لم دوخط

مؤلف

سپهر قاضی نظامی

آبان ۱۳۸۸

*لم دوخط یکی از قضایای پر کاربرد در نظریه اعداد است که چون در کتاب های نظریه اعداد نیامده است و آموزش آن به صورت ناهمگن به برخی دانش آموزان علاقه مند به المپیاد قبل از دوره های باشگاه دانش پژوهان داده می شود بر عهده این سایت است که به صورت خلاصه آن را توضیح دهد.

*این لم از قضایای پایه ای نظریه اعداد نیست و لازم است خواننده پیش از خواندن آن به مطالبی از قبیل عاد کردن ، همنهشتی و اعداد اول مسلط باشد همچنین به عقیده نویسنده مباحثی مانند قضیه کوچک فرما و قضیه اویلر و دستگاه های کامل و مخفف مانده ها (طبق کتاب نظریه اعداد خانم میرزاخانی) و مرتبه و ریشه اولیه از لحاظ اولویت در مرتبه بالاتری نسبت به این قضیه قرار دارند پس توصیه می شود ابتدا خواننده به آن مطالب مسلط شود.

*آموختن این لم ضرری دارد و آن این است که وقتی این لم را بلد نیستید در حل مسایل مجبور هستید هر بار که مسئله ای را حل می کنید تا حدی مراحلی را طی کنید و با ساختارهایی آشنا شوید که گذشته از این لم بسیار پر کاربرد هستند ولی در هنگام استفاده از این لم این مراحل و ساختارها همگی در این ابزار قرار و از چشم شما مخفی می مانند پس توصیه می شود که سعی کنید خود این لم را اثبات کنید و در صورتی که تلاش شما برای این کار نتیجه نداد بخشی از راه حل را نگاه کرده و سعی کنید حل را خود کامل کنید و آنقدر این کار را انجام دهید تا حل کامل شود همچنین اکیدا توصیه می شود مراحل بالا را برای تمامی مسائل انجام دهید تا نتیجه مطلوب را بگیرید.

*بخشی از آنچه در ادامه می آید از مقاله ای در در مجله ریاضیات ترجمه آقای ارشک حمیدی نقل شده است(مخصوصا تعداد زیادی از سوالات) بخشی دیگر از آن نیز از آنچه در دوره های المپیاد تدریس شده انتخاب شده و بخشی نیز از خود نویسنده(ها) است پس امید است که به سرقت علمی متهم نشویم!

*پیش از مطالعه این مطلب توجه کنید که در میان سوالات چند قضیه مهم نیز گنجانده شده است که مطالعه آنها به حل مسائلی که در ادامه شان می آیند کمک می کند.پس به این قضایا نیز توجه کنید.

قرار داد: در ادامه p و q را برای اعداد اول استفاده می کنیم.

تعریف :علامت دوخط $||$

این علامت نشان دهنده بزرگترین توانی از یک عدد اول است که عددی دیگر را عاد می کند.

مثال:

$$۳^۲||۶۳$$

$$p^{\alpha}||p^{\alpha}q^{\beta}$$

صورت دیگر: $||a||_p$

منظور بزرگترین توان p است که عدد a را می شمارد.

مثال:

$$\left|\left|p^{\alpha}q^{\beta}\right|\right|_{\mathrm{p}} = \alpha$$

نکته:واضح است که

$$||ab||_p = ||a||_p + ||b||_p$$

لم: اگر n و p نسبت به هم اول باشند و $p|x-y$ و p هیچ کدام از x و y را نشمرد آنگاه:

(۱):

$$||x^n - y^n||_p = ||x-y||_p$$

داریم که

$$x^{\mathrm{n}} - \mathrm{y}^{\mathrm{n}} = (\mathrm{x}-\mathrm{y})(\mathrm{x}^{\mathrm{n}-۱} + \mathrm{x}^{\mathrm{n}-۲}\mathrm{y}^{۱} + \mathrm{x}^{\mathrm{n}-۳}\mathrm{y}^{۲} + \cdots + \mathrm{y}^{\mathrm{n}-۱})$$

