سه آزمون اول بودن با پیچیدگی زمانی چندجمله‌ای

سهیل معماریان

۱ مقدمه

تشخیص اول یا مرکب بودن یک عدد داده شده از بنیادی‌ترین مسائل نظریه اعداد الگوریتمی است که پژوهش در این رابطه تاکنون ادامه دارد. AKS اولین الگوریتم قطعی با پیچیدگی زمانی چندجمله‌ای برای این مقصود بود که در سال ۲۰۰۲ طراحی شد. این الگوریتم به عنوان یکی از مهم‌ترین دستاوردهای ۲۰ سال اخیر در مواجهه با این سوال محسوب می‌شود که علاوه بر نتایج درخشان آن، زیبایی و ظرافت اثبات‌هایی که در آن به کار گرفته شده نیز قابل توجه است.

در این مقاله که بر اساس [۲] نوشته شده است، با رهیافت نظری به بررسی آزمون AKS و دو آزمون اول بودن تصادفی (سولوی–استرسن و میلر–رابین) پرداخته می‌شود به گونه‌ای که جز آشنایی با جبر و نظریه اعداد مقدماتی پیشنیاز دیگری فرض نشده است.

۲ قضیه‌ی کوچک فرما

در این بخش قضیه‌ی کوچک فرما و صورت‌های معادل آن را بیان می‌کنیم که در آزمون‌های اول بودن به‌کار می‌روند. این قضیه اولین بار توسط پیر دو فرما[1] در قرن هفدهم میلادی مطرح شد.

قضیه ۱. (*قضیه‌ی کوچک فرما*) *برای هر عدد اول p و هر عدد طبیعی a که $0 < a < p$ داریم:*

$$a^{p-1} \overset{p}{\equiv} 1.$$

اثبات ۱. چون $\mathbb{Z}_p^*$ یک گروه متناهی است، برای هر $a \in \mathbb{Z}_p^*$ داریم $\mathbb{Z}_p^* = a\mathbb{Z}_p^*$ ؛ در نتیجه حاصل‌ضرب اعضای آن‌ها نیز برابر است:

$$\prod_{b\in\mathbb{Z}_p^*} b \overset{p}{\equiv} \prod_{b\in\mathbb{Z}_p^*} ab \overset{p}{\equiv} a^{p-1} \prod_{b\in\mathbb{Z}_p^*} b \Rightarrow a^{p-1} \overset{p}{\equiv} 1.$$

لم ۱. *برای عدد صحیح a و عدد اول p اگر $a^2 \overset{p}{\equiv} 1$ آنگاه $a \overset{p}{\equiv} \pm 1$.*

اثبات ۲.

$$a^2 \overset{p}{\equiv} 1 \Rightarrow p|a^2-1 \Rightarrow p|(a-1)(a+1)$$

چون p اول است پس $p|(a-1)$ یا $p|(a+1)$.

قضیه ۲. *برای هر عدد اول فرد p و هر عدد طبیعی a که $0 < a < p$ داریم:*

$$a^{\frac{p-1}{2}} \overset{p}{\equiv} \pm 1$$

اثبات ۳. طبق قضیه ۱ داریم $a^{p-1} \overset{p}{\equiv} 1$. چون $p-1$ زوج است پس لم ۱ حکم را نتیجه می‌دهد.

قضیه ۳. *برای عدد اول فرد p که $p-1 = 2^s t$ و t عدد طبیعی فرد باشد و عدد طبیعی a که $0 < a < p$، دنباله ی*

$$a^t (mod\ p), a^{2t} (mod\ p), a^{2^2 t} (mod\ p), ..., a^{2^s t} (mod\ p)$$

[1] Pierre de Fermat

یا تماماً ۱ است یا زوجِ ۱ـ و ۱ در جایی از دنباله ظاهر می‌شود و بعد آن تماماً ۱ است.

اثبات ۴. طبق قضیه ۱ آخرین عضو دنباله ۱ است. اگر تمام اعضای دنباله ۱ باشد که حکم ثابت می‌شود در غیر این صورت آخرین جایی را در نظر بگیرید که ۱ نیست و آنرا با a نشان می‌دهیم. چون هر عضو توان دوم عنصر قبلی است پس $a^2 \stackrel{p}{\equiv} 1$. بنابر لم ۱ باید $a \stackrel{p}{\equiv} -1$.

