آلگوریتم کوانتومی برای تجزیه اعداد

وحیدکریمی پور_ دانشکده فیزیک _ دانشگاه صنعتی شریف

۳ خرداد ۱۳۹۷

۱ مقدمه

یک نمونه از مسائل دشوار در نظریه محاسبه، مسئله تجزیه یک عدد به عامل های اول آن است. هرگاه عددی مثل N داشته باشیم و بخواهیم یکی از عامل های آن را پیدا کنیم، بهترین آلگوریتم های کلاسیک این کار را در زمانی از مرتبه‌ی ... انجام می دهند. شُر نشان داده است که با استفاده از آلگوریتم های کوانتومی می توان این مسئله را در زمان چند جمله ای حل کرد. حل این مسئله توسط شُر [۱] علت اصلی توجه بسیارزیاد جامعه فیزیک، ریاضی وعلوم کامپیوتر به کامپیوترهای کوانتومی در یک دهه اخیر بوده است. دراین درس این آلگوریتم را به دقت توضیح می دهیم. آنچه را که تنها به اساس آلگوریتم کوانتومی شُر مربوط است در متن درس آورده‌ایم و خواننده می تواند تقریباً این آلگوریتم را با خواندن متن این درس بفهمد. اما برای فهم کامل این آلگوریتم خواندن ضمیمه این درس ضروری است. در این ضمیمه چند قضیه ابتدایی در نظریه اعداد توضیح داده شده است.

[۱] Peter Shor

۲ مبنای آلگوریتم شر

دراین بخش نشان می دهیم که مسئله یافتن یک عامل اول از یک عدد مثل N با مسئله یافتن پریود یک تابع معین یکسان است. فرض کنید که عددی نابدیهی مثل x آنچنان بیابیم که در معادله زیر صدق کند:

$$x^2 = 1 \quad mod \;\; N. \tag{۱}$$

منظور از جواب غیر بدیهی این است که

$$x \neq 1, -1 \quad mod \; N, \tag{۲}$$

یا

$$x - 1 \neq kN, \qquad x = 1 \neq kN \tag{۳}$$

دراین صورت می توانیم بنویسم

$$x^2 - 1 = 0 \quad mod \;\; N, \quad \text{یا} \quad (x-1)(x+1) = kN \tag{۴}$$

این معادله به این معناست که N حاصلضرب $(x-1)(x+1)$ را می شمارد یعنی

$$N \mid (x-1)(x+1) \tag{۵}$$

. اما از آنجا که بنا بر 2 N هیچ کدام از اعداد $x-1$ یا $x+1$ را نمی تواند بشمارد، پس نتیجه می گیریم که N تنها می تواند فاکتورهای مشترکی با یکی یا هردو از این اعداد داشته باشد.

مثال ۱: فرض کنید که $N = 15$ و $x = 4$. دراین صورت داریم

$$x^2 = 16 = 1 \;\; mod \;\; 15. \tag{۶}$$

ضمناً $x - 1 = 3$ و $x + 1 = 5$ مضرب هایی از 15 نیستند. از رابطه بالا نتیجه می گیریم که 15 حاصلضرب 3×5 را می شمارد، بدون اینکه 3 یا 5 را بشمارد. این تنها وقتی ممکن است که 15 با 3 یا 5 عامل مشترک داشته باشد.

مثال ۲: فرض کنید که $N = 115$ و $x = 24$. دراین صورت داریم

$$x^2 = 576 = 1 \ \ mod \ \ 115. \tag{۷}$$

ضمناً $x - 1 = 23$ و $x + 1 = 25$ مضرب هایی از 115 نیستند. از رابطه بالا نتیجه می گیریم که 115 حاصلضرب 23×25 را می شمارد، بدون اینکه 25 یا 23 را بشمارد. این تنها وقتی ممکن است که 115 با 32 یا 25 عامل مشترک داشته باشد.

در مثال های گذشته عدد x کوچکتر از N بود. ولی x می تواند هر عدد دلخواهِ کوچک تر یا بزرگ تر از N باشد.

پس از این کار براحتی می توانیم عامل مشترکِ دو عددِ N و $x - 1$ یا $x + 1$ را پیدا کنیم. یک آلگوریتم که به نام آلگوریتم اقلیدس مشهور است بزرگترین مقسوم علیه مشترک این دو عدد را بسادگی و درزمان چند جمله ای پیدا می کند.

بنابراین مسئله پیدا کردن یک عامل از عدد N به مسئله یافتن عددی مثل x که در شرط $x^2 = 1 \ \ mod \ \ N$ صدق کند کاهش می یابد. در نگاه اول می توانیم برای حل این مسئله به ترتیب زیر اقدام کنیم. یک عدد دلخواه که نسبت به N اول است مثل Y انتخاب می کنیم. همواره می توانیم چنین عددی را در زمان چندجمله ای پیدا کنیم زیرا بزرگترین مقسوم علیه مشترک دو عدد را با آلگوریتم اقلیدس می توانیم در زمان چندجمله ای محاسبه کنیم. اگر بزرگترین مقسوم علیه مشترک برابر با یک بود معلوم است که این دو عدد نسبت به هم اول هستند. ضمنا تعداد اعدادی که نسبت به یک عدد اول هستند کسر قابل ملاحظه ای از اعداد است و همیشه شانس خیلی خوبی داریم که یک عدد تصادفی که انتخاب می کنیم نسبت به N اول باشد. سپس این عدد را به توان های متوالی می رسانیم و مجموعه

$$S = \{Y, \ Y^2, \ Y^3, \ Y^4, \cdots\} \tag{۸}$$

را بوجود می آوریم که در آن تمام این توان ها به سنج N حساب شده اند یعنی منظور از Y^i عبارت است از $Y^i \ mod(N)$.
. تمام این اعداد کوچکتر از N هستند و حتما یکی از آنها برابر با 1 خواهد شد. یعنی حتما یک r پیدا می کنیم که

$$Y^r = 1 \quad mod \quad N. \tag{۹}$$

عدد r را که کوچکترین عددی است که این خاصیت را دارد رتبه Y می خوانیم. اگر این عدد زوج باشد انگاه خواهیم داشت

$$Y^r = Y^{2r'} = 1 \qquad mod(N), \tag{۱۰}$$

در نتیجه قرار می دهیم

$$X = Y^{r'} \tag{۱۱}$$

و این همان عددی است که برای محاسبه فاکتور عددN مورد استفاده ما خواهد بود.

در این جا چندنکته وجود دارد. اول این که ثابت می کنیم که واقعا رتبه r وجود دارد و کمتر از N است. دوم اینکه یک قضیه ریاضی که آن را بدون اثبات می پذیریم این است که نیمی از Y ها رتبه شان زوج است. پس اگر یک Y انتخاب کنیم احتمال این که رتبه آن زوج باشد برابر با $\frac{1}{2}$ است. اگر رتبه فرد بود یک عدد دیگر انتخاب کرده و روند را تکرار می کنیم. می توانیم بپرسیم که پس مشکل کجاست؟ پاسخ این است که محاسبه تمام اعضای مجموعه S محاسبه ای است که به صورت نمایی زمان می برد. (تصور کنید که N یک عدد ۱۰۰ رقمی باشد.) آلگوریتم شر [۲] دقیقا کارش این است که این رتبه را در زمان چندجمله ای پیدا می کند.

■ **قضیه:** هرگاه Y نسبت به N اول باشد، آنگاه $1 \leq r < N$.

اثبات: مجموعه اعدادِ $S = \{Y^1, Y^2, Y^3, \cdots Y^{N-1}\}$ را تشکیل می دهیم که در آن همه توانها به سنجِ N حساب شده‌اند. هرگاه دو عضو این مجموعه با هم مساوی باشند که مقصود حاصل شده است. به عنوان مثال هرگاه $Y^k = Y^l$ و $k > l$، نتیجه می گیریم که $Y^{k-l} = 1$ که معنایش این است که مرتبه‌ی Y از N کم تر است. اگر هم که همه عناصرِ S با هم متفاوت باشند به معنای این است که این مجموعه دارای $N-1$ عضو متمایز است که همگی از N کوچکترند. بنابرین عناصر مجموعه‌ی S تناظر یک به یک دارند با مجموعه‌ی $\{1, 2 \cdots N-1\}$. یعنی اینکه حتماً یکی از اعضای S برابر با ۱ است و این به این معناست که مرتبه Y از N کوچکتراست.

