آشنایی با نظریه اعداد

بخشپذیری، همنهشتی، اعداد اول و مرکب

مؤلف

امیر مسعود گیوه چی

دی ۱۳۸۸

در نظریه ی مقدماتی اعداد با مجموعه ی اعداد طبیعی $N = \{۱,۲,۳, \dots\}$ سروکار خواهیم داشت.شما در دوره ی راهنمایی احتمالا با مفاهیمی هم چون بخش پذیری و اعداد اول و ب.م.م و ک.م.م و .... آشنا شده اید .در این جا مجددا به این مفاهیم توجه می کنیم .(البته با دقتی بیشتر)و مطالبی را اثبات می نماییم که ممکن است شما از آن ها ناخودآگاه و بدون دلیل استفاده کرده باشید.

بخش پذیری و الگوریتم تقسیم و همنهشتی

عددی طبیعی مانند a را در نظر بگیرید .در آن صورت مجموعه ی $A = \{a, ۲a, ۳a, ۴a, \dots\}$ را مجموعه ی مضارب طبیعی a یا اعداد طبیعی بخشپذیر بر a می گوییم واگر b بر a بخش پذیر باشد آن را با $a|b$ نشان می دهیم.

همین جا می توانیم قضیه ی مهم الگوریتم تقسیم را بیان و اثبات کنیم.

قضیه ی ۱:فرض کنید a, b دو عدد طبیعی باشند.در آن صورت اعدادی طبیعی مانند q, r وجود دارد به گونه ای که $a = bq + r$ و $۰ \le r < b$.

اثبات:مجموعه ی $B = \{۰, b, ۲b, ۳b, \dots\}$ را در نظر بگیرید. عدد a یا بر یکی از اعضای این مجموعه منطبق است یا بین دوعضو آن مانند $tb, (t + ۱)b$ که $t \in \{۰,۱,۲,۳, \dots\}$ قرار می گیرد.در حالت اول که مسأله واضح است و r برابر با ۰ خواهد بود .در حالت دوم q را برابر با t قرار دهید و r را برابر با $a - tb$ قرار دهید .

در آن صورت با توجه به نحوه ی انتخاب t خواهیم داشت:

$$r = a - tb < (t + ۱)b - tb = b \Rightarrow r < b$$

همچنین $r \ge ۰$ پس مسأله حل است.

حال می خواهیم با مفهوم مهمی به نام همنهشتی آشنا شویم.

دو عدد x, y را به پیمانه ی عددی مانند a همنهشت می گوییم و می نویسیم (به پیمانه a) $x \equiv y$ یا $x \overset{a}{\equiv} y$ هر گاه اختلاف آن ها مضربی از a باشد. در واقع دو عدد هنگامی به پیمانه ی a هم نهشت هستند که باقی مانده ی آنها بر a یکسان باشد یا به عبارتی دیگر اختلاف آن ها در مجموعه ی $\{۰, a, ۲a, ۳a, ۴a, \dots\}$ قرار گیرد (این بیان اخیر بسیار مورد توجه است)

توجه داشته باشید که اعداد طبیعی تحت رابطه ی همنهشتی به پیمانه ی عدد a به a دسته افراز می شوند.

همنهشتی اعداد به پیمانه ی یک عدد ثابت مانند a خاصیت های مهمی دارد.

خاصیت اول :فرض کنید

$$x_1 \equiv y_1 (a \text{ به پیمانه})$$

$$x_2 \equiv y_2 (a \text{ به پیمانه})$$

در آن صورت خواهیم داشت:

$$x_1 + x_2 \equiv y_1 + y_2 (a \text{ به پیمانه})$$

اثبات(a به پیمانه $x_1 \equiv y_1$ بیان می کند که $x_1 - y_1$ مضربی از a است.پس به صورت na بیان می شود.به طریق مشابه $x_2 - y_2$ به صورت ma بیان می شود.حال توجه داشته باشید :

پس اختلاف دو عدد $x_1 + x_2$ و $y_1 + y_2$ به صورت مضربی از a است.پس می توان گفت:

$$x_1 + x_2 \equiv y_1 + y_2 (a \text{ به پیمانه})$$

خاصیت دوم :فرض کنید $x_1 \equiv y_1 (a$ به پیمانه $), x_2 \equiv y_2 (a$ به پیمانه $)$

درآن صورت خواهیم داشت(a به پیمانه $x_1 x_2 \equiv y_1 y_2$

اثبات :

بنا بر استدلالی مشابه حالت قبل $x_1 - y_1 = na, x_2 - y_2 = ma$ می تواند باشد .