لم ۲. *عدد طبیعی n، عدد اول است اگر و فقط اگر برای هر $0 < i < n$ داشته باشیم $n|\binom{n}{i}$.*

اثبات ۵. می‌دانیم $\binom{n}{i} = \frac{n!}{(n-i)!i!}$. حال در صورت یک عامل n وجود دارد. اگر n عدد اول باشد آنگاه هیچ عاملی کوچکتر از خودش ندارد؛ لذا در مخرج هیچ عاملی از n وجود ندارد و یک طرف حکم ثابت می شود.

اگر n عدد مرکب باشد، عامل اولی مانند q دارد. k را عدد طبیعی تعریف می‌کنیم که $q^k|n$ و $q^{k+1} \nmid n$. $q^k \nmid \binom{n}{q}$ چون $\binom{n}{q} = \frac{n(n-1)...(n-q+1)}{q(q-1)...(1)}$ و تعداد عامل q در صورت برابر k و در مخرج برابر 1 است.

قضیه ۴. *عدد طبیعی n، عدد اول است اگر و فقط اگر برای هر a که $0 < a < n$ داشته باشیم:*

$$(x+a)^n \stackrel{n}{\equiv} x^n + a$$

(در اینجا منظور از همنهشت بودن دو چندجمله‌ای، همنهشت بودن ضرایب آن‌هاست.)

اثبات ۶. از اتحاد نیوتن می‌دانیم:

$$(x+a)^n - x^n - a = \sum_{i=1}^{n-1} \binom{n}{i} x^i a^{n-i} + a^n - a.$$

اگر n عدد اول باشد، طبق لم۲ ، $(x+a)^n \stackrel{n}{\equiv} x^n + a^n$. همچنین طبق قضیه ۱، $a^n \stackrel{n}{\equiv} a$. پس یک طرف حکم ثابت شد.

اگر n عدد اول نباشد، $n \nmid \binom{n}{i}$. اگر a را چنان انتخاب کنیم که $(n, a^{n-i}) = 1$ آنگاه ضریب جمله ی x^i در پیمانه ی n ناصفر می‌شود.

۳ آزمون سولوی‌ـاسترسن

آزمون سولوی‌ـاسترسن[2] اولین الگوریتم کارآمدی بود که برای آزمون اول بودن مطرح شد. ایده‌ی اصلی آن استفاده از قضیه‌ی ۲ و قضیه۷ است.

قضیه ۵. (*محک اویلر*[3]) *اگر p عدد اول فرد باشد آنگاه برای هر عدد طبیعی m داریم:*

$$(\frac{m}{p}) \stackrel{p}{\equiv} m^{\frac{p-1}{2}}.$$

اثبات ۷. اگر m بر p بخش‌پذیر باشد، هر دو طرف تساوی برابر صفر است. اگر $(p, m) = 1$ و g مولد گروه $\mathbb{Z}_p^*$ باشد، آنگاه عدد طبیعی i وجود دارد که $g^i \stackrel{p}{\equiv} m$.

اگر m مانده‌ی مربعی باشد، i زوج و طرف چپ تساوی برابر ۱ است. طبق قضیه‌ی ۱ داریم:

$$m^{\frac{p-1}{2}} \stackrel{p}{\equiv} g^{j\frac{p-1}{2}} \stackrel{p}{\equiv} 1 = (\frac{m}{p}).$$

اگر m نامانده‌ی مربعی باشد، i فرد و طرف چپ تساوی برابر ۱ـ است. طبق قضیه‌ی ۲ داریم $m^{\frac{p-1}{2}} \stackrel{p}{\equiv} \pm 1$. کافی است ثابت کنیم ۱ امکان‌پذیر نیست. چون g مولد است مرتبه‌ی آن $p-1$ است. اگر $1 \stackrel{p}{\equiv} m^{\frac{p-1}{2}} \stackrel{p}{\equiv} g^{j\frac{p-1}{2}}$، این نتیجه می‌دهد $p-1|j\frac{p-1}{2}$ که این با فرد بودن j در تناقض است.

تعریف ۱. (نماد ژاکوبی[4]) برای اعداد طبیعی m و n که تجزیه استاندارد n به صورت $n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$ باشد، نماد ژاکوبی به صورت زیر تعریف می‌شود که منظور از $(\frac{m}{p_i})$ نماد لژاندار[5]است.

$$(\frac{m}{n}) = \prod_{i=1}^{r} (\frac{m}{p_i})^{\alpha_i}$$

ملاحظه ۱. از تعریف به سادگی بدست می‌آید $(\frac{a}{n}) = (\frac{a+n}{n})$.

