ضمیمه ۱ : مقدمه ای برنظریه اعداد

هدف ما دراین فصل آشنا 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 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:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1}$$

که درآن p_i ها اعداد اول هستند.

۲ 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

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

تعداد کلاس ها برابر است با n. یعنی

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

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 :

$$[a] + [b] := [a+b] \tag{4}$$

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 سنج 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 :

$$gcd(a,b) = xa + yb \qquad x,\ y \in Z. \tag{5}$$

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

$$s \leq gcd(a,b) \qquad , \qquad gcd(a,b) \leq s \tag{6}$$

و ازآنجا مطابق با قضیه ۱ نتیجه خواهیم گرفت که $gcd(a,b) = s$. برای این کارتوجه می کنیم که بنابرتعریف بزرگترین مقسوم علیه مشترک

$$gcd(a,b)|a \qquad , \qquad gcd(a,b)|b \tag{7}$$

درنتیجه با توجه به قضیه ۱، $gcd(a,b)|xa + yb$ و یا $gcd(a,b)|s$ که نتیجه می دهد

$$gcd(a,b) \leq s. \tag{8}$$

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

$$s \leq gcd(a,b). \tag{9}$$

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

$$a = ks + r, \tag{10}$$

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

$$r = a - ks \longrightarrow r = a - k(xa + yb) = (1 - kx)a - kyb \tag{11}$$

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

$$ba = 1 + kn \qquad , \qquad b'a = 1 + k'n \tag{12}$$

که از آن بدست می آوریم

$$(b - b')a = (k - k')n \longrightarrow b - b' \equiv 0 \ mod \ n \longrightarrow b = b' \ mod \ n. \tag{13}$$

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

$$gcd(a,b) = gcd(b,r). \tag{14}$$

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

$$m|b \quad , \quad m|a \ (since \ \ a = kb + r) \longrightarrow m \leq gcd(a,b) = M. \tag{15}$$

از طرف دیگر می دانیم که

$$M|b \quad , \quad M|r \ (since \ \ r = a - kb) \longrightarrow M \leq gcd(b, r) = m. \tag{16}$$

بنابراین $m = M$.

۱.۲ 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: $M := gcd(128, 62)$

$$\begin{aligned} 128 &= 2 \times 62 + 4 \longrightarrow M = gcd(62, 4) \\ 62 &= 15 \times 4 + 2 \longrightarrow M = gcd(4, 2) = 2. \end{aligned} \tag{17}$$

مثال دو: $M := gcd(150, 66)$

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

$$18 \quad = \quad 1 \times 12 + 6 \longrightarrow M = gcd(12, 6) = 2. \tag{18}$$

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:

$$\begin{aligned} 2 &= 62 - 15 \times 4 \\ &= 62 - 15 \times (128 - 2 \times 62) \\ &= 31 \times 62 - 15 \times 128. \end{aligned} \tag{19}$$

مثال دو:

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (66 - 3 \times 18) \\ &= 4 \times 18 - 66 = 4 \times (150 - 2 \times 66) - 66 \\ &= 4 \times 150 - 9 \times 66. \end{aligned} \tag{20}$$

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

$$xa = 1 - yn \longrightarrow x = a^{-1} \ mod \ n. \tag{21}$$

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

$$ax + b = c \ \ mod \ n \tag{22}$$

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

$$ax = c - b \ \ mod \ n \longrightarrow x = a^{-1}(c - b) \ \ mod \ n. \tag{23}$$

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 $Chineese\ Reminder\ Theorem$: **فرض کنید که اعداد** $m_1, m_2, \cdots m_n$ **اعداد صحیح مثبت باشند و** $gcd(m_i, m_j) = 1 \quad \forall i, j$. **دراین صورت دستگاه معادلات**

$$\begin{aligned} x &= a_1 \ \ mod\, m_1 \\ x &= a_2 \ \ mod\, m_2 \\ x &= a_3 \ \ mod\, m_3 \\ \cdots &= \cdots \\ x &= a_n \ \ mod\, m_n \end{aligned} \tag{24}$$

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**

$$M_i N_i = 1 \ \ mod\, m_i \tag{25}$$

حال قرار می دهیم

$$x := \sum_i a_i M_i N_i \tag{26}$$

براحتی دیده می شود که روابط زیر برقراند:

$$\begin{aligned} M_i N_i &= 1 \ \ mod\, m_i \\ M_i N_i &= 0 \ \ mod\, m_j \end{aligned} \tag{27}$$

