$. چون $d \mid ۳^{t} - ۱$ و به ازای $۱ \le k < t$ ، $d \nmid ۳^{k} - ۱$، بنابراین t کوچکترین عدد صحیح مثبتی است که

$$h^{۳^{t}-۱} \equiv ۱ \pmod n, \qquad h.h^{۳^{t}-۱} \equiv h^{۳^{t}} \equiv h \pmod n.$$

در نتیجه h رأسی از یک t-دور در $\Gamma(n)$ است و اثبات تمام است. □

قضیه 3-1-12 تعداد مؤلفه های $\Gamma(n)$، 3 است اگر و فقط اگر $n = ۴$ یا به ازای عدد طبیعی k، $n = ۳^{k}$ یا n عدد اولی به فرم $n = ۲.۳^{k} + ۱$ باشد.

اثبات. اگر $\Gamma(n)$ دقیقاً 3 مؤلفه داشته باشد، یعنی حداکثر 3 نقطه ثابت دارد. لذا بنا به قضیه 3-1-11، $n = ۴$ یا n توانی از یک عدد اول فرد است. همچنین ثابت می کنیم به ازای $t > ۱$، دوری به طول t وجود ندارد. فرض کنید دوری بطول 2 بین نقطه ثابت a و رأس b وجود داشته باشد. در اینصورت

$$\left.\begin{aligned} a^{۳} &\equiv b \pmod n \\ a^{۳} &\equiv a \pmod n \end{aligned}\right\} \Rightarrow a = b$$

که تناقض است. لذا دوری بطول بیشتر از 1 وجود ندارد. در نتیجه بنا به قضیه 3-1-12، $d \nmid ۳^{t} - ۱$ به ازای $t > ۱$ و هر مقسوم علیه زوج $d > ۲$ از تابع کارمایکل $\lambda(n)$. که با توجه به این مطلب، می‌توان نتیجه گرفت که $۳ \mid d$ و $\lambda(n) = ۲.۳^{l}$ به ازای عدد طبیعی l. در نهایت ثابت می کنیم به ازای عدد طبیعی

k، $n = ۳^k$ یا n عدد اول به فرم $n = ۲۰۳^k + ۱$ می باشد. فرض کنید $n = ۲^{\alpha} ۳^{\gamma} p_{۱}^{\beta_{۱}} ... p_s^{\beta_s}$ تجزیه n به عوامل اول باشد که در آن $p_i \geq ۵$ اعداد اول فرد مجزا هستند و $\alpha \geq 0$، $\beta_i \geq ۱$، $\gamma \geq 0$ و $s \geq 0$. در این صورت

$$\begin{aligned} \lambda(n) &= \text{lcm}\,[\lambda(۲^{\alpha}), \lambda(۳^{\gamma}), \lambda(p_{۱}^{\beta_{۱}}), ..., \lambda(p_s^{\beta_s})] \\ &= \text{lcm}\,[\lambda(۲^{\alpha}), ۲۰۳^{\gamma-۱}, (p_{۱}-۱)p_{۱}^{\beta_{۱}-۱}, ..., (p_s-۱)p_s^{\beta_s-۱}] \end{aligned}$$

حالت های زیر وجود دارد:

(i) اگر $\alpha = 0$، γ دلخواه و $\beta_{۱} = ... = \beta_s = ۱$، آنگاه

$$n = ۳^{\gamma} p_{۱} ... p_s \Rightarrow \lambda(n) = \text{lcm}\,[۲۰۳^{\gamma-۱}, (p_{۱}-۱), ..., (p_s-۱)] = ۲۰۳^l$$

(ii) اگر $\alpha = ۱$، γ دلخواه و $\beta_{۱} = ... = \beta_s = ۱$، آنگاه

$$n = ۲۰۳^{\gamma} p_{۱} ... p_s \Rightarrow \lambda(n) = \text{lcm}\,[۱۰۲۰۳^{\gamma-۱}, (p_{۱}-۱), ..., (p_s-۱)] = ۲۰۳^l$$

(iii) اگر $\alpha = ۲$، γ دلخواه و $\beta_{۱} = ... = \beta_s = ۱$، آنگاه

$$n = ۲^{۲} \cdot ۳^{\gamma} p_{۱} ... p_s \Rightarrow \lambda(n) = \text{lcm}\,[۲۰۲۰۳^{\gamma-۱}, (p_{۱}-۱), ..., (p_s-۱)]$$

(iv) اگر $\alpha = \gamma = 0$، $\beta_{۱} = ... = \beta_s = ۱$، آنگاه

$$n = p_{۱} ... p_s \Rightarrow \lambda(n) = \text{lcm}\,[(p_{۱}-۱), ..., (p_s-۱)] = ۲۰۳^l$$

همچنین می دانیم

$$\begin{cases} p_i - ۱ = ۲^{۰} \cdot ۳^k \Rightarrow p_i = ۳^k + ۱ \\ p_i - ۱ = ۲۰۳^k \Rightarrow p_i = ۲۰۳^k + ۱ \end{cases} \quad \because$$

لذا با توجه به حالت های بالا، $n = ۳^k$ یا n عدد اول به فرم $n = ۲۰۳^k + ۱$ می باشد.

برعکس، اگر $n = ۴$ آنگاه $\Gamma(n)$، دقیقاً 3 مؤلفه دارد. فرض کنید $n = ۳^k$ یا n عدد اول به فرم $n = ۲۰۳^k + ۱$ باشد. در این صورت $\Gamma(n)$، دقیقاً 3 نقطه ثابت دارد و $\lambda(n) = ۲,۳^l$. در این حالت اگر بیشتر از 3 مؤلفه داشته باشیم، با توجه به قضیه قبل دوری به طول $t > ۱$ وجود دارد که در آن $t = \text{ord}_d ۳$ و d مقسوم علیه مثبت زوج $\lambda(n)$ می باشد. در نتیجه t کوچکترین عدد صحیح مثبتی است که $۳^t \equiv ۱ \pmod{d}$ و $d | ۳^t - ۱$. از طرفی دیگر چون $d | \lambda(n) = ۲۰۳^l$، $d = ۲ | ۳^t - ۱$ یعنی $t = ۱$ که تناقض است. بنابراین تنها دور های $\Gamma(n)$ نقاط ثابت $۱,0$ و $n - ۱$ می باشد. □

