تعمیم قضیه‌ای از گاوس به گروههای متناهی

محمدرضا پورنکی*

قضیهٔ کوچک فرما حاکی است که اگر p عددی اول باشد، آنگاه

$$a^p \equiv a \ (\text{به پیمانهٔ } p)$$

به‌ازای هر عدد صحیح a صادق است. ممکن است این سؤال مطرح شود که تعمیم همنهشتی بالا به عدد صحیح مثبتِ دلخواهی مانند n (به‌جای عدد اول p) چیست. احساس می‌شود پاسخ این سؤال برای ریاضیدانان، حتی متخصصان نظریهٔ اعداد، کمی ناآشنا باشد؛ و علت این ناآشنایی را نیز می‌توان ظاهرنشدن این تعمیم در بسیاری از کتابها، دستکم در کتابهای متعارف، دانست. در واقع می‌توان تعمیم مذکور از همنهشتی بالا را که حکمی منسوب به گاوس است یکی از زیباترین احکام نظریهٔ کلاسیک اعداد به‌شمار آورد:

قضیهٔ گاوس. اگر n عدد صحیحِ مثبتی باشد، آنگاه همنهشتی

$$\sum_{d|n} \mu(n/d)a^d \equiv 0 \ \ (\text{به پیمانهٔ } n)$$

به‌ازای هر عدد صحیح a صادق است؛ در اینجا μ تابع موبیوس است و به این صورت تعریف می‌شود که $\mu(1) = 1$؛ $\mu(m) = 0$ اگر m بر مربع نباشد؛ و $\mu(m) = (-1)^r$ اگر $m = p_1 \dots p_r$، که p_iها اعداد اول متمایز فرض می‌شوند.

واضح است که قضیهٔ گاوس تعمیمی از قضیهٔ کوچک فرماست و با فرض اول بودن n قضیهٔ کوچک فرما را نتیجه می‌دهد. دیکسن در صفحات ۸۲ تا ۸۶ از کتاب خود [۲] تاریخچه‌ای از قضیهٔ گاوس آورده است. ما نیز در ادامه مختصراً به این تاریخچه اشاره می‌کنیم. گاوس حکم قضیهٔ خود را فقط توانسته بود به‌ازای aهای اول ثابت کند که این اثبات پس از مرگ وی در سال ۱۸۶۳ منتشر شد، لیکن در طول سالهای ۱۸۸۰ـ۱۸۸۳ چهار اثبات مستقل برای قضیهٔ گاوس (به‌ازای تمام aهای صحیح) توسط کانتور[1]، وی‌یر[2]، لوکاس[3]، و پلت[4] ارائه شد (برای یافتن مراجع رجوع کنید به [۲]؛ همچنین نگاه کنید به [۶]). در سال ۱۸۷۲، پیترسن [۴] قضیهٔ کوچک فرما را به کمک یک روش ترکیبیاتی ثابت کرد و تیو [۷] در سال ۱۹۱۰ با تعمیم این روش توانست اثباتی از قضیهٔ گاوس ارائه کند (خلاصه‌ای از اثبات وی در صفحهٔ ۸۲ از [۲] آمده است). همچنین تیو توانست به کمک قضیهٔ گاوس، قضیهٔ اویلر را که خود تعمیمی از قضیهٔ کوچک فرماست ثابت کند. قضیهٔ اویلر بیان می‌کند که همنهشتی

$$a^{\varphi(n)} \equiv 1 \ (\text{به پیمانهٔ } n)$$

به‌ازای هر عدد صحیح a که $\gcd(a,n) = 1$، صادق است، در اینجا φ تابع فی اویلر است و به صورت $\varphi(n) = n\prod_{\text{اول } p|n}(1-\frac{1}{p})$ تعریف می‌شود. سزله [۶] سه اثبات مختلف برای قضیهٔ گاوس ارائه کرد که مشابه اثباتهای ارائه شده توسط گراندی[1]، دیکسن، و تیو بود که به ترتیب در سالهای ۱۸۸۲، ۱۸۹۵، و ۱۹۱۰ عرضه شده بودند. سرانجام در سال ۱۹۸۶، اسمیت [۵] اثباتی «زنگی» برای یک تعمیم جزئی از قضیهٔ گاوس به‌دست داد. پس قضیهٔ گاوس از دو جنبه دارای اهمیت است: یکی از نظر تاریخی و دیگر از این نظر که تعمیمی از قضیه‌های کوچک فرما و اویلر است. در این مقاله تعمیمی از قضیهٔ گاوس به گروههای متناهی بیان و اثباتی به کمک جبر خطی کلاسیک برای آن ارائه خواهد شد.