درنتیجه این دو رابطه خواهیم داشت:

$$x = a_i \quad mod\, m_i \ \ \forall i \tag{28}$$

به این ترتیب x **یک حل از دستگاه معادلات** (24) **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

$$x - x' = k_1 m_1$$

$$\begin{aligned} x - x' &= k_2 m_2 \\ x - x' &= k_3 m_3 \\ \cdots &= \cdots \\ x - x' &= k_n m_n \end{aligned} \tag{29}$$

که از آن بدست می آوریم $x - x' = kM$ و این همان چیزی بود که می خواستیم ثابت کنیم یعنی این که هردوجوابی از این دستگاه به سنج M بایکدیگر مساوی هستند.

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 $p| \begin{pmatrix} p \\ k \end{pmatrix}$.

اثبات: می دانیم که

$$p(p-1)(p-2)\cdot(p-k+2)(p-k+1) = \begin{pmatrix} p \\ k \end{pmatrix} k(k-1)(k-2)\cdots 3.2.1 \tag{30}$$

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، 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

$$a^p = a \mod p. \tag{31}$$

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

$$\begin{aligned} (a+1)^p &= \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^k \\ &= 1 + a^p \mod p \end{aligned} \tag{32}$$

که درآن از لم ۱.۲ استفاده کرده ایم. اینک از فرض استقرا استفاده می کنیم و نتیجه می گیریم که

$$(1+a)^p = 1 + a \mod p. \tag{33}$$

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 مثبت α $\phi(p^\alpha) = p^{\alpha-1}(p-1)$. حال با استفاده از قضیه باقیمانده های چینی می توان قضیه زیررا ثابت کرد:

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

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

$$a^{\phi(n)} = 1 \mod n. \tag{34}$$

مثال :

$$\begin{aligned} n &= 5 \quad a = 2 \longrightarrow \phi(5) = 4 \longrightarrow 2^4 \mod 5 = 16 \mod 5 = 1 \\ n &= 6 \quad a = 5 \longrightarrow \phi(6) = 2 \longrightarrow 5^2 \mod 6 = 25 \mod 6 = 1 \end{aligned} \tag{35}$$

اثبات : نخست قضیه را برای حالتی که n به صورت $n = p^\alpha$ است ثابت می کنیم. برای این کار از استقرا روی α استفاده می کنیم. برای $\alpha = 1$ می دانیم که $a^{\phi(p)} = a^{p-1} = 1 \mod p$ که چیزی نیست جز همان قضیه کوچک فرما.
حال فرض کنید که قضیه برای $\alpha \geq 1$ صحیح باشد، یعنی

$$a^{\phi(p^\alpha)} = 1 \mod p^\alpha, \tag{36}$$

که به این معناست که

$$a^{\phi(p^\alpha)} = 1 + kp^\alpha \mod p^\alpha. \tag{37}$$

ازاین رابطه نتیجه می گیریم که

$$\begin{aligned} a^{\phi(p^{\alpha+1})} &= a^{p^\alpha(p-1)} = a^{\phi(p\alpha)p} = (1+kp\alpha)^p \\ &= \sum_{j=0}^{p} k^j p^{j\alpha} \left(\begin{array}{c} p \\ j \end{array} \right). \end{aligned} \tag{38}$$

اما چون $\forall j = 1, 2, \cdots p-1 \quad p | \left(\begin{array}{c} p \\ k \end{array} \right)$ و $p^\alpha | p^{j\alpha} \quad \forall j = 1, 2, \cdots p-1$ نتیجه می گیریم که

$$a^{\phi(p^{\alpha+1})} = 1 + p^{\alpha+1}R \longrightarrow a^{\phi(p^{\alpha+1})} = 1 \mod p^{\alpha+1}. \tag{39}$$

حال به اثبات حالت کلی می پردازیم. ////////// ناتمام :

