# درس یازدهم : آلگوریتم شر

## 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 [1] 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.

## 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:

$$x^2 = 1 \quad mod \ \ N. \tag{1}$$

منظور از جواب غیر بدیهی این است که

$$x \neq 1, -1 \quad mod\ N, \ \text{یا} \quad x - 1 \neq kN, \ x = 1 \neq kN \tag{2}$$

دراین صورت می توانیم بنویسم

$$x^2 - 1 = 0 \quad mod \ \ N, \text{یا} \quad (x-1)(x+1) = kN \tag{3}$$

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

$$x^2 = 16 = 1 \ \ mod \ \ 15. \tag{4}$$

[1] Peter Shor

ضمناً $x-1=3$ و $x+1=5$ مضرب هایی از 15 نیستند. از رابطه بالا نتیجه می گیریم که 15 حاصلضرب $3\times 5$ 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

$$x^2 = 576 = 1 \;\; mod \;\; 115. \tag{5}$$

ضمناً $x-1=23$ و $x+1=25$ مضرب هایی از 115 نیستند. از رابطه بالا نتیجه می گیریم که 115 حاصلضرب $23\times 25$ 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 دلخواه ِکوچک تر یا بزرگ تر از $N$ باشد.

پس از این کار براحتی می توانیم عامل مشترک ِ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.
برای حل این مسئله به ترتیب زیر اقدام می کنیم. عددی دلخواه مثل $Y$ در نظر می گیریم. می گوییم رتبه این عدد به سنج ِ$N$ برابر با $r$ است هرگاه $r$ کوچکترین عدد صحیح غیر صفری باشد که در رابطه زیر صدق کند:

$$Y^r = 1 \quad mod \quad N. \tag{6}$$

**قضیه:** هرگاه $Y$ نسبت به $N$ اول باشد، آنگاه $r\le N$ .

**اثبات:** مجموعه اعدادِ $S=\{Y^1, Y^2, Y^3, \cdots Y^{N-1}, Y^N\}$ را تشکیل می دهیم که در آن همه توانها به سنج ِ$N$ 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 $N$ عضو متمایز است که همگی ِاز $N$ کوچکترند. بنابرین عناصر مجموعه‌ی $S$ تناظر یک به یک دارند با مجموعه‌ی $\{0,1,2,\cdots N-1\}$. یعنی اینکه حتماً یکی از اعضای $S$ برابر با ۱ است و این به این معناست که مرتبه $Y$ از $N$ کوچکتراست.

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 ۱/۲. 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. این رتبه را با $r=2k$ نشان می دهیم. در نتیجه خواهیم داشت

$$Y^{2k} = 1 \quad mod \quad N, \longrightarrow X = Y^k, \quad X^2 = 1 \quad modN. \tag{7}$$

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

$$f(x) = Y^x \quad mod \;\; N \tag{8}$$

آنگاه

$$f(x+r) = f(x), \longrightarrow f(x+jr) = f(x) \quad j = 1, 2, 3, \cdots . \tag{9}$$

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

$$|\psi_0\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |\overline{0}\rangle. \tag{10}$$

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

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |Y^l \ \ mod \ \ N\rangle. \tag{11}$$

**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

$$|\phi\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |l_0 + jr\rangle \tag{12}$$

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:

$$U|k\rangle = \frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} e^{\frac{2\pi ikl}{Q}} |l\rangle. \tag{13}$$

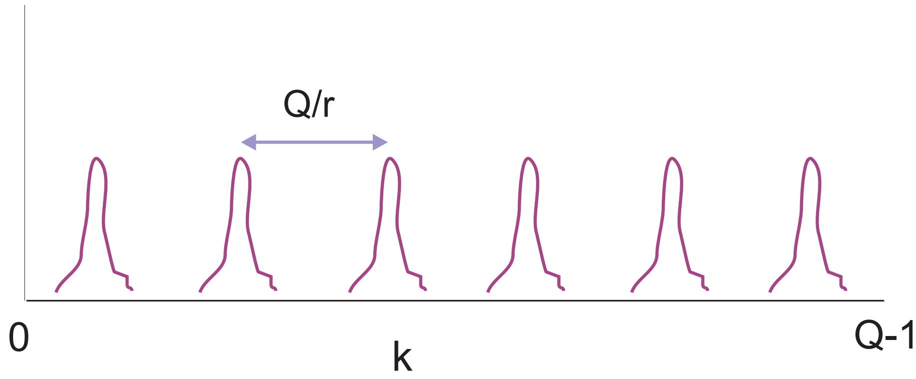
پس ازتبدیل فوریه حالت $|\phi\rangle$ به حالت زیر تبدیل می شود:

$$|\phi'\rangle = \frac{1}{\sqrt{A}} \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sum_{j=0}^{A-1} e^{\frac{2\pi ik(l_0+jr)}{Q}} |k\rangle \tag{14}$$