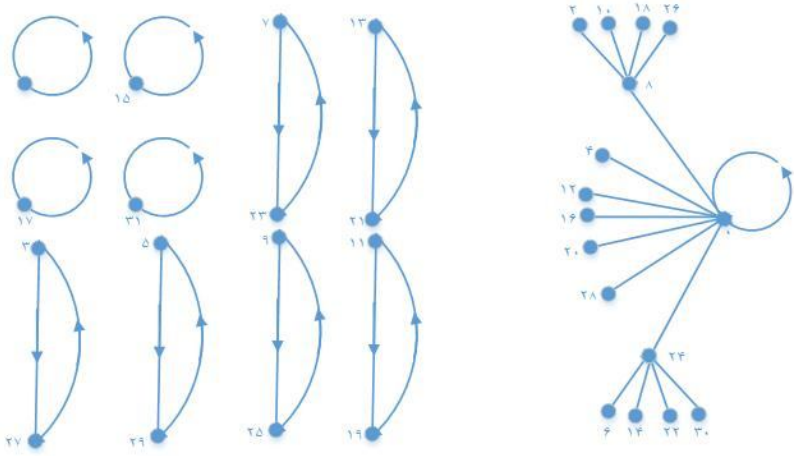
گراف های $\Gamma(۲^{۵})$ و $\Gamma(۳^{۳})$ را در نظر بگیرید. گراف $\Gamma_{۱}(۲^{۵})$ شامل 4 نقطه ثابت و 6 دور به طول 2 و گراف $\Gamma_{۲}(۲^{۵})$ درختی جهت دار با ریشه 0 می باشد (شکل 3-1-2 را ببینید). همچنین گراف $\Gamma_{۱}(۳^{۳})$ شامل دو درخت جهت دار یکریخت با ریشه های ۱ و $۲۶ = ۱ - ۳^{۳}$ و گراف $\Gamma_{۲}(۳^{۳})$ درختی جهت دار با ریشه 0 می باشد (شکل 3-1-3 را ببینید).

یادآوری. برای عدد حقیقی دلخواه a، کوچکترین عدد طبیعی بزرگتر یا مساوی a را با $\lceil a \rceil$ نمایش می دهیم.

قضیه 3-1-13 فرض کنید k عدد طبیعی باشد. گراف $\Gamma_{۱}(۲^{k})$ فقط شامل (بجز 4 نقطه ثابت) دور هایی به طول توان هایی از 2 و گراف $\Gamma_{۲}(۲^{k})$ درختی با ریشه 0 می باشد. علاوه بر این $indeg(0) = ۲^{k-\lceil k/۳ \rceil}$.

اثبات. اگر $n = ۲^{k}$، آنگاه هر گراف $\Gamma_{۱}(n)$ و $\Gamma_{۲}(n)$ دقیقا شامل $\varphi(n) = ۲^{k-۱}$ رأس است. همچنین چون $۳ \nmid \varphi(n)$، با توجه به نتیجه 3-1-9 $\Gamma_{۱}(۲^{k})$ فقط شامل دور است. به راحتی می توان بررسی کرد 4 نقطه ثابت $۱، ۲^{k-۱}-۱، ۲^{k-۱}+۱$ و $۲^{k}-۱$ در $\Gamma_{۱}(۲^{k})$ وجود دارد. بنا به قضیه* می دانیم دوری به طول t وجود دارد اگر و فقط اگر $t = \mathrm{ord}_{d}\, ۳$ به ازای مقسوم علیه مثبت زوج d از $\lambda(n) = ۲^{k-۲}$. البته رتبه t از 3 در گروه ضربی رئوس $\Gamma_{۱}(n)$، رتبه گروه را که برابر با $\varphi(n) = ۲^{k-۱}$ است، عاد می کند. در نتیجه t توان 2 می باشد.

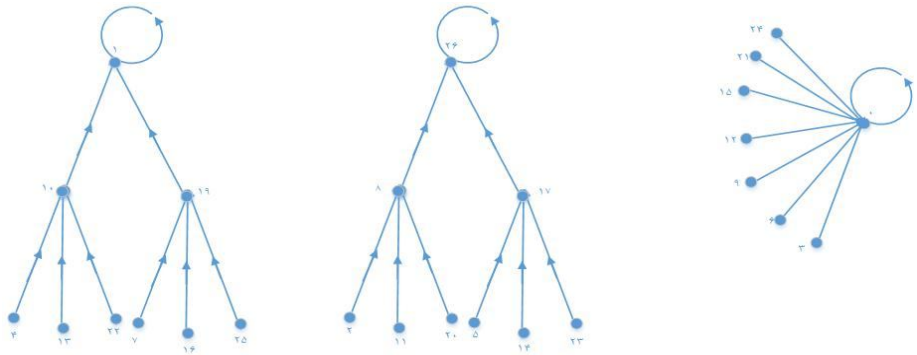
به آسانی می توان دید که $۲^{k-\lceil k/۳ \rceil}$ عنصر در $\Gamma_{۲}(۲^{k})$ وجود دارد که عبارتند از $۲^{\lceil k/۳ \rceil}, ۲.۲^{\lceil k/۳ \rceil}, ۳.۲^{\lceil k/۳ \rceil}, \ldots, ۲^{k-\lceil k/۳ \rceil}.۲^{\lceil k/۳ \rceil} = 0$ که به 0 نگاشته می شوند. همچنین همه رئوس w از $\Gamma_{۲}(۲^{k})$ مضارب 2 هستند که هر چه توان 2 بیشتر باشد، مسیر جهت دار از w به 0 کوتاه تر است. □



شکل 3-1-2. $\Gamma(۳^{۵})$

قضیه 3-1-14 فرض کنید k عدد طبیعی باشد. گراف $\Gamma_{۱}(۳^k)$ شامل دو درخت یکریخت با ریشه 1 و $۳^k - ۱$ می باشد. علاوه بر این، $\Gamma_{۲}(۳^k)$ درختی با ریشه ۰ است. همچنین $indeg(0) = ۳^{k-\lceil k/۳ \rceil}$.