۳ تجزیه یک عدد به عامل های اول آن

در این بخش به مسئله تجزیه یک عدد به عامل های اول آن می پردازیم. درواقع مسئله ساده تر آن است که هرگاه عددی مثل N داشته باشیم چگونه می توانیم دوعدد مثل p و q پیدا کنیم به قسمی که $N = pq$ باشد. اعداد p و q خود ممکن است که اول نباشند که دراین صورت آنها را نیز به همین نحو تجزیه می کنیم تا سرانجام عدد اولیه N به همه عامل های اول خود تجزیه شود. این مسئله چنانکه می دانیم مسئله سختی است به این معنی که تاکنون آلگوریتم کلاسیکی که بتواند آن را درزمان چند جمله ای حل کند یافته نشده است. چنانکه می دانیم اکنون یک آلگوریتم کوانتومی که مسئله فوق را درزمان چندجمله ای حل می کند وجود دارد. برای درک این آلگوریتم نیاز به مقدماتی درنظریه اعداد داریم که اکنون به آنها می پردازیم.

تعریف : Z_n^* مجموعه تمام اعدادی در Z_n است که به سنج n عضو وارون دارند. به عبارت دیگر Z_n^* مجموعه تمام اعدادی در Z_n است که نسبت به n اول هستند.

مثال :

$$Z_6^* = \{1, 5\} \qquad Z_{10}^* = \{1, 3, 7, 9\}. \tag{40}$$

قضیه : Z_n^* یک گروه است.

اثبات این قضیه ساده است.

قضیه : ${Z_{p^\alpha}}^*$ که درآن p یک عدد اول بجز ۲ است ، یک گروه دوره ای است.

اثبات این قضیه را می توان درکتاب های پیشرفته تر نظریه اعداد دید.

مثال : درگروه

$$Z_9^* = \{1, 2, 4, 5, 7, 8\} \tag{41}$$

همه اعداد توسط توان های عدد 2 تولید می شوند.

۱.۳ تحویل مسئله تجزیه به مسئله یافتن مرتبه

تعریف : هرگاه N و Y دو عدد صحیح مثبت باشند ، r مرتبه Y به سنج N خوانده می شود هرگاه

$$Y^r = 1 \qquad mod\ N. \tag{42}$$

دراین صورت می نویسیم $Rank(Y) \mod N = r$. به عنوان مثال $Rank(2) \mod 5 = 4$.

حال تحویل مسئله تجزیه را به یافتن رتبه دردومرحله انجام می دهیم.

مرحله اول : نشان می دهیم که هرگاه یک حل غیربدیهی از معادله

$$x^2 = 1 \mod N \tag{43}$$

داشته باشیم آنگاه می توانیم یک عامل از عدد N را پیداکنیم. منظور از حل غیربدیهی حلی است که درآن $x \neq \pm 1$ یا $x \neq 1, N-1$ باشد.
مرحله دوم : نشان می دهیم که اگر بطور تصادفی یک عدد Y که نسبت به N اول باشد انتخاب کنیم، احتمال آنکه مرتبه آن به سنج N زوج باشد، زیاداست. اگر این مرتبه را با r نشان دهیم آنگاه داریم

$$Y^r = 1 \mod N \longrightarrow (Y^{\frac{r}{2}})^2 = 1 \mod N. \tag{44}$$

درنتیجه هرگاه رتبه r را پیداکنیم عدد x را پیدا کرده ایم، زیرا قرارمی دهیم $x = Y^{\frac{r}{2}}$.
حال به توضیح هرکدام از دو مرحله فوق می پردازیم. نخست به یک قضیه احتیاج داریم.
قضیه : فرض کنید که N یک عدد L بیتی باشد و x نیز یک حل غیربدیهی از معادله $x^2 = 1 \mod N$ باشد. دراین صورت یکی از دو عدد $gcd(x-1, N)$ و یا $gcd(x+1, N)$ یک عامل N است.
اثبات: چون $x^2 = 1 \mod N$ نتیجه می گیریم که $x^2 - 1 = 0 \mod N$. بنابراین

$$(x-1)(x+1) = 0 \mod N. \tag{45}$$

درنتیجه N می بایست بایکی از اعداد $x+1$ و یا $x-1$ عامل مشترک داشته باشد. اما چون بنابه فرض غیربدیهی بودن x داریم $1 < x < N-1$ نتیجه می گیریم

$$x - 1 < x + 1 < N. \tag{46}$$

پس این عامل مشترک خود N نمی تواند باشد. بنابراین با استفاده از آلگوریتم اقلیدس $gcd(x-1, N)$ یا $gcd(x+1, N)$ را پیدا می کنیم که حاصل یکی از عامل های N است.
تااین جا قسمت ا ول را به انجام رساندیم. یعنی این که یک حل غیربدیهی از معادله $x^2 = 1 \mod N$ درزمان $O(L^3)$ منجر به یافتن یک عامل از عدد N می شود. حال می پردازیم به قسمت دوم که درآن یافتن رتبه یک عدد به سنج N اهمیت پیدا می کند.
قضیه : فرض کنید که p یک عدد اول فرد باشدو فرض کنید که 2^d بزرگ ترین عددی باشد که $\phi(p^\alpha)$ را می شمارد. دراین صورت دقیقاً نصف اعداد موجود در ${Z_{p^\alpha}}^*$ مرتبه شان به سنج p^α مضربی از 2^d ا ست.
نظر به صورت پیچیده این قضیه نخست چند مثال را طرح می کنیم.
مثال :

$$p = 3, \ \ \alpha = 2 \ \ p^\alpha = 9, \ \ \phi(p^\alpha) = \phi(9) = 6, \longrightarrow d = 1, \ \ 2^d = 2. \tag{47}$$

از طرفی

$${Z_{p^\alpha}}^* = {Z_9}^* = \{1, 2, 4, 5, 7, 8\} \tag{48}$$

حال می باید مرتبه اعداد این مجموعه را به سنج ۹ پیدا کنیم.براحتی معلوم می شود که درسنجه ۹:

$$Rank(1)=1,\quad Rank(2)=6,\quad Rank(4)=3,\quad Rank(5)=6,\quad Rank(7)=3,\quad Rank(8)=2, \tag{49}$$

که درآن همه رتبه ها به سنج ۹ حساب شده اند. می بینیم که دقیقا نصف اعضای این مجموعه مضرب 2 هستند و نصف دیگر نیستند.

حال به اثبات قضیه می پردازیم:

می دانیم که $\phi(p^\alpha)=p^{\alpha-1}(p-1)$. چون p فرد است پس $p-1$ زوج و درنتیجه $\phi(p^\alpha)$ زوج است. بنابراین $d\geq 1$. حال با توجه به دوره ای بودن ${Z_{p^\alpha}}^*$ می توان یک عضو دلخواه از آن را به صورت g^k نوشت که درآن g مولد ${Z_{p^\alpha}}^*$ است.

''

۱ — حساب باقیمانده ها

تعریف رابطه هم ارزی. اعمال جبری روی کلاس های باقیمانده ها.

تعریف : $a=b \quad modN$ ، اگر $a-b=kN$. اثبات این که این رابطه یک رابطه هم ارزی است.

تعریف میدان اعداد Z_N.

قضیه اساسی حساب

تعریف : بزرگترین مقسوم علیه مشترک دو عدد

قضیه : $gcd(a,b)$ کوچکترین عدد صحیح مثبتی است که می توان آن را به صورت $xa+yb$ نوشت.

قضیه : هرگاه a و b دو عدد صحیح باشند و باقیمانده تقسیم a بر b برابر با r باشد آنگاه $gcd(a,b)=gcd(b,r)$.

آلگوریتم اقلیدس برای پیدا کردن بزرگترین مقسوم علیه مشترک دو عدد.

قضیه : معکوس یک عدد a به سنج N و جود دارد اگر و فقط اگر $gcd(a,N)=1$.

قضیه : تعریف گروه Z_N^*

قضیه باقیمانده های چینی

قضیه کوچک فرما

تعریف : تابع $\phi(n)$ برابر با تعداد اعدادی است که از عدد n کوچکترند و نسبت به آن اول هستند.

قضیه : هرگاه دو عدد p و q نسبت به یکدیگر اول باشند آنگاه $\phi(pq)=\phi(p)\phi(q)$.

قضیه اویلر

قضیه : هرگاه p یک عدد فرد اول باشد آنگاه گروه Z_{p^α} یگ گروه دوره ای است.

قضیه : هرگاه 2^d بزرگترین عددی باشد که $\phi(p)$ را بشمارد آنگاه رتبه نیمی از اعداد متعلق به Z_{p^α} مضربی از 2^d است ونیمی دیگر مضربی از چنین عددی نیستند.

۲ — معادل بودن تجزیه اعداد با پیداکردن رتبه اعداد

۳ — روش کسرهای مسلسل