پس خواهیم داشت:

$$x_1 x_2 - y_1 y_2 =$$
$$(y_1 + na)(y_2 + ma) - y_1 y_2 = a(ny_2 + my_1 + nma)$$

پس می توان گفت که $x_1 x_2 - y_1 y_2$ مضربی از عدد a است.

این دو خاصیت قبلی منجر به این می شود که در همنهشتی به پیمانه ی a تنها با مجموعه $z_a = \{0,1,2,\dots,a-1\}$ که در واقع هر کدام از اعضای این مجموعه نماینده ی یک رده ی همنهشتی به پیمانه ی aمی باشد سر و کار داشته باشیم و جمع و ضرب را بین اعضای این مجموعه طوری تعریف کنیم که تساوی ها درواقع نمایانگر همنهشتی به پیمانه ی a باشند و اعضای این مجموعه را دستگاه کامل مانده ها به پیمانه یa می گوییم.

اعداد اول

عددی را اول می گوییم که بر هیچ یک از اعداد طبیعی کوچکتر از خود به جز ۱ بخش پذیر نباشد.(البته همان طور که می دانید!)

شما تا کنون با تحزیه ی یک عدد طبیعی به اعداد اول آشنا شده اید.اما آیا تا کنون از خود پرسیده اید که شاید یک عدد را بتوان به دو طریق به اعداد اول تجزیه کرد؟ اصلا آیا تا کنون از خود پرسیده اید که اگر p,q دو عدد اول مختلف باشند چرا برای α,βطبیعی خواهیم داشت $p^\alpha \neq q^\beta$.احتمالاجواب می دهید که q^β نمی تواند برp بخش پذیر باشد.حال باز هم ازخودتان بپرسید چرا؟آیا جوابی دارید؟ قضیه ی زیر می تواند به این سوال پاسخ بدهد.

قضیه ۲ :فرض کنید p عددی اول و$a,b\in N$ و$p|ab$.در آن صورت $p|a$ یا $p|b$.

اثبات:فرض خلف کنید.همچنین فرض کنید

$$a \equiv r(p \text{ به پیمانه }), b \equiv s(p \text{ به پیمانه })$$

که در این روابط داریم:$0<r,s<p$.

$$ab \equiv rs(p \text{ به پیمانه }), p|ab$$

بنا براین خواهیم داشت:$p|rs$.

با توجه به الگوریتم تقسیم اعدادی طبیعی مانند k,s_1 وجود خواهند داشت که $p = ks + s_1, 0 \le s_1 < s$.توجه داشته باشید که$s_1 \neq 0$.(زیرا اگر $s_1 = 0$در ان صورت $s|p$ و در آن صورت $s = 1$ اما داشتیم $p|rs$ پس می توان گفت $p|s$ که با $s<p$ تناقض دارد.)

$$P|rs \Rightarrow p|rsk$$

از $p|rsk$ و $p|rp$ نتیجه می شود $p|r(p-sk)$ پس $p|rs_1$

توجه داشته باشید که اگر $s_1 = 1$ در ان صورت خواهیم داشت $p|r$ که دوباره تناقض است.

حال توجه داشته باشید که کاری که کردیم این بود که از عدد s با خاصیت $p|rs$ به عددی دیگر مانند s_1 رسیدیم که $1 < s_1 < s$ و $p|rs_1$.حال به طریق مشابه از روی s_1 به عدد دیگری مانند s_2 می رسیم که $1 < s_2 < s_1$ و $p|rs_2$ و این کار را دوباره انجام می دهیم و .... اگر دقت کنید این روند تا بی نهایت ادامه نخواهد داشت زیرا دنباله ای نا متناهی و اکیدا نزولی از اعداد طبیعی نخواهیم داشت.این تناقض نشان می دهد که فرض $p|rs$ از اول اشتباه بوده است و این مسأله را حل می کند.

حال می توانیم توضیح دهیم که چرا تجزیه ی یک عدد طبیعی به اعداد اول یکتاست. البته اجازه دهید قبل از آن توضیح دهیم که چرا اصولا یک عدد را می توان به اعداد اول تجزیه کرد.