قضیهٔ اصلی

در این بخش تعمیم مذکور از قضیهٔ گاوس را تحت عنوان قضیهٔ اصلی بیان می‌کنیم. سپس ارتباط این قضیه را با نظریهٔ سرشت گروههای متناهی شرح خواهیم داد.

قضیهٔ اصلی. فرض کنیم G یک گروه متناهی از مرتبهٔ n باشد و $\mathbb{C}^\times$ را گروه ضربی اعداد مختلط ناصفر در نظر می‌گیریم. اگر $f : G \to \mathbb{C}^\times$

1. Kantor 2. Weyr 3. Lucas 4. Pellet

1. Grandi

یک همریختی باشد، آنگاه همنهشتی

$$\sum_{g\in G} f(g)\, a^{n/o(g)} \equiv 0 \pmod{n \text{ به پیمانهٔ}}$$

به‌ازای هر عدد صحیح a صادق است که $o(g)$ مرتبهٔ عضو g است.

ابتدا نشان می‌دهیم که قضیهٔ اصلی واقعاً تعمیمی از قضیهٔ گاوس است. برای این منظور فرض می‌کنیم $G=\langle x\rangle$ گروه دوری از مرتبهٔ n باشد و همریختی $f: G\to \mathbb{C}^\times$ را به صورت $f(x^l)=\exp(2\pi i l/n)$، $1\le l\le n$، تعریف می‌کنیم. با توجه به [۱، قضیهٔ ۶.۸ و مثال بعد از قضیهٔ ۸.۸] به‌دست می‌آوریم:

$$\begin{aligned}
\sum_{g\in G} f(g)a^{n/o(g)} &= \sum_{l=1}^{n} \exp(2\pi i l/n)\, a^{n/o(x^l)} \\
&= \sum_{l=1}^{n} \exp(2\pi i l/n)\, a^{\gcd(l,n)} \\
&= \sum_{d\mid n} \Big(\sum_{\substack{l=1\\ \gcd(l,n)=d}}^{n} \exp(2\pi i l/n)\Big) a^d \\
&= \sum_{d\mid n} \Big(\sum_{\substack{l'=1\\ \gcd(l',n/d)=1}}^{n/d} \exp(2\pi i l' d/n)\Big) a^d \\
&= \sum_{d\mid n} \mu(n/d) a^d .
\end{aligned}$$

بنابر قضیهٔ اصلی، $\sum_{g\in G} f(g)a^{n/o(g)}$ بر n بخش‌پذیر است، لذا برابریهای بالا نشان می‌دهند که $\sum_{d\mid n}\mu(n/d)a^d$ نیز بر n بخش‌پذیر است که این همان قضیهٔ گاوس است. پس قضیهٔ اصلی، قضیهٔ گاوس را نتیجه می‌دهد و لذا تعمیمی از آن است.

حتی می‌توانیم با در نظرگرفتن حالات خاص در قضیهٔ اصلی تعمیمهایی زیبا از قضیهٔ کوچک فرما به‌دست آوریم. مثلاً اگر برای گروه داده شدهٔ G از مرتبهٔ n، $f: G\to \mathbb{C}^\times$ را همریختی‌ای با تعریف $f(g)=1$، $g\in G$، در نظر بگیریم آنگاه همنهشتی

$$\sum_{g\in G} a^{n/o(g)} \equiv 0 \pmod{n \text{ به پیمانهٔ}} \qquad (1)$$

به‌ازای هر عدد صحیح a و هر گروه G از مرتبهٔ n صادق است. همنهشتی بالا با فرض $G=\mathbb{Z}_p$، p اول، به قضیهٔ کوچک فرما تبدیل می‌شود و لذا می‌توان آن را تعمیمی از قضیهٔ کوچک فرما به گروههای متناهی در نظر گرفت. بالاخص می‌توانیم نتیجهٔ زیر را به‌دست آوریم که تعمیمی از قضیهٔ کوچک فرما و مشابه با قضیهٔ گاوس است.

نتیجه. اگر n عدد صحیح مثبتی باشد، آنگاه همنهشتی

$$\sum_{d\mid n} \varphi(n/d)\, a^d \equiv 0 \pmod{n \text{ به پیمانهٔ}}$$

که در آن φ تابع فی اویلر است، به‌ازای هر عدد صحیح a صادق است.

