بخشپذیری و الگوریتم تقسیم :

بخشپذیری:

می‌گوییم که a بر b بخشپذیر است اگر به ازای m ای، داشته باشیم $a = mb$ ، که در آن a, b و m اعداد صحیح هستند. یا به عبارتی a بر b بخشپذیر است اگر هیچ باقی‌مانده ای از حاصل تقسیم a بر b وجود نداشته باشد، در آنصورت نشان می‌دهیم $b|a$.

متعابقاً، به یک سری از خصوصیات ساده بخشپذیری نیازمندیم که به صورت زیر است:

- اگر $a|1$ ، آنگاه $a = \pm 1$.
- اگر $a|b$ و $b|a$ ، آنگاه $a = \pm b$.
- به ازای هر $b \neq 0$ ، $b|0$.
- اگر $a|b$ و $b|c$، آنگاه $a|c$.

مثال : $11|66$ و $11|198 \Rightarrow 11|198$

- اگر $b|g$ و $b|h$، آنگاه به ازای هر n و m دلخواه داریم $b|(mg + nh)$.

برای اثبات نکته اخر :

- اگر $b|g$، آنگاه g به ازای عددی چون g_1 به فرم $g = b \times g_1$ است.
- اگر $b|h$، آنگاه h به ازای عددی چون h_1 به فرم $h = b \times h_1$ است.

پس :

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1).$$

بنابراین $mg + nh$ بر b بخشپذیر است.

الگوریتم تقسیم :

با داشتن هر **عدد صحیح مثبت دلخواه n** و عدد صحیح a، اگر a را بر n تقسیم کنیم، عدد صحیح q را بعنوان خارج قسمت و عدد صحیح r را بعنوان باقی‌مانده بدست می‌آوریم که از رابطه زیر تبعیت می‌کند:

$$a = qn + r \qquad 0 \leq r < n\,; \quad q = \left\lfloor \frac{a}{n} \right\rfloor \qquad (4.1)$$

که در آن $\lfloor x \rfloor$ بزرگترین عدد صحیحی است که کم‌تر یا مساوی x است. رابطه (4.1) را الگوریتم تقسیم می‌نامیم.

مثال :

$a = 11; \quad n = 7; \quad 11 = 1 \times 7 + 4; \quad r = 4\ , \quad q = 1$

$a = -11; \quad n = 7; \quad -11 = (-2) \times 7 + 3; \quad r = 3\ , \quad q = -2$

الگوریتم اقلیدسی :

یکی از تکنیک های بنیادین در نظریه اعداد، **الگوریتم اقلیدسی** است، که آن یک رویه ساده ای برای تعیین بزرگترین مقسوم علیه مشترک بین دو عدد صحیح مثبت می‌باشد. ابتدا به یک تعریف ساده نیازمندیم: دو عدد صحیح، **نسبت به یکدیگر اول** هستند اگر **بزرگترین مقسوم‌علیه مشترک** آنها، عدد صحیح ۱ باشد.

بزرگ‌ترین مضرب مشترک :

یادآوریم می‌کنیم که عدد ناصفر b را مقسم a تعریف می‌کنیم اگر عدد m وجود داشته باشد بگونه ای که $a = mb$ که در آن، a ، b و m صحیح هستند.

ما از نماد $\gcd(a,b)$ برای نشان دادن **بزرگ‌ترین مضرب مشترک** بین دو عدد a و b استفاده می‌کنیم. همچنین تعریف می‌کنیم $\gcd(0,0) = 0$.

به طور رسمی تر، عدد صحیح مثبت بزرگترین مقسوم علیه مشترک a و b است اگر :

۱ : c یک مقسم از a و از b باشد. (c، a و b را عاد کند.)

۲ : هر مقسم از a و b، مقسم c نیز باشد.

تعریف معادل به صورت زیر است:

$$\gcd(a,b) = \max[\ k, such\ that\ k|a\ and\ k|b\ ]$$

چون ما نیاز داریم که بزرگترین مقسوم علیه مشترک مثبت باشد؛ $\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b), \gcd(-a,-b)$. بنابراین داریم : $\gcd(a,b) = \gcd(|a|,|b|)$.