مرحله ی اول اثبات این است که ثابت کنیم برای هر عدد طبیعی مانند a عددی اول مانند p وجود دارد به گونه ای که $p|a$.اگر a اول باشد که مسأله واضح است.در غیر این صورت عددی مانند a_1 وجود دارد که $a_1|a$.اگر a_1 اول باشد مسأله حل است.در غیر این صورت باز بر روی a_1 همین کار را انجام می دهیم و .... سرانجام به یک عدد اول خواهیم رسید (چون در غیر این صورت این روند تا بی نهایت ادامه خواهد داشت)

ادامه ی اثبات بدین صورت است که برای عدد a ابتدا یک عامل اول از آن مانند p پیدا کرده a را بر p تقسیم کرده . برای عدد حاصل نیز همین عملیات را تکرار کرده و.... هنگامی که به ۱ برسیم a را می توانیم به صورت حاصل ضرب عوامل اول بنویسیم .

حال به سراغ یکتایی تجزیه به عوامل اول می رویم .فرض کنید عدد طبیعی a را بتوان به دو صورت $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$ تجزیه کرد .چون $p_1 | q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$ پس بنا بر قضیه ی ۲ p_1 باید یکی از اعداد $q_1, q_2, \dots q_l$ را عاد کند و به عبارتی دقیق تر یکی از $q_1^{\beta_1}, q_2^{\beta_2}, \dots, q_l^{\beta_l}$ و چون این اعداد اول هستند پس j وجود دارد به گونه ای که $p_1 = q_j$.فرض کنید $j = 1$.حال کافی است قضیه را برای $\frac{a}{p_1}$ که به دو صورت $p_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ و $q_1^{\beta_1 - 1} q_2^{\beta_2} \dots q_l^{\beta_l}$ تجزیه شده است ثابت کنیم.برای این عدد دوباره همین کار را انجام می دهیم یعنی یک عامل مشترک را از دو طرف می کنیم و .... تا در یک طرف به یک عدد اول برسیم در آن صورت طرف دیگر باالاجبار باید با همان عدد اول برابر باشد . بدین ترتیب یکتایی تجزیه ثابت می شود.

در قسمت های قبل با دستگاه کامل مانده ها به پیمانه ی عدد دلخواه n آشنا شده ایم. قضیه ی ۲ منجر به این می شود که دستگاه کامل مانده ها به پیمانه ی عدد اول p دارای این خاصیت باشد که حاصل ضرب هر دو عضو ناصفر آن ناصفر باشد .این خاصیت به همراه متناهی بودن مجموعه z_p (یادآوری :$z_p = \{۰,۱,۲, \dots, p-۱\}$) منجر به این می شود که هر عضو دلخواه آن یک وارون ضربی داشته باشد. بدین معنا که برای هر عضو آن مانند a عضوی مانند b وجود دارد به گونه ای که $ab = ۱$ (یعنی $ab \equiv ۱ (p$ به پیمانه $)$)

اثبات بدین صورت است که در مجموعه ی $\{a, ۲a, ۳a, \dots, (p-۱)a\}$ هیچ دو عضوی همنهشت نیستند چرا که اگر مثلا ia با ja به پیمانه p همنهشت باشد داریم که $ia \equiv ja (p$ به پیمانه $)$ یا $(i-j)a \equiv ۰ (p$ به پیمانه $)$ پس $i-j \equiv ۰ (p$ به پیمانه $)$ یا $a \equiv ۰ (p$ به پیمانه $)$ که هیچ کدام امکان ندارد)

از طرفی هیچ کدام از اعضا هم صفر نیستند پس می توانیم بگوییم که مجموعه ی

$$\{a, ۲a, ۳a, \dots, (p-۱)a\}$$

با مجموعه ی

$$\{۱,۲,۳, \dots p-۱\}$$

به پیمانه p برابر است.

(سعی کنید از این به بعد لازم نباشد که بنویسم "به پیمانه ی p" !) پس عددی مانند b وجود دارد که $ab = ۱$.(آیا می توانید بگویید که در کدام قسمت از متناهی بودن z_p استفاده کرده ایم؟)

خاصیت اخیر در مورد z_p بسیار مهم است به گونه ای که به طور کلی مجموعه هایی با این خاصیت (داشتن وارون ضربی برای عضو نا صفر)بسیار مورد توجه هستند.

بزرگترین مقسوم علیه مشترک و کوچکترین مضرب مشترک

تعریف: بزرگترین مقسوم علیه مشترک a, b بزرگترین مقسوم علیه مشترک a, b است ! و آن را با $gcd(a, b)$ نشان می دهیم .خاصیت مهمی که $gcd(a, b)$ دارد این است که بر هر مقسوم علیه مشترک a, b بخش پذیر است. در ادامه سعی می کنیم آن را ثابت کنیم .