[2] Solovay-Strassen
[3] Euler
[4] Jacobi
[5] Legendre

قضیه ۶. *(قانون تقابل مربعی برای نماد ژاکوبی) برای اعداد فرد* n, m *که* $(n, m) = 1$*، داریم:*

$$(\frac{n}{m})(\frac{m}{n}) = (-1)^{\frac{(n-1)(m-1)}{4}}$$

اثبات آن را می‌توان در [۳] دید. توجه کنید که برای عدد مرکب n، لزومی ندارد که $(\frac{a}{n}) \overset{n}{\equiv} a^{\frac{n-1}{2}}$.

با استفاده از قضیه‌ی ۶ و ملاحظه‌ی ۱، با تقسیمات متوالی می‌توانیم الگوریتمی از مرتبه‌ی $O((log\ n)^2)$ برای محاسبه‌ی $(\frac{a}{n})$ بیان کنیم.

قضیه ۷. *n را عدد فردی در نظر بگیرید که توان کامل عدد اولی نباشد. عدد تصادفی a که $0 < a < n$، یا $(a, n) > 1$ یا با احتمال حداقل $\frac{1}{2}$ داریم:*

$$(\frac{a}{n}) \overset{n}{\not\equiv} a^{\frac{n-1}{2}}.$$

اثبات ۸. چون n مربع کامل نیست پس می‌توان نوشت $n = p^k m$ که p عدد اول و k عدد فرد باشد و نیز $(p, m) = 1$. حال تعریف می کنیم:

$$A = \{0 < a < p^k | (a, p) = 1\}.$$

به وضوح $|A| = p^{k-1}(p-1)$ و دقیقاً $\frac{p^k(p-1)}{2}$ تااز اعضای A مانده‌ی مربعی و دقیقاً $\frac{p^k(p-1)}{2}$ تااز اعضای A نامانده‌ی مربعی هستند. اگر a_0،b_0 به ترتیب مانده‌ی مربعی و نامانده‌ی مربعی به پیمانه p در A باشند، عدد دلخواه c را که $0 < c < m$ و $(c, m) = 1$ را نیز در نظر بگیرید. با توجه به قضیه باقی‌مانده‌ی چینی، اعداد طبیعی یکتایی $0 < a, b < n$ وجود دارند که $a_0 \overset{p^k}{\equiv} a,\ b_0 \overset{p^k}{\equiv} b$ و $a \overset{m}{\equiv} b \overset{m}{\equiv} c$. حال داریم:

$$(\frac{a}{n}) = (\frac{a_0}{p})^k (\frac{c}{m}) = (\frac{c}{m})(*)$$

$$(\frac{b}{n}) = (\frac{b_0}{p})^k (\frac{c}{m}) = -(\frac{c}{m})(**)$$

اگر $(\frac{a}{n}) \overset{n}{\equiv} a^{\frac{n-1}{2}}$ و نیز $(\frac{b}{n}) \overset{n}{\equiv} b^{\frac{n-1}{2}}$ از $(*)$ و $(**)$ نتیجه می‌شود $a^{\frac{n-1}{2}} \overset{n}{\equiv} -b^{\frac{n-1}{2}}$. لذا خواهیم داشت:

$$c^{\frac{n-1}{2}} \overset{m}{\equiv} a^{\frac{n-1}{2}} \overset{m}{\equiv} -b^{\frac{n-1}{2}} \overset{m}{\equiv} -c^{\frac{n-1}{2}}$$

اما این امکان ندارد چون $(c, m) = 1$. پس یا $(\frac{a}{n}) \overset{n}{\not\equiv} a^{\frac{n-1}{2}}$ یا $(\frac{b}{n}) \overset{n}{\not\equiv} b^{\frac{n-1}{2}}$. چون تعداد مانده‌های مربعی با تعداد نامانده‌های مربعی برابر بود پس برای عدد تصادفی a که $0 < a < n$ و $(a, n) = 1$ با احتمال حداقل $\frac{1}{2}$،

$$(\frac{a}{n}) \overset{n}{\not\equiv} a^{\frac{n-1}{2}}.$$

در هر سه آزمون اول بودنی که در این مقاله بررسی شده است ابتدا باید مطمئن باشیم که عدد داده شده توان کامل نیست. اما الگوریتم چک کردن این فرض دشوار نیست و به طور دقیق‌تر خواننده می‌تواند برای دیدن این الگوریتم به [۴] مراجعه کند. همچنین توجه کنید اگر صرفاً دنبال الگوریتم تصادفی برای آزمون اول بودن باشیم، اعدادی که به صورت توان کامل باشند برایمان مشکل‌ساز نخواهند بود زیرا ایناعداد در اعداد طبیعی چگالی صفر دارند و جمع معکوساتشان ۲ است:

$$\sum_{n=1}^{\infty}\sum_{k=2}^{\infty}\frac{1}{n^k} = 1 + \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 2$$

بنابر قضیه ۷ و قضیه ۲ می‌توان الگوریتم سولوی‌ـ استرسن برای آزمون اول بودن را مطرح کرد. این الگوریتم در صورتی که فقط یکبار اجرا شود به احتمال حداقل $\frac{1}{2}$ به جواب درست خواهد رسید. تعداد محاسبات مورد نیاز این الگوریتم، $O((log\ n)^3)$ است.