اثبات. فرض می‌کنیم $G=\langle x\rangle$ گروه دوری از مرتبهٔ n باشد. می‌توانیم بنویسیم

$$\begin{aligned}
\sum_{g\in G} a^{n/o(g)} &= \sum_{l=1}^{n} a^{n/o(x^l)} \\
&= \sum_{l=1}^{n} a^{\gcd(l,n)} \\
&= \sum_{d\mid n} \Big(\sum_{\substack{l=1\\ \gcd(l,n)=d}}^{n} 1\Big) a^d \\
&= \sum_{d\mid n} \varphi(n/d) a^d .
\end{aligned}$$

با توجه به (۱)، $\sum_{g\in G} a^{n/o(g)}$ بر n بخش‌پذیر است، لذا $\sum_{d\mid n}\varphi(n/d)\,a^d$ نیز چنین است و این، نتیجه را به اثبات می‌رساند. □

قبل از اثبات قضیهٔ اصلی، توضیح مختصری دربارهٔ ارتباط آن با نظریهٔ سرشت گروههای متناهی می‌دهیم. فرض کنیم G یک گروه متناهی دلخواه باشد که (از راست) روی یک مجموعهٔ متناهی دلخواه S به‌طور وفادار[1] عمل می‌کند. برای هر عضو $g\in G$، گیریم $t(g)$ تعداد دورهای g با احتساب دورهایِ به طول یک (یعنی تعداد مدارهای $\langle g\rangle$ در عمل روی S) باشد. برای مثال، اگر G گروه متقارن S_5 با عمل طبیعی روی $S=\{1,2,3,4,5\}$ باشد و g عضو مرتبهٔ ۲ی $g=(1\ 2)(3\ 4)$ باشد آنگاه $t(g)=3$. یک حالت خاص و مهم وقتی پیش می‌آید که $S=G$، یعنی وقتی که گروه دلخواه G روی خودش با ضرب گروه عمل می‌کند. در این حالت به‌راحتی دیده می‌شود که $t(g)=n/o(g)$؛ $n=|G|$. این عمل از گروه G روی G را عمل منظم می‌نامیم.

حال M را مجموعهٔ تمام نگاشتهای از S به یک مجموعهٔ متناهی A ($|A|=a$) در نظر می‌گیریم (مفید است اعضای A را «رنگ» تصور کنیم و اعضای M را نیز یک رنگ‌آمیزی از اعضای S در نظر بگیریم). اکنون می‌خواهیم عملی از گروه G روی مجموعهٔ M تعریف کنیم. فرض می‌کنیم $g\in G$ و $m\in M$. در این صورت $m\cdot g$ عضوی از M است که آن را با ضابطهٔ $(m\cdot g)(x)=m(x\cdot g^{-1})$، $x\in S$، تعریف می‌کنیم (بررسی اینکه این ضابطه واقعاً یک عمل روی M تعریف می‌کند، یعنی به‌ازای هر $g,h\in G$، $(m\cdot g)\cdot h=m\cdot(gh)$ سر راست است).

به‌ازای $g\in G$ داده شده، $\pi(g)$ را تعداد اعضایی از M در نظر می‌گیریم که توسط g ثابت نگه داشته می‌شود. لذا π سرشت جایگشتی عمل G روی M است. سؤال این است که چگونه می‌توان $\pi(g)$ را محاسبه کرد؟ به‌راحتی دیده می‌شود که یک رنگ‌آمیزی m توسط g ثابت نگه داشته می‌شود اگر و فقط اگر تمام نقاط در هر مدار از $\langle g\rangle$ در عمل روی S، رنگی یکسان داشته باشد. از اینجا نیز نتیجه می‌شود که $\pi(g)=a^{t(g)}$. بالاخص در عمل منظم گروه G از مرتبهٔ n داریم $\pi(g)=a^{n/o(g)}$.