اثبات. با توجه به قضیه 3-1-12 گراف $\Gamma(۳^k)$ دقیقا 3 مؤلفه با نقاط ثابت ۱,0 و $۳^k - ۱$ دارد. به آسانی می توان دید که $۳^{k-\lceil k/۳ \rceil}$ عنصر در $\Gamma_{۲}(۳^k)$ وجود دارد که عبارتند از $۳^{\lceil k/۳ \rceil}, ۲.۳^{\lceil k/۳ \rceil}, ۳.۳^{\lceil k/۳ \rceil}, \ldots, ۳^{k-\lceil k/۳ \rceil}.۳^{\lceil k/۳ \rceil} = 0$ که به 0 نگاشته می شوند. همچنین همه رئوس w از $\Gamma_{۲}(۳^k)$ مضارب 3 هستند که هر چه توان 3 بیشتر باشد، مسیر جهت دار از w به 0 کوتاه تر است. از آنجا که $۳ | \varphi(n) = ۲.۳^{k-۱}$ لذا $\Gamma_{۱}(۳^k)$ گراف نیم منظم است و درجه هر رأس یا 0 یا 3 می باشد. با توجه به مشاهدات ساده، گراف $\Gamma_{۱}(۳^k)$ شامل دو درخت یکریخت با $۳^k - ۱$ رأس در هر درخت است. □



شکل 3-1-3. $\Gamma(۳^{۳})$

2-3 گراف مقسوم علیه صفر حلقه Z_n

مفهوم گراف مقسوم علیه صفر حلقه های جابجایی توسط بک [۲] در سال 1988 معرفی شد. چنین گراف هایی با استفاده از ابزار گراف های تئوریک، برای مطالعه خواص جبری حلقه ها به ما کمک می کنند. در این پروژه فقط حلقه Z_n با عمل دوتایی جمع و ضرب به پیمانه n و مجموعه عناصر $Z_n = \{0,۱,\ldots,n-۱\}$ در نظر گرفته شده است. گراف مقسوم علیه صفر حلقه Z_n را با $G(Z_n)$ نشان می دهیم که رئوس آن متعلق به مجموعه $Z_n - \{0\}$ می باشد و دارای این خاصیت است که رئوس x و y مجاور هستند اگر و فقط اگر $x \neq y$ و $x.y \equiv 0 \pmod n$.

تعریف 3-2-1 عدد رنگی (تعداد یال های رنگی) گراف، کمترین تعداد رنگ هایی که بتوان به رئوس (یال ها) اختصاص داد به طوری که هر دو رأس (یال) مجاور، رنگ های متفاوتی داشته باشند.

تعریف 3-2-2 زیر گراف K_m را با m رأس یک **دسته** به اندازه m گوییم اگر هر دو رأس مجزای

آن مجاور باشند. تعداد دسته، کوچکترین کران بالای اندازه دسته هاست.

بک در سال 1988 نشان داد که عدد رنگی گراف $G(Z_n)$ برابر با تعداد دسته ها است. اکبری و محمدیان در سال 2004 ثابت کردند که تعداد یال های رنگی $G(Z_n)$ برابر با حداکثر درجه است (شکل 3-1-1 را ببینید). ما در این جا فرمول هایی برای محاسبه تعداد دسته ها و حداکثر درجه $G(Z_n)$ ارائه می دهیم.

فرض کنید $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} ... p_s^{\alpha_s}$ تجزیه n به عوامل اول باشد که در آن $p_۱ < p_۲ < ... < p_s$ اعداد اول مجزا هستند و $\alpha_i \geq ۱$، $s \geq ۱$. دو قضیه زیر را داریم.

گزاره 3-2-3 $n/p_۱$ رأسی با درجه ماکزیمال $n/p_۱ - ۱$ است.

اثبات. به آسانی می توان دید رأس $n/p_۱$ ، دقیقا $n/p_۱ - ۱$ همسایه در $G(Z_n)$ دارد که عناصر $p_۱, ۲p_۱, ۳p_۱, ..., (n/p_۱ - ۱)p_۱$ می باشد. عدد $p_۱$ کوچکترین عدد اول در تجزیه n می باشد. در نتیجه $n/p_۱ - ۱$ درجه ماکسیمم $G(Z_n)$ است. □

گزاره 3-2-4 فرض کنید n فاقد مربع کامل باشد، در این صورت تعداد دسته گراف $G(Z_n)$، 2 تا است. اگر α_i، به ازای $۱ \leq i \leq s$ اعداد زوج باشند، آنگاه تعداد دسته گراف $G(Z_n)$، برابر $(p_۱^{\alpha_۱/۲} p_۲^{\alpha_۲/۲} ... p_s^{\alpha_s/۲} - ۱)$ می باشد. از طرفی دیگر تعداد دسته، $(p_۱^{\beta_۱} p_۲^{\beta_۲} ... p_s^{\beta_s})$ می باشد که در آن $\beta_i = \alpha_i/۲$ به ازای α_i زوج و $\beta_i = (\alpha_i - ۱)/۲$ به ازای α_i فرد است.

اثبات. فرض کنید $n = p_۱ p_۲ ... p_s$، به ازای $۱ \leq i \leq s$، p_i اعداد اول مجزا هستند. در این صورت عناصر $p_۱$ و $p_۱ p_۲ ... p_s$ دو سر دسته $k_۲$ می باشند و دسته ای با اندازه ۳ وجود ندارد.

حال، فرض کنید $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} ... p_s^{\alpha_s}$ تجزیه n به عوامل اول باشد که در آن α_i، $۱ \leq i \leq s$، زوج هستند. در این صورت عنصر $\nu = p_۱^{\alpha_۱/۲} p_۲^{\alpha_۲/۲} ... p_s^{\alpha_s/۲}$ و عناصر ۲ν، ۳ν، ۴ν، ...، $(\nu - ۱)\nu$ یک دسته از $G(Z_n)$ را تشکیل می دهند، یعنی حاصلضرب هر جفت از این $(\nu - ۱)$ عنصر مضرب n است. عنصر ν کوچکترین عدد است به طوری که مضرب $(p_۱^{\alpha_۱/۲} p_۲^{\alpha_۲/۲} ... p_s^{\alpha_s/۲} - ۱)\nu$ بزرگترین عدد متعلق به Z_n می باشد و بنابراین تعداد دسته در این حالت برابر با $p_۱^{\alpha_۱/۲} p_۲^{\alpha_۲/۲} ... p_s^{\alpha_s/۲} - ۱$ است.

