ارتباط نظریه اعداد با نظریه گراف

مرضیه رحمتی

دانشکده علوم پایه، دانشگاه پیام نور، تهران، ایران

Rahmati_m61@yahoo.com

چکیده

در این مقاله، گراف جهت دار $\Gamma(n)$ را که مجموعه رئوسش $H=\{\circ,1,\ldots,n-1\}$ است بررسی می کنیم بطوری که یک یال جهت دار از a به b وجود دارد اگر $a^2\equiv b \pmod n$ به ازای $a,b\in\{\circ,1,\ldots,n-1\}$. 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 می شوند. شرایط منظم بودن و نیم منظم بودن $\Gamma_1(n)$ را ارائه می دهیم.

کلید واژه ها: گراف جهت دار، گراف منظم، گراف نیم منظم.

مقدمه

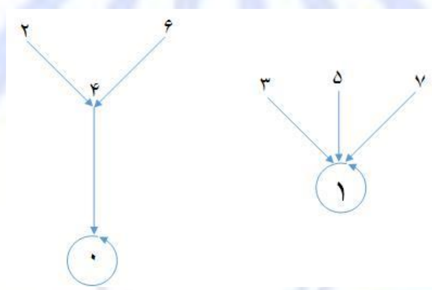
فرض کنید $n\geq 1$ و $H=\{\circ,1,\ldots,n-1\}$. گراف جهت دار $\Gamma(n)$ را با رئوس متعلق به H در نظر بگیرید به طوری که یک یال جهت دار از a به b وجود داشته باشد اگر و فقط اگر

$a^2 \equiv b \pmod{n}$. در این مقاله برخی روابط بین نظریه اعداد، نظریه گراف و نظریـه گـروه را که توسط برایانت(1967)،کریزک (2004)، چاسی (1986)، کریزک (2001) بصورت گـراف متناظر با رابطه همنهشتی $a^2 \equiv b \pmod{n}$ در نظر گرفته شده است، نشان می دهیم.

دو زیر گراف برای $\Gamma(n)$ معرفی می کنیم. فرض کنید $\Gamma_1(n)$ توسط رئوسی کـه نسـبت بـه n اولند و $\Gamma_2(n)$ توسط رئوسی که نسبت به n اول نیستند، القا می شوند. واضح اسـت کـه $\Gamma_1(n)$ و $\Gamma_2(n)$ مجزا هستند و $\Gamma(n)=\Gamma_1(n)\cup\Gamma_2(n)$. شرایط منظم بودن و نیم منظم بودن زیر گراف $\Gamma_1(n)$ ارایه دادیم.

2- مبانی نظری و پیشینه پژوهش

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



شکل 2-1 (گراف $\Gamma(8)$)

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

$$a_1^2 \equiv a_2 \pmod{n},\quad a_2^2 \equiv a_3 \pmod{n},\ \ldots\ ,a_t^2 \equiv a_1 \pmod{n}.$$

در این صورت $a_1,a_2,\ldots,a_t$ یک دور به طول t تشکیل مـی دهنـد. دوری بـه طـول یـک 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 $\Gamma_1(n)$ توسط رئوسی که نسبت به n اولند و $\Gamma_2(n)$ توسط رئوسی که نسبت به n اول نیستند، القا می شوند. واضح است که $\Gamma_1(n)$ و $\Gamma_2(n)$ مجزا هستند و $\Gamma(n) = \Gamma_1(n) \cup \Gamma_2(n)$. 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 $\Gamma_1(n)$ داده شده اند.

3- بحث و نتیجه گیری

این بخش را با گزاره زیر شروع می کنیم.

گزاره 3-1 عدد 0 نقطه ثابت مجزای $\Gamma(n)$ است اگر و فقط اگر n فاقد مربع کامل باشد.

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

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

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 $x \equiv 0 \ (\bmod n)$ تنها جواب همنهشتی $x^2 \equiv 0 \ (\bmod n)$ می باشد. بنابراین 0 نقطه ثابت مجزای $\Gamma(n)$ است.

قضیه 3-۲ 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 $2|n$ 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 $a\not\equiv 0 \pmod n$، لذا $2|n$ و $b\equiv\frac{n}{2} \pmod n$.