همانطور که در ابتدا گفتیم در نظریه اعداد نشان می دهند که هرگاه یک عدد دلخواه Y که نسبت به N اول است اختیار کنیم، آنگاه احتمال آن که مرتبه آن زوج باشد برابر است با ۲/۱. بنابراین اگر یک عدد تصادفی مثل Y اختیار کنیم و بتوانیم رتبه آن را به سنج N پیدا کنیم به احتمال ۵۰ درصد رتبه این عدد زوج خواهد بود.بنابراین مشروط بر اینکه رتبه عدد Y را بتوانیم پیدا کنیم عدد X و درنتیجه یک عامل از N را پیدا خواهیم کرد. آنچه که شُر انجام داده است ارایه یک آلگوریتم برای پیدا کردن رتبه یک عدد دلخواه به سنج N است. این کار چیزی جز یک

[۲] Shor Algorithm

مسئله یافتن پریود $Period\ Finding$ نیست، زیرا هرگاه تابعی مثل تابع زیر تعریف کنیم،

$$f(l) = Y^l \quad mod \ \ N \tag{۱۲}$$

آنگاه

$$f(l+r) = f(l), \longrightarrow f(l+jr) = f(l) \quad j = 1, 2, 3, \cdots . \tag{۱۳}$$

بنابراین مسئله یافتن مرتبه عددِ Y به سنجِ N عبارت است از پیدا کردن پریود تابع فوق و برای و برای آن می توان آلگوریتمی مثل آلگوریتم سایمن با کمی پیچیدگی بیشتر به کار برد.

۳ مراحل آلگوریتم شر

می توانیم مسئله را به شکل کلی تری طرح کنیم و آن اینکه هرگاه یک تابع متناوب دلخواه مثل $f : Z_N \longrightarrow Z_N$ داشته باشیم، چگونه می توانیم دوره تناوب آن را پیداکنیم. اگر دوره تناوب این تابع r باشد چند بارمی بایست تابع را بخوانیم تا بتوانیم این دوره تناوب را پیداکنیم؟ کمی دقت نشان می دهد که تعداد دفعات خواندن تابع از مرتبه N است. می خواهیم بااستفاده از توازی کوانتومی آلگوریتمی بسازیم که بتواند این دوره تناوب را با خواندن تابع به تعداد بسیارکمتری پیداکند. روش کار بسیار شبیه به روشی است که درآلگوریتم سیمون بکاربرده ایم. این آلگوریتم را به چند مرحله تقسیم می کنیم.

مرحله یک : حالت $|\overline{0}\rangle \otimes |\overline{0}\rangle$ راتهیه می کنیم که درآن $|\overline{0}\rangle = |0, 0, \cdots, 0\rangle$ و طول هرکدام ازاین حالت هاچنان است که می توان یک عدد بسیار بزرگ مثل Q رادرآن نوشت. فعلاً تنها فرض می کنیم که این عدد از N بزرگ تراست . این که چقدر می بایست بزرگ تر باشد درادامه معلوم خواهد شد.

مرحله دو: با اعمال عملگرهای هادامارد حالت اول را به یک ترکیب خطی از همه اعداد 0 تا $Q-1$ تبدیل می کنیم. بنابراین درپایان این مرحله حالت فوق تبدیل می شود به

$$|\psi_0\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |\bar{0}\rangle. \tag{۱۴}$$

مرحله سه : حال تابع را فرامی خوانیم که حالت فوق را به حالت زیر تبدیل می کند:

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |Y^l \;\; mod \;\; N\rangle. \tag{۱۵}$$

مرحله چهار: روی ثبت کننده دوم یک اندازه گیری انجام می دهیم. فرض کنید که نتیجه اندازه گیری عدد $Y^{l_0} \;\; mod \;\; N$ باشد، دراین صورت حالت ثبت کننده اول کاهش پیدامی کند به

$$|\phi\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |l_0 + jr\rangle \tag{۱۶}$$

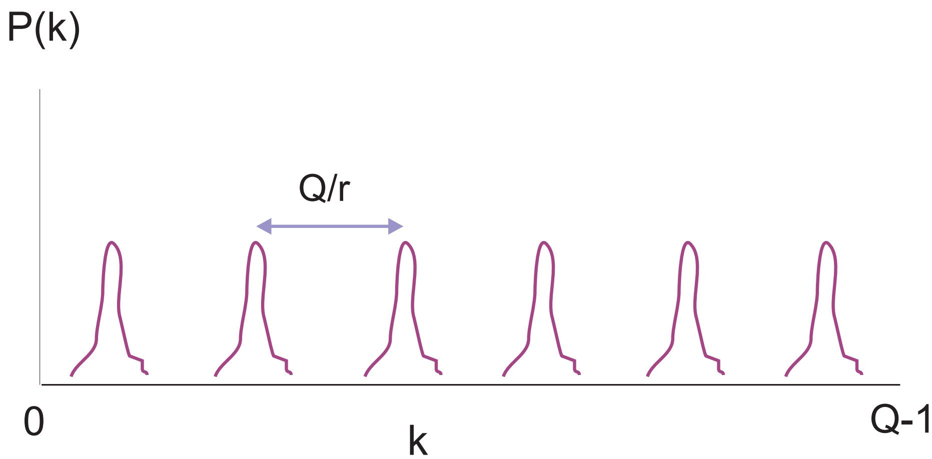
دراین جا A تعداد دوره های تناوبی است که درفاصله $[0, Q-1]$ جامی شود. بدیهی است که با اندازه گیری این حالت نمی توان عدد A و درنتیجه دوره تناوب r را بدست آورد. هم چنین با اندازه گیری ثبت کننده اول تنها یکی از اعداد $\cdots, l_0-2r, l_0-r, l_0, l_0+r, l_0+2r, \cdots$ یافته خواهند شد که با توجه به اینکه مقدار l_0 را نمی دانیم نمی توانیم از آن برای تعیین r کمک بگیریم. راهی که باقی می ماند آن است که درست مثل آلگوریتم سیمون ازتبدیل فوریه استفاده کنیم. این بار می بایست از تبدیل فوریه روی Z_Q استفاده کنیم. فرض می کنیم که $Q = 2^n$ و بنابراین تبدیل فوریه ما روی گروه Z_{2^n} تعریف می شود. تبدیل فوریه روی $Z_Q = Z_{2^n}$ به شکل زیر تعریف می شود:

$$U|k\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} e^{\frac{2\pi i k l}{Q}} |l\rangle. \tag{۱۷}$$

پس ازتبدیل فوریه حالت $|\phi\rangle$ به حالت زیر تبدیل می شود:

$$|\phi'\rangle = \frac{1}{\sqrt{A}} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sum_{j=0}^{A-1} e^{\frac{2\pi i k (l_0 + jr)}{Q}} |k\rangle \tag{۱۸}$$

مرحله پنج : حال ثبت کننده اول را اندازه می گیریم. احتمال اینکه دراین اندازه گیری مقدار k بدست آید برابراست با:



شکل ۱: شکل تابع $P(k)$ درحالت کلی وقتی که Q/r عدد صحیحی نیست.

$$
\begin{aligned}
P(k) &= \frac{1}{QA} \mid \sum_{j=0}^{A-1} e^{\frac{2\pi i k(jr+l_0)}{Q}} \mid^2 \\
&= \frac{1}{QA} \mid \sum_{j=0}^{A-1} e^{\frac{2\pi i kjr}{Q}} \mid^2 \\
&= \frac{1}{QA} \mid \frac{1-e^{\frac{2\pi i krA}{Q}}}{1-e^{\frac{2\pi i kr}{Q}}} \mid^2 = \frac{1}{QA} \mid \frac{\sin\frac{\pi krA}{Q}}{\sin\frac{\pi kr}{Q}} \mid^2 .
\end{aligned} \tag{۱۹}
$$

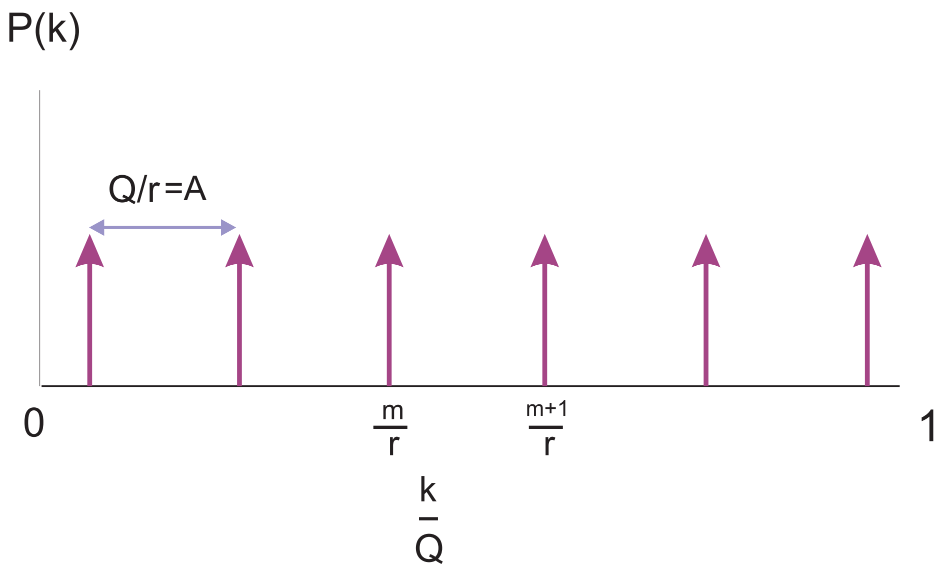
این تابع یک تابع تقریباً پریودیک است که پریود آن تقریباً برابر است با $A \approx \frac{Q}{r}$. بنابراین در فاصله‌ی $[0, Q-1]$ شکل این تابع به طور تقریب A بار تکرار می شود، شکل 1.

