حدس کارتان[۱]

سینا رضازاده بقال

در این مقاله اثبات Mihailecu Preda را برای حدس کارتان بررسی می‌کنیم.

حدس کارتان: تنها دو عدد متوالی کامل ۸ و ۹ هستند. به بیانی دیگر در دنباله‌ی زیر تنها دو عدد ۸ و ۹ متوالی هستند.

$$۱, ۴, ۸, ۹, ۱۶, ۲۵, ۲۷, ۳۲, ۳۶, \ldots$$

البته توجه کنید، برای هر $k \geq ۲$ ثابت، اعداد توان kام کامل به اندازه‌ی کافی از یکدیگر فاصله دارند. بنابراین باید نشان دهیم که معادله‌ی $x^n - y^m = ۱$ که $n, m \geq ۲$، $x, y \in \mathbb{Z}$ تنها دارای جواب $n = ۲, m = ۳$ و $x = ۳, y = ۲$ است.

بدون کاسته شدن از کلیت می‌توان فرض کرد که n, m اعداد اول هستند، زیرا که اگر $p \mid m$ و $q \mid n$ در این صورت:

$$x^n - y^m = ۱ \Rightarrow (x^{\frac{n}{q}})^q - (y^{\frac{m}{p}})^p = ۱$$

پس صورت نهایی حدس کارتان به صورت زیر است.

حدس کارتان: معادله‌ی $x^p - y^q = ۱$ که p, q اعدادی اول هستند، دارای جواب یکتای $(x, y, p, q) = (۳, ۲, ۲, ۳)$ است.

$p = ۲$ و $q = ۲$ را هر کدام به صورت جداگانه اثبات می‌کنیم. اما اثبات برای حالتی که p و q اعداد اول فرد هستند را در مقاله‌های بعدی می‌آوریم. البته برای اثبات این حالت ابتدا سه قضیه زیر را ثابت می‌کنیم.

قضیه ۱. *اگر $x^p - y^q = ۱$ جواب نابدیهی داشته باشد و p و q فرد باشند، آنگاه:*

$$p^{q-۱} \equiv ۱ \mod q^۲, q^{p-۱} \equiv ۱ \mod p^۲$$

قضیه ۲. *اگر $x^p - y^q = ۱$ جواب نابدیهی داشته باشد و p, q فرد باشند آنگاه:*

$$p \equiv ۱ \mod q \quad \text{یا} \quad q \equiv ۱ \mod p$$

قضیه ۳. *اگر $x^p - y^q = ۱$ جواب نابدیهی داشته باشد و p, q فرد باشند آنگاه:*

$$p < ۴q^۲, q < ۴p^۲$$

حال نشان می‌دهیم که این سه قضیه چگونه حدس کارتان را در حالت p, q فرد نتیجه می‌دهد.

طبق قضیه‌ی ۲، $p \equiv ۱ \mod q$ یا $q \equiv ۱ \mod p$. اما اگر (x, y, p, q) جواب مساله باشد، در این صورت $(-y, -x, q, p)$ نیز در معادله صدق می‌کند. پس بدون کاسته شدن از کلیت می‌توان فرض کرد $p \equiv ۱ \mod q$. اگر $p = qt + ۱$ آنگاه:

$$p^{q-۱} = (qt + ۱)^{q-۱} \equiv (q - ۱)qt + ۱ \equiv ۱ \mod q^۲ \Rightarrow q \mid t \Rightarrow p \equiv ۱ \mod q^۲$$

اما طبق قضیه ۳، $p < ۴q^۲$، پس $p \in \{q^۲ + ۱, ۲q^۲ + ۱, ۳q^۲ + ۱\}$. اگر $q \neq ۳$ آنگاه $۳ \mid ۲q^۲ + ۱$ و $q^۲ + ۱, ۳q^۲ + ۱$ هم زوج هستند. پس $q = ۳$ و $p = ۱۹$. اما در این حال $۳^{۱۸}$ به پیمانه‌ی $۱۹^۲$ با ۱ همنهشت نیست و طبق قضیه ۱ حکم نتیجه می‌شود.

اکنون مساله را برای $q = ۲$ ثابت می‌کنیم.