مثال : $\gcd(60,24) = \gcd(60,-24) = 12$

چون تمام اعداد صحیح ناصفر، صفر را تقسیم می‌کنند، داریم $\gcd(a,0) = |a|$.

a و b نسبت به هم اول هستند اگر و فقط اگر $\gcd(a,b) = 1$.

پیدا کردن بزرگترین مقسوم علیه مشترک:

هم‌اکنون الگوریتمی را که منتسب به اقلیدس است برای ساده یافتن **بزرگترین مقسوم علیه مشترک** بیان می‌کنیم، این الگوریتم نقش چشمگیری در این فصل ایفاء می‌کند. فرض می‌کنیم که دو عدد صحیح a و b را داشته باشیم بطوریکه $d = \gcd(a,b)$. چون $\gcd(|a|,|b|) = \gcd(a,b)$، در آنصورت مشکلی وجود نخواهد داشت اگر فرض کنیم : $a \geq b > 0$. اکنون با تقسیم a بر b و اعمال الگوریتم تقسیم، می‌توانیم بیان کنیم :

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b \qquad (4.2)$$

اگر $r_1 = 0$، آنگاه $b|a$ و $d = \gcd(a,b) = b$. اما اگر $r_1 \neq 0$، می‌توانیم بگوییم که $d|r_1$،که این به دلیل خصوصیات پایه ای بخشپذیری است: روابط $d|a$ و $d|b$ ایجاب می‌کنند که $d|(a - q_1 b)$ که برابر است با $d|r_1$. قبل از ادامه پروسه معرفی الگوریتم اقلیدسی، نیاز به جواب به این سوال را داریم: $\gcd(b,r_1)$ چیست؟ می‌دانیم که $d|b$ و $d|r_1$. حال عدد صحیح دلخواهی چون c را درنظر می‌گیریم بطوریکه c ، b و r_1 را عاد کند. بنابراین $c|(q_1 b + r_1) = a$. چون c هم a را عاد می‌کند و هم b را بنابراین باید $c \leq d$ که بزرگترین مقسوم علیه مشترک a و b است. پس : $d = \gcd(b,r_1)$.

برگردیم به معادله (4.2) و فرض کنیم که $r_1 \neq 0$. چون $b > r_1$، می‌توانیم b را توسط r_1 تقسیم کنیم و الگوریتم تقسیم را اعمال می‌کنیم تا معادله زیر را بدست آوریم:

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

همانند قبل، اگر $r_2 = 0$، آنگاه $d = r_1$ و اگر $r_2 \neq 0$، آنگاه $d = \gcd(r_1,r_2)$. رویه تقسیم ادامه پیدا می‌کند تازمانی که باقیمانده صفر نمایان شود. بزارید بگوییم در مرحله $(n+1)$ ام جاییکه r_{n-1} بر r_n تقسیم شده است. نتیجه به صورت دستگاه زیر است:

$$\left.\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 & \\
d = \gcd(a,b) = r_n &
\end{array}\right\} \qquad \textbf{(4.3)}$$

در هرتکرار، داریم $d = \gcd(r_i, r_{i+1})$ تا در نهایت $d = \gcd(r_n, 0) = r_n$. بنابراین، می‌توانیم بزرگترین مقسوم علیه مشترک را به وسیله برنامه تکرار الگوریتم تقسیم بدست آوریم. این طرح را به عنوان **الگوریتم اقلیدسی** می‌شناسیم.

اکنون نگاه به مثالی با اعداد نسبتاً بزرگ می‌اندازیم تا به قدرت این الگوریتم پی‌ببریم:

To find $d = \gcd(a,b) = \gcd(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2516 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

در این مثال، ما با تقسیم ۱۱۶۰۷۱۸۱۷۴ بر ۳۱۶۲۵۸۲۵۰، خارج قسمت ۳ را با باقیمانده ۲۱۱۹۴۳۴۲۴ به دست می‌آوریم. سپس ۳۱۶۲۵۸۲۵۰ را می‌گیریم و آن را بر ۲۱۱۹۴۳۴۲۴ تقسیم می‌کنیم. این روند تا زمانی ادامه می‌یابد که به جواب ۱۰۷۸ به همراه باقی‌مانده از ۰ برسد.