مرحله شش : حال به تجزیه تحلیل نتیجه می پردازیم.

حالت اول : نخست حالت ساده ای را درنظر می گیریم که Q مضرب صحیحی از دوره تناوب است. دراین صورت $A = \frac{Q}{r}$ و درنتیجه از رابطه 19 معلوم می شود که جمع سری هندسی برابرباصفر است مگر درمواقعی که $\frac{kr}{Q}$ خود عدد صحیحی مثل m باشد که دراین صورت جمع سری برابر با $\frac{1}{QA}A^2 = \frac{1}{r}$ خواهد بود. بنابراین دراین حالت تابع احتمال برابراست با:

$$P(k) = \frac{1}{r}\delta_{\frac{k}{Q},\frac{m}{r}} . \tag{۲۰}$$

تابع $P(k)$ دراین حالت مطابق شکل 2 است. این رابطه بیان می کند که دراین حالت هربارکه ثبت کننده اول را اندازه بگیریم عددی بدست



شکل ۲: شکل تابع $P(k)$ درحالتی که Q/r عدد صحیحی است . این عدد صحیح همان A است.

می آوریم که اگرآن را بر Q تقسیم کنیم کسری مثل $\frac{m}{r}$ است. به عنوان مثال اگر r برابر با ۱۰۰ باشد،دراندازه گیری ثبت کننده اول یکی از اعداد

$$\{\frac{0}{100},\frac{1}{100},\frac{2}{100},\frac{3}{100},\cdots\frac{99}{100}\}$$

بدست خواهند آمد. مخرج این کسرها همان دوره تناوب r (دراینجا ۱۰۰)است. البته باید توجه داشت که تعدادی از کسرهای فوق مثل $\frac{2}{100},\frac{4}{100},\frac{5}{100},\frac{6}{100}$ ویا مثلاً $\frac{50}{100}$ و بترتیب منجر به مخرج هایی مثل $50,20,25,50$ و یا 2 می شوند که هیچ کدام دوره تناوب واقعی نیستند. نکته این است که تعداد قابل ملاحظه ای از کسرهای دیگر وجود دارند که صورت و مخرج آنها نسبت به هم اول هستند وساده نمی شوند مثل $\frac{19}{100}\frac{13}{100},\frac{11}{100},\frac{7}{100},\frac{3}{100}$ و نظایرآن. درواقع برای اعداد بزرگ r تعداد اعداد کوچکتراز r که نسبت به آن اول هستند ازمرتبه $\frac{r}{ln\ \ r}$ است. و این به آن معناست که درهر۱۰۰ باراندازه گیری، حدوداً در $21\sim 100\times\frac{1}{ln\ \ 100}$ دفعه آن به اعداد ساده نشدنی برمی خوریم که مخرج آنها از همه مخرج های دیگر بزرگتراست. این مخرج ها همان دوره تناوب مورد نظرهستند.

حالت دوم: تجزیه تحلیل قبلی مربوط به یک حالت ایده آل بود که فرض کرده بودیم عدد Q مضرب صحیحی از دوره تناوب است و درنتیجه عدد A دقیقاً برابر است با $\frac{Q}{r}$. ولی چون ما دوره تناوب را ازقبل نمی دانیم این فرض صحیح نیست و تنها چیزی که می دانیم آن است که جزء صحیح $\frac{Q}{r}$ برابربا A است. دراین حالت k هایی که اندازه می گیریم دیگر به صورت $Q(\frac{m}{r})$ نخواهند بود و براحتی نمی توان ازروی آنها r را تعیین

کرد. تابع $P(k)$ دراین حالت دیگر مطابقِ شکل 2 مجموعه‌ای از توابع دلتای کرونکر در نقاط $\frac{m}{r}$ نخواهد بود. این تابع هنوز شکل پریودیک خود را حفظ می کند ولی هر تابعِ دلتای کرونکر کمی پهن می شود به این معنا که بجز مقادیر $\frac{m}{r}$ مقادیرِ کمی نزدیک نیز بدست می آیند. برای جلو رفتن دو کار می کنیم.

الف : k های خوب را k هایی تعریف می کنیم که درشرط

$$\mid \frac{k}{Q} - \frac{m}{r} \mid < \frac{1}{2Q} \tag{۲۱}$$

صدق کنند. به عبارت بهتر این k ها تفاوتشان از $Q(\frac{m}{r})$ از $\frac{1}{2}$ کمتراست. کمی بعد نشان می دهیم که چرا این k ها k های خوب هستند. برای توضیحات بیشتر، خواننده هم چنین می تواند به ضمیمه این درس تحت عنوان کسرهای مسلسل مراجعه کند. درواقع نشان خواهیم داد که بازهم می توان ازاین k ها دوره تناوب r را البته نه به آسانی قبل پیداکرد. این امر درقضیه زیر بیان شده است.

قضیه : اگر Q به اندازه کافی بزرگ باشد، کسر $\frac{k}{Q}$ را تنها به یک صورت می توان به صورت کسری با مخرج کوچکتراز N ساده کرد. اگر این کسر را به صورت $\frac{m}{r}$ بنویسیم، r همان دوره تناوب خواهد بود. (یادآوری می کنیم که r از N کوچکتراست.)

اثبات : فرض کنید که علاوه بر کسر $\frac{m}{r}$ ، کسر $\frac{m'}{r'}$ نیز درشرط 21 صدق کند، یعنی داریم :

$$\mid \frac{k}{Q} - \frac{m'}{r'} \mid < \frac{1}{2Q} \tag{۲۲}$$

دراین صورت با جمع دو نامساوی فوق و استفاده از نامساوی مثلث به رابطه زیر می رسیم :

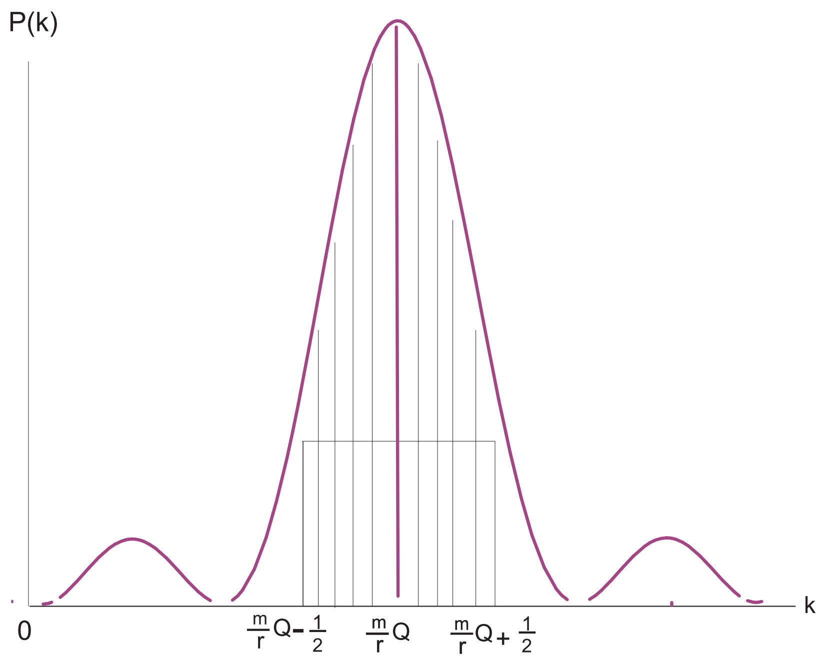
$$\mid \frac{m}{r} - \frac{m'}{r'} \mid < \frac{1}{Q} \tag{۲۳}$$

از طرفی می دانیم که

$$\mid \frac{m}{r} - \frac{m'}{r'} \mid = \mid \frac{mr' - m'r}{rr'} \geq \frac{1}{N^2} \tag{۲۴}$$

با توجه به 24 و 23 به این نتیجه می رسیم که اگر Q را از N^2 بزرگتر انتخاب کنیم این اتفاق یعنی وجود دو کسر با مخرج کوچکتر از N اتفاق نخواهد افتاد.

ب : نشان می دهیم که احتمال پیداکردن یک k خوب به اندازه کافی بالاست، به عبارت دقیق تر نشان خواهیم داد که احتمال یافتن چنین k هایی از $\frac{4}{\pi^2}$ بیشتراست. برای این کار به شکل تابع $P(k) = \frac{1}{QA} \mid \frac{\sin\frac{\pi k r A}{Q}}{\sin\frac{\pi k r}{Q}} \mid^2$ در اطراف یکی از نقطه ها مثلاً نقطه $k = \frac{Q}{r}$ نگاه می کنیم. در



شکل ۳: شکل تابع $P(k)$ در نزدیکی یکی از نقاط $\frac{k}{Q}=\frac{m}{r}$. شکل کامل تکراری از این منحنی است و تعداد تکرار ها نیز r تاست.

