۳. تمام nهایی را بیابید که $n + ۲^n | n + ۸^n$.

حل. با توجه به اتحاد چاق و لاغر و رابطه خود سوال داریم:

$$\left.\begin{array}{l} n + ۲^n | n + ۸^n \\ n + ۲^n | n^۳ + ۸^n \end{array}\right\} \Rightarrow n + ۲^n | n^۳ - n$$

اما با استفاده از استقرا می‌توانیم ثابت کنیم برای $۱۰ \leqslant n$ داریم $n^۳ < ۲^n$. بنابراین خواهیم داشت

$$n + ۲^n > n^۳ - n$$

برای $۱۰ > n$ نیز می‌توانیم اعداد را در عبارت سوال امتحان کنیم. در نهایت عددهای ۱ و۲ و۴ و۶ جواب مسئله خواهند بود. ▷

۷. ثابت کنید به ازای هر عدد فرد و اول p، بی‌نهایت عدد طبیعی n وجود دارد که $n۲^n + ۱$ بر p بخش‌پذیر باشد.

حل. باید بی‌نهایت n بیابیم که $n۲^n \overset{p}{\equiv} -۱$. داریم $۲^{p-۱} \overset{p}{\equiv} ۱$. در نتیجه $۲^{(p-۱)k} \overset{p}{\equiv} ۱$. فرض کنید n به صورت $k(p-۱)$ باشد. در آن صورت باید داشته باشیم $(p-۱)k۲^{(p-۱)k} \overset{p}{\equiv} -۱$ که معادل است با $k \overset{p}{\equiv} ۱$. پس به ازای هر l طبیعی، $n = (p-۱)(pl+۱)$ در رابطه‌ی $n۲^n \overset{p}{\equiv} -۱$ صدق می‌کند. ▷

۸. همه اعداد طبیعی و فرد n را پیدا کنید که برای آن‌ها عدد $(n-1)!$ بر n^2 بخش‌پذیر نباشد.

حل. نشان می‌دهیم n برابر عددی اول و یا $n = 9$ است.

اگر n عددی مرکب باشد و بتوان آن را به صورت $n = ab (a \neq b, a, b \geqslant 3)$ نمایش داد، در این صورت چون $b, 2b, a, 2a$ همگی از $n-1$ کوچکترند، بنابراین $n^2 | (n-1)!$. در غیر این صورت n یا عددی اول است و یا به صورت $n = p^2$ که p عددی است اول.

اگر n عددی اول باشد، مشخص است که $p^2 \nmid (p-1)!$.

اگر $n = p^2$ و $p \geqslant 5$ باشد، آنگاه $p^2 - 1 \geqslant 4p$ است در نتیجه $p^4 | (p^2-1)!$.

اگر $p = 3$ باشد، آنگاه $n = 9$ می‌باشد که $9^2 \nmid 8!$، بنابراین جواب مسئله است. ▷

۹. ثابت کنید در دنباله‌ی $۱, ۳۱, ۳۳۱, ۳۳۳۱, \ldots$ بی‌نهایت عدد مرکب وجود دارد.

حل. n امین عضو دنباله را با a_n نشان می‌دهیم. به سادگی به دست می‌آید $a_n = \frac{۱۰^n - ۷}{۳}$. فرض کنیم $a_m = p$ که p عددی اول است. (اگر چنین عضوی وجود نداشته باشد، چیزی برای اثبات باقی نمی‌ماند). در این صورت داریم

$$a_m = \frac{۱۰^m - ۷}{۳} = p \Rightarrow ۱۰^m \overset{p}{\equiv} ۷$$

طبق قضیه فرما می‌دانیم $۱۰^{p-۱} \overset{p}{\equiv} ۱$، بنابراین خواهیم داشت $۱۰^{m+k(p-۱)} \overset{p}{\equiv} ۷$؛ یعنی $a_{m+k(p-۱)}$ بر p بخش‌پذیر است یعنی به ازای هر $k \geqslant ۲$، $a_{m+k(p-۱)}$ مرکب است، پس بی‌نهایت عدد مرکب در دنباله $\{a_n\}$ وجود دارد. $\triangleright$

۱۰. تمام nهایی را بیابید که $n^{۴}+n^{۲}+۱=p^{k}$ که pعددی اول است.