الگوریتم ۱. *(آزمون اول بودن سولوی‌ـ استرسن)*

input: n

output: prime or composite

if $\exists\, m,\ k \in \mathbb{N};\ n = m^k\ ,\ k > 1$

return composite

End if

if $(\frac{a}{n}) = a^{\frac{n-1}{2}} (mod\ n)$

return prime

End if

return composite

۴ آزمون میلر ـ رابین

مایکل رابین[6] در [۶] با انجام تغیراتی در آزمون میلر[7] این الگوریتم را طراحی نمود. میلر با فرض درستی حدس ریمان تعمیم یافته[8] ثابت کرد برای عدد مرکب n که بیش از یک عامل اول داشته باشد، قضیه ۳ حداقل برای یک a که $0 < a < (log\ n)^2$ برقرار نیست. همچنین میلر ثابت کرد بدون پذیرفتن هیچ فرضی برای a تصادفی با احتمال بالایی قضیه‌ی ۳ برقرار نیست.

قضیه ۸. *اگر n عدد مرکبی باشد که بیش از یک عامل اول دارد و $n-1 = 2^s t$، با احتمال حداقل $\frac{1}{2}$، دنباله‌ی*

$$a^t(mod\ n), a^{2t}(mod\ n), a^{2^2 t}(mod\ n), ..., a^{2^s t}(mod\ n)$$

هیچ یک از این دو خاصیت را ندارد:

- *تماماً ۱ است.*
- *زوجِ ۱ـ و ۱ در جایی از دنباله ظاهر می‌شود و بعد آن تماماً ۱ است.*

اثبات ۹. p و q را دو عامل اول فرد n و k را بزرگترین توانی از p در نظر بگیرید که n را عاد می کند همچنین vوw اعداد طبیعی باشند که $p-1 = 2^v w$ و $(w,2) = 1$. ابتدا حالتی را بررسی می‌کنیم که حداقل یک ۱ـ در دنباله وجود داشته باشد. مجموعه A_u را برای $0 \le u < s$ به صورت زیر تعریف می‌کنیم:

$$A_u = \{a | (0 < a < n) \wedge (a^{2^u t} \overset{p^k}{\equiv} -1)\}.$$

پس برای هر $a \in A_u$ داریم $a^{2^u t} \overset{p^k}{\equiv} -1$. مجموعه $A_{p,u}$ را به صورت زیر تعریف می‌کنیم:

$$A_{p,u} = \{a\ (mod\ p^k) | a \in A_u\}.$$

چون تعداد اعضای گروه حاصل‌ضرب به پیمانه p^k، برابر $p^{k-1}(p-1)$ است برای هر $a \in A_{p,u}$ داریم $a^{p^{k-1}(p-1)} \overset{p^k}{\equiv} 1$. بنابراین $a^{(p^{k-1}(p-1), 2^{u+1}t)} \overset{p^k}{\equiv} 1$. p ، t را عاد نمی‌کند چون در غیر این صورت باید $n-1$ را عاد کند که امکان ندارد. لذا داریم $a^{(p-1, 2^{u+1}t)} \overset{p^k}{\equiv} 1$. چون t فرد است و $p-1 = 2^v w$ پس $a^{2^{min\{u+1,v\}}(w,t)} \overset{p^k}{\equiv} 1$. اگر $v \le u$ آنگاه خواهیم داشت $a^{2^u t} \overset{p^k}{\equiv} 1$ که امکان ندارد. پس $v > u$ که دو نتیجه در بردارد:
اولاً $a^{2^u (w,t)} \overset{p^k}{\equiv} -1$؛ چراکه باید $a^{2^{u+1}(w,t)} \overset{p^k}{\equiv} 1$ (به لم ۱ توجه کنید.) و می‌دانستیم $a^{2^u t} \overset{p^k}{\equiv} -1$.
ثانیاً $2^{2u-v}(w,t) \le p-1$؛ چراکه $2u \le 2v$ و $(w,t) \le w$ نتیجه می‌دهد $2^{2u-v}(w,t) \le 2^v w = p-1$.
از سوی دیگر برای $l | p-1$ معادله $x^l \overset{p^k}{\equiv} -1$ حداکثر l جواب دارد لذا با توجه به دو نتیجه بیان شده داریم:

$$|A_{p,u}| \le 2^u (w,t) \le \frac{p-1}{2^{u-v}}.$$

با تکرار همین استدال برای $q-1 = 2^{v'} w'$ که $(w',2) = 1$ می‌توانیم بدست‌آوریم $|A_{q,u}| \le \frac{q-1}{2^{u-v'}}$ که $u < v'$ و $A_{q,u}$ به طور مشابه تعریف می‌شود. فرض کنید n فقط دو عامل اول p, q را داشته باشد. تعریف می‌کنیم $v'' = min\{v, v'\}$. از قضیه‌ی باقیمانده چینی داریم:

$$|A_u| < |A_{p,u}||A_{q,u}| \le \frac{p-1}{2^{u-v}} \frac{q-1}{2^{u-v'}} \le \frac{pq-1}{2^{2u-2v''}} \le \frac{n-1}{4^{u-v''}}.$$

بوضوح در صورتی که تعداد عوامل اول u بیشتر باشد نیز همین استدلال کارا است لذا برای $u < v''$، $|A_u| \le \frac{n-1}{4^{u-v''}}$. بنابراین

$$\sum_{0 \le u < s} |A_u| \le \sum_{0 \le u < v''} \frac{n-1}{4^{u-v''}} = (\frac{1}{3} - \frac{1}{3 \times 4^{v''}}).(n-1).$$

با توجه به تعریف A_u، $\frac{\sum_{0 \le u < s} |A_u|}{n-1}$ برابر است با احتمال اینکه در این دنباله در جایی ۱ـ بیاید و بعد آن ۱ باشد. لذا احتمال وقوع این احتمال حداکثر $\frac{1}{3} - \frac{1}{3 \times 4^{v''}}$ است. برای حالت تماماً ۱ نیز استدلال مشابه نتیجه می‌دهد تعداد a هایی که در دنباله ظاهر می‌شوند حداکثر برابر $\frac{1}{4^{v''}}(n-1)$ است. پس احتمال اینکه دنباله تولید شده حداقل یکی از دو خاصیت را داشته باشد کمتر $\frac{1}{3} - \frac{1}{3 \times 4^{v''}} + \frac{1}{4^{v''}}$ است که چون v'' حداقل ۱ است (عوامل اول فرد در نظر گرفته شده بودند.) این احتمال کمتر از $\frac{1}{2}$ است.

[6] Micheal Rabin
[7] Miller
[8] Extended Riemann hypothesis

آزمون اول بودن میلر–رابین با توجه به قضیه ۳ و قضیه ۸ با هر بار اجرا شدن با احتمال حداقل $\frac{1}{2}$ اول بودن یک عدد داده شده را درست تشخیص می‌دهد. این آزمون یک الگوریتم تصادفی با $O((log\ n)^2)$ محاسبه است.

الگوریتم ۲. *(آزمون اول بودن میلر– رابین)*

input: n

output: prime or composite

if $\exists\, m,\ k \in \mathbb{N};\ n = m^k\ ,\ k > 1$

return composite

End if

$a \leftarrow \{1, 2, ..., n\}$

$t \leftarrow n$

$k \leftarrow 0$

while $(t, 2) > 1$

$k \leftarrow k + 1$

$t \leftarrow \frac{t}{2}$

End while

if $(a, n) > 1$

return composite

End if

if $a^t = 1(mod\ n)$

return prime

End if

for $i = 0 : k$

$A[i] \leftarrow a^{2^i t}(mod\ n)$

if $i > 0, A[i] = 1, A[i-1] \neq -1$

return composite

End if

End for

return prime

۵ آزمون AKS

در سال ۲۰۰۴ کایال[9]و ساکسنا [10]این الگوریتم را در پروژه‌ی کارشناسی خود تحت نظر آگراول[11]طراحی کردند. برخلاف دو آزمون سولوی–استرسن و میلر–رابین، الگوریتم AKS قطعی است.