---

[۱] Conjecture Cartan

قضیه ۴. ($V.A.Lebesgue - ۱۸۵۰$) *برای هر عدد اول $p \geq ۲$، معادله‌ی $x^p = y^۲ + ۱$ جواب صحیح نابدیهی ندارد.*

اثبات. اگر $p = ۲$ که به وضوح حکم برقرار است. اما اگر p فرد باشد در این صورت چون که $x^p = (۱ + iy)(۱ - iy)$ و چون تمام یکال‌های $\mathbb{Z}[i]$ توان pام هستند، نتیجه می‌شود که $۱ + iy$ و $۱ - iy$ هر دو توان pام کامل در $\mathbb{Z}[i]$ هستند. بنابراین $c \in \mathbb{Z}[i]$ وجود دارد که $۱ + iy = c^p, ۱ - iy = \bar{c}^p$. در نتیجه:

$$۲ = (c + \bar{c})(c^{p-۱} - \cdots + \bar{c}^{p-۱}) \Rightarrow c + \bar{c} \mid ۲$$

و چون $c + \bar{c}$ صحیح است پس $c + \bar{c} = \pm ۲$ و لذا $c = \pm(۱ + bi)$ که $b \in \mathbb{Z}$. از طرفی $c \nmid ۱ + i$. چون اگر $c \mid ۱ + i$ آن‌گاه $۱ + i \mid ۱ + iy$ و لذا y فرد خواهد بود. پس x زوج است و چون $p \geq ۳$ پس $۸ \mid y^۲ + ۱$ که غیرممکن است. پس $c \nmid ۱ + i$ ولذا b نیز زوج است. داریم

$$(۱ + bi)^p + (۱ - bi)^p = \pm ۲ \Rightarrow \binom{p}{۲}(bi)^۲ + \cdots + \binom{p}{p-۱}(bi)^{p-۱} = ۰$$

اما توجه کنید که:

$$Ord_۲(\binom{p}{k}(bi)^k) > Ord_۲(\binom{p}{۲}(bi)^۲)$$

چون که:

$$\binom{p}{k}(bi)^k \binom{p}{۲}^{-۱}(bi)^{-۲} = \binom{p-۲}{k-۲} . \frac{۲}{k(k-۱)}(bi)^{k-۲}$$

اما k زوج است و در نتیجه:

$$Ord_۲(۲(bi)^{k-۲}) \geq k - ۱ > \frac{\log k}{\log ۲} \geq Ord_۲(k) = Ord_۲(k(k-۱))$$

پس

$$Ord_۲(\binom{p}{k}(bi)^k) > Ord_۲(\binom{p}{۲}(bi)^۲)$$

برای هر $k > ۲$ و زوج. اکنون به لم زیر توجه کنید.

لم ۵. *اگر $Ord_p(x_۱) < Ord_p(x_i)$ برای $n \geq i \geq ۲$ که $x_i \in \mathbb{Q}_p$، در این صورت:*

$$Ord_p(\sum x_i) = Ord_p(x_۱)$$

که p عدد اول دلخواه است.

پس داریم:

$$Ord_۲(\sum_{k=۱}^{\frac{p-۱}{۲}} \binom{p}{۲k}(bi)^{۲k}) = Ord_۲(\binom{p}{۲}(bi)^۲)$$

اما $Ord_۲(۰) = +\infty$ و لذا بایستی داشته باشیم $b = ۰$ و لذا $c = \pm ۱$ و $y = ۰$. □

اکنون حدس را برای حالت $p = ۲$ نشان می‌دهیم.

قضیه ۶. *معادله‌ی*

$$x^۲ = y^q + ۱ \qquad (۱)$$

در مجموعه‌ی اعداد صحیح دارای تنها جواب نابدیهی $x = ۳, y = ۲, q = ۳$ است.

برای اثبات قضیه، ابتدا لم‌های زیر را ثابت می‌کنیم.

لم ۷. *اگر $q \geq ۳$، عددی فرد باشد و در معادله‌ی (۱) صدق کند، در این صورت x یا $-x$ در معادله‌های زیر صدق می‌کند:*

(i) $a,b\in\mathbb{Z}$ با $(2a,b)=1$ *وجود دارند که:*

$$x-1=2^{q-1}a^q,\ x+1=2b^q,\ y=2ab$$

(ii) $y\geq 2^{q-1}-2$

اثبات. i) $(x-1)(x+1)=y^q$. اگر x زوج باشد آن‌گاه $(x-1,x+1)=1$ و چون هر دو توان qام کامل هستند و اختلاف ۲ دارند پس بایستی ±1 باشند ولذا $x=0$.