حل. ابتدا عبارت سمت چپ را تجزیه می‌کنیم:

$$n^{۴}+n^{۲}+۱=(n^{۲}+n+۱)(n^{۲}-n+۱)$$

بنابراین خواهیم داشت

$$\begin{cases} n^{۲}+n+۱=p^{i} \\ n^{۲}-n+۱=p^{k-i} \end{cases}$$

با توجه به آن که $n^{۲}+n+۱>n^{۲}-n+۱$ پس داریم $i>k-i$ پس داریم

$$p^{k-i}|p^{i}\Rightarrow n^{۲}-n+۱|n^{۲}+n+۱\Rightarrow(n^{۲}-n+۱,n^{۲}+n+۱)=n^{۲}-n+۱$$

اما از طرفی داریم:

$$\left.\begin{array}{l} d|n^{۲}-n+۱ \\ d|n^{۲}+n+۱ \end{array}\right\}\Rightarrow d|۲n$$

از طرفی عدد $n^{۲}-n+۱$ عددی فرد است بنابراین $d|n$. پس داریم:

$$\left.\begin{array}{l} d|n\Rightarrow d|n^{۲}-n \\ d|n^{۲}-n+۱ \end{array}\right\}d|۱\Rightarrow d=۱$$

بنابراین داریم $n^{۲}-n+۱=۱$ پس داریم $n=۱$. تنها عدد یک جواب مسئله خواهد بود. ▷

۱۱. تمام p, qهای اول را بیابید که داشته باشیم $۲^m p^۲ + ۱ = q^۵$.

حل. عدد یک را به سمت راست برده و عبارت راست را تجزیه می‌کنیم:

$$۲^m p^۲ = (q - ۱)(q^۴ + q^۳ + q^۲ + q + ۱)$$

چون عدد $q^۴ + q^۳ + q^۲ + q + ۱$ حتما عددی فرد است پس داریم $۲^m | q - ۱$. اگر داشته باشیم $p | q - ۱$ آنگاه داریم $۲^m p \geqslant q - ۱$، بنابراین داریم $p \geqslant q^۴ + q^۳ + q^۲ + q + ۱$. بنابراین خواهیم داشت $q - ۱ > q^۴ + q^۳ + q^۲ + q + ۱$ که نادرست است. پس:

$$\begin{cases} p^۲ = q^۴ + q^۳ + q^۲ + q + ۱ \\ q - ۱ = ۲^m \end{cases}$$

اگر $m \geqslant ۳$ باشد، آنگاه $q \overset{۸}{\equiv} ۱$، بنابراین $q^۴ + q^۳ + q^۲ + q + ۱ = p^۲ \overset{۸}{\equiv} ۵$ که نمی‌شود (زیرا $p^۲$ عددی فرد است و اعداد مربع کامل فرد، باقیمانده‌شان به ۸، یک است). پس m یا یک است یا دو. با جایگذاری متوجه می‌شویم اگر $m = ۲$، مسئله جواب ندارد و اگر $m = ۱$، آنگاه داریم $q = ۳, p = ۱۱$. ▷

۱۲. اگر a و b دو عدد اول متمایز باشند، نشان دهید:

$$a^{b-۱} + b^{a-۱} \overset{ab}{\equiv} ۱$$

حل. بنابر قضیه فرما می‌دانیم $a^{b-۱} \overset{b}{\equiv} ۱$ و چون $b^{a-۱} \overset{b}{\equiv} ۰$ خواهیم داشت $b^{a-۱} + a^{b-۱} \overset{b}{\equiv} ۱$، به طور مشابه داریم $a^{b-۱} + b^{a-۱} \overset{a}{\equiv} ۱$.