با استفاده از قضیه ۴ می‌توان یک آزمون به این صورت طراحی کرد که برای تشخیص اینکه n عدد اول است یا نه، به ازای همه‌ی $0 < a < n$ ها قضیه ۴ را امتحان کند. مشکلی که این آزمون دارد برای محاسبه‌ی ضرایب $(x+a)^n$ (یعنی $\binom{n}{i}$) به $\Omega(n)$ محاسبه نیاز دارد. برای حل کردن این مشکل قضیه‌ی ۴ را به‌این‌صورت بیان می‌کنیم:

گزاره ۱. *عدد طبیعی n اول است اگر و فقط اگر برای هر عدد طبیعی r و عدد طبیعی $a < n$ رابطه‌ی زیر برقرار باشد:*

$$(x+a)^n \equiv x^n + a\ (mod\ n, x^r - 1)$$

در قضیه‌ی ۱۰ ثابت خواهیم کرد که اگر گزاره ۱ برای r که به اندازه‌ی کافی کوچک انتخاب شده و تعداد کمی از aها برقرار باشد، آنگاه n باید عدد اول یا توانی از یک عدد طبیعی باشد. از طرفی چون r به اندازه‌ی کافی کوچک است، محاسبه ضرایب آسان می‌شود.

قضیه ۹. *اگر کوچکترین مضرب مشترک را با lcm نشان دهیم برای $n \geq 7$ داریم:*

$$lcm(1, 2, ..., n) \geq 2^n.$$

برای اثبات این قضیه می‌توانید به [۵] مراجعه کنید.

لم ۳. *برای هر عدد طبیعی n، عدد طبیعی r وجود دارد که مرتبه n در پیمانه r بیشتر از $log(n)^2$ است و $r \leq max\{3, (log\ n)^5 + 1\}$.*

(منظور از $log\ n$ ، لگاریتم n در مبنای دو است)

اثبات ۱۰. برای $n = 2$ و $r = 3$ حکم برقرار است. برای $n > 2$ حکم را بررسی می‌کنیم. چون $n > 2$ باید $(log\ n)^5 + 1 \geq 8$.

[9] Kayal
[10] Saxena
[11] Agrawal

$r_1, r_2, ..., r_m$ را تمام اعداد کمتر از n در نظر بگیرید که یا مقسوم علیه n هستند یا مرتبه n در آن پیمانه کمتر از $(log\ n)^2$ است. پس برای $1 \leq i \leq m$ داریم:

$$r_i | n. \prod_{i=1}^{i \leq (log\ n)^2} (n^i - 1).$$

همچنین

$$n. \prod_{i=1}^{i \leq (log\ n)^2} (n^i - 1) < n.n^{\sum_{i=1}^{i=(log\ n)^2}} < n^{(log\ n)^4} \leq 2^{(log\ n)^5}.$$

از طرفی طبق قضیه ۹ بزرگترین مضرب مشترک $(log\ n)^5$ عدد طبیعی ابتدایی بزرگتر از $2^{(log\ n)^5}$ است. پس عدد طبیعی کمتر از $(log\ n)^5$ مانند k وجود دارد که $k \notin \{r_1, r_2, ..., r_m\}$. اگر $(k, n) = 1$ باید مرتبه‌ی n به پیمانه k بیشتر از $(log\ n)^2$ باشد در غیر این صورت چون $k \nmid n$ پس $\frac{k}{(k,n)} \notin \{r_1, r_2, ..., r_m\}$ و در نتیجه مرتبه‌ی n به پیمانه $\frac{k}{(k,n)}$ بیشتر از $(log\ n)^2$ است.

قضیه ۱۰. *مرتبه‌ی عدد طبیعی n به پیمانه عدد طبیعی r بزرگتر از $(log\ n)^2$ است.(طبق لم ۳ ، چنین r ای وجود دارد.) اگر برای هر $0 \leq a \leq \sqrt{r} log\ n$ رابطه‌ی*

$$(x + a)^n \overset{n}{\equiv} x^n + a$$

برقرار باشد، n فقط یک عامل اول دارد.

اثبات ۱۱. p را عامل اولی از n در نظر بگیرید. دو مجموعه‌ی AوB را به صورت زیر تعریف می‌کنیم.