حال فرض کنید $p^2|n$ 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

$$\frac{n}{2}m\equiv\frac{n}{2} \pmod n. \tag{3.1}$$

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 (3.1) مشاهده می کنیم که

$$a\equiv b^2\equiv\frac{n}{2}\frac{n}{2}\equiv\frac{n}{2} \pmod n. \tag{3.2}$$

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 (3.1) و (3.2) می توان نتیجه گرفت که

$$\frac{n}{2}\frac{n}{2} \equiv \frac{n}{2} \pmod{n}, \tag{3.۳}$$

و $\frac{n}{2}$ نقطه ثابت گراف $\Gamma(n)$ است. فرض کنید $b^2 \equiv \frac{n}{2} \pmod{n}$. چون $\frac{n}{2}$ فـرد و n زوج است، لذا $b \equiv 1 \pmod{2}$. از آنجا که $\frac{n}{2}$ فاقد مربع کامل است و $\frac{n}{2} \mid n$، براحتـی مـی تـوان نتیجه گرفت $b \equiv 0 \pmod{\frac{n}{2}}$. توجه کنید $\gcd(2,\frac{n}{2}) = 1$. از اینرو بنا بـه قضـیه باقیمانـده چینی، b به پیمانه n منحصر به فرد است و با توجـه بـه (3.۳)، $b \equiv \frac{n}{2} \pmod{n}$. لـذا $\frac{n}{2}$ نقطه ثابت مجزای گراف $\Gamma(n)$ و اثبات کامل است. □

نتیجه 3-3 هر گراف $\Gamma(n)$، حداکثر دو نقطه ثابت مجـزا دارد. همچنـین $\Gamma(n)$ دقیقـاً دو نقطه ثابت مجزا دارد اگر و فقط اگر $2 \mid n$ و n فاقد مربع کامل باشد. در ایـن حالـت 0 و $\frac{n}{2}$ تنها نقاط ثابت مجزا هستند.

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

$$\varepsilon(n) = \begin{cases} -1 & 2 \| n \\ 0 & 4 \| n \text{ یا } 2 \nmid n \\ 1 & 8 \mid n. \end{cases} \tag{3.۴}$$

لم 3-4 اگر $\gcd(a,n) = 1$ و $N_n(a) > 0$، آن گاه $N_n(a) = 2^{\omega(n)+\varepsilon(n)}$.

اثبات. در حالتی که $n = 1$، نتیجه واضح است. بنابراین فرض مـی کنـیم $n > 1$. از آن جـایی که عناصری که نسبت به n اولند، یک گروه ضربی به پیمانه n تشکیل می دهند، به راحتـی می توان دید اگر $\gcd(a,n) = 1$ و $N_n(a) > 0$، $N_n(a) = N_n(1)$. لذا کـافی اسـت $N_n(1)$ را مشخص کنیم.

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

$$a^2 \equiv 1 \pmod{p^k} \tag{3.5}$$

اگر و فقط اگر

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

فرض کنید p عدد اول فرد باشد. چون $\gcd(a+1,a-1) \mid 2$، رابطه (3.5) 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 (3.5) 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 (3.5) برقرار است اگر و فقط اگر $a \equiv 1 \pmod 2$ به ازای $1 \le k \le 3$ و $a \equiv \pm 1 \pmod{2^{k-1}}$ به ازای $k \ge 4$. بنابراین $N_{2^k}(1)=2^{1+\varepsilon(2^k)}$. نتیجه بنا به قضیه باقیمانده چینی بدست می آید.

قضیه 3-5 گراف جهت دار $\Gamma_1(n)$ به ازای هر عدد صحیح مثبت n، نیم منظم است. علاوه بر این، درجه ورودی هر رأس $\Gamma_1(n)$ یا برابر 0 یا $2^{\omega(n)+\varepsilon(n)}$ می باشد.

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

$$\begin{aligned}
&\lambda(1)=1=\varphi(1),\\
&\lambda(2)=1=\varphi(2),\\
&\lambda(4)=2=\varphi(4),\\
&\lambda(2^k)=2^{k-2}=\frac{1}{2}\varphi(2^k) \quad k\ge 3,\\
&\lambda(p^k)=(p-1)p^{k-1}=\varphi(p^k)
\end{aligned}$$

به ازای عدد اول فرد p و $k \ge 1$،

$$\lambda(p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s})=\operatorname{lcm}\,[\lambda(p_1^{k_1}),\lambda(p_2^{k_2}),\ldots,\lambda(p_s^{k_s})],$$

که به ازای $k_i \ge 1$ و $i \in \{1,\ldots,s\}$، $p_1,p_2,\ldots,p_s$ 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، $\lambda(n) \mid \varphi(n)$ و $\lambda(n)=\varphi(n)$ اگر و فقط اگر $n \in \{1,2,4,q^k,2q^k\}$ که q عدد اول فرد و $k \ge 1$.

فرض کنید رتبه ضربی g به پیمانه n را به صورت $t=\operatorname{ord}_n g$ نشان مـی دهـیم (یعنـی t کوچکترین عدد طبیعی است به طوری که $g^t\equiv 1 \pmod n$).