1. faithfully

حال می‌توانیم سرشت جایگشتی را به صورت ترکیبی خطی از سرشتهای تحویل‌ناپذیر G با ضرایب صحیحِ نامنفی بنویسیم. اگر χ یکی از این سرشتهای تحویل‌ناپذیر باشد، آنگاه با توجه به روابط تعامد برای سرشتهای تحویل‌ناپذیر، ضریب χ در این تجزیه برابر است با $(1/n)\sum_{g\in G}\chi(g)\pi(g)$ که $n=|G|$. بالاخص برای هر انتخاب χ از تجزیهٔ π، $\sum_{g\in G}\chi(g)\pi(g)$ بر n بخش‌پذیر است. پس

$$\sum_{g\in G}\chi(g)\,a^{t(g)}=\sum_{g\in G}\chi(g)\,\pi(g)\equiv 0 \quad (n \text{ به پیمانهٔ})$$

چون هر همریختی از G به $\mathbb{C}^\times$ یک سرشت خطی تحویل‌ناپذیر از گروه G است ملاحظه می‌کنیم که قضیهٔ اصلی حالت خاصی از همنهشتی کلی بالاست که در آن عمل G را منظم فرض کرده‌ایم و χ را سرشت خطی. در نتیجه قضیهٔ اصلی و ایده‌هایی که در این مقاله به‌کار رفته‌اند آشنا هستند ولی به زبانی پیچیده بیان می‌شوند که اغلب برای دانشجویان دورهٔ کارشناسی ناآشناست. در ادامه می‌خواهیم قضیهٔ اصلی را به زبانی ساده و به کمک روشهای جبرخطی کلاسیک ثابت کنیم. برای ملاحظهٔ دیدگاهی دیگر به [۳] نگاه کنید.

اثبات قضیهٔ اصلی

مقاله را با اثبات قضیهٔ اصلی ادامه می‌دهیم. بدون از دست رفتن کلّیّت موضوع می‌توانیم فرض کنیم $G=\{1,\dots,n\}$. در ادامه، آزادانه از G به‌عنوان یک مجموعهٔ اندیس استفاده خواهیم کرد.

ابتدا فرض می‌کنیم a عدد صحیحِ مثبتی باشد. فرض کنیم V یک فضای برداری از بعد a روی میدان $\mathbb{C}$ باشد و $\overset{n}{\otimes}V$ را حاصلضرب تانسوری V در خودش به تعداد n بار در نظر می‌گیریم. گیریم $v_1\otimes\cdots\otimes v_n$ به‌ازای v_1، …، v_n یک تانسور تجزیه‌پذیر را که عضوی از $\overset{n}{\otimes}V$ است نمایش دهد. به‌ازای هر $i\in G$ $A_i:\overset{n}{\times}V\to\overset{n}{\otimes}V$ را به صورت زیر تعریف می‌کنیم

$$A_i(v_1,\dots,v_n)=v_{i1}\otimes\cdots\otimes v_{in}.$$

به‌راحتی می‌توانیم ثابت کنیم A_i یک تابع n خطی است و لذا بنابر خاصیت عام حاصلضرب تانسوری، عملگر خطی منحصر به‌فرد $T_i:\overset{n}{\otimes}V\to\overset{n}{\otimes}V$ موجود است که عمل آن روی تانسورهای تجزیه‌پذیر به صورت زیر است

$$T_i(v_1\otimes\cdots\otimes v_n)=v_{i1}\otimes\cdots\otimes v_{in}.$$

لم زیر با عملیات سر راستی به‌دست می‌آید.

لم ۱. *به‌ازای هر $i,j\in G$، $T_iT_j=T_{ij}$.*

اکنون به کمک میانگین T_iها عمگر خطی $T:\overset{n}{\otimes}V\to\overset{n}{\otimes}V$ را به صورت زیر تعریف می‌کنیم

$$T=\frac{1}{n}\sum_{i\in G}f(i)T_i.$$

لم ۲. *اثر T، $\operatorname{tr}T$، یک عدد صحیحِ نامنفی است.*

اثبات. ادعا می‌کنیم که T عملگری خود توان است. در حقیقت، بنابر لم ۱

$$\begin{aligned}T^2&=\left(\frac{1}{n}\sum_{i\in G}f(i)\,T_i\right)\left(\frac{1}{n}\sum_{j\in G}f(j)\,T_j\right)\\&=\frac{1}{n^2}\sum_{i\in G}\left(\sum_{j\in G}f(i)\,f(j)\,T_iT_j\right)\\&=\frac{1}{n^2}\sum_{i\in G}\left(\sum_{j\in G}f(ij)\,T_{ij}\right)\\&=\frac{1}{n^2}\sum_{i\in G}\left(\sum_{j\in G}f(j)\,T_j\right)\\&=\frac{1}{n}\sum_{j\in G}f(j)\,T_j\\&=T.\end{aligned}$$