شکل 3 تابع $P(k)$ در نزدیکی یکی از نقطه ها رسم شده است. دقت کنید که تابع را برحسب k/Q رسم کرده‌ایم و تنها یکی از دوره های تناوب تابع را نشان داده ایم.

سطح هاشور خورده، احتمال پیدا کردن یک k خوب در اطراف این نقطه را نشان می دهد که هنوز می توان پریود ِ r را با دانستن آن پیدا کرد. مساحت ِ سطح هاشور خورده مسلماً بیشتر از سطح مستطیل ِ نشان داده شده است. مساحت مستطیل برابراست با:

$$2\times\frac{1}{2}\times P(k=\frac{mQ}{r}+\frac{1}{2})=P(k=\frac{1}{2})=\frac{1}{QA}(\frac{\sin\frac{\pi rA}{2Q}}{\sin\frac{\pi r}{2Q}})^2 \qquad (۲۵)$$

اما می دانیم که $Q\approx Ar$ و $\frac{\pi r}{2Q}\ll 1$. درنتیجه این عبارت تقریباً برابر است با:

$$\frac{4}{\pi^2}\frac{1}{r}. \qquad (۲۶)$$

بنابراین مساحت قسمت هاشور خورده از این مقدار بیشتر است و از آنجا که تعداد r تاپریود داریم احتمال پیدا کردن k های خوب از $\frac{4}{\pi^2}$ بیشتر خواهد بود.

بطور خلاصه در حالت اول که Q مضرب صحیحی از یک پریود است در اندازه گیری ثبت کننده اول به طور قطع اعدادی بدست می آوریم که در هرگاه آنها را بر Q تقسیم کنیم اعدادی به صورت $\frac{m}{r}$ بدست می آید و در حالت دوم بااحتمال بیشتر از $\frac{4}{\pi^2}$ اعدادی بدست می آوریم که می توان آنها را به صورت $\frac{m}{r}$ نوشت. در هردو صورت می توان r را در زمان چند جمله ای پیدا کرد.

تنها چیزی که از الگوریتم شُر باقی مانده است آن است که نشان دهیم تبدیل فوریه کوانتومی را می توان به صورت یک مدار کوانتومی آنهم به صورت کارآمد (یعنی با تعداد کمی عملگر) ساخت. این کار را در بخش بعدی انجام می دهیم.

۴ تبدیل فوریه کوانتومی

تبدیل فوریه ای که در الگوریتم شر به آن احتیاج داریم، یک تبدیل فوریه روی Z_Q یعنی روی مجموعه اعداد $\{0, 1, 2, \cdots Q-1\}$ است. در زیر این تبدیل فوریه را شرح می دهیم. البته در متن زیر به طور کلی تبدیل فوریه روی یک مجموعه Z_N را شرح داده ایم.

تبدیل فوریه کوانتومی را به صورت یک نگاشت خطی به صورت زیرتعریف می کنیم. فرض کنید که یک فضای هیلبرتِ N بعدی داریم که بردارهای پایه آن را با $\{|0\rangle, |1\rangle, |2\rangle, \cdots |N-1\rangle\}$ نشان می دهیم. دراین صورت تبدیل فوریه کوانتومی یا $Quantum\ Fourier\ Transform\ (QFT)$ به صورت زیرتعریف می شود:

$$U|k\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{-2\pi ikl}{N}}|l\rangle. \quad (۲۷)$$

هرگاه $|f\rangle$ یک برداردلخواه دراین فضا باشد مولفه های این بردارتحت تبدیل فوریه به شکل زیرتبدیل خواهند شد:

$$\langle k|U|f\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}}\langle l|f\rangle, \quad (۲۸)$$

ویا

$$\tilde{f}_k = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}} f_l. \quad (۲۹)$$

۱.۴ یک مدارکوانتومی برای محاسبه تبدیل فوریه کوانتومی

برای سادگی فرض می کنیم که N عددی مثل 2^m-1 است. می دانیم که تبدیل فوریه کوانتومی به شکل زیراست:

$$U|a\rangle = \frac{1}{\sqrt{N}}\sum_{b} e^{\frac{2\pi iab}{N}}|b\rangle, \quad a,\ \ b\in Z_N. \quad (۳۰)$$

می دانیم که

$$\begin{aligned} a &= (a_1, a_2, a_3, \cdots a_m) = a_1 \times 2^{m-1} + a_2 \times 2^{m-2} + \cdots a_m \times 2^0, \\ b &= (b_1, b_2, b_3, \cdots b_m) = b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + \cdots b_m \times 2^0. \end{aligned} \tag{۳۱}$$

بنابراین

$$\begin{aligned} U|a\rangle &= \frac{1}{\sqrt{2^m}} \sum_b e^{\frac{2\pi i a}{2^m}\left[b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + \cdots b_m \times 2^0\right]} |b\rangle \\ &= \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a b_1}{2}} |b_1\rangle\right) \left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i a b_2}{2^2}} |b_2\rangle\right) \cdots \left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i a b_m}{2^m}} |b_m\rangle\right) \end{aligned} \tag{۳۲}$$

اما می توان عبارت سمت راست را به شکل زیرنیز نوشت:

$$U|a\rangle = \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a_m b_1}{2}} |b_1\rangle\right) \left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i (2a_{m-1} + a_m) b_2}{2^2}} |b_2\rangle\right) \cdots \left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i (2^{m-1} a_1 + \cdots 2a_0) b_m}{2^m}} |b_m\rangle\right) \tag{۳۳}$$

بنابراین می توانیم بنویسیم

$$U|a\rangle = |\phi_1(a_m)\rangle |\phi_2(a_m, a_{m-1})\rangle \cdots |\phi_m(a_m, a_{m-1}, \cdots a_1)\rangle, \tag{۳۴}$$

که درآن

$$\begin{aligned} &|\phi_1(a_m)\rangle := \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2\pi i a_m}{2}} |1\rangle\right], \\ &|\phi_2(a_m, a_{m-1})\rangle := \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2\pi i (2a_{m-1} + a_m)}{2^2}} |1\rangle\right], \\ &\cdots \\ &\cdots \end{aligned} \tag{۳۵}$$

نکته ای که در این جا براحتی دیده می شود این است که خروجی مدار تبدیل فوریه اولا به صورت یک حالت جدا ا ز هم است و در هم تنیده نیست یعنی این حالت خروجی به صورت یک حالت ضربی نوشته شده است. حال یک مدارکوانتومی معرفی می کنیم که تبدیل فوریه کوانتومی را انجام دهد. نخست عملگرهای یک کیوبیتی زیر را معرفی می کنیم:

$$R_k(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i \alpha}{2^k}} \end{pmatrix}. \tag{۳۶}$$

خواننده براحتی می تواند نشان دهد که تساوی های زیربرقرارهستند:

$$\begin{aligned}
|\phi_1(a_m)\rangle &= H|a_m\rangle \\
|\phi_2(a_m,a_{m-1})\rangle &= R_2(a_m)H|a_{m-1}\rangle \\
|\phi_3(a_m,a_{m-1},a_{m-2})\rangle &= R_2(a_{m-1})R_3(a_m)H|a_{m-2}\rangle \\
|\phi_4(a_m,a_{m-1},a_{m-2},a_{m-3})\rangle &= R_2(a_{m-2})R_3(a_{m-1})R_4(a_m)H|a_{m-3}\rangle \\
\cdots &\quad \cdots \\
\cdots &\quad \cdots
\end{aligned} \tag{۳۷}$$

هرکدام از عملگرهای $R_k(\alpha)$ در واقع به صورت یک عملگر کنترلی عمل می کنند که اگر مقدارِ α برابر با صفر باشد، هیچ کاری انجام نمی دهند واگر مقدارِ α برابر با 1 باشد، عمل ِ R_k را انجام می دهند. بنابراین به سادگی می توان مدار مربوط به عملگر تبدیل فوریه کوانتومی را ساخت. انجام این کار را به عهده خواننده می گذاریم.

■ تمرین: مدار تبدیل فوریه را برای وقتی که $Q=16$ است رسم کنید.

۵ ضمیمه: چند قضیه مفید در باره اعداد

هدف ما دراین ضمیمه فراهم آوردن مقدماتی از نظریه اعداد است که برای کامل کردن مطالب مربوط به آلگوریتم شُر لازم هستند. ظاهرا درسالهای اخیر اغلب این مطالب دردروس دبیرستانی آموزش داده می شوند. بنابراین دانشجویانی که با این مطالب آشنایی قبلی دارند می توانند از خواندن این ضمیمه صرف نظر کنند. شاید بعضی از این مطالب برای آن دسته از دانشجویان قدیمی تر تازه باشد. شاید هم همهاین مطالب برای دانشجویان خیلی قدیمی تر مثل خودمن کاملا تازه باشند. به هرحال یک آشنایی با خواص مقدماتی اعداد می تواند به خودی خود فرح بخش باشد.

۱.۵ تعاریف اساسی

■ **تعریف :** می گوییم عدد صحیح a عدد صحیح b را می شمارد و می نویسیم $a|b$ هرگاه عدد صحیحی مثل k یافت شود به قسمی که $b = ka$. هرگاه چنین نباشد می نویسیم $a \mid b$.