بنابراین $a^{b-۱} + b^{a-۱} - ۱$ هم بر a و هم بر b بخش‌پذیر است و چون $(a, b) = ۱$، پس بر حاصل ضرب ab نیز بخش‌پذیر است. ▷

۱۳. فرض کنید a,b,c,d اعدادی طبیعی باشند که داشته باشیم $ab=cd$. ثابت کنید اعداد زیر اعدادی مرکب هستند.

$$T=a^{۲}+b^{۲}+c^{۲}+d^{۲},\ ۲^{T}-۱$$

حل. فرض کنید $m=(a,c)$، می‌توانیم بنویسیم $c=mc_{۱}$ و $a=ma_{۱}$ به طوری که $(a_{۱},c_{۱})=۱$. با جایگذاری در $ab=cd$ خواهیم داشت:

$$ma_{۱}b=mc_{۱}d\Rightarrow a_{۱}b=c_{۱}d\overset{(a_{۱},c_{۱})=۱}{\Rightarrow}a_{۱}|d$$

با فرض $d=a_{۱}t$ داریم $b=c_{۱}t$، بنابراین

$$T=a_{۱}^{۲}m^{۲}+c_{۱}^{۲}t^{۲}+c_{۱}^{۲}m^{۲}+a_{۱}^{۲}t^{۲}=a_{۱}^{۲}(m^{۲}+t^{۲})+c_{۱}^{۲}(m^{۲}+t^{۲})=(m^{۲}+t^{۲})(a_{۱}^{۲}+c_{۱}^{۲})$$

بنابراین T مرکب است. بنابراین می‌توان نوشت:

$$۲^{T}-۱=۲^{(m^{۲}+t^{۲})(a_{۱}^{۲}+c_{۱}^{۲})}-۱\Rightarrow ۲^{m^{۲}+t^{۲}}-۱|۲^{T}-۱$$

پس $۲^{T}-۱$ نیز مرکب است. $\triangleright$

۱۴. تمام زوج‌های p, q از اعداد اول را بیابید که برای آن‌ها داشته باشیم:

$$p^{۳} - q^{۵} = (p+q)^{۲}$$

حل. واضح است که $p > q$. فرض کنید $p, q \neq ۳$ پس $p^{۲} \overset{۳}{\equiv} q^{۲} \overset{۳}{\equiv} ۱$، بنابراین $p^{۳} - q^{۵} \overset{۳}{\equiv} p - q$. اگر $p \overset{۳}{\equiv} q$، آنگاه $p - q \overset{۳}{\equiv} ۰$ ولی $(p+q)^{۲} \overset{۳}{\equiv} ۴p^{۲} \overset{۳}{\equiv} ۱$ پس باید داشته باشیم $p \overset{۳}{\not\equiv} q$. در این صورت $(p+q)^{۲} \overset{۳}{\equiv} ۰$ ولی $p - q \overset{۳}{\not\equiv} ۰$. پس در این حالت هم مسئله جواب ندارد. به بررسی حالات دیگر می‌پردازیم.

اگر $q = ۳$، آنگاه:

$$p^{۳} - ۳^{۵} = (p+۳)^{۲} = p^{۲} + ۶p + ۹$$

بنابراین:

$$p(p^{۲} - p - ۶) = ۹ \times ۲۸ \Rightarrow p(p-۳)(p+۲) = ۳^{۲} \times ۲^{۲} \times ۷$$

پس $p = ۷$. بنابراین $(p, q) = (۷, ۳)$ تنها حواب مسئله است. ▷

۱۵. همه اعداد طبیعی a و b را بیابید که داشته باشیم:

$$a + b | ۴ab + ۱, (۲a - ۱, ۲b + ۱) = ۱$$

حل. داریم

$$a + b | ۴ab + ۱ = (۲a - ۱)(۲b - ۱) + ۲(a + b)$$

بنابراین

$$a + b | (۲a - ۱)(۲b - ۱)$$

فرض کنیم $d = (a + b, ۲a - ۱)$. در این صورت داریم

$$\left.\begin{array}{l} d | a + b | ۲a + ۲b \\ d | ۲a - ۱ \end{array}\right\} \Rightarrow d | ۲b + ۱$$