در آخر، فرض کنید $n = q_۱^{\theta_۱} q_۲^{\theta_۲} ... q_t^{\theta_t} h_۱^{\delta_۱} h_۲^{\delta_۲} ... h_r^{\delta_r}$ تجزیه n به عوامل اول باشد که در آن θ_i، $۱ \leq i \leq t$ فرد و δ_i، $۱ \leq i \leq r$ فرد هستند. در این صورت عنصر $u = q_۱^{(\theta_۱ - ۱)/۲} q_۲^{(\theta_۲ - ۱)/۲} ... q_t^{(\theta_t - ۱)/۲} h_۱^{\delta_۱/۲} h_۲^{\delta_۲/۲} ... h_r^{\delta_r/۲}$ و $(u - ۱)$ مضارب $w = q_۱^{(\theta_۱ + ۱)/۲} q_۲^{(\theta_۲ + ۱)/۲} ... q_t^{(\theta_t + ۱)/۲} h_۱^{\delta_۱/۲} h_۲^{\delta_۲/۲} ... h_r^{\delta_r/۲}$ هستند یعنی w، $۲w$، $۳w$، ...، $(u - ۱)w$ یک دسته (حاصلضرب هر جفت از این u عنصر مضرب n است) را تشکیل می دهند.

عنصر w کوچکترین عدد است به طوری که مضرب $(u-۱)w$ بزرگترین عدد متعلق به Z_n می باشد و بنابراین تعداد دسته در این حالت برابر با $u = q_۱^{(\theta_۱-۱)/۲} q_۲^{(\theta_۲-۱)/۲} .. q_t^{(\theta_t-۱)/۲} h_۱^{\delta_۱/۲} h_۲^{\delta_۲/۲} .. h_r^{\delta_r/۲}$ است. □

مثال 3-2-5 (۱) گراف مقسوم علیه صفر $G(Z_{۶۰})$ را در نظر بگیرید. $۶۰ = ۲^{۲} . ۳ . ۵$ بنابراین $۳۰ = ۲ . ۳ . ۵$ رأسی با درجه ماکزیمال $۲۹ = ۱ - ۲ . ۳ . ۵$ است و تعداد دسته ها برابر با ۲ می باشد.

(۲) اگر $n = ۲^{۵} . ۵^{۳} . ۷^{۲}$، آن گاه با توجه به گزاره 3-2-3 و 3-2-4، درجه ماکزیمال گراف $G(Z_n)$ برابر با $۱ - ۲^{۴} . ۵^{۳} . ۷^{۲}$ و تعداد دسته ها برابر با $۲^{۲} . ۵ . ۷$ می باشد.

فصل چهارم

1-4 ساختار گراف $\Gamma(n)$

تعریف 4-1-1 گراف جهت دار $\Gamma(n)$ را با رئوس متعلق به مجموعه $H = \{0,1,...,n-1\}$ گراف **جهت دار مکرر** می نامیم به طوری که دقیقاً یک یال جهت دار از $a \in H$ به $b \in H$ وجود دارد اگر و فقط اگر $a^5 \equiv b \pmod{n}$.

شکل 4-1-1

گراف $\Gamma(13)$ در شکل 4-1-1 داده شده است.

فرض کنید $a_1, a_2, \ldots, a_t \in H$ دو بدو مجزا باشند و

$$a_1^5 \equiv a_2 \pmod{n},$$

$$a_2^5 \equiv a_3 \pmod{n},$$

$$\vdots$$

$$a_t^5 \equiv a_1 \pmod{n}.$$

در این صورت $a_1, a_2, \ldots, a_t$ یک دور به طول t تشکیل می دهند.

گزاره 4-1-2 عدد 0 نقطه ثابت مجزای $\Gamma(n)$ است اگر و فقط اگر n فاقد مربع کامل باشد.

اثبات. فرض کنید $p^2 \mid n$ به ازای عدد اول p. در این صورت

$$\left(\frac{n}{p}\right)^5 = n.\frac{n}{p^2}.(\frac{n}{p})^3 \equiv 0 \pmod n.$$

لذا $\frac{n}{p}$ به 0 نگاشته می شود و 0 نقطه ثابت مجزا نیست.

برعکس، فرض کنید n فاقد مربع کامل باشد. در این صورت واضح است که $x \equiv 0 \pmod n$ تنها جواب همنهشتی $x^5 \equiv 0 \pmod n$ است. بنابراین 0 نقطه ثابت مجزا است. □

فرض کنید

$$\varepsilon(n) = \begin{cases} t+1 & 25 \mid n \\ t & 25 \nmid n \end{cases}$$

که در آن t تعداد اعداد اول مجزایی است که n را عاد می کند و در همنهشتی $p \equiv 1 \pmod 5$ صدق می کند.

قضیه زیر یکی از کاربرد های نظریه گروه و نظریه اعداد می باشد.

قضیه 4-1-3 گراف جهت دار $\Gamma_1(n)$ نیم منظم است اگر و فقط اگر $5 \mid \varphi(n)$. در این حالت درجه ورودی هر رأس $\Gamma_1(n)$ یا برابر $5^{\varepsilon(n)}$ یا 0 می باشد.

اثبات. از آنجا که رئوس $\Gamma_1(n)$ یک گروه با مرتبه $\varphi(n)$ ($\varphi(n)$ تابع اویلر) نسبت به ضرب به پیمانه n تشکیل می دهند، ثابت می کنیم اگر $\text{indeg}(a) > 0$ و $\gcd(a,n) = 1$، آنگاه $\text{indeg}(a) = \text{indeg}(1)$. یعنی تعداد جواب های همنهشتی های $x^5 \equiv a \pmod n$ و $x^5 \equiv 1 \pmod n$ برابر است. همچنین ادعا می کنیم اگر $x_1, x_2, \ldots, x_k$ تنها جواب های همنهشتی $x^5 \equiv 1 \pmod n$ و b جوابی از $x^5 \equiv a \pmod n$ باشند، آنگاه $x_1 b, x_2 b, \ldots, x_k b$ تنها جواب های همنهشتی $x^5 \equiv a \pmod n$ است. چون

$$(x_i b)^5 \equiv x_i^5 b^5 \equiv a \pmod n \qquad i = 1, \ldots, k$$

و

$$x_i b = x_j b \Rightarrow x_i = x_j \qquad i, j = 1, \ldots, k$$

همچنین اگر c جواب دیگری از همنهشتی $x^5 \equiv a \pmod n$ باشد داریم:

$$c^5 \equiv b^5 \pmod n \Rightarrow c^5 b^{-5} \equiv 1 \pmod n \Rightarrow (cb^{-1})^5 \equiv 1 \pmod n \Rightarrow cb^{-1} = x_i \Rightarrow c = x_i b.$$

ابتدا فرض کنید $n = p^\alpha$ به ازای عدد اول p و $\alpha \geq 1$. تعداد جواب های همنهشتی:

$$x^5 \equiv 1 \pmod n \quad \Leftrightarrow \quad (x\text{-}1)(x^4 + x^3 + x^2 + x + 1) \equiv 0 \pmod n$$