پس ادعا ثابت می‌شود. اما اثر یک عملگر خطیِ خودتوان با رتبهٔ آن برابر است و چون رتبهٔ T یک عدد صحیحِ نامنفی است، پس $\operatorname{tr}T$ نیز چنین است. □

اکنون $\operatorname{tr}T$ را محاسبه می‌کنیم. برای این منظور لم زیر کارساز است (نمادگذاری Γ_a^n مجموعهٔ تمام nتایی‌های مرتب $(\gamma_1,\dots,\gamma_n)$ را نمایش می‌دهد که به‌ازای هر $i\in G$، $\gamma_i\in\{1,\dots,a\}$).

لم ۳. *به‌ازای هر $i\in G$، تعداد nتایی‌های مرتب $(\gamma_1,\dots,\gamma_n)\in\Gamma_a^n$ که $(\gamma_1,\dots,\gamma_n)=(\gamma_{i1},\dots,\gamma_{in})$ برابر ۱ است با $a^{n/o(i)}$.*

اثبات. فرض کنیم j_1، …، j_s هم‌مجموعه‌های راستِ متمایز $\langle i\rangle$ در G باشد که در آن $s=[G:\langle i\rangle]=n/o(i)$. به‌راحتی دیده می‌شود که $(\gamma_1,\dots,\gamma_n)=(\gamma_{i1},\dots,\gamma_{in})$ اگر و فقط اگر برای هر $1\le t\le s$،

$$\gamma_{ij_t}=\dots=\gamma_{i^{o(i)}j_t}.$$

پس تعداد nتایی‌های مرتب $(\gamma_1,\dots,\gamma_n)\in\Gamma_a^n$ که $(\gamma_1,\dots,\gamma_n)=(\gamma_{i1},\dots,\gamma_{in})$، برابر است با تعداد nتایی‌های مرتب $(\gamma_1,\dots,\gamma_n)\in\Gamma_a^n$ که به‌ازای هر $1\le t\le s$،

$$\gamma_{ij_t}=\dots=\gamma_{i^{o(i)}j_t}.$$

اما به‌ازای هر $1\le t\le s$ فقط a انتخاب برای تعریف

$$\gamma_{ij_t}=\dots=\gamma_{i^{o(i)}j_t}$$

داریم. در نتیجه تعداد مطلوب در حکم برابر است با $a^s=a^{n/o(i)}$. □

حال پایهٔ $\mathfrak{B}=\{e_1,\dots,e_a\}$ را برای V انتخاب می‌کنیم. بنابراین

$$\mathfrak{B}^{\otimes}=\{e_{\gamma_1}\otimes\cdots\otimes e_{\gamma_n}\,|\,(\gamma_1,\dots,\gamma_n)\in\Gamma_a^n\}$$

پایه‌ای برای $\overset{n}{\otimes} V$ خواهد بود. به‌ازای هر $i \in G$،

$$T_i(e_{\gamma_1} \otimes \cdots \otimes e_{\gamma_n}) = e_{\gamma_{i1}} \otimes \cdots \otimes e_{\gamma_{in}}$$

نشان می‌دهد که درایه‌های ماتریس T_i نسبت به پایهٔ $\mathfrak{B}^{\otimes}$ برابر با ۰ یا ۱ است. پس $\operatorname{tr} T_i$ برابر است با تعداد nتاییهای مرتب $(\gamma_1, \ldots, \gamma_n) \in \Gamma_a^n$ که $e_{\gamma_1} \otimes \cdots \otimes e_{\gamma_n} = e_{\gamma_{i1}} \otimes \cdots \otimes e_{\gamma_{in}}$. اکنون از لم ۳ نتیجه می‌گیریم که $\operatorname{tr} T_i = a^{n/o(i)}$. بنابراین

$$\begin{aligned} \operatorname{tr} T &= \operatorname{tr}\left(\frac{1}{n}\sum_{i\in G} f(i)\, T_i\right) \\ &= \frac{1}{n}\sum_{i\in G} f(i) \operatorname{tr} T_i \\ &= \frac{1}{n}\sum_{i\in G} f(i)\, a^{n/o(i)}\,. \end{aligned}$$

در نتیجه بنابر لم ۲

$$\sum_{i\in G} f(i)\, a^{n/o(i)} \equiv 0 \ (\text{به پیمانهٔ } n)\,.$$

یعنی قضیهٔ اصلی ثابت شده است، اما فقط برای aهای مثبت. لم زیر اثبات قضیهٔ اصلی را کامل خواهد کرد.