پس کافی است که نشان دهیم

$$p \nmid \mathrm{x}^{\mathrm{n}-۱} + \mathrm{x}^{\mathrm{n}-۲}\mathrm{y}^{۱} + \mathrm{x}^{\mathrm{n}-۳}\mathrm{y}^{۲} + \cdots + \mathrm{y}^{\mathrm{n}-۱}$$

یا

$$x^{n-1} + x^{n-2}y^1 + x^{n-3}y^2 + \cdots + y^{n-1} \not\equiv 0 \left(p \text{ به پیمانه}\right)$$

ولی داریم که

$$x \equiv y \left(p \text{ به پیمانه}\right)$$

پس

$$\begin{aligned} x^{n-1} + x^{n-2}y^1 + x^{n-3}y^2 + \cdots + y^{n-1} &\equiv x^{n-1} + x^{n-2}x^1 + x^{n-3}x^2 + \cdots + x^{n-1} \\ &\equiv nx^{n-1} \left(p \text{ به پیمانه}\right) \end{aligned}$$

پس باید نشان دهیم که nx^{n-1} بر p بخش پذیر نباشد که واضح است.

لم: اگر n (عددی فرد) باشد و n و p نسبت به هم اول باشند و $p|x+y$ آنگاه اگر p هیچ کدام از x و y را نشمرد داریم:

(۲):

$$||x^n + y^n||_p = ||x + y||_p$$

داریم که

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y^1 + x^{n-3}y^2 - \cdots + y^{n-1})$$

پس کافی است که نشان دهیم

$$p \nmid x^{n-1} - x^{n-2}y^1 + x^{n-3}y^2 - \cdots + y^{n-1}$$

یا

$$x^{n-1} - x^{n-2}y^1 + x^{n-3}y^2 - \cdots + y^{n-1} \not\equiv 0 \left(p \text{ به پیمانه}\right)$$

ولی داریم که

$$x \equiv -y \left(p \text{ به پیمانه}\right)$$

پس

$$\begin{aligned} x^{n-1} - x^{n-2}y^1 + x^{n-3}y^2 - \cdots + y^{n-1} &\equiv x^{n-1} - x^{n-2}(-x)^1 + x^{n-3}(-x)^2 - \cdots + (-x)^{n-1} \\ &\equiv nx^{n-1} \left(p \text{ به پیمانه}\right) \end{aligned}$$

پس باید نشان دهیم که nx^{n-1} بر p بخش پذیر نباشد که واضح است.

حالت اول لم دوخط:

اگر p عددی اول جز ۲ باشد و $p|x-y$ و x و y هیچ کدام بر p بخشپذیر نباشد آنگاه:

(۳):

$$||x^n - y^n||_p = ||x-y||_p + ||n||_p$$

اثبات:

با استقرا روی عوامل اول n حکم را ثابت می کنیم برای این منظور ابتدا عبارت زیر را با تمام فرض های صورت لم اثبات می کنیم:

(۴):

$$||x^p - y^p||_p = ||x-y||_p + ۱$$

مانند آنچه در اثبات لم آمد کافی است نشان دهیم که

$$p|x^{p-۱} + x^{p-۲}y^{۱} + x^{p-۳}y^{۲} + \cdots + y^{p-۱}$$

و

$$p^{۲} \nmid x^{p-۱} + x^{p-۲}y^{۱} + x^{p-۳}y^{۲} + \cdots + y^{p-۱}$$

برای حکم اول داریم که

$$x^{p-۱} + x^{p-۲}y^{۱} + x^{p-۳}y^{۲} + \cdots + y^{p-۱} \equiv px^{p-۱} \equiv ۰ \left(\text{به پیمانه } p\right)$$

برای حکم دوم نیز داریم که $y = x + kp$

حال یک نکته را نشان می دهیم.اگر $۱ < t < p$ نشان می دهیم که :

$$y^t x^{p-۱-t} \equiv x^{p-۱} + tkpx^{p-۲} \left(\text{به پیمانه } p^{۲}\right)$$