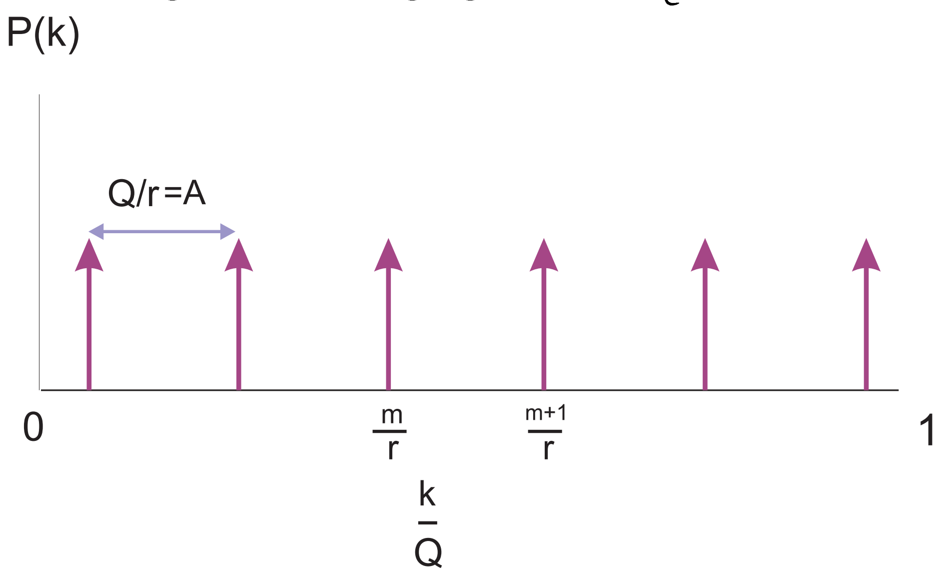
**مرحله پنج :** حال ثبت کننده اول را اندازه می گیریم. احتمال اینکه دراین اندازه گیری مقدار $k$ بدست آید برابراست با:

$$\begin{aligned} P(k) &= \frac{1}{QA} \mid \sum_{j=0}^{A-1} e^{\frac{2\pi ik(jr+l_0)}{Q}} \mid^2 \\ &= \frac{1}{QA} \mid \sum_{j=0}^{A-1} e^{\frac{2\pi ikjr}{Q}} \mid^2 \\ &= \frac{1}{QA} \mid \frac{1 - e^{\frac{2\pi ikrA}{Q}}}{1 - e^{\frac{2\pi ikr}{Q}}} \mid^2 = \frac{1}{QA} \mid \frac{\sin \frac{\pi krA}{Q}}{\sin \frac{\pi kr}{Q}} \mid^2 . \end{aligned} \tag{15}$$

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 ۱.




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




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

**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 $\frac{Q}{r} = A$ و درنتیجه از رابطه 15 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:

$$P(k) = \frac{1}{r}\delta_{\frac{k}{Q},\frac{m}{r}}. \tag{16}$$

تابع $P(k)$ دراین حالت مطابق شکل ۲ است. این رابطه بیان می کند که دراین حالت هربارکه ثبت کننده اول را اندازه بگیریم عددی بدست 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 $100\times\frac{1}{ln\ \ r}$ 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 ۲ 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

$$|\ \frac{k}{Q}-\frac{m}{r}\ |<\frac{1}{2Q} \tag{17}$$

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. 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.