لم ۴. فرض کنیم $F(X)$ یک چند جمله‌ای در $\mathbb{C}[X]$ باشد که به‌ازای مقادیر صحیح و نامنفی X، مقادیر صحیح را به خود می‌گیرد. در این صورت $F(X)$ به‌ازای هر مقدار صحیح دلخواه X نیز چنین می‌کند.

اثبات. به‌ازای عدد صحیح دلخواه $k \neq 0$، چند جمله‌ای درجهٔ kی $\binom{X}{k}$ را به صورت زیر تعریف می‌کنیم. به‌ازای $k = 0$، این چندجمله‌ای چیزی نیست جز چندجمله‌ای ثابت ۱ و به‌ازای $k > 0$،

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}\,.$$

به‌راحتی می‌توانیم ثابت کنیم که این «ضرایب دوجمله‌ای» یک پایه برای فضای $\mathbb{C}[X]$ تشکیل می‌دهند و لذا می‌توانیم بنویسیم

$$F(X) = \sum_{k=0}^{m} a_k \binom{X}{k}$$

که در آن ضرایب a_k اعدادی مختلط هستند و m درجهٔ F است. از آنجایی که این چندجمله‌ایهای «ضرایب دوجمله‌ای» به‌ازای Xهای صحیح مقادیر صحیح را به‌خود می‌گیرند، لذا برای اثبات لم کافی است ثابت کنیم به‌ازای هر $0 \leq j \leq m$، $a_j \in \mathbb{Z}$. این حکم را نیز به کمک استقرا روی j با شروع از $j = 0$ ثابت می‌کنیم. واضح است که این حکم به‌ازای $j = 0$ درست است. حال فرض می‌کنیم این حکم به‌ازای اندیسهای کمتر از j درست باشد. چون $\binom{j}{j} = 1$ و برای $k > j$، $\binom{j}{k} = 0$، لذا

$$a_j = F(j) - \sum_{k=0}^{j-1} a_k \binom{j}{k}$$

در نتیجه ضریب a_j برابر است با یک ترکیب صحیح از عدد صحیح $F(j)$ (فرض) و اعداد صحیح a_k، $0 \leq k < j$ (فرض استقرا). پس این حکم به‌ازای اندیس j نیز برقرار است و لذا لم به کمک استقرا ثابت است. □

اکنون قرار می‌دهیم

$$F(X) = \frac{1}{n}\sum_{i\in G} f(i)\, X^{n/o(i)}.$$

توجه می‌کنیم که $F(X)$ یک چندجمله‌ای از X با ضرایب مختلط است. بنابر توضیحات قبل از لم ۴، $F(X)$ به‌ازای Xهای صحیح نامنفی مقادیر صحیح را به‌خود می‌گیرد. لذا لم ۴ نتیجه می‌دهد که $F(X)$ به‌ازای تمام Xهای صحیح چنین می‌کند و این نیز به معنی این است که به‌ازای هر $a \in \mathbb{Z}$،

$$\sum_{i\in G} f(i)\, a^{n/o(i)} \equiv 0 \ (\text{به پیمانهٔ } n)$$

که همان قضیهٔ اصلی است.

سپاسگزاری

نگارنده از حمایت مالی پژوهشگاه دانش‌های بنیادی (IPM) در طی نگارش این مقاله سپاسگزار است.

مراجع

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York (1976).
2. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York (1971).
3. I. M. Isaacs, M. R. Pournaki, "Orbit counting and Fermat's theorem", *Amer. Math. Monthly*, To Appear.
4. J. Petersen, *Tidsskrift for Mathematik*, (3) **2** (1872) 64-65.
5. C. J. Smyth, "A coloring proof of a generalization of Fermat's little theorem", *Amer. Math. Monthly*, (6) **93** (1986) 469-471.
6. T. Szele, Une généralisation de la congruence de Fermat, *Mat. Tidsskr. B.* **1948** (1948) 57-59.
7. A. Thué, *Ein Kombinatorischer Beweis eines Satzes von Fermat*, In Selected Mathematical Papers of Axel Thué, Universitetsforlaget (1977). (Originally Kra. Vidensk. Selsk, Skrifter. I. Mat. Nat. Kl. (1910) No. 3).

******

* محمدرضا پورنکی، دانشگاه صنعتی شریف

pournaki@ipm.ir