بنابراین $5 \mid 115$ و $6 \mid 8$.

■ **تعریف:** عدد p اول خوانده می شود هرگاه تنها توسط عدد یک و خود ش شمرده شود.

اثبات قضیه زیر آسان است.

■ **قضیه:**

الف: هرگاه $a|b$ و $b|c$ ، آنگاه $a|c$.

ب: هرگاه $a|b$ و $a|c$ ، و x, y دو عدد صحیح باشند، آنگاه $a|xb + yc$.

پ: اگر $a|b$ و $b|a$ ،آنگاه $a = b$.

ت: هرگاه $ab|n$ ، آنگاه حتماً یکی از دوعدد a یا b عدد n را می شمارد. یعنی حتما یکی از دو شرط $a|n$ و یا $b|n$ برقرار خواهند بود.

■ **قضیه اساسی حساب:** هر عدد صحیح $n \in Z$ بسط ضربی یکتایی برحسب عامل های اول خود دارد. این بسط تنها تحت جایگشت های عامل های اول خود یکتا نیست. به عبارت دیگر باصرف نظر کردن از امکان جایگشت عامل ها هرعدد صحیح را می توان به شکل

یکتایی به عامل های اول به صورت زیر تجزیه کرد:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad (۳۸)$$

که درآن p_i ها اعداد اول هستند.

۲.۵ حساب باقیمانده ها و آلگوریتم اقلیدس

■ **تعریف:** می گوییم اعداد صحیح a و b به سنج n هم باقیمانده یا هم ارز هستند هرگاه $n|a-b$، یعنی اینکه عدد صحیحی مثل k وجود داشته باشد به قسمی که $a - b = kn$. واضح است که این رابطه یک رابطه هم ارزی است و بدین ترتیب تمام اعداد صحیح به کلاس های هم باقیمانده به سنج n افراز می شوند. کلاس هم باقیمانده با i را با $[i]$ نشان می دهیم. بنابراین داریم

$$[i] = \{i, i+n, i+2n, i+3n, \cdots\}. \qquad (۳۹)$$

تعداد کلاس ها برابر است با n. یعنی

$$\begin{aligned}
&[0] = \{0,\ n,\ 2n,\ 3n, \cdots\} \\
&[1] = \{1,\ 1+n,\ 1+2n,\ 1+3n, \cdots\} \\
&[2] = \{2,\ 2+n,\ 2+2n,\ 2+3n, \cdots\} \\
&\cdots \\
&[n-1] = \{n-1,\ n-1+n,\ n-1+2n,\ n-1+3n, \cdots\}.
\end{aligned} \qquad (۴۰)$$

مجموعه این کلاس ها را با عمل جمعی که از Z روی آن القا شده است با Z_n نمایش می دهیم. به عبارت دیگر درZ_n داریم :

$$[a] + [b] := [a+b] \qquad (۴۱)$$

با این تعریف Z_n تبدیل به یک گروه آبلی می شود که عضو خنثی آن $[0]$ و عضو معکوس هرعضو مثل $[i]$ ، $[n-i]$ است. معمولاً از نوشتن علامت براکت صرف نظر می کنیم و گروه Z_n را به سادگی به صورتِ $Z_n = \{0,\ 1,\ 2, \cdots n-1\}$ می نویسیم که درآن جمع به سنجِ n انجام می شود.

تعریف: بزرگتری مقسوم علیه مشترک دو عدد صحیح a و b ، بزرگترین عدد صحیحی است که هردوعدد را بشمارد. این عدد را با $gcd(a,b)$ نشان می دهیم که درآن gcd از لفظ انگلیسی greatest common divisor به معنای بزرگترین مقسوم علیه مشترک گرفته شده است. بنابراین اگر عددی مثل r داشته باشیم که $r|a$ و $r|b$ آنگاه $r \geq gcd(a,b)$. به زبان فارسی این رابطه های می گویند که اگر عددی مثل r، عددِ a و b را بشمارد، حتماً این عدد از بزرگترین مقسوم علیه آن دو عدد کوچکتراست یا با آن مساوی است.

دراینجا به بیان یک قضیه مهم و مفید می پردازیم:

قضیه: بزرگترین مقسوم علیه مشترک دو عدد a, b کوچکترین عدد صحیح مثبتی است که می توان آن را به صورت زیر نوشت :

$$gcd(a,b) = xa + yb \qquad x,\ y \in Z. \tag{۴۲}$$

اثبات: فرض کنید که عدد $s = xa + yb$ کوچکترین عدد صحیح مثبتی باشد که بتوان آن را به این فرم نوشت. نشان خواهیم داد که

$$s \leq gcd(a,b) \qquad , \qquad gcd(a,b) \leq s \tag{۴۳}$$

و ازآنجا مطابق با قضیه ۱.۵ نتیجه خواهیم گرفت که $gcd(a,b) = s$. برای این کار توجه می کنیم که بنابرتعریف بزرگترین مقسوم علیه مشترک

$$gcd(a,b)|a \qquad , \qquad gcd(a,b)|b \tag{۴۴}$$

درنتیجه با توجه به قضیه 5.1، $gcd(a,b)|xa + yb$ و یا $gcd(a,b)|s$ که نتیجه می دهد

$$gcd(a,b) \leq s. \tag{۴۵}$$

حال نشان می دهیم که $s|a$ و $s|b$ که با توجه به تعریف بزرگترین مقسوم علیه مشترک به این معناست که

$$s \leq gcd(a,b). \tag{۴۶}$$

بنابراین هرگاه صحت رابطه اخیرانشان دهیم باترکیب آن با رابطه قبلی اش به این نتیجه می رسیم که $gcd(a,b) = s$ وقضیه ثابت می شود. اما برای نشان دادن این که $s|a$ ، به برهان خلف متوسل می شویم. فرض کنید که چنین نباشد . دراین صورت خواهیم داشت

$$a = ks + r, \tag{۴۷}$$

که درآن r عدد صحیحی است که درشرط $0 < r < s$ صدق می کند. بنابراین خواهیم داشت

$$r = a - ks \longrightarrow r = a - k(xa + yb) = (1 - kx)a - kyb \tag{۴۸}$$

بنابراین یک عدد مثبت کوچکتر از s یافته ایم که می توان آن را به صورت ترکیب خطی a و b نوشت که مخالف فرض اولیه ماست مبنی براین که s کوچکترین عدد با این خاصیت بوده است. بنابراین نتیجه می گیریم که $s|a$. با همین نوع استدلال نتیجه می گیریم که $s|b$. به این ترتیب اثبات قضیه کامل می شود.

قضیه: فرض کنید که $c|a$ و $c|b$ ، آنگاه $c|gcd(a,b)$.

اثبات: باتوجه به این که $gcd(a,b) = xa + yb$، این قضیه واضح است.

قضیه: فرض کنید که $n > 1$ و a اعداد صحیح باشند. دراین صورت $a^{-1}\ mod\ n$ وجود دارد اگر وفقط اگر داشته باشیم $gcd(a,n) = 1$، یعنی اینکه اگر و فقط اگر a و n نسبت به هم اول باشند.

اثبات: اگر $a^{-1}\ mod\ n$ وجود داشته باشد نتیجه می گیریم $a^{-1}a = 1 + kn$ و از آنجا $1 = a^{-1}a - kn$. بنابراین با توجه به قضیه**??** نتیجه می گیریم که $1 = gcd(a,n)$. برعکس اگر $gcd(a,n) = 1$ باشد آنگاه $1 = xa + yn$ و ازآنجا $xa = 1 + yn$ که به این معناست که x همان $a^{-1}\ mod\ n$ است.

قضیه هرگاه a یک عدد دلخواه باشد که نسبت به n اول است، آنگاه معکوس ضربی a عدد به سنج n یکتاست.

اثبات: فرض کنید که $b = a^{-1}\ mod\ n$ و $b' = a^{-1}\ mod\ n$. دراین صورت نتیجه می گیریم که

$$ba = 1 + kn \qquad , \qquad b'a = 1 + k'n \tag{۴۹}$$

که از آن بدست می آوریم

$$(b-b')a=(k-k')n \longrightarrow b-b' \equiv 0 \ mod \ n \longrightarrow b=b' \ mod \ n. \qquad (۵۰)$$

دراین جا به بیان قضیه مهمّی می پردازیم که مبنای آلگوریتم اقلیدس برای یافتن بزرگترین مقسوم علیه مشترک دوعدد است.

■ **قضیه:** فرض کنید که $a \geq b$ اعداد صحیح مثبت باشند و فرض کنید که r باقیمانده تقسیم a بر b باشد یعنی $a=kb+r$. دراین صورت

$$gcd(a,b)=gcd(b,r). \qquad (۵۱)$$

اثبات: برای سادگی قرارمی دهیم $M:=gcd(a,b)$ و $m:=gcd(b,r)$. حال می دانیم که

$$m|b \quad , \quad m|a \ (since \ \ a=kb+r) \longrightarrow m \leq gcd(a,b)=M. \qquad (۵۲)$$

از طرف دیگر می دانیم که

$$M|b \quad , \quad M|r \ (since \ \ r=a-kb) \longrightarrow M \leq gcd(b,r)=m. \qquad (۵۳)$$

بنابراین $M=m$.