پس x فرد است و لذا $2^q \mid (x-1)(x+1)$، با تغییر علامت x می‌توان فرض کرد که $x\equiv 1 \mod 4$.

$$\left(\frac{x-1}{2^{q-1}}\right)\left(\frac{x+1}{2}\right)=\left(\frac{y}{2}\right)^q$$

ولی $(\frac{x-1}{2^q},\frac{x+1}{2})=1$، پس:

$$\frac{x-1}{2^{q-1}}=a^q,\ \frac{x+1}{2}=b^q$$

پس قسمت اول ثابت شد.

حال برای (ii) داریم:

$$2^{q-1}\mid x-1\Rightarrow 2b^q\equiv 2 \mod 2^{q-1}\Rightarrow b^q\equiv 1 \mod 2^{q-2}$$

اما $Ord(b)$ در $\mathbb{Z}^*_{2^{q-2}}$ توانی از ۲ است زیرا که $|\mathbb{Z}^*_{2^{q-2}}|$ توان ۲ است. پس از رابطه‌ی بالا نتیجه می‌شود که $b\equiv 1 \mod 2^{q-2}$. لذا:

$$|b|\geq 2^{q-2}-1\Rightarrow |2ab|\geq 2^{q-1}-2$$

پس این لم نیز ثابت می‌شود. $\square$

لم ۸. *فرض کنید* $q\geq 3$ *عددی اول و* $x^2-y^q=1$. *در این صورت* $q\mid x$.

اثبات. داریم $x^2=(y+1)(\frac{y^q+1}{y+1})$. اگر $d=\gcd(y+q,\frac{y^q+1}{y+1})$، آن‌گاه:

$$\frac{y^q+1}{y+1}=y^{q-1}-y^{q-2}+\cdots-1\equiv -q \mod d\Rightarrow d\mid q$$

اگر $q\nmid x$ آن‌گاه $(d,q)=1$ پس $d=1$. بنابراین $y+1$ و $\frac{y^q+1}{y+1}$ هردو مربع کامل هستند. و مثلا $u^2=y+1$ و $v^2=\frac{y^q+1}{y+1}$.

حال $(x,y^{\frac{q-1}{2}})$ جوابی برای $x^2-Yy^2=1$ است. چون $u^2=y+1$ پس y مربع کامل نیست. و لذا در $\mathbb{Z}[\sqrt{y}]$، $x+y^{\frac{q-1}{2}}\sqrt{y}$ یکال است. حال به لم زیر توجه کنید:

لم ۹. *گروه یکال‌های* $\mathbb{Z}[\sqrt{y}]$ *در حالتی که* $y+1=u^2$ *توسط* $u+\sqrt{y}$ *تولید می‌شوند.*

برهان لم: اگر $a+b\sqrt{y}$ در $\mathbb{Z}[\sqrt{y}]$ یکال باشد، در این صورت $k\in\mathbb{Z}$ را به گونه‌ای انتخاب می‌کنیم که:

$$1\leq (a+b\sqrt{y})(u+\sqrt{y})^k<u+\sqrt{y}$$

پس از ابتدا بدون کاسته شدن از کلیت فرض کنید $1\leq a+b\sqrt{y}<u+\sqrt{y}$.

چون $a+b\sqrt{y}$ یکال است پس $a^2-b^2y=\pm1$. به راحتی می‌توان بررسی کرد برای $a\neq 1$ رابطه‌ی

$$1\leq a+b\sqrt{y}<u+\sqrt{y}$$

نمی‌تواند برقرار باشد. پس $a=1, b=0$ و لذا برای هر یکال مانند $a+b\sqrt{y}$ در $\mathbb{Z}[\sqrt{y}]$ توان $k\in\mathbb{Z}$ وجود دارد که $(u+\sqrt{y})^k=a+b\sqrt{y}$.