چون داریم $(۲a - ۱, ۲b + ۱) = ۱$، بنابراین $d | ۱$ و در نتیجه $d = ۱$. بنابراین $a + b | ۲b - ۱$. واضح است که $\frac{۲b-۱}{۲} > a + b$، بنابراین باید داشته باشیم $a + b = ۲b - ۱$. در این صورت $a = b - ۱$. واضح است که عبارت $a + b | ۴ab + ۱$ برقرار است. پس صرفا عبارت دوم را چک می‌کنیم تا مطمئن شویم برای عدد b محدودیتی وجود ندارد:

$$\left.\begin{array}{l} d | ۲b + ۱ \\ d | ۲a - ۱ = ۲b - ۳ \end{array}\right\} \Rightarrow d | ۴$$

d نمی‌تواند برابر ۴ یا ۲ باشد. زیرا هر دو عدد $۲b - ۳$ و $۲b + ۱$ اعدادی فرد هستند. بنابراین $d = ۱$. بنابراین برای هر عدد طبیعی $b > ۱$ و $a = b - ۱$ خواسته‌های سوال برقرارند. ▷

۱۶. معادله‌ی $x^y - y^x = xy^۲ - ۱۱$ را در اعداد اول حل کنید.

حل. طبق قضیه فرما داریم $x^{y-۱} \overset{y}{\equiv} ۱$ بنابراین

$$x^y \overset{y}{\equiv} x \Rightarrow x^y - y^x \overset{y}{\equiv} x$$

از طرفی به خاطر عبارت صورت سوال $x^y - y^x \overset{y}{\equiv} -۱۱$، بنابراین داریم $y|x + ۱۱$، پس $y \leqslant x + ۱۱$. به طور مشابه خواهیم داشت $x|y - ۱۱$، پس اگر فرض کنیم $y > ۱۱$، داریم $x + ۱۱ \geqslant y$، پس خواهیم داشت $y = x + ۱۱$. اگر x عدد اول فرد باشد، y زوج است و چون اول است مجبور است ۲ باشد که با $y > ۱۱$ تناقض دارد. پس x زوج و برابر با ۲ است. بنابراین y برابر با ۱۳ خواهد بود. اما اگر در عبارت سوال جایگذاری کنیم، به تناقض می‌خوریم.

اگر فرض کنیم $y > ۱۱$، آنگاه می‌دانیم $y - ۱۱|x$، پس خواهیم داشت $x + y \leqslant ۱۱$. اگر اعداد اول کوچکتر از ۱۱ را در عبارت سوال امتحان کنیم، تنها جواب مسئله $(x, y) = (۳, ۲)$ خواهد بود. ▷

۱۷. همه‌ی اعداد طبیعی n را بیابید که $n^n + ۱$ و $(۲n)^{۲n} + ۱$ هردو اول باشند.

حل. اگر $n \neq ۱$ و n فرد باشد یا یک عامل فرد داشته باشد، آنگاه $n^n + ۱$ تجزیه می‌شود و مرکب است. پس $n = ۲^k$. و در نتیجه :

$$\begin{aligned} n^n + ۱ &= ۲^{kn} + ۱ \\ (۲n)^{۲n} + ۱ &= ۲^{(k+۱)۲n} + ۱ \end{aligned}$$

اگر هر یک از k یا $k + ۱$ فرد باشد، یکی از عبارت‌ها مرکب است، مگر اینکه $k = ۰$ یا $k = ۱$ و در نتیجه $n = ۱$ یا $n = ۲$. ▷

۱۸. تمام اعداد طبیعی m و n را بیابید که

$$m^۲ + n^۲ \mid m^۳ + n$$
$$m^۲ + n^۲ \mid n^۳ + m$$

حل.