۱.۲.۵ آلگوریتم اقلیدس

آلگوریتم اقلیدس، آلگوریتمی است که برای یافتن بزرگترین مقسوم علیه مشتریک دو عدد به کار می رود. به کمک این آلگوریتم می توان در زمان چندجمله‌ای بزرگترین مقسوم علیه مشترک دو عدد a و b را یافت. یعنی می خواهیم $M \equiv gcd(a,b)$ را با این آلگوریتم پیدا کنیم. مراحل آلگوریتم به شرح زیراست:

۱ ـ a را بر b تقسیم کنید . باقیمانده r_1 خواهد بود. دراین صورت قرار دهید $M=gcd(b,r_1)$.

۲ ـ b را بر r_1 تقسیم کنید . باقیمانده r_2 خواهد بود. دراین صورت $M = gcd(r_1, r_2)$.

۳ ـ r_1 را بر r_2 تقسیم کنید . باقیمانده r_3 خواهد بود. دراین صورت $M = gcd(r_2, r_3)$.

....

این عمل را آنقدرادامه دهید تا به $r_k = 0$ برسید.

■ **مثال یک:** $M := gcd(128, 62)$

$$\begin{aligned} 128 &= 2 \times 62 + 4 \longrightarrow M = gcd(62, 4) \\ 62 &= 15 \times 4 + 2 \longrightarrow M = gcd(4, 2) = 2. \end{aligned} \qquad (۵۴)$$

■ **مثال دو:** $M := gcd(150, 66)$

$$\begin{aligned} 150 &= 2 \times 66 + 18 \longrightarrow M = gcd(66, 18) \\ 66 &= 3 \times 18 + 12 \longrightarrow M = gcd(18, 12) \\ 18 &= 1 \times 12 + 6 \longrightarrow M = gcd(12, 6) = 6. \end{aligned} \qquad (۵۵)$$

با استفاده از آلگوریتم اقلیدس می توان هم چنین کوچکترین عدد صحیح s که بتوان آن را به صورت $s = xa + yb$ نوشت را بدست آورد. برای این کارکافی است که مراحل آلگوریتم اقلیدس را به صورت معکوس طی کرد. این کار را برای دو مثال بالا نشان می دهیم.

■ **مثال یک:**

$$2 = 62 - 15 \times 4$$

$$
\begin{aligned}
&= 62 - 15 \times (128 - 2 \times 62) \\
&= 31 \times 62 - 15 \times 128. \qquad (۵۶)
\end{aligned}
$$

مثال دو:

$$
\begin{aligned}
6 &= 18 - 12 \\
&= 18 - (66 - 3 \times 18) \\
&= 4 \times 18 - 66 = 4 \times (150 - 2 \times 66) - 66 \\
&= 4 \times 150 - 9 \times 66. \qquad (۵۷)
\end{aligned}
$$

آلگوریتم اقلیدس را درزمان $O(L^3)$ که درآن L طول بیت های اعداد a و b است ، می توان انجام داد. ضمناً از این آلگوریتم می توان برای یافتن $a^{-1}\ mod\ n$ استفاده کرد، زیرا این عدد درصورتی وجود دارد که $gcd(a,n)=1$ باشد. بنابراین با آلگوریتم اقلیدس به روش بالا اعداد x و y ای را پیدا می کنیم که در رابطه $xa+yb=1$ صدق کنند. درنتیجه خواهیم داشت

$$xa = 1 - yn \longrightarrow x = a^{-1}\ mod\ n. \qquad (۵۸)$$

می توان از این هم یک قدم فراتر رفت و معادله زیر را حل کرد:

$$ax + b = c\ \ mod\ n \qquad (۵۹)$$

که درآن $gcd(a,n)=1$ است. برای حل این معادله به ترتیب زیر عمل می کنیم:

$$ax = c - b\ \ mod\ n \longrightarrow x = a^{-1}(c-b)\ \ mod\ n. \qquad (۶۰)$$

بازهم می توان فراتر رفت و دستگاه معادلاتی از نوع فوق را حل کرد. این موضوع نظر به اهمیت آن تحت عنوان یک قضیه جداگانه بیان می شود.

قضیه باقیمانده های چینی:[۳] فرض کنید که اعداد $m_1, m_2, \cdots m_n$ اعداد صحیح مثبت باشند و $gcd(m_i,m_j)=1\ \ \forall i,j$. دراین صورت دستگاه معادلات

$$x = a_1\ \ mod\ m_1$$

[۳] Chineese Reminder Theorem

$$
\begin{aligned}
x &= a_2 \ \ mod\, m_2 \\
x &= a_3 \ \ mod\, m_3 \\
\cdots &= \cdots \\
x &= a_n \ \ mod\, m_n
\end{aligned} \tag{۶۱}
$$

دارای یک جواب یکتا به سنج $M = m_1m_2m_3\cdots m_n$ است.

اثبات: قرارمی دهیم $M_i = \frac{M}{m_i}$. دراین صورت M_i و m_i نسبت به هم اول هستند. درنتیجه M_i به سنج m_i یک وارون دارد که آن را با N_i نمایش می دهیم. درنتیجه داریم

$$M_iN_i = 1 \ \ mod\, m_i \tag{۶۲}$$

حال قرار می دهیم

$$x := \sum_i a_iM_iN_i \tag{۶۳}$$

براحتی دیده می شود که روابط زیر برقراند:

$$
\begin{aligned}
M_iN_i &= 1 \ \ mod\, m_i \\
M_iN_i &= 0 \ \ mod\, m_j
\end{aligned} \tag{۶۴}
$$

درنتیجه این دو رابطه خواهیم داشت:

$$x = a_i \quad mod\, m_i \ \ \forall i \tag{۶۵}$$

به این ترتیب x یک حل از دستگاه معادلات (61) است. برای نشان دادن یکتایی آن فرض می کنیم که x' حل دیگری از همان دستگاه معادلات باشد. دراین صورت خواهیم داشت،

$$x - x' = 0 \quad mod \ \ m_i \ \ \forall i$$

یعنی اینکه

$$x - x' \quad = \quad k_1m_1$$

$$
\begin{aligned}
x - x' &= k_2 m_2 \\
x - x' &= k_3 m_3 \\
\cdots &= \cdots \\
x - x' &= k_n m_n.
\end{aligned} \qquad (۶۶)
$$

یعنی m_i ها همه فاکتورهای عددِ $x - x'$ هستند. از آنجا که اعدادِ m_i همگی نسبت به هم اول هستند، نتیجه می گیریم که حاصل ضرب آنها نیز فاکتورِ $x - x'$ است، یعنی $x - x' = kM$ و این همان چیزی بود که می خواستیم ثابت کنیم یعنی این که هردوجوابی از این دستگاه به سنج M بایکدیگر مساوی هستند.

■ **مثال ۱:** دستگاه معادلات زیر را در نظر بگیرید:

$$
\begin{aligned}
x &= 2 \quad mod\ 3 \\
x &= 3 \quad mod\ 4 \\
x &= 4 \quad mod\ 5.
\end{aligned} \qquad (۶۷)
$$

بنابراین عددی می خواهیم که باقیمانده تقسیم‌اش بر 3 ، 4 و 5 به ترتیب برابر باشد با 2 ، 3 و 4. چگونه‌این عدد را پیدا کنیم. قضیه باقیمانده‌های چینی پاسخ ما را می دهد. می بایست به ازای تمام i ها وارون عددِ M_i را نسبت به m_i پیدا کنیم. یعنی عددی مثل N_i که در رابطه‌ی $N_i M_i = 1 + k m_i$ صدق کند. اما می دانیم که می توانیم هر مضربی از m_i را از M_i کم کنیم بدون اینکه عددِN_i تغییر کند، زیرا از رابطه قبلی بدست می آوریم که $N_i(M_i - l m_i) = 1 + (k - l) m_i$ به عبارت دیگر

$$
M_i^{-1} \quad mod\ \ m_i = (M_i - l m_i)^{-1} \quad mod\ \ m_i. \qquad (۶۸)
$$

بنابراین برای محاسبه N_i خیلی اوقات کاربرد مراحل متعددِ آلگوریتم اقلیدس ضروری نیست و می توان خیلی زود با جستجو N_i را پیدا کرد. جدول ۱.۲.۵ نشان می دهد که اعداد مختلف در قضیه باقیمانده های چینی برای این مثال خاص چه هستند:

علامتِ $\equiv$ برای این به کار رفته است که نشان دهد دو عدد طرفین آن به سنجِ m_i باهم برابرند.

$$
x = \sum_i a_i M_i N_i = 2 \times 20 \times 2 + 3 \times 15 \times 3 + 4 \times 12 \times 3 = 359. \qquad (۶۹)
$$

$N_i := M_i^{-1} \ mod \ m_i$	M_i	m_i	a_i
2	$20 \equiv 2$	3	2
3	$15 \equiv 3$	4	3
3	$12 \equiv 2$	5	4

جدول ۱: جدول اعداد برای حل مثال ۱ در قضیه باقیمانده های چینی

از آنجا که $m_1m_2m_3 = 60$ نتیجه می گیریم که کوچکترین عددی که معادلات ۶۷ را حل می کند برابر است با 59.