را تعیین می کنیم. اگر $5^2 \mid n$ یا $p \equiv 1 \pmod 5$، آن گاه $p-1=5k$، به ازای متغیر k. با انتخاب $x=5k, 5k\pm1, 5k\pm2$ به ازای متغیر k داریم:

$$x=5k \Rightarrow (x-1)(x^4+x^3+x^2+x+1)=(5k-1)((5k)^4+(5k)^3+(5k)^2+(5k)+1)=(5k)^5-1\neq 0$$
$$x=5k-1 \Rightarrow (x-1)(x^4+x^3+x^2+x+1)=(5k-2)((5k)^4+(5k)^3+(5k)^2+(5k)+1)\neq 0$$
$$x=5k+1 \Rightarrow (x-1)(x^4+x^3+x^2+x+1)=(5k)((5k)^4+(5k)^3+(5k)^2+(5k)+1)=(5k)(5\beta)=0$$
$$x=5k+2 \Rightarrow (x-1)(x^4+x^3+x^2+x+1)=(5k-1)((5k+2)^4+(5k+2)^3+(5k+2)^2+(5k+2)+1)\neq 0$$
$$x=5k-2 \Rightarrow (x-1)(x^4+x^3+x^2+x+1)=(5k-3)((5k-2)^4+(5k-2)^3+(5k-2)^2+(5k-2)+1)\neq 0$$

بنابراین به ازای $x=5k+1$، $(x^4+x^3+x^2+x+1)$ فقط شامل یک عامل 5 و $(x-1)$ شامل بقیه عوامل 5 است. از طرفی چون $x^5 \equiv 1 \pmod{p^\alpha}$ و $3^5 \mid p^\alpha$ ، $\alpha \geq 2$. بنابراین $x^5 \equiv 1 \pmod{5^\alpha}$.

اگر $x=5^{\alpha-1}t+1$ به ازای متغیر t، آنگاه

$$\begin{aligned}(x-1)(x^4+x^3+x^2+x+1) &= (5^{\alpha-1}t)((5^{\alpha-1}t+1)^4+(5^{\alpha-1}t+1)^3+(5^{\alpha-1}t+1)^2+5^{\alpha-1}t+1+1)\\ &=(5^{\alpha-1}t)((5^{2(\alpha-1)}t^2+20\cdot 5^{\alpha-1}t+1)(5^{2(\alpha-1)}t^2+20\cdot 5^{\alpha-1}t+1)+\ldots+1))\\ &=(5^{\alpha-1}t)(5^{2(\alpha-1)}t^2k+20\cdot 5^{\alpha-1}t\cdot 5+5)\\ &=(5^{\alpha-1}t)(5\beta)\\ &=5^\alpha t\beta\end{aligned}$$

در نتیجه $x^5-1\equiv 0 \pmod{5^\alpha}$. از این رو به ازای $t=0,1,2,3,4$،

$$x=1,5^{\alpha-1}+1,2\cdot 5^{\alpha-1}+1,3\cdot 5^{\alpha-1}+1,4\cdot 5^{\alpha-1}+1$$

تنها جواب های همنهشتی $x^5 \equiv 1 \pmod n$ می باشند. فرض کنید $\rho(n)$ تعداد جواب های همنهشتی $x^5 \equiv 1 \pmod n$ باشد. در این صورت

$$\rho(n)=\begin{cases}5 & 5^2 \mid n \text{ ، } p\equiv 1 \pmod 5\\ 1 & \text{در غیر این صورت}\end{cases}$$

علاوه بر این، اگر n عدد طبیعی دلخواه و f چند جمله ای با ضرایب صحیح باشد، آنگاه تابع

$$\rho_f(n)= \left|\{0\leq m\leq n-1:\ f(m)\equiv 0 \pmod n\}\right|$$

ضربی است. لذا $\operatorname{indeg}(a)=1$ یا $\operatorname{indeg}(a)=5^{\omega(n)}$.

فرض کنید $\Gamma_1(n)$ نیم منظم است و $a\in\Gamma_1(n)$ به طوری که $\operatorname{indeg}(a)=5^{\omega(n)}$. اگر

$$H=\{0\leq m\leq n-1 \mid (n,m)=1,\ m^5\equiv 1 \pmod n\}.$$

آن گاه زیر گروهی از $\Gamma_1(n)$ است. در نتیجه مرتبه H مرتبه $\Gamma_1(n)$ را عاد می کند یعنی

$$5^{\omega(n)} \mid \varphi(n) \Rightarrow 5 \mid \varphi(n).$$

بر عکس فرض کنید $5 \nmid \varphi(n)$. در این صورت درجه ورودی هر رأس $\Gamma_1(n)$ برابر 1 است و در نتیجه هر مؤلفه $\Gamma_1(n)$ دور است. □

نتیجه زیر به آسانی از قضیه بالا به دست می آید.

نتیجه 4-1-4 گراف جهت دار $\Gamma_1(n)$ منظم است اگر و فقط اگر $5 \nmid \varphi(n)$.

قضیه 4-1-5 هر مؤلفه گراف جهت دار $\Gamma(n)$ دور است اگر و فقط اگر $5 \nmid \varphi(n)$ و n فاقد مربع کامل باشد.

اثبات. فرض کنید $5 \nmid \varphi(n)$ و n فاقد مربع کامل باشد. نشان می دهیم $\Gamma_2(n)$ منظم است. فرض کنید $a \neq 0$ یک رأس دلخواه $\Gamma_2(n)$ باشد و $d = \gcd(a,n)$ که در آن $\gcd(a,n)$ بزرگترین مقسوم علیه مشترک a و n است.

ابتدا فرض کنید $p \mid d$ به ازای عدد اول p. اگر b جواب همنهشتی $b^5 \equiv a \pmod n$ باشد، آنگاه

$$\left.\begin{matrix} d \mid b^5 - a \\ p \mid d \end{matrix}\right\} \Rightarrow p \mid b^5 \Rightarrow p \mid b \Rightarrow b \equiv 0 \pmod p$$

به ازای اعداد اول p که $p \mid d$. همچنین $b^5 \equiv a \equiv 0 \pmod p$، به ازای تمام اعداد اول p که $p \mid d$. با توجه به گزاره 4-1-2 جواب b یکتاست یعنی اگر $b^5 \equiv a \pmod n$ و $p \mid d$، آن گاه $p \mid a$ و $b^5 \equiv a \equiv 0 \pmod p$. لذا $p \mid b^5$ و در نتیجه $p \mid b$، به ازای تمام اعداد اول p که $p \mid d$.