که اثبات آن به صورت رو به رو است :

$$y^t x^{p-1-t} \equiv (x+kp)^t x^{p-1-t} \equiv \left(x^t + t(kp)(x^{t-1}) + \frac{t(t-1)}{2}(kp)^2(x^{t-2}) + \cdots\right)x^{p-1-t}$$
$$\equiv \left(x^t + t(kp)(x^{t-1})\right)x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2} \left(\text{به پیمانه } p^2\right)$$

آنچه اثبات کردیم ابزاری است برای نشان دادن حکم دوم:

$$x^{p-1} + x^{p-2}y^1 + x^{p-3}y^2 + \cdots + y^{p-1}$$
$$\equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + (x^{p-1} + 3kpx^{p-2}) + \cdots$$
$$+ (x^{p-1} + (p-1)kpx^{p-2}) \equiv px^{p-1} + (1+2+\cdots+p-1)kpx^{p-2}$$
$$\equiv px^{p-1} + \left(\frac{p(p-1)}{2}\right)kpx^{p-2} \equiv px^{p-1} + \frac{p-1}{2}kp^2x^{p-1} \equiv px^{p-1}$$
$$\not\equiv 0 \left(\text{به پیمانه } p^2\right)$$

پس حکم دوم نیز اثبات شد.

حال فرض کنید $n = p^\alpha b$ که $(p,b) = 1$ پس (با توجه به این که برای هر k طبیعی چون $x-y|x^k-y^k$ آنگاه $p|x^k-y^k$) داریم که

$$||x^n - y^n||_p = \left|\left|\left(x^{p^\alpha}\right)^b - \left(y^{p^\alpha}\right)^b\right|\right|_p = ||x^{p^\alpha} - y^{p^\alpha}||_p = \left|\left|\left(x^{p^{\alpha-1}}\right)^p - \left(y^{p^{\alpha-1}}\right)^p\right|\right|_p$$
$$= ||x^{p^{\alpha-1}} - y^{p^{\alpha-1}}||_p + 1 = \left|\left|\left(x^{p^{\alpha-2}}\right)^p - \left(\boldsymbol{y^{p^{\alpha-2}}}\right)^{\boldsymbol{p}}\right|\right|_{\boldsymbol{p}} + \mathbf{1}$$
$$= ||\boldsymbol{x^{p^{\alpha-2}}} - \boldsymbol{y^{p^{\alpha-2}}}||_{\boldsymbol{p}} + \mathbf{2} = \cdots = \left|\left|\left(\boldsymbol{x^{p^1}}\right)^{\mathbf{1}} - \left(\boldsymbol{y^{p^1}}\right)^{\mathbf{1}}\right|\right|_{\boldsymbol{p}} + \boldsymbol{\alpha} - \mathbf{1}$$
$$= ||\boldsymbol{x-y}||_{\boldsymbol{p}} + \boldsymbol{\alpha} = ||\boldsymbol{x-y}||_{\boldsymbol{p}} + ||\boldsymbol{n}||_{\boldsymbol{p}}$$

که در تساوی دوم از لم (۱) و در تساوی ۴ یا ۶ و برخی دیگر از (۴) استفاده شده.

پس اثبات کامل است.

حالت دوم لم دوخط:

اگر p عددی اول باشد و $p|x+y$ و x و y هیچ کدام بر p بخشپذیر نباشد و n فرد باشد آنگاه:

(۵):

$$||x^n + y^n||_p = ||x+y||_p + ||n||_p$$

اثبات:

تقریبا اثبات قسمت قبل را تکرار می کنیم.

باز هم با استقرا روی عوامل اول n حکم را ثابت می کنیم برای این منظور ابتدا عبارت زیر را با تمام فرض های صورت لم اثبات می کنیم:

(۶):

$$||x^p + y^p||_p = ||x+y||_p + ۱$$

مانند آنچه در اثبات لم آمد کافی است نشان دهیم که

$$p|\mathrm{x}^{\mathrm{p}-۱} - \mathrm{x}^{\mathrm{p}-۲}\mathrm{y}^{۱} + \mathrm{x}^{\mathrm{p}-۳}\mathrm{y}^{۲} - \cdots + \mathrm{y}^{\mathrm{p}-۱}$$

و

$$p^{۲} \nmid \mathrm{x}^{\mathrm{p}-۱} - \mathrm{x}^{\mathrm{p}-۲}\mathrm{y}^{۱} + \mathrm{x}^{\mathrm{p}-۳}\mathrm{y}^{۲} - \cdots + \mathrm{y}^{\mathrm{p}-۱}$$

مشابه حالت قبل برای حکم با توجه به رابطه $x \equiv -y$ داریم که

$$\mathrm{x}^{\mathrm{p}-۱} - \mathrm{x}^{\mathrm{p}-۲}\mathrm{y}^{۱} + \mathrm{x}^{\mathrm{p}-۳}\mathrm{y}^{۲} - \cdots + \mathrm{y}^{\mathrm{p}-۱} \equiv px^{p-۱} \equiv ۰ \ (\text{به پیمانه } p)$$

برای حکم دوم نیز داریم که $y = -x + kp$ و $۱ < t < p$.

پس داریم که :

$$y^t x^{p-1-t} \equiv (-x+kp)^t x^{p-1-t}$$
$$\equiv \left((-x)^t + t(kp)((-x)^{t-1}) + \frac{t(t-1)}{2}(kp)^2((-x)^{t-2}) + \cdots\right) x^{p-1-t}$$
$$\equiv \left((-x)^t + t(kp)((-x)^{t-1})\right) x^{p-1-t}$$
$$\equiv (-1)^t x^{p-1} + (-1)^{t-1} tkpx^{p-2} \left(\text{به پیمانه } p^2\right)$$

پس

$$x^{p-1} - x^{p-2}y^1 + x^{p-3}y^2 - \cdots + y^{p-1}$$
$$\equiv x^{p-1} - (-x^{p-1} + kpx^{p-2}) + (x^{p-1} - 2kpx^{p-2}) - (-x^{p-1} + 3kpx^{p-2}) + \cdots$$
$$+ (x^{p-1} - (p-1)kpx^{p-2}) \equiv px^{p-1} - (1+2+\cdots+p-1)kpx^{p-2}$$
$$\equiv px^{p-1} - \left(\frac{p(p-1)}{2}\right) kpx^{p-2} \equiv px^{p-1} - \frac{p-1}{2} kp^2 x^{p-1} \equiv px^{p-1}$$
$$\not\equiv 0 \left(\text{به پیمانه } p^2\right)$$

پس حکم دوم نیز اثبات شد.

حال فرض کنید $n = p^\alpha b$ که $(p,b) = 1$ پس (با توجه به این که برای هر k طبیعی فرد چون $x+y | x^k + y^k$ آنگاه $p | x^k + y^k$) داریم که

$$||x^n + y^n||_p = \left|\left|\left(x^{p^\alpha}\right)^b + \left(y^{p^\alpha}\right)^b\right|\right|_p = ||x^{p^\alpha} + y^{p^\alpha}||_p = \left|\left|\left(x^{p^{\alpha-1}}\right)^p + \left(y^{p^{\alpha-1}}\right)^p\right|\right|_p$$
$$= ||x^{p^{\alpha-1}} + y^{p^{\alpha-1}}||_p + 1 = \left|\left|\left(x^{p^{\alpha-2}}\right)^p + \left(y^{p^{\alpha-2}}\right)^p\right|\right|_p + 1$$
$$= ||x^{p^{\alpha-2}} + y^{p^{\alpha-2}}||_p + 2 = \cdots = \left|\left|\left(x^{p^1}\right)^1 + \left(y^{p^1}\right)^1\right|\right|_p + \alpha - 1 = ||x+y||_p + \alpha$$
$$= ||x+y||_p + ||n||_p$$

که در تساوی دوم از لم (۲) و در تساوی ۴ یا ۶ و برخی دیگر از (۶) استفاده شده است.

سوال ۱: چرا حالت $p = 2$ را جدا کردیم؟ کجای اثبات به مشکل بر می خورد؟

پس از حل کردن سوال بالا یا خواندن راه حل آن مساله های زیر را نشان دهید:

سوال ۲: اگر $4|x-y$ و x و y هیچ کدام بر ۲ بخشپذیر نباشد آنگاه:

(۷):

$$\left||x^n - y^n|\right|_2 = \left||x-y|\right|_2 + ||n||_2$$

سوال ۳:اگر $2|x-y$ و x و y هیچ کدام بر ۲ بخشپذیر نباشند و $2|n$ آنگاه:

(۸):

$$\left||x^n - y^n|\right|_2 = \left||x-y|\right|_2 + \left||x+y|\right|_2 + ||n||_2 - 1$$

سوال ۴:با استفاده از لم دوخط برای حالت تفریق آن لم را برای حالت جمع اثبات کنید.

جمع بندی:

فرض کنید p عددی اول باشد و x و y هیچ کدام بر p بخش پذیر نباشند آنگاه:

الف) اگر n طبیعی

اگر $p \neq ۲$ و $p|x-y$ آنگاه:

$$\left|\left|x^n - y^n\right|\right|_p = \left|\left|x-y\right|\right|_p + ||n||_p$$

اگر $p = ۲$ و $۴|x-y$ آنگاه:

$$\left|\left|x^n - y^n\right|\right|_۲ = \left|\left|x-y\right|\right|_۲ + ||n||_۲$$

یا رابطه کلی تر اگر $p = ۲$ و $۲|x-y$ و $۲|n$:

$$\left|\left|x^n - y^n\right|\right|_۲ = \left|\left|x-y\right|\right|_۲ + \left|\left|x+y\right|\right|_۲ + ||n||_۲ - ۱$$

ب) اگر n فرد و $p|x+y$ آنگاه:

$$\left|\left|x^n + y^n\right|\right|_p = \left|\left|x+y\right|\right|_p + ||n||_p$$

ج) خوب است که به یاد داشته باشید اگر $(p\,,n) = ۱$:

$$||x^n - y^n||_p = ||x-y||_p$$

اگر n فرد باشد نیز:

$$||x^n + y^n||_p = ||x+y||_p$$

که البته قسمت ج کاملا از قسمت های الف و ب نتیجه نمی شود.

۵. k عددی طبیعی است.همه n های طبیعی را بیابید که $۳^k | ۲^n - ۱$

۶.(مسابقه یونسکو ۱۹۹۵)فرض کنید n و a عددهایی طبیعی باشند، p اول و فرد که

$$a^p \equiv ۱ \left(\text{به پیمانه } p^n\right)$$

نشان دهید:

$$a \equiv ۱ \left(\text{به پیمانه } p^{n-۱}\right)$$

۷.با فرض اینکه اگر $(a,p) = ۱$ آنگاه $p | a^{p-۱} - ۱$ نشان دهید اگر $(a,n) = ۱$ آنگاه $n | a^{\varphi(n)} - ۱$ که

$$\varphi\left(p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k}\right) = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k} \left(۱ - \frac{۱}{p_۱}\right)\left(۱ - \frac{۱}{p_۲}\right) \dots \left(۱ - \frac{۱}{p_k}\right)$$

که

$$p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k}$$

تجزیه n به عوامل اول است.

۸.فرض کنید $p \neq ۲$ ریشه اولیه دارد نشان دهید p^k هم ریشه اولیه دارد.

۹.(مرحله دو ایران ۱۳۸۷) نشان دهید تنها عدد طبیعی a، که برای هر n طبیعی $۴(a^n + ۱)$ مکعب کامل باشد، یک است.(توجه کنید که راه حل لم دوخط راه حل خوبی برای این سوال نیست و لازم است که آن را به طریقی دیگر نیز حل کنید.)

۱۰.(مرحله ۳ ایران) فرض کنید $k > ۱$ عددی طبیعی باشد.نشان دهید نامتناهی n طبیعی وجود دارد که:

$$n | ۱^n + ۲^n + ۳^n + \dots + k^n$$

قضیه:اگر a وb اعدادی طبیعی باشند و $a > b$ آنگاه $a^n - b^n > n(a-b)$

اثبات:داریم

$$(a^n - b^n) = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})$$

پس داریم $a - b \geq 1$ و چون $a^{n-k}b^{k-1} \geq 1$ پس

$$(a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}) \geq n$$

و حالت تساوی هم وجود ندارد زیرا در این صورت باید $a = b = 1$ باشد و اثبات کامل است.

۱۱.نشان دهید $a^n - b^n$ عامل اولی دارد که $a - b$ ندارد.

۱۲.(ایرلند ۱۹۹۶) فرض کنید p اول باشد و a و n اعدادی صحیح و مثبت.اگر $2^p + 3^p = a^n$ نشان دهید $n = 1$

۱۳.(روسیه ۱۹۹۶)همه اعداد طبیعی n را بیابید که اعداد صحیح و نسبت به هم اول x و y و عدد $k > 1$ وجود داشته باشند به طوری که $3^n = x^k + y^k$.

۱۴.(روسیه ۱۹۹۶)فرض کنید x, y, p, n, k اعدادی طبیعی باشند که $x^n + y^n = p^k$.ثابت کنید اگر n فرد و p اول و فرد باشد آنگاه n توانی از p است.

۱۵.با فرض اول بودن p معادله $a^p - 1 = p^k$ را در اعداد طبیعی حل کنید.

۱۶.تمام جواب های معادله $(n - 1)! + 1 = n^m$ را در اعداد طبیعی بیابید.

قضیه: a و b دو عدد طبیعی متمایز نسبت به هم اول:

$$(a^n - b^n, a^m - b^m) = a^{(m,n)} - b^{(m,n)}$$

اثبات: حکم را با استقرا روی ماکسیمم m و n اثبات می کنیم.اگر این مقدار ۱ باشد که مساله واضح است (پایه) در غیر این صورت با فرض $n > m$ داریم:

$$\begin{aligned}(a^n - b^n, a^m - b^m) &= (a^n - b^n - a^{n-m}(a^m - b^m), a^m - b^m)\\ &= (a^n - b^n - a^n + a^{n-m}b^m, a^m - b^m) = (b^m(a^{n-m} - b^{n-m}), a^m - b^m)\\ &= (a^{n-m} - b^{n-m}, a^m - b^m)\end{aligned}$$

که ماکسیمم $n - m$ و m از n کمتر است.

پس طبق استقرا و رابطه $(n, m) = (n - m, m)$ داریم

$(a^{n-m} - b^{n-m}, a^m - b^m) = a^{(n,m)} - b^{(n,m)}$ ***پس اثبات کامل است.***

۱۷.(بلغارستان ۱۹۹۵)نشان دهید اگر به ازای n طبیعی $۳^n - ۲^n$ توانی از عددی اول باشد، آنوقت n هم عددی اول است.

۱۸.(SL۱۹۹۷) فرض کنید b، m و n عددهایی طبیعی باشند که $b > ۱$ و $m \neq n$.ثابت کنید که اگر مقسوم علیه های اول عددهای $b^m - ۱$ و $b^n - ۱$ یکسان باشند، $b + ۱$ توانی از ۲ است.

۱۹.(SL۱۹۹۱) بزرگترین k ای را بیابید که :

$$1991^k | 1990^{1991^{1992}} + 1992^{1991^{1990}}$$

۲۰.(بالکان ۱۹۹۳)فرض کنید p عددی اول باشد و m عددی طبیعی باشد و $m > ۱$.ثابت کنید اگر x و y عددهایی طبیعی و بزرگتر از ۱ باشند و

$$\frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m$$

آن وقت $m = p$.

۲۱.(مسابقه چک-اسلواکی ۱۹۹۶)همه عددهای طبیعی مانند x و y را پیدا کنید که $p^x - y^p = ۱$.که در آن p عددی اول و فرد است.

۲۲.(رومانی TST۱۹۹۳) ثابت کنید اگر n عددی طبیعی و خالی از مربع باشد، عددهایی طبیعی و نسبت به هم اول مانند x و y وجود ندارند که $(x+y)^3$ ، x^n+y^n را بشمارد.

۲۳.نشان دهید اگر x و y اعدادی حقیقی و مثبت باشند طوری که به ازای هر n طبیعی ، x^n-y^n طبیعی باشد آنوقت x و yطبیعی هستند.