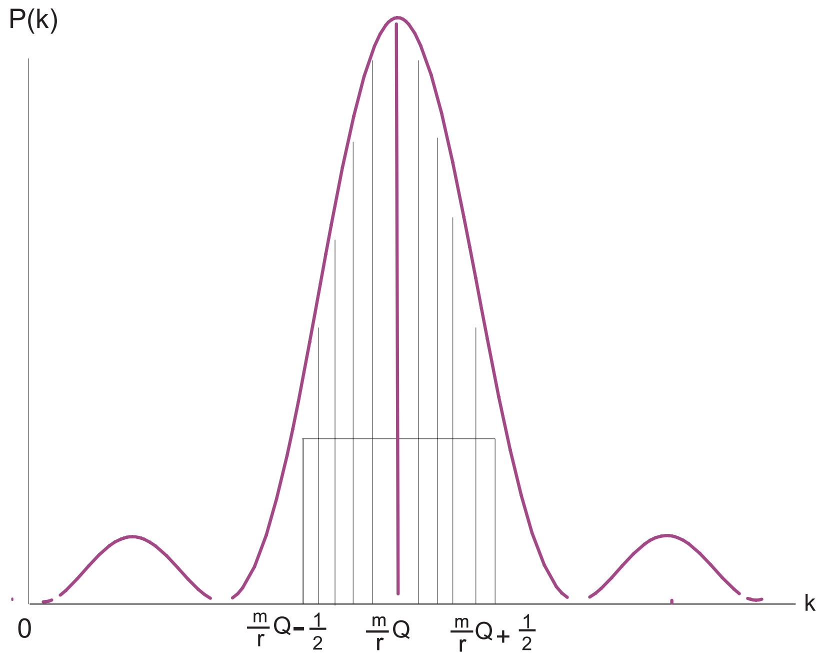
**قضیه :** اگر $Q$ به اندازه کافی بزرگ باشد، کسر $\frac{k}{Q}$ را تنها به یک صورت می توان به صورت کسری با مخرج کوچکتراز $N$ ساده کرد. اگر این کسر را به صورت $\frac{m}{r}$ بنویسیم، $r$ همان دوره تناوب خواهد بود. (یادآوری می کنیم که $r$ از $N$ کوچکتراست. )

اثبات : فرض کنید که علاوه بر کسر $\frac{m}{r}$ ، کسر $\frac{m'}{r'}$ نیز درشرط 17 صدق کند، یعنی داریم :

$$|\ \frac{k}{Q}-\frac{m'}{r'}\ |<\frac{1}{2Q} \tag{18}$$

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

$$|\ \frac{m}{r}-\frac{m'}{r'}\ |<\frac{1}{Q} \tag{19}$$




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.

از طرفی می دانیم که

$$|\frac{m}{r}-\frac{m'}{r'}|=|\frac{mr'-m'r}{rr'}\geq\frac{1}{N^2} \tag{20}$$

20 و 19 به این نتیجه می رسیم که اگر $Q$ را از $N^2$ بزرگتر انتخاب کنیم این اتفاق یعنی وجود دوکسر با مخرج کوچکتراز $N$ 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 $P(k)=\frac{1}{QA}\mid\frac{\sin\frac{\pi krA}{Q}}{\sin\frac{\pi kr}{Q}}\mid^2$ در اطراف یکی از نقطه ها مثلاً نقطه $k=\frac{Q}{r}$ نگاه می کنیم. در شکل ۳ 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:

$$2\times\frac{1}{2}\times P(k=\frac{mQ}{r}+\frac{1}{2})=P(k=\frac{1}{2})=\frac{1}{QA}(\frac{\sin\frac{\pi rA}{2Q}}{\sin\frac{\pi r}{2Q}})^2 \tag{21}$$

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

$$\frac{4}{\pi^2}\frac{1}{r}. \tag{22}$$

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 آلگوریتم 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 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:

$$U|k\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{-2\pi ikl}{N}}|l\rangle. \tag{23}$$

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

$$\langle k|U|f\rangle = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}}\langle l|f\rangle, \tag{24}$$

ویا

$$\tilde{f}_k = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}} f_l. \tag{25}$$

## 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:

$$U|a\rangle = \frac{1}{\sqrt{N}} \sum_b e^{\frac{2\pi i ab}{N}} |b\rangle, \quad a, \ \ b \in Z_N. \tag{26}$$