فرض کنید ب.م.م m و n برابر با d باشد و در نتیجه $m = m'd$ و $n = n'd$.

$$\begin{cases} d^۲\left(m'^۲ + n'^۲\right) | d^۳m'^۳ + dn' \\ d^۲\left(m'^۲ + n'^۲\right) | d^۳n'^۳ + dm' \end{cases} \Rightarrow \begin{cases} d\left(m'^۲ + n'^۲\right) | d^۲m'^۳ + n' \\ d\left(m'^۲ + n'^۲\right) | d^۲n'^۳ + m' \end{cases}$$

$$\Rightarrow \begin{cases} d|n' \\ d|m' \end{cases} \Rightarrow d|\left(m', n'\right) = ۱ \Rightarrow d = ۱ \Rightarrow (m, n) = ۱$$

در نتیجه خواهیم داشت:

$$\left.\begin{array}{l} m^۲ + n^۲|m^۳ + n \\ m^۲ + n^۲|m^۳ + mn^۲ \end{array}\right\} \Rightarrow m^۲ + n^۲|mn^۲ - n = n(mn - ۱)$$

با توجه به اینکه m و n نسبت به هم اول هستند، پس $m^۲ + n^۲$ نیز نسبت به n اول است و می‌توان نتیجه گرفت که $m^۲ + n^۲|mn - ۱$. طرف راست این رابطه همواره کوچکتر است و این رابطه فقط زمانی برقرار است که $mn - ۱ = ۰$ و در نتیجه $m = ۱$ و $n = ۱$ باشد. ▷

۲۱. تمامی $p, x \in N$ را بیابید که p اول و $p^x - 1$ مکعب کامل باشد.

حل.

$$p^x - 1 = k^3 \Rightarrow p^x = k^3 + 1 \Rightarrow p^x = (k+1)(k^2+1-k)$$

در اینصورت ۳ حالت به وجود می‌آید:

(آ) حالت اول : $k+1$ و k^2+1-k هر دو توانی از p باشند. فرض کنید $k+1 = p^m$ و $k^2+1-k = p^n$. در این صورت p و k نیز نسبت به هم اول هستند.

$$k^2 + 1 - k = p^n \Rightarrow (k+1)^2 - 3k = p^n \Rightarrow p^{2m} - p^n = 3k \Rightarrow p|3k$$

با توجه به اینکه p و k نسبت به هم اول هستند، پس $p = 3$ و در نتیجه $3^x = (k+1)(k^2+1-k)$. با توجه به اینکه دو پرانتز ضرب شده حداکثر یک عامل ۳ مشترک دارند، باید داشته باشیم $k+1 = 3$ یا $k+1 = 1$. در حالت اول به دست می‌آید $k = 2, x = 2, p = 3$ و حالت دوم نیز ممکن نمی‌باشد.

(ب) حالت دوم: $k+1 = 1$ باشد. در اینصورت $k = 0$ و $p^x = 1$. در نتیجه $x = 0$ که با طبیعی بودن آن در تناقض است.

(ج) حالت سوم : $k^2 + 1 - k = 1$ باشد. اگر $k = 0$ مشابه حالت قبل به تناقض می‌رسیم. در غیر اینصورت $k = 1$ و $p^x = 2$. پس خواهیم داشت $p = 2$ و $x = 1$.

▷

۲۲. همه اعداد اول p و q و r را بیابید که $pqr = ۵(p+q+r)$.

حل. با توجه به اینکه pqr بر ۵ بخش‌پذیر است، ۳ حالت ممکن می‌شود:

(آ) حالت اول : هر ۳ عدد p, q, r برابر با ۵ باشند. در اینصورت باید داشته باشیم $۱۵ \times ۵ = ۱۲۵$ که تناقض است.