قضیه 3-6 دوری به طول t در گراف $\Gamma(n)$ وجود دارد اگر و فقط اگر $t=\operatorname{ord}_d 2$ بـه 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

$$a^{2^t}\equiv a \pmod n.$$

ثابت می کنیم t کوچکترین عدد صحیح مثبتی است که در رابطه بالا صدق می کنـد. کـافی است ثابت کنیم در $\Gamma(n)$ دورها مجزایند. اگر فرض کنید دو دور به طول t_1 و t_2 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_1 و دیگری متعلق به دور t_2 است و با این مطلب که درجه خروجـی هـر رأس برابر 1 است در تناقض است. لذا در $\Gamma(n)$ دورها مجزایند.

t کوچکترین عدد صحیح مثبتی است که

$$a^{2^t}-a\equiv a(a^{2^t-1}-1)\equiv 0 \pmod n. \qquad (3.6)$$

چون $\gcd(a,a^{2^t-1}-1)=1$، لـذا از رابطـه (3.6) نتیجـه مـی شـود اگـر $n_1=\gcd(a,n)$ و $n_2=\dfrac{n}{n_1}$، آنگاه ثابت می کنیم t کوچکترین عدد صحیح مثبت است به طوری که

$$a\equiv 0 \pmod{n_1}, \qquad a^{2^t-1}\equiv 1 \pmod{n_2} \qquad (3.7)$$

و $\gcd(n_1,n_2)=1$. فرض کنید $t_1<t$ به طوری که

$$\left.\begin{aligned} a^{2^{t_1}-1}&\equiv 1 \pmod{n_2}\\ a^{2^{t_1}-1}&\equiv 1 \pmod{n_1}\end{aligned}\right\}\Rightarrow \left.\begin{aligned} a^{2^{t_1}}&\equiv a \pmod{n_2}\\ a^{2^{t_1}}&\equiv a\equiv 0 \pmod{n_1}\end{aligned}\right\}\Rightarrow a^{2^{t_1}}\equiv a \pmod n$$

که با رابطه (3.6) تناقض دارد. برعکس اگر فرض کنید $t_1<t$ به طوری که

$$a^{2^{t_1}}\equiv a \pmod n\Rightarrow\begin{cases}(a,n)=1\Rightarrow a^{2^{t_1}}\equiv 1 \pmod n\Rightarrow a^{2^{t_1}}\equiv 1 \pmod{n_2}\\ (a,n)\neq 1\Rightarrow a^{2^{t_1}}\equiv 1 \pmod n\Rightarrow a^{2^{t_1}}\equiv 1 \pmod{n_2}\end{cases}$$

که با رابطه (3.7) تناقض دارد. بنا به قضیه باقیمانده چینی عدد صحیح b وجود دارد به طوری که

$$b \equiv 1 \pmod{n_1}, \qquad b \equiv a \pmod{n_2}. \tag{3.8}$$

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

$$\left.\begin{aligned} b^{2^t-1} &\equiv 1 \pmod{n_1} \\ b^{2^t-1} &\equiv a^{2^t-1} \equiv 1 \pmod{n_2} \end{aligned}\right\} \Rightarrow b^{2^t-1} \equiv 1 \pmod{n}. \tag{3.9}$$

فرض کنید $t_1 < t$ به قسمی که:

$$\left.\begin{aligned} a^{2^{t_1}} &\equiv a \pmod{n_2} \\ a^{2^{t_1}} &\equiv a \equiv 0 \pmod{n_1} \end{aligned}\right\} \Rightarrow a^{2^{t_1}} \equiv a \pmod{n}$$

که تناقض است.

حال فرض کنید $d = \mathrm{ord}_n b$. در این صورت $d \mid 2^t - 1$. با توجه به رابطه(3.9)، t کوچکترین عدد صحیح مثبت است به طوری که $d \mid 2^t - 1$. لذا $t = \mathrm{ord}_d 2$. 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

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

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

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

منابع

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

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

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

- Bryant, S. (1967). Groups, grphs and Fermats last theorem, Amer. Math. Monthly, 74, 152-156.
- Carmichael, R. D. (1910). Note on a new number theory function, Bull. Amer. Math. Soc, 16, 232-238.
- Chasse, G. (1986). Combinatorial cycles of a polynomial map over a commutative field, Discrete Math. 61, 21-26.
- Harary, F. (1969). Graph Theory. Addison-Wesley Publ. Company, London.
- Krizek, M., Somer, L. (2001). A necessary and sufficient condition for the primality of Fermat numbers. Math. Bohem. 126, 541-549.
- Krizek, M., Somer, L. (2004). On a connection of number theory with graph theory, Czechoslovak Math. J. 54(129), 465-485.
- Robert, F. (1986). Discrete iterations. Springer Series in Comput. Math. Vol. Springer-Verlag, Berlin.
- Rogers, T. D. (1996). The graph of the square mapping on the prime fields, Discrete Math. 148, 317-324.
- Szalay, L. (1992). A discrete iteration in number theory, BDTF Tud. Kzl. 8, 71-91.