پس، $m\in\mathbb{Z}$ وجود دارد که $x+y^{\frac{q-1}{2}}\sqrt{y}=(u+\sqrt{y})^m$. از آن‌جا که $(u+\sqrt{y})^{-1}=-(-u+\sqrt{y})$ بنابراین:

$$x\equiv\pm(u^m+umm^{m-1}\sqrt{y}) \mod y\mathbb{Z}[\sqrt{y}]$$

پس $x\pm u^m\equiv mu^{m-1}\sqrt{y}$ به پیمانه‌ی $y\mathbb{Z}[\sqrt{y}]$ و در نتیجه $mu^{m-1}\equiv 0 \mod y$ ولی $(y,u)=1$ و لذا $y\mid m$. اما y زوج است و لذا m نیز زوج است. داریم:

$$x+y^{\frac{q-1}{2}}\sqrt{y}=\pm(u^2+y+2u\sqrt{y})^{\frac{m}{2}}$$

اگر دو طرف معادله را به پیمانه $u\mathbb{Z}[\sqrt{y}]$ در نظر بگیریم، بدست می‌آید:

$$x + y^{\frac{q-1}{2}}\sqrt{y} \equiv \pm y^{\frac{m}{2}} \mod u\mathbb{Z}[\sqrt{y}]$$
$$\Rightarrow u \mid x + y^{\frac{q-1}{2}}\sqrt{y} \pm y^{\frac{m}{2}}$$
$$\Rightarrow u \mid y^{\frac{q-1}{2}}$$

اما $(y,u) = 1$ پس $u = 1$ و $y = 0$. تناقض حاصل نشان می‌دهد که فرض خلف باطل است و $q \mid x$. □

اکنون با توجه به لم زیر حکم به راحتی نتیجه می‌شود.

لم ۱۰. *اگر* $q \geq 3$ *و* $x^2 - y^q = 1$ *در این صورت* $x \equiv \pm 3 \mod q$.

اثبات. می‌دانیم که $x - 1 = 2^{q-1}a^q$ و $x + 1 = 2b^q$ برای $a, b \in \mathbb{Z}$ که $(2a, b) = 1$. داریم:

$$b^{2q} - (2a)^q = (\frac{x+1}{2})^2 - 2(x-1) = (\frac{x-3}{2})^2$$
$$\Rightarrow (b^2 - 2a)(\frac{b^{2q} - (2a)^q}{b^2 - 2a}) = (\frac{x-3}{2})^2$$

حال اگر $\gcd(b^2 - 2a, \frac{b^{2q}-(2a)^q}{b^2-2a}) = 1$ آن‌گاه، $b^2 \geq 2a$. زیرا که اگر $b^2 < 2a$ آن‌گاه سمت چپ عبارت بالا منفی خواهد شد. پس $b^2 - 2a = c^2$. داریم:

$$\mid 2a \mid = \mid c^2 - b^2 \mid \geq 2 \mid b \mid -1 \Rightarrow \mid a \mid \geq \mid b \mid$$

از طرفی دیگر:

$$\mid a \mid^q = \frac{\mid x-1 \mid}{2^{q-1}} \leq \frac{\mid x-1 \mid}{16} < \frac{\mid x+1 \mid}{2} = \mid b \mid^q \Rightarrow \mid a \mid < \mid b \mid$$

توجه کنید که برای $q = 3$ حکم از لم قبل نتیجه می‌شود، پس فرض کردیم $q \geq 5$.

تناقض حاصل نشان می‌دهد که $\gcd(b^2 - 2a, \frac{b^{2q}-(2a)^q}{b^2-2a}) = 1$ برقرار نیست، اما می‌دانیم که اگر $(x,y) = 1$ آنگاه $\gcd(x-y, \frac{x^q-y^q}{x-y}) \mid q$. زیرا که اگر $d = \gcd(b^2 - 2a, \frac{b^{2q}-(2a)^q}{b^2-2a})$ آن‌گاه:

$$d \mid x^{q-1} + x^{q-2}y + \cdots + y^{q-1} \Rightarrow qx \equiv 0 \mod d$$

اما $(d,x) = 1$، پس $q \mid d$. بنابراین $q \mid (\frac{x-3}{2})^2$ و لذا $x \equiv 3$ به پیمانه q. اما بایستی $-x$ را هم در نظر بگیریم، چون x را به گونه‌ای انتخاب کرده بودیم که $x \equiv 1 \mod 4$ پس در حالت کلی $x \equiv \pm 3 \mod q$. □

پس کافی است حالت $x^2 - y^3 = 1$ را حل کنیم که آن را در مقاله‌ی بعد بررسی می‌کنیم.