می دانیم که

$$\begin{aligned} a &= (a_1, a_2, a_3, \cdots a_m) = a_1 \times 2^{m-1} + a_2 \times 2^{m-2} + \cdots a_m \times 2^0, \\ b &= (b_1, b_2, b_3, \cdots b_m) = b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + \cdots b_m \times 2^0. \end{aligned} \tag{27}$$

بنابراین

$$\begin{aligned} U|a\rangle &= \frac{1}{\sqrt{2^m}} \sum_b e^{\frac{2\pi i a}{2^m}\left[b_1 \times 2^{m-1} + b_2 \times 2^{m-2} + \cdots b_m \times 2^0\right]} |b\rangle \\ &= \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a b_1}{2}} |b_1\rangle\right) \left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i a b_2}{2^2}} |b_2\rangle\right) \cdots \left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i a b_m}{2^m}} |b_m\rangle\right) \end{aligned} \tag{28}$$

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

$$U|a\rangle = \left(\frac{1}{\sqrt{2}} \sum_{b_1} e^{\frac{2\pi i a_m b_1}{2}} |b_1\rangle\right) \left(\frac{1}{\sqrt{2}} \sum_{b_2} e^{\frac{2\pi i (2a_{m-1} + a_m) b_2}{2^2}} |b_2\rangle\right) \cdots \left(\frac{1}{\sqrt{2}} \sum_{b_m} e^{\frac{2\pi i (2^{m-1} a_1 + \cdots 2a_0) b_m}{2^m}} |b_m\rangle\right) \tag{29}$$

بنابراین می توانیم بنویسیم

$$U|a\rangle = |\phi_1\rangle|\phi_2\rangle \cdots |\phi_m\rangle, \tag{30}$$

که درآن

$$\begin{aligned} |\phi_1\rangle &:= \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2\pi i a_m}{2}} |1\rangle\right], \\ |\phi_2\rangle &:= \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2\pi i (2a_{m-1} + a_m)}{2^2}} |1\rangle\right], \\ &\cdots \\ &\cdots \end{aligned} \tag{31}$$

حال یک مدارکوانتومی معرفی می کنیم که تبدیل فوریه کوانتومی را انجام دهد. نخست عملگرهای یک کیوبیتی زیر را معرفی می کنیم:

$$R_k(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i\alpha}{2^k}} \end{pmatrix}. \tag{32}$$

خواننده براحتی می تواند نشان دهد که تساوی های زیربرقرارهستند:

$$\begin{aligned}
|\phi_1\rangle &= H|a_m\rangle \\
|\phi_2\rangle &= R_2(a_m)H|a_{m-1}\rangle \\
|\phi_3\rangle &= R_2(a_{m-1})R_3(a_m)H|a_{m-2}\rangle \\
|\phi_4\rangle &= R_2(a_{m-2})R_3(a_{m-1})R_4(a_m)H|a_{m-3}\rangle \\
\cdots & \quad \cdots \\
\cdots & \quad \cdots
\end{aligned} \tag{33}$$

هرکدام از عملگرهای $R_k(\alpha)$ در واقع به صورت یک عملگر کنترلی عمل می کنند که اگر مقدارِ $\alpha$ برابر با صفر باشد، هیچ کاری انجام نمی دهند واگر مقدارِ $\alpha$ برابر با $1$ باشد، عملِ $R_k$ 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.

# 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 $a \nmid b$.

بنابراین $5 \mid 115$ و $8 \nmid 6$.

**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:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{34}$$

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

$$[i] = \{i, i + n, i + 2n, i + 3n, \cdots\}. \tag{35}$$

تعداد کلاس ها برابر است با $n$. یعنی

$$[0] = \{0,\ n,\ 2n,\ 3n, \cdots\}$$
$$[1] = \{1,\ 1 + n,\ 1 + 2n,\ 1 + 3n, \cdots\}$$

$$[2]=\{2,\ 2+n,\ 2+2n,\ 2+3n,\cdots\}$$
$$\cdots$$
$$[n-1]=\{n-1,\ n-1+n,\ n-1+2n,\ n-1+3n,\cdots\}. \tag{36}$$