حال فرض کنید $p \mid \frac{n}{d}$ به ازای اعداد اول p. در گروه دوری $\square_{p-1}$، چون $5 \nmid (p-1)$، لذا 5 مولد گروه است و معکوس ضربی دارد. در نتیجه وجود دارد x به طوری که $5x \equiv 1 \pmod{(p-1)}$. قرار دهید $b \equiv a^x \pmod p$. با ضرب طرفین همنهشتی در b^4 داریم:

$$b^5 \equiv b^4 a^x \equiv (a^x)^5 \pmod p \Rightarrow b^5 \equiv a^{5x} \pmod p \qquad (4,1)$$

از آن جایی که

$$\begin{aligned} 5x \equiv 1 \pmod{(p-1)} &\Rightarrow 5x - 1 = k(p-1) \Rightarrow 5x = k(p-1) + 1 \\ &\Rightarrow a^{5x} \equiv a^{k(p-1)+1} \equiv a^{k(p-1)}.a \equiv a \pmod p. \end{aligned} \qquad (4,2)$$

در رابطه بالا، با توجه به $a \in \Gamma_2(n)$، $(a,n) \neq 1$، $p \nmid a$ و بنا به قضیه کوچک فرما، $a^{(p-1)} \equiv 1 \pmod p$ برقرار است. همچنین بنا به رابطه های (4,1) و (4,2)، $b^5 \equiv a \pmod p$.

با توجه به قضیه چینی، نتیجه می شود که $b^5 \equiv a \pmod n$. چون 5 به پیمانه $p-1$ وارون پذیر است و بنا به قضیه کوچک فرما، جواب b یکتا است. فرض کنید

$$\left.\begin{matrix} b_1^5 \equiv a \pmod n \\ b_2^5 \equiv a \pmod n \end{matrix}\right\} \Rightarrow b_1^5 \equiv b_2^5 \pmod n \Rightarrow b_1^5 \equiv b_2^5 \pmod p$$
$$\Rightarrow b_1^{5x} \equiv b_2^{5x} \pmod p \Rightarrow b_1^{k(p-1)+1} \equiv b_2^{k(p-1)+1} \pmod p$$
$$\Rightarrow b_1^{k(p-1)}.b_1 \equiv b_2^{k(p-1)}.b_2 \pmod p \Rightarrow b_1 \equiv b_2 \pmod p \Rightarrow b_1 \equiv b_2 \pmod n.$$

با توجه به نتیجه قبل، $\Gamma_1(n)$ منظم و لذا $\Gamma(n)$ منظم است.

جهت عکس قضیه از گزاره **4-1-2** و نتیجه **4-1-4** بدست می آید. □

قضیه 4-1-6 فرض کنید $n = 2^\alpha 5^\beta p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$ تجزیه n به عوامل اول باشد که در آن p_i و q_i اعداد اول مجزا هستند، $p_i \notin \{2,5\}$، $p_i \equiv -1 \pmod 4$ و $q_i \equiv 1 \pmod 4$. در این صورت تعداد $L(n)$ از نقاط ثابت گراف $\Gamma(n)$ برابر است با:

$$L(n) = 3^s \times 5^t \times \begin{cases} \alpha+1 & \alpha \in \{0,1,2\} \\ 5 & \alpha = 3 \\ 3^2 & \alpha \geq 4 \end{cases}$$

اثبات. فرض کنید $f(x) = x^5 - x$. به آسانی دیده می شود $\rho f(2^2) = 3, \rho f(2) = 2$ و $\rho f(2^3) = 5$. به ازای $n = 2^\alpha$، $\alpha \geq 4$ صفرهای f متعلق به مجموعه

$$\{0,\ 1,\ 2^{\alpha-1} \pm 1,\ 2^{\alpha-2} \pm 1,\ 3.2^{\alpha-2} \pm 1,\ n-1\}$$

می باشند. لذا $\rho f(2^\alpha) = 3^2$.

برای $n = p^\alpha$ که p عدد اول فرد است به طوری که $p \equiv -1 \pmod 4$ و $\alpha \geq 1$، صفرهای f متعلق به مجموعه $\{0,\ 1,\ n-1\}$ می باشند. بنابراین $\rho f(p^\alpha) = 3$.

اگر $n = q^\beta$ که q عدد اول فرد است به طوری که $q \equiv 1 \pmod 4$ و $\beta \geq 1$، در نتیجه بنا به [21، نتیجه 42,2]، $\rho f(q^\beta) = 5$. □

قضیه 4-1-7 فرض کنید $n > 2$. در این صورت دوری به طول t در گراف $\Gamma(n)$ وجود دارد اگر و فقط اگر $t = \mathrm{ord}_d 5$ به ازای مقسوم علیه مثبت d از $\lambda(n)$.

اثبات. فرض کنید a رأسی از یک t-دور در $\Gamma(n)$ باشد. در این صورت

$$a^{5^t} \equiv a \pmod n. \qquad (4,3)$$

t کوچکترین عدد صحیح مثبتی است که

$$a^{۵^t} - a \equiv a(a^{۵^{t-۱}} - ۱) \equiv ۰ \pmod{n}.$$

چون $\gcd(a, a^{۵^{t-۱}} - ۱) = ۱$، لذا اگر $n_۱ = \gcd(a,n)$ و $n_۲ = n/n_۱$، آنگاه t کوچکترین عدد صحیح مثبت است به طوری که

$$a \equiv ۰ \pmod{n_۱}, \qquad a^{۵^{t-۱}} \equiv ۱ \pmod{n_۲} \qquad (4,4)$$

و $\gcd(n_۱, n_۲) = ۱$. بنا به قضیه باقیمانده چینی عدد صحیح b وجود دارد به طوری که

$$b \equiv ۱ \pmod{n_۱}, \qquad b \equiv a \pmod{n_۲}.$$

لذا t کوچکترین عدد صحیح مثبت است به طوری که

$$\left.\begin{array}{l} b^{۵^{t-۱}} \equiv ۱ \pmod{n_۱} \\ b^{۵^{t-۱}} \equiv a^{۵^{t-۱}} \equiv ۱ \pmod{n_۲} \end{array}\right\} \Rightarrow b^{۵^{t-۱}} \equiv ۱ \pmod{n}.$$

فرض کنید $d = \mathrm{ord}_n b$. لذا t کوچکترین عدد صحیح مثبت است به طوری که $۵^t \equiv ۱ \pmod{d}$. در این صورت $t = \mathrm{ord}_d ۵$.چون $d = \mathrm{ord}_n b$ و $\gcd(b,n) = ۱$، بنا به قضیه کارمایکل $d | \lambda(n)$.