(ب) حالت دوم : دو تا از آنها مثلاً p و q برابر با ۵ باشند. در اینصورت خواهیم داشت $۲۵r = ۵(۱۰ + r)$ و جوابی برای r پیدا نمی‌شود.

(ج) حالت سوم : فقط یکی از آنها مثلاً p برابر با ۵ باشد. در اینصورت:

$$۵qr = ۵(۵ + q + r) \Rightarrow qr = ۵ + q + r \Rightarrow ۶ = qr - q - r + ۱ = (q - ۱)(r - ۱)$$

در اینصورت دو حالت ممکن است. در حالت اول $q - ۱ = ۲$ و $r - ۱ = ۳$ است که با اول بودن r تناقض دارد. در حالت دوم $q - ۱ = ۶$ و $r - ۱ = ۱$ است. پس جواب نهایی $p = ۵, q = ۷, r = ۲$ می‌باشد.

▷

۲۳. مقادیر n, p, q را در $\mathbf{N} \cup \{۰\}$ طوری بیابید که $۲^n + n^۲ = ۳^p \times ۷^q$.

حل. با توجه به اینکه باقی‌مانده توان‌های ۲ بر ۷ برابر ۲، ۱ یا ۴ و همچنین باقی‌مانده مربعات کامل بر ۷ برابر ۰، ۱، ۲ یا ۴ است، حاصل $۲^n + n^۲$ نمی‌تواند بر ۷ بخش‌پذیر باشد. پس $q = ۰$ و در نتیجه $۲^n + n^۲ = ۳^p$.
اگر $n \geqslant ۲$ باشد، در این صورت n فرد است و $n^۲ \overset{۴}{\equiv} ۱$. همچنین چون $۲^n \overset{۴}{\equiv} ۰$، پس داریم $۳^p \overset{۴}{\equiv} ۱$. پس نتیجه میگیریم که p زوج و در نتیجه ۳^p مربع کامل است. فرض کنید $۳^p = k^۲$ و $۲^n = (k-n)(k+n)$.

$$\left.\begin{aligned} k - n &= ۲^a \\ k + n &= ۲^{n-a} \end{aligned}\right\} \Rightarrow ۲n = ۲^a\left(۲^{n-۲a} - ۱\right)$$

با توجه به فرد بودن n، مقدار a باید برابر با ۱ باشد. پس خواهیم داشت $n = ۲^{n-۲} - ۱$. سمت راست این تساوی به ازای $n \geqslant ۵$ از سمت چپ بزرگتر است و این تساوی نمی‌تواند برقرار باشد.
حال باید حالت $n < ۲$ را بررسی کنیم. در این حالت به دو جواب زیر می‌رسیم:

$$n = ۱, q = ۰, p = ۱$$
$$n = ۰, q = ۰, p = ۰$$

▷

۲۴. ثابت کنید اگر n عددی فرد باشد، آنگاه $۲^{n!} - ۱$ بر n قابل قسمت است.

حل. چون $\phi(n)$ عددی کمتر از n است، حتما خواهیم داشت: $\phi(n)|n!$. پس k وجود دارد که $n! = k \times \phi(n)$. از طرفی چون n عددی فرد است داریم: $(n, ۲) = ۱$. در نتیجه طبق قضیه اویلر خواهیم داشت:

$$۲^{n!} - ۱ \overset{n}{\equiv} ۲^{k \times \phi(n)} - ۱ \overset{n}{\equiv} \left(۲^{\phi(n)}\right)^k - ۱ \overset{n}{\equiv} ۱^k - ۱ \overset{n}{\equiv} ۱ - ۱ \overset{n}{\equiv} ۰ \Rightarrow n|۲^{n!} - ۱$$

۲۶. (آ) فرض کنید باقی مانده عدد اول p بر ۴ برابر ۳ باشد. ثابت کنید اگر $p|x^۲ + y^۲$ آنگاه $p|x$ و $p|y$.