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 در$Z_n$ داریم :

$$[a]+[b]:=[a+b] \tag{37}$$

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 صورت $Z_n=\{0,\ 1,\ 2,\cdots n-1\}$ 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 $gcd(a,b)\geq r$. 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 :

$$gcd(a,b)=xa+yb \qquad x,\ y\in Z. \tag{38}$$

**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

$$s\leq gcd(a,b) \qquad , \qquad gcd(a,b)\leq s \tag{39}$$

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

$$gcd(a,b)|a \qquad , \qquad gcd(a,b)|b \tag{40}$$

درنتیجه با توجه به قضیه ۱.۵، $gcd(a,b)|xa+yb$ و یا $gcd(a,b)|s$ که نتیجه می دهد

$$gcd(a,b) \leq s. \tag{41}$$

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

$$s \leq gcd(a,b). \tag{42}$$

بنابراین هرگاه صحت رابطه اخیررانشان 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

$$a = ks + r, \tag{43}$$

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

$$r = a - ks \longrightarrow r = a - k(xa + yb) = (1 - kx)a - kyb \tag{44}$$

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

$$ba = 1 + kn \qquad , \qquad b'a = 1 + k'n \tag{45}$$

که از آن بدست می آوریم

$$(b-b')a=(k-k')n \longrightarrow b-b' \equiv 0 \ mod \ n \longrightarrow b=b' \ mod \ n. \tag{46}$$

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

$$gcd(a,b)=gcd(b,r). \tag{47}$$

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

$$m|b \quad , \quad m|a \ (since \ \ a=kb+r) \longrightarrow m \leq gcd(a,b)=M. \tag{48}$$

از طرف دیگر می دانیم که

$$M|b \quad , \quad M|r \ (since \ \ r=a-kb) \longrightarrow M \leq gcd(b,r)=m. \tag{49}$$

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

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

۳ $-$ $r_1$ 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:** $M := gcd(128, 62)$

$$\begin{aligned} 128 &= 2 \times 62 + 4 \longrightarrow M = gcd(62, 4) \\ 62 &= 15 \times 4 + 2 \longrightarrow M = gcd(4, 2) = 2. \end{aligned} \tag{50}$$

**مثال دو:** $M := gcd(150, 66)$

$$\begin{aligned} 150 &= 2 \times 66 + 18 \longrightarrow M = gcd(66, 18) \\ 66 &= 3 \times 18 + 12 \longrightarrow M = gcd(18, 12) \\ 18 &= 1 \times 12 + 6 \longrightarrow M = gcd(12, 6) = 6. \end{aligned} \tag{51}$$

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:**

$$\begin{aligned} 2 &= 62 - 15 \times 4 \\ &= 62 - 15 \times (128 - 2 \times 62) \\ &= 31 \times 62 - 15 \times 128. \end{aligned} \tag{52}$$

**مثال دو:**

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (66 - 3 \times 18) \\ &= 4 \times 18 - 66 = 4 \times (150 - 2 \times 66) - 66 \\ &= 4 \times 150 - 9 \times 66. \end{aligned} \tag{53}$$

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 $1=xa+yb$ صدق کنند. درنتیجه خواهیم داشت

$$xa = 1 - yn \longrightarrow x = a^{-1}\ mod\ n. \tag{54}$$

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

$$ax + b = c\ \ mod\ n \tag{55}$$

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

$$ax = c - b\ \ mod\ n \longrightarrow x = a^{-1}(c-b)\ \ mod\ n. \tag{56}$$

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:**[2] 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

$$\begin{aligned} x &= a_1\ \ mod\ m_1 \\ x &= a_2\ \ mod\ m_2 \\ x &= a_3\ \ mod\ m_3 \\ \cdots &= \cdots \\ x &= a_n\ \ mod\ m_n \end{aligned} \tag{57}$$

دارای یک جواب یکتا به سنج $M = m_1 m_2 m_3 \cdots m_n$ 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. درنیتجه داریم

$$M_i N_i = 1\ \ mod\ m_i \tag{58}$$

حال قرار می دهیم

$$x := \sum_i a_i M_i N_i \tag{59}$$

[2] Chineese Reminder Theorem

براحتی دیده می شود که روابط زیر برقراند:

$$\begin{aligned} M_iN_i &= 1 \ \ mod\ m_i \\ M_iN_i &= 0 \ \ mod\ m_j \end{aligned} \tag{60}$$

