**بخشپذیری و الگوریتم تقسیم :**

**بخشپذیری:**

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

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

* اگر ، آنگاه .
* اگر و ، آنگاه .
* به ازای هر ، .
* اگر و ، آنگاه .
* اگر و ، آنگاه به ازای هر و دلخواه داریم .

برای اثبات نکته اخر :

* اگر ، آنگاه به ازای عددی چون به فرم است.
* اگر ، آنگاه به ازای عددی چون به فرم است.

پس :

بنابراین بر بخشپذیر است.

**الگوریتم تقسیم :**

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

که در آن بزرگترین عدد صحیحی است که کم‌تر یا مساوی است. رابطه را الگوریتم تقسیم می‌نامیم.

**الگوریتم اقلیدسی :**

مثال :

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 را مقسم تعریف می‌کنیم اگر عدد وجود داشته باشد بگونه ای که ‌ که در آن، ، و صحیح هستند.

ما از نماد برای نشان دادن **بزرگ‌ترین مضرب مشترک** بین دو عدد و استفاده می‌کنیم. همچنین تعریف می‌کنیم .

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

**۱ :**  یک مقسم از ‌ و از باشد. (، و را عاد کند. )

**۲ :** هر مقسم از و ، مقسم نیز باشد.

تعریف معادل به صورت زیر است:

چون ما نیاز داریم که بزرگترین مقسوم علیه مشترک مثبت باشد؛ . بنابراین داریم : .

چون تمام اعداد صحیح ناصفر، صفر را تقسیم می‌کنند، داریم .

**و نسبت به هم اول هستند اگر و فقط اگر .**

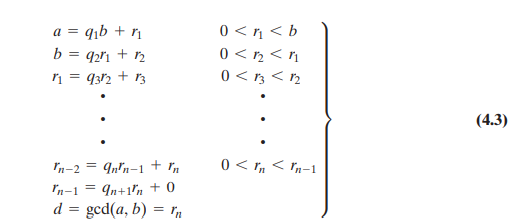
**پیدا کردن بزرگترین مقسوم علیه مشترک:**

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 و را داشته باشیم بطوریکه . چون ، در آنصورت مشکلی وجود نخواهد داشت اگر فرض کنیم : . اکنون با تقسیم بر و اعمال الگوریتم تقسیم، می‌توانیم بیان کنیم :

اگر ، آنگاه و . اما اگر ، می‌توانیم بگوییم که ،که این به دلیل خصوصیات پایه ای بخشپذیری است:‌ روابط و ایجاب می‌کنند که که برابر است با . قبل از ادامه پروسه معرفی الگوریتم اقلیدسی، نیاز به جواب به این سوال را داریم: چیست؟ می‌دانیم که و . حال عدد صحیح دلخواهی چون را درنظر می‌گیریم بطوریکه ، و را عاد کند. بنابراین . چون هم را عاد می‌کند و هم را بنابراین باید که بزرگترین مقسوم علیه مشترک ‌ و ‌ است. پس : .

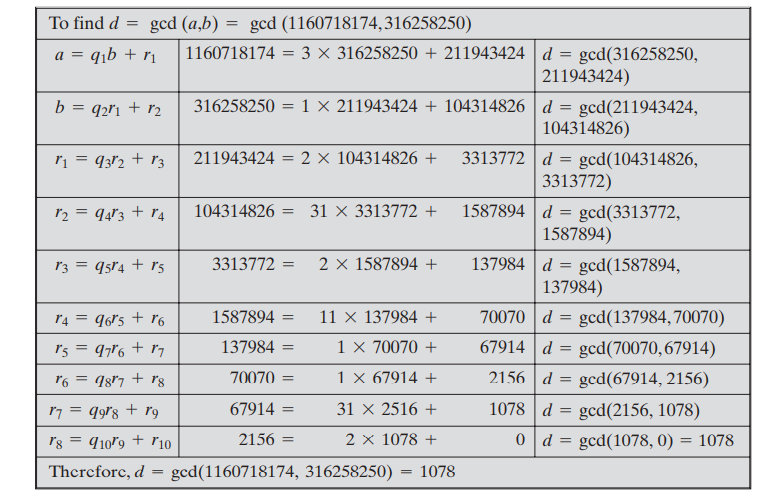
برگردیم به معادله ‌ و فرض کنیم که . چون ، می‌توانیم را توسط تقسیم کنیم و الگوریتم تقسیم را اعمال می‌کنیم تا معادله زیر را بدست آوریم:

همانند قبل، اگر ، آنگاه و اگر ، آنگاه. رویه تقسیم ادامه پیدا می‌کند تازمانی که باقیمانده صفر نمایان شود. بزارید بگوییم در مرحله ام جاییکه بر ‌ تقسیم شده است. نتیجه به صورت دستگاه زیر است:



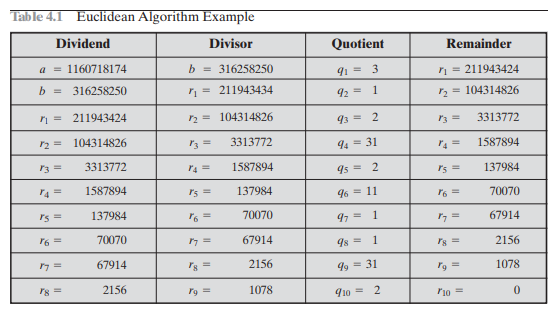
در هرتکرار، داریم ‌ تا در نهایت . بنابراین، می‌توانیم بزرگترین مقسوم علیه مشترک را به وسیله برنامه تکرار الگوریتم تقسیم بدست آوریم. این طرح را به عنوان **الگوریتم اقلیدسی** می‌شناسیم.