۲۴.نشان دهید اگر x و y اعدادی گویا و مثبت باشند طوری که به ازای نامتناهی n طبیعی ، x^n-y^n طبیعی باشد آنوقت x وy طبیعی هستند.

راه حل برخی سوال ها:

۱:برای اثبات این لم در قسمتی که می خواستیم رابطه (۴) را نشان دهیم نوشتیم که

$$x^{p-1}+x^{p-2}y^{1}+x^{p-3}y^{2}+\cdots+y^{p-1}$$
$$\equiv x^{p-1}+(x^{p-1}+kpx^{p-2})+(x^{p-1}+2kpx^{p-2})+(x^{p-1}+3kpx^{p-2})+\cdots$$
$$+(x^{p-1}+(p-1)kpx^{p-2})\equiv px^{p-1}+(1+2+\cdots+p-1)kpx^{p-2}$$
$$\equiv px^{p-1}+\left(\frac{p(p-1)}{2}\right)kpx^{p-2}\equiv px^{p-1}+\frac{p-1}{2}kp^{2}x^{p-1}\equiv px^{p-1}$$
$$\not\equiv 0\left(\text{به پیمانه } p^{2}\right)$$

و چون فرض کرده بودیم که p فرد است از رابطه زیر استفاده کردیم

$$\left(\frac{p(p-1)}{2}\right)kpx^{p-2}=\frac{p-1}{2}kp^{2}x^{p-1}\equiv 0\left(\text{به پیمانه } p^{2}\right)$$

و به وضوح این کار وقتی معتبر است که $\frac{p-1}{2}$ ضریبی صحیح باشد.

۲:برای تنوع هم که شده این رابطه را به طریقی دیگر نشان می دهیم:

به وضوح با توجه به رابطه (۱) کافی است نشان دهیم:

$$\left|\left|x^{2^n}-y^{2^n}\right|\right|_{2}=\left|\left|x-y\right|\right|_{2}+n$$

داریم که:

(۹)

$$x^{2^n}-y^{2^n}=\left(x^{2^{n-1}}+y^{2^{n-1}}\right)\times\left(x^{2^{n-2}}+y^{2^{n-2}}\right)\times\left(x^{2^{n-3}}+y^{2^{n-3}}\right)\times\ \ldots$$
$$\times(x^{2}+y^{2})\times(x+y)\times(x-y)$$

داریم که

$$x\equiv y\equiv\pm 1\left(\text{به پیمانه } 4\right)$$

پس

$$x^{2^k}\equiv y^{2^k}\equiv\pm 1\left(\text{به پیمانه } 4\right)$$

پس

$$x^{۲k} + y^{۲k} \equiv ۲ \left(\text{به پیمانه } ۴\right)$$

پس هر یک از عوامل حاصل ضرب (۹) به جز $x - y$ دقیقا یک عامل ۲ دارد و پس از این نیز مساله به سادگی اثبات می شود.

۳:داریم که مربع هر عدد فرد به فرم $۸k + ۱$ است پس اگر x و y اعدادی فرد باشند داریم که $۴|x^{۲} - y^{۲}$ پس با فرض $k > ۰$ و m فرد داریم:

$$\begin{aligned} ||x^n - y^n||_{۲} &= \left|\left|x^{m۲^k} - y^{m۲^k}\right|\right|_{۲} = \left|\left|x^{۲^k} - y^{۲^k}\right|\right|_{۲} = \left|\left|(x^{۲})^{۲^{k-۱}} - (y^{۲})^{۲^{k-۱}}\right|\right|_{۲} \\ &= ||x^{۲} - y^{۲}||_{۲} + k - ۱ = ||x - y||_{۲} + ||x + y||_{۲} + ||n||_{۲} - ۱ \end{aligned}$$

۴:اگر $p = ۲$ این لم را برای حالت جمع به دست آوردیم(کی؟) پس با با جایگزین کردن $-y$ به جای y به هدف مطلوب می رسیم:

$$||x^n + y^n||_{۲} = ||x^n - (-y)^n||_{۲} = ||x - (-y)||_{۲} + ||n||_{۲} = ||x + y||_{۲} + ||n||_{۲}$$