(ب) نشان دهید بی‌نهایت عدد اول p وجود دارد که برای هر عدد طبیعی زوج x، هیچ‌یک از جمله‌های دنباله‌ی

$$x^x + ۱, x^{x^x} + ۱, x^{x^{x^x}} + ۱, \dots$$

بر p قابل قسمت نیست.

حل.

(آ) فرض کنید $p \nmid x$ (فرض خلف). پس $p \nmid y$. دو طرف رابطه $x^۲ \overset{p}{\equiv} -y^۲$ را به توان $\frac{p-۱}{۲}$ می‌رسانیم که عددی فرد است. پس داریم $x^{p-۱} \overset{p}{\equiv} (-۱)^{\frac{p-۱}{۲}} y^{p-۱}$. پس با توجه به قضیه کوچک فرما خواهیم داشت:

$$۱ \overset{p}{\equiv} (-۱)^{\frac{p-۱}{۲}} = -۱$$

پس $p|۲$ که این تناقض است.

(ب) اگر p عددی اول به فرم $۴k + ۳$ باشد، با توجه به (الف) می‌دانیم معادله $x^۲ \overset{p}{\equiv} -۱$ به ازای هیچ x طبیعی دارای جواب نیست. از آنجا که x عددی زوج است، اگر یکی از جملات دنباله بالا بر x بخش‌پذیر باشد به ازای یک m طبیعی داریم: $x^{۲m} \overset{p}{\equiv} -۱$ و این یعنی $(x^m)^۲ \overset{p}{\equiv} -۱$. اما طبق (الف) اگر p به فرم $۴k + ۳$ باشد، چنین چیزی ممکن نیست.

۲۷. می‌دانیم عدد طبیعی n وجود دارد به طوری که $n^۵ = ۲۷^۵ + ۸۴^۵ + ۱۱۰^۵ + ۱۳۳^۵$. عدد n را بیابید.

حل. طبق قضیه کوچک فرما می‌دانیم $n^۵ \overset{۵}{\equiv} n$. پس خواهیم داشت:

$$۳ + ۰ + ۴ + ۷ \overset{۵}{\equiv} n$$
$$۴ \overset{۵}{\equiv} n$$

حال دو طرف معادله را به پیمانه ۳ بررسی می‌کنیم.

$$-۱ + ۱ + ۰ + ۰ \overset{۳}{\equiv} n$$
$$۰ \overset{۳}{\equiv} n$$

پس n بر ۳ بخش‌پذیر بوده و باقی مانده آن بر ۵ برابر ۴ است. واضحا n از ۱۳۳ بزرگتر است. دو گزینه ممکن برای آن ۱۴۴ و ۱۷۴ است. با توجه به اینکه مقدار ۱۷۴ برای برقراری معادله خیلی بزرگ است، تنها گزینه باقی‌مانده ۱۴۴ است.

▷

۲۸. عدد صحیح $n > ۱$ را در نظر بگیرید. نشان دهید اگر به ازای هر n $۱ < a < n$ رابطه $a^{n-۱} \overset{n}{\equiv} ۱$ برقرار باشد آنگاه n عددی اول است. (راهنمایی: نشان دهید اگر رابطه $a^{n-۱} \overset{n}{\equiv} ۱$ برقرار باشد، آنگاه $(a, n) = ۱$.)

حل. فرض کنید $a^{n-۱} \overset{n}{\equiv} ۱$. در اینصورت:

$$\exists k : a^{n-۱} - ۱ = nk \Rightarrow a^{n-۱} - nk = ۱$$

فرض کنید $(a, n) = d$. اگر $a = db$ و $n = dm$ ، داریم:

$$(db)^{n-۱} - dmk = ۱ \Rightarrow d \times (d^{n-۲}b^{n-۱} - mk) = ۱$$

با توجه به اینکه حاصل‌ضرب d در یک عدد صحیح برابر ۱ شده است، در نتیجه d می‌تواند فقط ۱ باشد.

$\triangleright$