مثال ۲: دستگاه معادلات زیر را در نظر بگیرید:

$$\begin{aligned} x &= 1 \qquad mod \ \ 3 \\ x &= 2 \qquad mod \ \ 4 \\ x &= 4 \qquad mod \ \ 5 \\ x &= 3 \qquad mod \ \ 7 \\ x &= 8 \qquad mod \ \ 11. \end{aligned} \tag{۷۰}$$

بنابراین عددی می خواهیم که باقیمانده تقسیم‌اش بر 3 ، 4 ، 5 ،7 و 11 به ترتیب برابر باشد با 1 ، 4 و 6 ، 7 و 2. اعدادی که در جدول زیر نوشته‌ایم همان اعدادی هستند که مطابق با قضیه باقیمانده های چینی بدست می آیند: اعداد N_i با استفاده از آلگوریتم اقلیدس بدست آمده‌اند. بنابراین عددِ x یعنی عددی که به دنبال آن هستیم برابر است با

$$x = \sum_i a_iM_iN_i = 1 \times 1540 \times 1 + 2 \times 1155 \times 3 + 4 \times 924 \times 4 + 3 \times 660 \times 4 + 8 \times 420 \times 6 = 51334. \tag{۷۱}$$

از انجا که $m_1m_2m_3m_4m_5 = 4620$، نتیجه می گیریم که کوچکترین عددی که معادلاتِ ۷۰ را حل می کند برابر است با 514.

درادامه به بیان یک قضیه مفید و مهم دیگر موسوم به قضیه کوچک فرما می پردازیم. نخست به یک لم ساده احتیاج داریم:

$N_i := M_i^{-1} \ mod \ m_i$	M_i	m_i	a_i
1	$1540 \equiv 1$	3	1
3	$1155 \equiv 3$	4	2
4	$924 \equiv 4$	5	4
4	$660 \equiv 2$	7	3
6	$420 \equiv 2$	11	8

جدول ۲: جدول اعداد برای حل مثال ۲ در قضیه باقیمانده های چینی

■ **لم:** فرض کنید که p یک عدد اول و k یکی از اعداد متعلق به مجموعه $\{1, 2, \cdot p-1\}$ باشد. دراین صورت $p|\begin{pmatrix} p \\ k \end{pmatrix}$.

اثبات: می دانیم که

$$p(p-1)(p-2)\cdot(p-k+2)(p-k+1) = \begin{pmatrix} p \\ k \end{pmatrix} k(k-1)(k-2)\cdots 3.2.1 \tag{۷۲}$$

حال توجه می کنیم که p طرف چپ تساوی بالا را می شمارد. پس طرف راست را نیز می بایست بشمارد. اما p نمی تواند $K :=$ $k(k-1)(k-2)\cdot 3.2.1$ را بشمارد، بنابراین ، بنابرقضیه 5.1، p می بایست $\begin{pmatrix} p \\ k \end{pmatrix}$ را بشمارد.

■ **قضیه کوچک فرما:** فرض کنید که p یک عدد اول و a هرعددصحیحی باشد. دراین صورت

$$a^p = a \quad mod \ \ p. \tag{۷۳}$$

اثبات: برای اثبات از استقرا استفاده می کنیم. می دانیم که $1^p = 1 \quad mod \ \ p$. حال فرض کنید که $a^p = a \quad mod \ \ p$. دراین صورت

$$(a+1)^p \quad = \quad \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^k$$

$$= \quad 1 + a^p \quad mod \;\; p \qquad (۷۴)$$

که درآن از لم $5.2.1$ استفاده کرده ایم. اینک از فرض استقرا استفاده می کنیم و نتیجه می گیریم که

$$(1+a)^p = 1 + a \quad mod \;\; p. \qquad (۷۵)$$

■ **تعریف:** فرض کنید که n عدد صحیح مثبتی است. $\phi(n)$ را تعداد اعدادصحیح کوچکتراز n می گیریم که نسبت به آن اول باشند. به عنوان مثال $\phi(4) = 2$ و $\phi(7) = 6$.

مسلم است که برای هر عدداول p ، داریم $\phi(p) = p - 1$. براحتی می توان ثابت کرد که به ازای هر عدد اول p و هرعدد صحیح مثبتِ α،

$$\phi(p^\alpha) = p^{\alpha-1}(p-1)$$

. در واقع تعداد اعداد کوچکتراز p^α برابر است با $p^\alpha - 1$. از این لیست اعدادِ

$$\{p(p^{\alpha-1}-1),\; p(p^{\alpha-1}-2),\; p(p^{\alpha-1}-3),\; \cdots\; p(2),\; p(1)\} \qquad (۷۶)$$

را باید کسر کنیم، زیرا این اعداد تنها اعدادی هستند که با p^α عامل مشترک دارند. بنابراین تعداد کل اعدای که نسبت به p^α اول هستند و از آن کوچکترند برابر است با $p^\alpha - 1 - (p^{\alpha-1}-1) = p^{\alpha-1}(p-1)$.

حال با استفاده از قضیه باقیمانده های چینی می توان قضیه زیررا ثابت کرد. اثبات این قضیه و قضیه بعدی را خواننده می تواند در ضمیمه کتابِ $Nielsen, Chuang$ پیدا کند.

■ **قضیه:** هرگاه a و b نسبت به هم ا ول باشند آنگاه $\phi(ab) = \phi(a)\phi(b)$.

■ **قضیه اویلر:** : فرض کنید که a نسبت به n اول است. آنگاه

$$a^{\phi(n)} = 1 \quad mod \;\; n. \qquad (۷۷)$$

مثال :

$$n \quad = \quad 5 \quad a = 2 \quad \longrightarrow \phi(5) = 4 \longrightarrow 2^4 \;\; mod \;\; 5 = 16 \;\; mod \;\; 5 = 1$$

$$n \;=\; 6 \quad a=5 \quad \longrightarrow \phi(6)=2 \longrightarrow 5^2 \ \ mod\ \ 6 = 25\ \ mod\ \ 6 = 1 \tag{۷۸}$$

۳.۵ کسرهای مسلسل

- تمامی این قسمت شامل استدلال ها، روابط و قضایا و اثبات آنها توسط آقای مرتضی مرادی دانشجوی این درس در نیمسال اول ۹۷ تدوین شده و خود ایشان نیز زحمت تایپ آن را به عهده داشته اند.

میخواهیم روش پیدا کردن $\frac{m}{r}$ را با توجه به $\frac{K}{Q}$ بیان کنیم. برای این کار ابتدا باید کسر مسلسل $\frac{K}{Q}$ را بصورت مقابل بنویسیم:

$$\frac{K}{Q} = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \tag{۷۹}$$

ثابت میکنیم که هر عدد گویا مثل $\frac{b_1}{b_0} < 1$ را میتوان بصورت یک کسر مسلسل متناهی مانند

$$\frac{b_1}{b_0} = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \tag{۸۰}$$

نوشت که تعداد کسرهای مسلسل آن (یعنی عدد n) کمتر از $2\log_2^{b_0}$ است. برای اینکار کافیست عدد b_0 را بر عدد b_1 تقسیم کنیم تا خارج قسمت a_0 و باقیمانده b_2 بدست بیاید. به همین ترتیب عدد b_1 را بر عدد b_2 تقسیم کنیم تا خارج قسمت a_1 باقیمانده b_3 بدست بیاید و ...

$b_0 = b_1 a_0 + b_2; b_1 > b_2$

$b_1 = b_2 a_1 + b_3; b_2 > b_3$

$b_2 = b_3 a_2 + b_4; b_3 > b_4$

:

$b_{n-1} = b_n a_{n-1} + 1; b_n := a_n \geq 2$

پس میتوان کسر مسلسل $\frac{b_1}{b_0}$ را به شکل مقابل نوشت :

$$\frac{b_1}{b_0} = \frac{1}{\frac{b_0}{b_1}} = \frac{1}{\frac{b_1 a_0+b_2}{b_1}} = \frac{1}{a_0+\frac{b_2}{b_1}} = \frac{1}{a_0+\frac{1}{\frac{b_1}{b_2}}} = \frac{1}{a_0+\frac{1}{\frac{b_2 a_1+b_3}{b_2}}} = \frac{1}{a_0+\frac{1}{a_1+\frac{b_3}{b_2}}} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\frac{b_2}{b_3}}}} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\frac{b_3 a_2+b_4}{b_3}}}} =$$
$$\frac{1}{a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{b_4}{b_3}}}} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{1}{\ddots+\frac{1}{a_n}}}}}$$