بر عکس، فرض کنید $t = \mathrm{ord}_d ۵$ و d مقسوم علیه مثبت $\lambda(n)$ باشد. بنا به قضیه کارمایکل، باقیمانده g به پیمانه n وجود دارد به طوری که $\mathrm{ord}_n g = \lambda(n)$. قرار دهید $h = g^{\lambda(n)/d}$، لذا $\mathrm{ord}_n h = d$. چون $d | ۵^t - ۱$ و به ازای $۱ \le k < t$ ، $d \nmid ۵^k - ۱$، بنابراین t کوچکترین عدد صحیح مثبتی است که

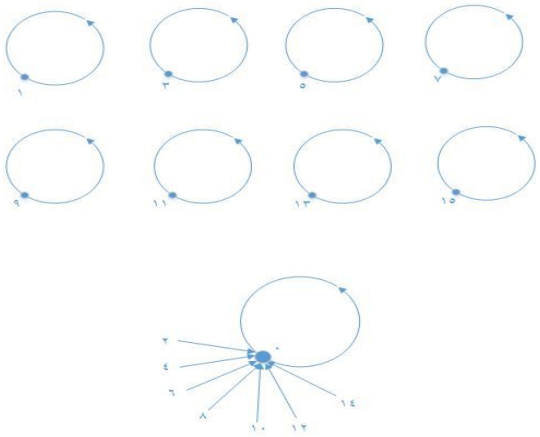
$$h^{۵^{t-۱}} \equiv ۱ \pmod{n}, \qquad h.h^{۵^{t-۱}} \equiv h^{۵^t} \equiv h \pmod{n}.$$

در نتیجه h رأسی از یک t-دور در $\Gamma(n)$ است و اثبات تمام است. □

قضیه 4-1-8 فرض کنید k عدد طبیعی باشد. گراف $\Gamma_۱(۲^k)$ فقط شامل (بجز 8 نقطه ثابت) دور هایی به طول توان هایی از 2 و گراف $\Gamma_۲(۲^k)$ درختی با ریشه 0 می باشد. علاوه بر این $indeg(0) = ۲^{k-\lceil k/۵ \rceil}$.

اثبات. اگر $n = ۲^k$، آنگاه هر گراف $\Gamma_۱(n)$ و $\Gamma_۲(n)$ دقیقا شامل $n = ۲^{k-۱}$ رأس است. همچنین چون $۵ \nmid \varphi(n)$، $\Gamma_۱(۲^k)$ فقط شامل دور است. به راحتی می توان بررسی کرد $۱ - ۲^k \pm ۱, ۳.۲^{k-۲} \pm ۱, ۲^{k-۲} \pm ۱, ۲^{k-۱} \pm ۱, ۰$ نقاط ثابت $\Gamma_۱(۲^k)$ می باشند. بنا به قضیه 4-1-7 می دانیم دوری به طول t وجود دارد اگر و فقط اگر $t = \mathrm{ord}_d ۵$ به ازای مقسوم علیه d از $\lambda(n) = ۲^{k-۲}$. البته رتبه t از 5 در گروه ضربی رئوس $\Gamma_۱(n)$، رتبه گروه را که برابر با $\varphi(n) = ۲^{k-۱}$ است، عاد می کند. در نتیجه t توان 2 می باشد.

به آسانی می توان دید که $2^{k-\lceil k/5\rceil}$ عنصر در $\Gamma_2(2^k)$ وجود دارد که عبارتند از $0 = 2^{\lceil k/5\rceil}.2^{k-\lceil k/5\rceil}, \ldots, 3.2^{\lceil k/5\rceil}, 2.2^{\lceil k/5\rceil}, 2^{\lceil k/5\rceil}$ که به 0 نگاشته می شوند. همچنین همه رئوس w از $\Gamma_2(2^k)$ مضارب 2 هستند که هر چه توان 2 بیشتر باشد، مسیر جهت دار از w به 0 کوتاه تر است. □



شکل 4-1-2

قضیه 4-1-9 فرض کنید k عدد طبیعی باشد. گراف $\Gamma_1(5^k)$ شامل چهار درخت یکریخت می باشد. علاوه بر این، $\Gamma_2(5^k)$ درختی با ریشه ۰ است. همچنین $indeg(0) = 5^{k-\lceil k/5\rceil}$.

اثبات. گراف $\Gamma(5^k)$ دقیقاً 5 مؤلفه با 5 نقطه ثابت دارد. به آسانی می توان دید که $5^{k-\lceil k/5\rceil}$ عنصر $\Gamma_2(5^k)$ عبارتند از $0 = 5^{\lceil k/5\rceil}.5^{k-\lceil k/5\rceil}, \ldots, 3.5^{\lceil k/5\rceil}, 2.5^{\lceil k/5\rceil}, 5^{\lceil k/5\rceil}$ که به 0 نگاشته می شوند. از آنجا که $5 | \varphi(n) = 4.5^{k-1}$ لذا $\Gamma_1(5^k)$ گراف نیم منظم است و درجه هر رأس یا 0 یا 5 می باشد. بنابراین $\Gamma_1(5^k)$ شامل چهار درخت یکریخت است. حال فرض کنید $\{1, n-1, a, n-a\}$ مجموعه تمام نقاط ثابت $\Gamma_1(5^k)$ باشد. اگر $T_1, T_{n-1}, T_a, T_{n-a}$ بترتیب درختان شامل $1, n-1, a, n-a$ باشند، آنگاه بنا به تعریف $\Gamma(n)$، داریم $T_1 \cong T_{n-1}$ و $T_a \cong T_{n-a}$. چون $(a,n) = 1$، لذا اگر هر رأس از درخت T_1 را در عدد a ضرب کنیم درخت T_a بدست می آید. در نتیجه $T_1 \cong T_a$. لذا اثبات کامل است. □