برای اثبات این موضوع توجه شما را به روشی که در دوره ی راهنمایی تحت نام روش نردبانی با آن آشنا شده اید جلب می کنیم.در این روش در واقع به طریقه ی زیر عمل می کردیم :

فرض کنید دو عدد طبیعی مانند a,b داشته باشیم که $a>b$.با توجه به الگوریتم تقسیم اعدادی مانند q_1و b_1 وجود دارند که $a = bq_1 + b_1$ و $0 \leq b_1 < b$

در آن صورت هر مقسوم علیه مشترک a,b یک مقسوم علیه مشترک b,b_1 نیز هست و بالعکس . پس می توان گفت $gcd(a,b) = gcd(b,b_1)$. (توجه کنید که اگر $b_1 = 0$وفرض کنیم $\forall x \in N: gcd(x,0) = 0$ باز هم گزاره ی قبلی صادق است)

اگر $b_1 = 0$در آن صورت $gcd(a,b) = gcd(b,b_1) = b$.

اگر $b_1 \neq 0$ در آن صورت باز بر روی زوج (b,b_1) همان کاری را انجام می دهیم که بر روی (a,b) انجام دادیم.یعنی الگوریتم تقسیم را بر روی آنها انجام می دهیم و b_2 را به گونه ای به دست می آوریم که

$0 \leq b_2 < b_1$ و $gcd(b,b_1) = gcd(b_1,b_2)$و... یعنی دنباله ی b_i ها را بدین گونه به دست می آوریم و هنگامی که یک عضو از دنباله صفر شد

متوقف می شویم.(این اتفاق می افتد زیرا دنباله ی b_i اکیدا نزولی است.)

پس فرض کنید به ازای j طبیعی $b_j = 0$.ما گفتیم که مقسوم علیهای مشترک a,b همان مقسوم علیهای مشترک b,b_1 هستند.به طریق مشابه می توان گفت این ها همان مقسوم علیهای مشترک b_1,b_2یا همان مقسوم علیهای مشترک b_2,b_3هستندو... پس می توان گفت مقسوم علیهای مشترک a,bهمان مقسوم علیهای مشترک $b_{j-1},0$ یا همان مقسوم علیه های b_{j-1} هستند. b_{j-1} مقسوم علیه خودش هست پس $gcd(a,b) = b_{j-1}$ و همچنین همان طور که اندکی پیش گفتیم اگر $d|a,b$ در آن صورت $d|b_{j-1}$ و این همان خاصیتی است که دنبالش می گشتیم.

حال می خواهیم بحث نسبتا مشابهی را در مورد کوچکترین مضرب مشترک (a,b) که آن را با $Lcm(a,b)$ نشان می دهیم بکنیم.در واقع می خواهیم بگوییم هر مضرب مشترک a,b بر $Lcm(a,b)$ بخش پذیر است.

باز هم الگوریتم تقسیم کلید اصلی حل مساله است.فرض کنید r بر a,b بخش پذیر باشد و همچنین فرض کنید r بر $Lcm(a,b)$ بخش پذیر نباشد.

بنا برالگوریتم تقسیم :

$$\exists s,t \in N: r = t\ Lcm(a,b) + s, 0 < s < Lcm(a,b)$$

$a,b|r$ و $a,b|\ Lcm(a,b)$.پس می توان گفت $a,b|r-t\ Lcm(a,b)$

پس می توان گفت$a,b|s$.اما $s < Lcm(a,b)$ و این با تعریف کوچکترین مضرب مشترک (a,b)در تناقض است.

البته توجه داشته باشید که اگر a,bرا به صورت حاصل ضرب عوامل اول آن ها بنویسیم بیان ساده ای برای $gcd(a,b)$ و $Lcm(a,b)$خواهیم داشت که قضایای بالا را به راحتی نتیجه می دهند.اما توجه داشته باشید که این طرز برخورد با مقسوم علیه های یک عدد(یعنی این که عوامل اول مقسوم علیه های یک عدد زیر مجموعه ی عوامل اول این عدد هستند)به قضیه ی ۲ $(p|ab\Rightarrow p|a\text{یا}p|b)$ بر می گردد و خود این قضیه نیز به الگوریتم تقسیم بر می گردد و ما در اثبات های بالا نیز ازالگوریتم تقسیم استفاده کردیم.پس می بینید که الگوریتم تقسیم خاصیتی بنیادین و بسیار مهم از اعداد طبیعی است .