$$A = \{m | (x+a)^m = x^m + a (mod\ p, x^r - 1), 0 < a < \sqrt{r} log\ n\}$$

$$B = \{g(x) | g(x)^m = g(x^m) (mod\ p, x^r - 1), m \in A\}$$

با توجه به فرض، $p, n \in A$ و برای $0 \leq a \leq \sqrt{r} log\ n$، $x + a \in B$. از تعریف AوB روشن است که هر دو مجموعه نسبت به ضرب بسته هستند. در نتیجه هر دو مجموعه نامتناهی هستند. همچنین چون $p, n \in A$، برای اعداد طبیعی i و j، $(\frac{n}{p})^i p^j \in A$. دو مجموعه متناهی A_0 و B_0 را به صورت زیر تعریف می‌کنیم و با پیدا کردن کران برای $|A_0|$و$|B_0|$ حکم را ثابت می‌کنیم. چندجمله‌ای $h(x)$ دایره‌بر مرتبه r در $\mathbb{F}_p$ به عوامل تجزیه‌ناپذیری تجزیه می‌شود. $h(x)$ را یکی از این عوامل و $F = \frac{\mathbb{F}_p[x]}{(h(x))}$ در نظر بگیرید.

$$A_0 := \{m (mod\ r) | m \in A\}$$

$$B_0 := \{g(x) (mod\ p, h(x)) | g(x) \in B\}$$

ابتدا ثابت می‌کنیم $(log\ n)^2 < |A_0| < r$. $(n, r) = 1$ (چون در غیر این صورت n در پیمانه rمرتبه نخواهد داشت.) پس اعضای A_0 زیرمجموعه‌ای از $\mathbb{Z}_r^*$ هستند، لذا $|A_0| \leq \phi(r) < r$. همچنین چون مرتبه‌ی n در مرتبه‌ی r بزرگتر از $(log\ n)^2$ است و A_0 تمام توان‌های n را شامل است؛ درنتیجه $|A_0| > (log\ n)^2$.

حال ثابت می‌کنیم $|B_0| \leq p^{r-1} \leq 2^{\sqrt{|A_0|} log\ n}$. چون اعضای B_0 چندجمله‌ایهای به پیمانه $h(x)$ هستند و درجه‌ی $h(x)$ کمتر از r است پس $|B_0| \leq p^{r-1}$.

برای اثبات کران پایین، ابتدا ثابت می‌کنیم دو چندجمله‌ای متمایز از درجه‌ی حداکثر $|A_0| - 1$ در B به دو چندجمله‌ای متمایز در B_0 نگاشته می‌شوند. فرض کنید چنین نباشد، پس $f(x), g(x) \in B$ وجود دارند که درجه‌ی آن‌ها کمتر از $|A_0|$ باشند و $f(x) = g(x) (mod\ p, h(x))$. این یعنی برای هر $m \in A_0$ داریم:

$$f(x^m) = f(x)^m = g(x)^m = g(x^m) (mod\ p, h(x)).$$

در نتیجه برای هر $m \in A_0$، x^m ریشه‌ی چندجمله‌ی $q(y) = f(y) - g(y)$ است. چون A_0 زیرمجموعه‌ای از $\mathbb{Z}_r^*$ بود، $(m, r) = 1$. پس هر چنین x^m ریشه‌ی rام واحد است. پس $q(y)$ حداقل $|A_0|$ ریشه در F دارد. اما از طرفی با توجه به درجه‌ی f و g، درجه‌ی q کمتر از $|A_0|$ است. این یعنی $f(x)$ و $g(x)$ دو چندجمله‌ای متحد روی B هستند.

تک‌جمله‌ای‌های $X, X+1, ..., X + \lfloor \sqrt{|r|}\ log\ n \rfloor$ در $F[X]$ متمایزند. حال هر جواب صحیح نامنفی از نامعادله‌ی $k_0 + k_1 + ... + k_{\lfloor \sqrt{|r|}\ log\ n \rfloor} \leq |A_0| - 1$ مانند $(k_0, k_1, ..., k_{\lfloor \sqrt{|r|}\ log\ n \rfloor})$ را متناظر کنید به چندجمله‌ی $(X)^{k_0} (X+1)^{k_1} ... (X + \lfloor \sqrt{|r|}\ log\ n \rfloor)^{k_{\lfloor \sqrt{|r|}\ log\ n \rfloor}}$. پس تعداد چندجمله‌ای‌های حداکثر از درجه $|A_0| - 1$ در $F[X]$ بیشتر از

$\binom{\lfloor\sqrt{r}\ log\ n\rfloor+|A_0|}{\lfloor\sqrt{r}\ log\ n\rfloor+1}$ است. باتوجه به کران پایینی که برای $|A_0|$ بدست آوردیم $|A_0| > \sqrt{|A_0|}log\ n$. لذا داریم:

$$\binom{\lfloor\sqrt{r}\ log\ n\rfloor+|A_0|}{\lfloor\sqrt{r}\ log\ n\rfloor+1} \geq \binom{\lfloor\sqrt{r}\ log\ n\rfloor+\sqrt{|A_0|}log\ n+1}{\lfloor\sqrt{r}\ log\ n\rfloor+1}$$
$$= \binom{\lfloor\sqrt{r}\ log\ n\rfloor+\sqrt{|A_0|}log\ n+1}{\sqrt{|A_0|}log\ n}$$