واژه نامه فارسی به انگلیسی

Induction	استقراء
Prime	اول
Primitive	اولیه
Euler	اویلر
Remainder	باقیمانده
Chinese remainder	باقیمانده چینی
Expansion	بسط
Binomial expansion	بسط دوجمله ای
Greatest common divisor	بزرگترین مقسوم علیه مشترک
Dimension	بعد
Fundamental	بنیادی
φ-Function	تابع φ
Factorization	تجزیه
Definition	تعریف
Resolution	تحلیل
Power	توان
Empty	تهی
Ring	حلقه
Quotient	خارج قسمت
Complete quotient	خارج قسمت کامل
Linear	خطی
Domain	دامنه
Degree	درجه
Quadratic	درجه دو
Complete residue system	دستگاه کامل مانده ها

Sequence	دنباله
Digit	رقم
Root	ریشه
Even	زوج
Integer	صحیح
Multiplication	ضرب
Multiplicative	ضربی
Length	طول
Divides	عاد می کند
Odd	فرد
Fermat	فرما
Divisible	قابل قسمت
Complete	کامل
Completion	کامل‌شده
Least common multiple	کوچکترین مضرب مشترک
Proposition	گزاره
Residue	مانده
Positive	مثبت
Order	مرتبه
Multiple	مضرب
Divisor	مقسوم علیه
Iterated	مکرر
Residue field	میدان باقیمانده
Incongruent	ناهمنهشت
Corollary	نتیجه
Congruent	هم نهشت
Congruence	هم نهشتی
Modulus	هنگ

یکتا	Unique

واژه نامه انگلیسی به فارسی

Binomial expansion	بسط دوجمله ای
Chinese remainder	باقیمانده چینی
Complete	کامل
Completion	کامل شده
Complete residue system	دستگاه کامل مانده ها
Congruence	هم نهشتی
Congruent	هم نهشت
Corollary	نتیجه
Definition	تعریف
Degree	درجه
Digit	رقم
Dimension	بعد
Divides	عاد می کند
Divisible	قابل قسمت
Divisor	مقسوم علیه
Domain	دامنه
Empty	تهی
Euler	اویلر
Even	زوج
Expansion	بسط
Factorization	تجزیه
φ-Function	تابع φ
Fundamental	بنیادی
Greatest common divisor	بزرگترین مقسوم علیه مشترک

Incongruent	ناهمنهشت
Induction	استقراء
Integer	صحیح
Iterated	مکرر
Least common multiple	کوچکترین مضرب مشترک
Length	طول
Linear	خطی
Modulus	هنگ
Multiple	مضرب
Multiplication	ضرب
Multiplicative	ضربی
Odd	فرد
Order	مرتبه
Positive	مثبت
Power	توان
Prime	اول
Primitive	اولیه
Proposition	گزاره
Quotient	خارج قسمت
Remainder	باقیمانده
Residue	مانده
Residue field	میدان باقیمانده
Resolution	تحلیل
Ring	حلقه
Root	ریشه
Unique	یکتا

منابـــع

[۱]جانسون با، ریچارد. ساختمان های گسسته. ترجمه ابراهیم زاده قلزم، حسین. انتشارات سیمای دانش (1380)

[۲]مک کوی، نیل. اچ. نظریه اعداد. ترجمه بهروزفر، غلامحسین و میرنیا، میرکمال. نشر دانش امروز (1370).

[۳]نقی پور، علیرضا و صدیقی، جواد. نظریه میدان و گالوا. انتشارات دانشگاه شهرکرد (1390).

[٤] Akbari, S., and Mohamadian, A., On the zero-divisor graph of a commutative ring, J. Algebra ۲۷۴, ۸۴۷-۸۵۵ (۲۰۰۴).

[٥] Beck, I., Coloring of commutative rings, J. Algebra ۱۱۶, ۲۰۸-۲۲۶ (۱۹۸۸).

[٦] Bryant, S, Groups, grphs and Fermats last theorem, Amer. Math. Monthly ۷۴, ۱۵۲-۱۵۶ (۱۹۶۷).

[۷] Carmichael, R. D., Note on a new number theory function, Bull. Amer. Math. Soc. ۱۶, ۲۳۲-۲۳۸ (۱۹۱۰).

[۸] Carmichael, R. D., The Theory of Numbers. New York: John Wiley & Sons, ۱۹۱۴.

[۹] Chartrand, G., and Lesniak, L., Graph and Digraphs (Third edition). Chapman & Hall, London, ۱۹۹۶.

[۱۰] Chassé, G., Applications d'un corps fini dans lui-même. Dissertation, Univ. de Rennes I, ۱۹۸۴.

[۱۱] Chassé, G., Combinatorial cycles of a polynomial map over a commutative field, Discrete Math. ۶۱, ۲۱-۲۶ (۱۹۸۶).

[۱۲] Harary, F., "Graph Theory" , Addison-Wesley Publ. Company, London, ۱۹۶۹.

[۱۳] Křížek, M., and Somer, L., A necessary and sufficient condition for the primality of Fermat numbers. Math. Bohem. ۱۲۶, ۵۴۱-۵۴۹ (۲۰۰۱).

[١٤] Křížek, M., and Somer, L., On a connection of number theory with graph theory, Czechoslovak Math. J. ٥٤, ٤٦٥-٤٨٥ (١٢٩) (٢٠٠٤).

[١٥] Křížek, M., and Luca, F., and Somer, L., ١٧ Lectures on the Fermat Numbers From Number Theory to Geometry, Springer-Verlag. New York ٢٠٠١.

[١٦] Křížek, M., and Somer, L., Sophie Germain little suns, Math. Slovaca ٥٤, ٤٣٣-٤٤٢ (٢٠٠٤).

[١٧] Niven, I, H. S. Zuckerman., An Introduction to the Theory of numbers , Jhon Wiley and Sons, ١٩٦٠.

[١٨] Niven, I, H. S. Zuckerman, and H. L. Montgomery, "An introduction to the theory of numbers" , Jhon Wiley and Sons, Inc., ١٩٩١

[١٩] Robert, F., Discrete iterations. Springer Series in Comput. Math. Vol. Springer-Verlag, Berlin, ١٩٨٦.

[٢٠] Rogers, T. D., the graph of the square mapping on the prime fields, Discrete Math. ١٤٨, ٣١٧-٣٢٤ (١٩٩٦).

[٢١] Sierpiński, W., "Elementary Theory of Numbers" , North-Holland, ١٩٨٨.

[٢٢] Skowronek-Kaziów, J., Some digraphs arising from number theory and remarks on the zero-divisor graph of the Z_n, Information Processing Letters, ١٠٨, ١٦٥-١٦٩ (٢٠٠٨).

[٢٣] Szalay, L., A discrete iteration in number theory, BDTF Tud. Kzl. ٨, ٧١-٩١ (١٩٩٢).