درنتیجه این دو رابطه خواهیم داشت:

$$x = a_i \quad mod\ m_i \ \ \forall i \tag{61}$$

به این ترتیب $x$ یک حل از دستگاه معادلات (57) 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

$$\begin{aligned} x - x' &= k_1m_1 \\ x - x' &= k_2m_2 \\ x - x' &= k_3m_3 \\ \cdots &= \cdots \\ x - x' &= k_nm_n. \end{aligned} \tag{62}$$

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:

$$\begin{aligned} x &= 2 \qquad mod\ \ 3 \\ x &= 3 \qquad mod\ \ 4 \\ x &= 4 \qquad mod\ \ 5. \end{aligned} \tag{63}$$

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 $N_iM_i = 1 + km_i$ صدق کند. اما می دانیم که می توانیم هر مضربی از $m_i$ را از $M_i$ کم کنیم بدون اینکه عددِ$N_i$ تغییر کند، زیرا از رابطه قبلی بدست می آوریم که $N_i(M_i - lm_i) = 1 + (k - l)m_i$ به عبارت دیگر

$$M_i^{-1} \quad mod \ \ m_i = (M_i - lm_i)^{-1} \quad mod \ \ m_i. \tag{64}$$

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

جدول اعداد برای حل مثال ۱ در قضیه باقیمانده های چینی :1

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.

$$x = \sum_i a_i M_i N_i = 2 \times 20 \times 2 + 3 \times 15 \times 3 + 4 \times 12 \times 3 = 359. \tag{65}$$

از آنجا که $m_1 m_2 m_3 = 60$ نتیجه می گیریم که کوچکترین عددی که معادلات 63 را حل می کند برابر است با 59.

**مثال ۲:** دستگاه معادلات زیر را در نظر بگیرید:

$$\begin{aligned} x &= 1 \qquad mod \ \ 3 \\ x &= 2 \qquad mod \ \ 4 \\ x &= 4 \qquad mod \ \ 5 \\ x &= 3 \qquad mod \ \ 7 \\ x &= 8 \qquad mod \ \ 11. \end{aligned} \tag{66}$$

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

$$x = \sum_i a_i M_i N_i = 1 \times 1540 \times 1 + 2 \times 1155 \times 3 + 4 \times 924 \times 4 + 3 \times 660 \times 4 + 8 \times 420 \times 6 = 51334. \tag{67}$$

از انجا که $m_1 m_2 m_3 m_4 m_5 = 4620$، نتیجه می گیریم که کوچکترین عددی که معادلاتِ 66 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:

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

**اثبات:** می دانیم که

$$p(p-1)(p-2) \cdot (p-k+2)(p-k+1) = \left(\begin{array}{c} p \\ k \end{array}\right) k(k-1)(k-2) \cdots 3.2.1 \tag{68}$$

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

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

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 ۱.۵، $p$ 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

$$a^p = a \quad mod \;\; p. \tag{69}$$

**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

$$\begin{aligned} (a+1)^p &= \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^k \\ &= 1 + a^p \quad mod \;\; p \end{aligned} \tag{70}$$

که درآن از لم ۱.۲.۵ استفاده کرده ایم. اینک از فرض استقرا استفاده می کنیم و نتیجه می گیریم که

$$(1+a)^p = 1 + a \quad mod \;\; p. \tag{71}$$

**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 $\alpha$،

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

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

$$\{p(p^{\alpha-1}-1),\; p(p^{\alpha-1}-2),\; p(p^{\alpha-1}-3),\; \cdots\; p(2),\; p(1)\} \tag{72}$$

را باید کسر کنیم، زیرا این اعداد تنها اعدادی هستند که با $p^\alpha$ عامل مشترک دارند. بنابراین تعداد کل اعدای که نسبت به $p^\alpha$ 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

$$a^{\phi(n)} = 1 \quad mod \;\; n. \tag{73}$$

مثال :

$$\begin{aligned} n &= 5 \quad a = 2 \quad \longrightarrow \phi(5) = 4 \longrightarrow 2^4 \;\; mod \;\; 5 = 16 \;\; mod \;\; 5 = 1 \\ n &= 6 \quad a = 5 \quad \longrightarrow \phi(6) = 2 \longrightarrow 5^2 \;\; mod \;\; 6 = 25 \;\; mod \;\; 6 = 1 \end{aligned} \tag{74}$$