چون $r > |A_0|$ با جایگذاری در نامساوی بالا داریم:

$$\binom{\lfloor\sqrt{r}\ log\ n\rfloor+|A_0|}{\lfloor\sqrt{r}\ log\ n\rfloor+1} \geq \binom{2\lfloor\sqrt{|A_0|}\ log\ n\rfloor+1}{\lfloor\sqrt{|A_0|}\ log\ n\rfloor}$$
$$\geq 2^{\sqrt{|A_0|}\ log\ n} = n^{\sqrt{|A_0|}}.$$

در نتیجه $|B_0| > n^{\sqrt{|A_0|}}$.

برای $0 \leq i_1, i_2, j_1, j_2 \leq \sqrt{|A_0|}$ وجود دارد $(i_1, j_1) \neq (i_2, j_2)$ که $(\frac{n}{p})^{i_1}p^{j_1} \overset{r}{\equiv} (\frac{n}{p})^{i_2}p^{j_2}$ زیرا تعداد این زوج‌ها بیشتر از $|A_0|$ است و $(\frac{n}{p})^{i_1}p^{j_1}, (\frac{n}{p})^{i_2}p^{j_2} \in A$. همچنین چون $g(x) \in B_0$ داریم:

$$g(x)^{(\frac{n}{p})^{i_1}p^{j_1}} = g(x^{(\frac{n}{p})^{i_1}p^{j_1}}) = g(x^{(\frac{n}{p})^{i_2}p^{j_2}})$$
$$= g(x)^{n^{(\frac{n}{p})^{i_2}p^{j_2}}} (mod\ p, h(x)).$$

بنابراین $g(x)$ ریشه چندجمله‌ی $T(y) = y^{(\frac{n}{p})^{i_1}p^{j_1}} - y^{(\frac{n}{p})^{i_2}p^{j_2}}$ است. با توجه به کرانی که برای i_1, i_2, j_1, j_2 انتخاب شد، درجه‌ی چندجمله‌ای T حداکثر $n^{\sqrt{|A_0|}}$ است اما از طرفی تمام اعضای B_0 ریشه‌ی این چندجمله‌ای هستند. چون ثابت کرده‌ایم $|B_0| > n^{\sqrt{|A_0|}}$، این یعنی چندجمله T متحد با صفر است بنابراین باید $(\frac{n}{p})^{i_1}p^{j_1} = (\frac{n}{p})^{i_2}p^{j_2}$. در نتیجه داریم $n^{i_1-i_2} = p^{i_1+j_2-i_2-j_1}$ و این یعنی n توانی از یک عدد اول است.

آزمون AKS یک الگوریتم قطعی با کمتر از $O((log\ n)^5)$ محاسبه است که بنابر قضیه ۴، قضیه ۱۰ و لم ۳ آزمون توانایی تشخیص عدد اول از عدد مرکب را در زمان چندجمله‌ای دارد.

الگوریتم ۳. (*آزمون اول بودن* AKS)

input: n

output: prime or composite

if $\exists\, m,\ k \in \mathbb{N};\ n = m^k\ ,\ k > 1$

return composite

End if

$r \leftarrow$ the smallest r such that: $ord(n)\ \text{mod}\ r > (log(n))^2$

for $a = 0 : \lceil\sqrt{r}log\ n\rceil$

if $(n, a) \neq 1$ or $(x + a)^n \neq x^n + a(mod\ n,\ x^r - 1)$

return composite

End if

End for

return prime

مراجع

[1] M. Agrawal, N. Kayal, N. Saxena. PRIMES is in P. Annals of Mathematics, page 781–793, 2004.

[2] Manindra Agrawal. Primality tests based on fermat's little theorem.

[3] Tom M. Apostol. Introduction to Analytic Number Theory. deeplearningbook.org.

[4] Daniel J. Bernstein. Detecting perfect powers in essentially linear time. Mathematics of computation, 1998.

[5] Mohan Nair. On chebyshev-type inequalities for prime. Amer. Math. Monthly, page 126–129, 1982.

[6] Michael O. Rabin. Probabilistic algorithm for testing primality. Number Theory, page 128.

[7] Volker Strassen Robert M. Solovay. A fast monte-carlo test for primality. SIAM Journal on Computing, page 84–86, 1977.