در ادامه ، بازنویسی محاسبات فوق به صورت جدولی مفید خواهد بود.که در آن برای هر مرحله از تکرار، مقسوم و مقسوم علیه و خارج قسمت و باقی‌مانده را در هر ستون داریم. جدول (۴,۱) نتایج را خلاصه می‌کند.

Table 4.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

الگوریتم اقلیدسی تعمیم یافته :

اکنون به بررسی تعمیم الگوریتم اقلیدسی می پردازیم که در محاسبات در حوزه میدان های متناهی و در الگوریتم های رمزگذاری مانند RSA مهم خواهد بود. برای اعداد صحیح داده شده a و b , الگوریتم اقلیدسی توسعه یافته نه تنها بزرگترین مقسوم علیه مشترک بلکه دو عدد صحیح اضافی x و y را نیز محاسبه می کند که معادله زیر را برآورده می‌شود.

$$ax + by = d = \gcd(a, b)$$

اکنون نشان می‌دهیم که چگونه الگوریتم اقلیدسی را برای تعیین (x, y, d) تعمیم بدهیم.

دوباره سمت دنباله تقسیم هایی که در معادله ۴,۳ نشان داده شد، می‌رویم و فرض می‌کنیم که در هر قدم i می‌توانیم x_i و y_i را به گونه ای پیدا کنیم که در $r_i = ax_i + by_i$ صدق کنند. دنباله زیر را خواهیم داشت:

$$\begin{array}{ll}
a = q_1 b + r_1 & r_1 = ax_1 + by_1 \\
b = q_2 r_1 + r_2 & r_2 = ax_2 + by_2 \\
r_1 = q_3 r_2 + r_3 & r_3 = ax_3 + by_3 \\
\bullet & \bullet \\
\bullet & \bullet \\
\bullet & \bullet \\
r_{n-2} = q_n r_{n-1} + r_n & r_n = ax_n + by_n \\
r_{n-1} = q_{n+1} r_n + 0 &
\end{array}$$

مشاهده کنید که می‌توانیم عبارت های سمت چپ را به صورت زیر بازنویسی کنیم:

$$r_i = r_{i-2} - r_{i-1}q_i$$

همچنین، در ردیف های $i-1$ و $i-2$، مقدار های زیر را می‌یابیم:

$$\begin{aligned} r_i &= (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_i \\ &= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) \end{aligned}$$

اما پیش‌تر فرض کرده بودیم که $r_i = ax_i + by_i$. بنابراین :

$$x_i = x_{i-2} - q_i x_{i-1} \quad \text{و} \quad y_i = y_{i-2} - q_i y_{i-1}$$

اکنون محاسبات را در جدول زیر خلاصه می‌کنیم:

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

در اینجا نیاز داریم که چند کامنت در مورد جدول بالا اضافه کنیم:

در هر ردیف، باقی‌مانده جدید r_i بر اساس باقی‌مانده های دو ردیف قبلی به نام های r_{i-1} و r_{i-2} بدست می‌آید. برای شروع الگوریتم، به یه مقدار های r_0 و r_{-1} نیاز داریم، که همان a و b است. پس آنگاه تعیین مقادیر x_0 و x_{-1} و y_0 و y_{-1} سر راست خواهد بود. از الگوریتم اقلیدسی دریافتیم که رویه با رسیدن به باقی‌مانده صفر پایان می‌یابد و بزرگترین مقسوم علیه مشترک a و b برابر $d = \gcd(a, b) = r_n$ است. اما اکنون تعیین کردیم که $d = r_n = ax_n + by_n$ بنابراین در معادله (4.7)، $x = x_n$ و $y = y_n$.

بعنوان مثال، فرض کنیم $a = 1759$ و $b = 550$ سپس معادله $1759x + 550y = \gcd(1759, 550)$

را حل می‌کنیم. جواب ها در جدول ۴,۴ نشان داده شده است. بنابراین داریم:

$$1759 \times (-111) + 550 \times 355 = -195249 + 195250 = 1$$

Table 4.4 Extended Euclidean Algorithm Example

i	r_i	q_i	x_i	y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$