ابتدا ثابت می کنیم $n < 2\log_2^{b_0}$ که به سادگی قابل اثبات است :

$$b_0 = b_1 a_0 + b_2 \geq b_1 + b_2 > 2b_2$$

$$b_2 = b_3 a_2 + b_4 \geq b_3 + b_4 > 2b_4$$

$$\vdots$$

$$b_{2k-2} = b_{2k-1} a_{2k-2} + b_{2k} \geq b_{2k-1} + b_{2k} > 2b_{2k}$$

$$\vdots$$

$$b_{2\lfloor\frac{n}{2}\rfloor} = b_{2\lfloor\frac{n}{2}\rfloor+1} a_{2\lfloor\frac{n}{2}\rfloor} + 1 \geq 1(n = even)or2(n = odd)$$

$$\Rightarrow b_0 > 2b_2 > 2^2 b_4 > 2^3 b_6 > \cdots > 2^k b_{2k} > \cdots > 2^{\lfloor\frac{n}{2}\rfloor} b_{2\lfloor\frac{n}{2}\rfloor} \geq 2^{\frac{n}{2}}$$

$$\Rightarrow \log_2^{b_0} > \frac{n}{2} \to 2log_2^{b_0} > n$$

اکنون که دیدیم کسر مسلسل عدد $\frac{K}{Q}$ را با کمتر از $2\log_2^Q$ مرحله تقسیم متوالی میتوان نوشت ، پس به روش پیدا کردن کسر $\frac{m}{r}$ از روی کسر مسلسل عدد $\frac{K}{Q}$ میپردازیم. به این صورت که اگر

$$\frac{K}{Q} = \frac{1}{a_0 + \frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_{n-1}+\frac{1}{a_n}}}}} \tag{۸۱}$$

باشد ، آخرین جمله از این کسر مسلسل را حذف میکنیم و با محاسبه کسر مسلسل جدید و بازگرداندن آن و ساده کردن صورت و مخرج (تا حد امکان) ، عدد بدست آمده همان $\frac{m}{r}$ است (که بنا به تعریف m و r نسبت به هم اول هستند):

$$\frac{m}{r} = \frac{1}{a_0 + \frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_{n-1}}}}} \tag{۸۲}$$

برای اثبات این ادعا باید ثابت کنیم :

$$|\frac{K}{Q} - \frac{m}{r}| < \frac{1}{2Q} \tag{۸۳}$$

که این موضوع را به کمک استقراء روی تعداد کسرهای مسلسل (یعنی عدد n) ثابت میکنیم .

چنانچه فرض کنیم $Q = N^2$ باشد نیز نتیجه می شود $(K,Q) = 1$. چرا که اگر این دو عدد نسبت به هم اول نباشند ، با توجه به اینکه هدف ما پیدا کردن عوامل عدد N است ، با محاسبه ب م م K و Q عوامل عدد N بدست می آید.

ـ پایه استقراء :

$n = 1:$

$\frac{K}{Q} = \frac{1}{a_0+\frac{1}{a_1}} = \frac{a_1}{a_0a_1+1}; (K,Q) = 1 \Rightarrow a_0a_1 + 1 \geq Q$

$\frac{m}{r} = \frac{1}{a_0}; (m,r) = 1 \Rightarrow a_0 = r \geq 2$

$\Rightarrow |\frac{K}{Q} - \frac{m}{r}| = |\frac{1}{a_0+\frac{1}{a_1}} - \frac{1}{a_0}| = \frac{1}{a_0(a_0a_1+1)} \leq \frac{1}{2Q}$

اینکه فرض کردیم $r \geq 2$ است ، به این دلیل است که اگر $a_0 = r = 1$ باشد ، در این صورت

$\frac{K}{Q} = \frac{1}{1+\frac{1}{a_1}} = \frac{a_1}{a_1+1} = \frac{Q-1}{Q} = 1 - \frac{1}{Q}$

خواهد شد . حال به سادگی میتوان نشان داد که برای این $\frac{K}{Q} = 1 - \frac{1}{Q}$ هیچ کسری مانند $\frac{p}{q} < 1$ وجود ندارد که $|\frac{K}{Q} - \frac{p}{q}| < \frac{1}{2Q}$ و $q \leq \sqrt{Q}$ باشد :

$\frac{p}{q} < 1, q \leq \sqrt{Q} \Rightarrow \frac{q-p}{q} \geq \frac{1}{q} \geq \frac{1}{\sqrt{Q}} \Rightarrow -\frac{p}{q} \geq \frac{1}{\sqrt{Q}}-1 \Rightarrow \frac{K}{Q}-\frac{p}{q} \geq (\frac{K}{Q})+(\frac{1}{\sqrt{Q}}-1) = (1-\frac{1}{Q})+(\frac{1}{\sqrt{Q}}-1) = \frac{\sqrt{Q}-1}{Q} > \frac{1}{2Q}$

پس چون $|\frac{K}{Q} - \frac{p}{q}| > \frac{1}{2Q}$ است ، یعنی در حالت $r = 1$ ، K ی خوب نداریم و در نتیجه حالت r=۱ در پایه استقراء رخ نمیدهد.

ـ فرض استقراء :

$n = k :\Rightarrow \frac{K}{Q} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_{k-1}+\frac{1}{a_k}}}}}; \frac{m}{r} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_{k-1}}}}} \Rightarrow\Rightarrow |\frac{K}{Q} - \frac{m}{r}| < \frac{1}{2Q}$

یعنی برای هر کسر $\frac{K}{Q}$ که کسر مسلسل آن از مرتبه k است ، تفاضل کسر $\frac{m}{r}$ (که از حذف جمله آخر کسر $\frac{K}{Q}$ بدست می آید) با کسر $\frac{K}{Q}$ کمتر از $\frac{1}{2Q}$ است.

ـ حکم استقراء :

$n = k+1 \Rightarrow \frac{K}{Q} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_k+\frac{1}{a_{k+1}}}}}}; \frac{m}{r} = \frac{1}{a_0+\frac{1}{a_1+\frac{1}{\ddots+\frac{1}{a_k}}}} \Rightarrow^{?}\Rightarrow |\frac{K}{Q} - \frac{m}{r}| < \frac{1}{2Q}$

برای اثبات حکم استقراء ابتدا عدد Q را بر عدد K تقسیم کنیم تا خارج قسمت a_0 و باقیمانده $K^{'}$ بدست بیاید. همچنین عدد r را بر عدد m تقسیم کنیم تا خارج قسمت a_0 و باقیمانده $m^{'}$ بدست بیاید. در این صورت میتوان نوشت :

$$Q = Ka_0 + K^{'} \Rightarrow \frac{K}{Q} = \frac{K}{Ka_0+K^{'}} = \frac{1}{\frac{Ka_0+K^{'}}{K}} = \frac{1}{a_0+\frac{K^{'}}{K}} = \cfrac{1}{a_0+\cfrac{1}{a_1+\cfrac{1}{\ddots+\cfrac{1}{a_k+\cfrac{1}{a_{k+1}}}}}}$$

$$r = ma_0 + m^{'} \Rightarrow \frac{m}{r} = \frac{m}{ma_0+m^{'}} = \frac{1}{\frac{ma_0+m^{'}}{m}} = \frac{1}{a_0+\frac{m^{'}}{m}} = \cfrac{1}{a_0+\cfrac{1}{a_1+\cfrac{1}{\ddots+\cfrac{1}{a_k}}}}$$

با توجه به روابط اخیر داریم :

$$\frac{K^{'}}{K} = \cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots+\cfrac{1}{a_k+\cfrac{1}{a_{k+1}}}}}}; \qquad \frac{m^{'}}{m} = \cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots+\cfrac{1}{a_k}}}} \tag{۸۴}$$

پس با استفاده از فرض استقراء برای $\frac{K^{'}}{K}$ که کسر مسلسل آن از مرتبه k است میتوان نوشت :

$$|\frac{K^{'}}{K} - \frac{m^{'}}{m}| < \frac{1}{2K} \Rightarrow |mK^{'} - m^{'}K| < \frac{m}{2}$$

اکنون به کمک نتیجه اخیر حکم استقراء را ثابت میکنیم:

$$|\frac{K}{Q} - \frac{m}{r}| = |\frac{K}{Ka_0+K^{'}} - \frac{m}{ma_0+m^{'}}| = |\frac{K(ma_0+k^{'})-m(Ka_0+K^{'})}{(Ka_0+K^{'})(ma_0+m^{'})}| = |\frac{Km^{'}-mK^{'}}{(Ka_0+K^{'})(ma_0+m^{'})}| = \frac{|mK^{'}-m^{'}K|}{Q(ma_0+m^{'})} < \frac{(\frac{m}{2})}{Q(ma_0+m^{'})} < \frac{1}{2Q}$$

پس با استفاده از استقراء ثابت شد که $\frac{m}{r}$ بدست آمده از روی کسر مسلسل $\frac{K}{Q}$ در رابطه ی $|\frac{K}{Q} - \frac{m}{r}| < \frac{1}{2Q}$ صدق می کند . در نتیجه با کمتر از $2log_2^Q$ مرتبه تقسیم متوالیِ عدد Q میتوانیم برای K های خوب عدد r را بدست بیاوریم.