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



در این مثال، ما با تقسیم 1160718174 بر 316258250، خارج قسمت 3 را با باقیمانده 211943424 به دست می‌آوریم. سپس 316258250 را می‌گیریم و آن را بر 211943424 تقسیم می‌کنیم. این روند تا زمانی ادامه می‌یابد که به جواب ۱۰۷۸ به همراه باقی‌مانده از 0 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.

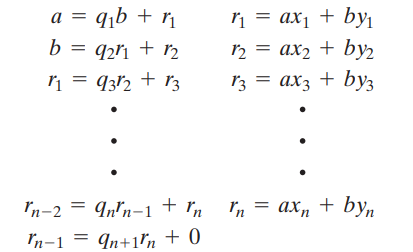


**الگوریتم اقلیدسی تعمیم یافته :**

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 و , الگوریتم اقلیدسی توسعه یافته نه تنها بزرگترین مقسوم علیه مشترک بلکه دو عدد صحیح اضافی و را نیز محاسبه می کند که معادله زیر را برآورده می‌شود.

اکنون نشان می‌دهیم که چگونه الگوریتم اقلیدسی را برای تعیین تعمیم بدهیم.

دوباره سمت دنباله تقسیم هایی که در معادله ۴.۳ نشان داده شد، می‌رویم و فرض می‌کنیم که در هر قدم می‌توانیم و را به گونه ای پیدا کنیم که در صدق کنند. دنباله زیر را خواهیم داشت:

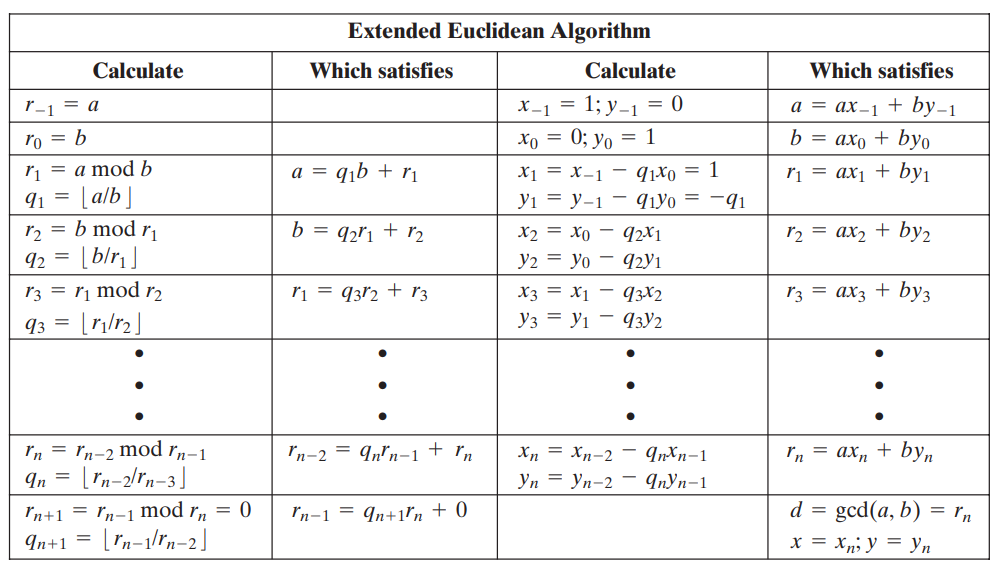


مشاهده کنید که می‌توانیم عبارت های سمت چپ را به صورت زیر بازنویسی کنیم:

همچنین، در ردیف های و ، مقدار های زیر را می‌یابیم:

اما پیش‌تر فرض کرده بودیم که. بنابراین :‌

اکنون محاسبات را در جدول زیر خلاصه می‌کنیم:



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

در هر ردیف، باقی‌مانده جدید بر اساس باقی‌مانده های دو ردیف قبلی به نام های و بدست ‌می‌آید. برای شروع الگوریتم، به یه مقدار های و نیاز داریم، که همان و است. پس آنگاه تعیین مقادیر و و و سر راست خواهد بود. از الگوریتم اقلیدسی دریافتیم که رویه با رسیدن به باقی‌مانده صفر پایان می‌یابد و بزرگترین مقسوم علیه مشترک و برابر است. اما اکنون تعیین کردیم که بنابراین در معادله ‌، و . بعنوان مثال، فرض کنیم و سپس معادله

را حل می‌کنیم. جواب ها در جدول ۴.۴ نشان داده شده است. بنابراین داریم:

