MTH621M-Number Theory

DIVISIVILITY IN THE SET OF INTEGERS

Francis Joseph Campeña, Ph.D.
Mathematics and Statistics Department
De La Salle University-Manila

Theorem (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $a > 0$. There exists a unique pair of integers q, r satisfying

$$b = qa + r,\ 0 \leq r < a.$$

The following corollary shows that the divisor need not be a postive integers.

Corollary

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exists a unique pair of integers q, r satisfying

$$b = qa + r,\ 0 \leq r < |a|.$$

Example

1. Let $b = 27, a = 12$. We have, $27 = 2 * (12) + 3$
2. Let $b = -17, a = 5$. We have, $-17 = -4 * (5) + 3$

Theorem (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $a > 0$. There exists a unique pair of integers q, r satisfying

$$b = qa + r, \ 0 \leq r < a.$$

The following corollary shows that the divisor need not be a postive integers.

Corollary

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exists a unique pair of integers q, r satisfying

$$b = qa + r, \ 0 \leq r < |a|.$$

Example

1. Let $b = 27, a = 12$. We have, $27 = 2 * (12) + 3$
2. Let $b = -17, a = 5$. We have, $-17 = -4 * (5) + 3$

If $a = 2$ in the division algorithm, then $r = 0$ or $r = 1$. Thus by the general Division Algorithm, we say that b is an even integer if $b = 2q + 0$ for some $q \in \mathbb{Z}$ and we say that b is an odd integer if $b = 2q + 1$ for some $q \in \mathbb{Z}$

Example

Use the division algorithm to show that the square of any integer is of the form either $3k + 1$ or $3k$.

To show this, consider an integer x. Using the division algorithm, the possible remainders would be $0, 1, 2$. This means we can write x in the following forms: $3q, 3q + 1, 3q + 2$. Verify that in each case, we either have $3k + 1$ or $3k$.

Examples

Example

1. Let $b = 27,\ a = 12$. We have 27 = 12(2) + 3, so $q = 2$ and $r = 3$.
2. Let $b = -42,\ a = 12$. We take the multiple of 12 closest to and not greater than -42. This will be -48, so we have $-42 = -48 + 6 = 12(-4) + 6$, so that $q = -4$ and $r = 6$.
3. Let $b = 70,\ a = -11$. The largest multiple of -11 which does not exceed 70 is 66, so we have $70 = (-11)(-6) + 4$, and so we have $q = -6,\ r = 4$.

Examples

Example

1. Use the division algorithm to show that the square of any integer is of the form either $3k+1$ or $3k$, for some positive integer k.

   Solution:

   Let x be any integer. If x is divided by 3, then the possible remainders are 0, 1 or 2. By the division algorithm, we can write x in any of the following forms: $3q,\ 3q+1$ or $3q+2$.

   If $x = 3q:\quad x^2 = (3q)^2 = 9q^2 = 3(3q^2) = 3k$, where $k = 3q^2$.

   If $x = 3q+1$**:** $\quad x^2 = (3q+1)^2 = 9q^2+6q+1 = 3(3q^2+2q)+1 = 3k+1$, where $k = 3q^2+2q$.

   If $x = 3q+2$**:** $\quad x^2 = (3q+2)^2 = 9q^2+12q+4 = 3(3q^2+4q+1)+1 = 3k+1$, where $k = 3q^2+4q+1$.

Divisibility

Definition

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that b is divisible by a or that a divides b, if there exists an integer c such that $b = ac$. In symbols we have, $a|b$.

Remark

Other terms for the divisibility property $a|b$ is that a is a divisor of b, and that b is a multiple of a.

Divisibility Properties Part 1

Theorem

Let $a, b, c \in \mathbb{Z}$.

1. $a|0, \ 1|a, \ a|a$
2. $a|1$ *if and only if* $a = \pm 1$.
3. *If* $a|b$ *and* $c|d$*, then* $ac|bd$.
4. *If* $a|b$ *and* $b|c$*, then* $a|c$.
5. $a|b$ *if and only if* $ac|bc$ *for all nonzero integers* c.
6. *If* $a|b$ *and* $b|a$*, then* $a = \pm b$.

Divisibility Properties Part 1

Theorem

Let $a, b, c \in \mathbb{Z}$.

1. *If* $a|b,\ b \neq 0$, *then* $|a| \leq |b|$.
2. *If* $a|b$ *and* $a|c$, *then* $a|(bx + cy)$ *for all* $x,\ y \in \mathbb{Z}$.
3. *If* $ab|c$, *then* $a|c$.
4. *If* $a|b$ *then* $a|bc$ *for any integer* c.
5. $a|b$ *if and only if* $ma|mb, m \neq 0$

Common Divisor

Definition

If $c|a$ and $c|a$, we call c a **common divisor** of b and a. If at least one of b and a is nonzero, then they only have a finite number of common divisors. The largest positive common divisor of b and a is called the **greatest common divisor** of b and a, and is denoted by (a, b) or by $\gcd(a, b)$. Thus, the greatest common divisor satisfies the following conditions: If $d = \gcd(a, b)$, then

- $d|a$ and $d|b$
- If c is a positive integer such that $c|a$ and $c|b$, then $c \leq d$

Example: Common Divisor

Example

Let $a = 24,\ b = -30$. The positive divisors of a are 1, 2, 3, 4, 6, 8, 12 and 24, while the positive divisors of -30 are 1, 2, 3, 5, 6, 10, 15 and 30. This shows that the common positive divisors of 24 and -30 are 1, 2, 3 and 6, so that the greatest common divisor is $(24,\ -30) = 6$.

Aside from the properties given in the definition, we have the following properties of the greatest common divisor:

Theorem

Properties of the GCD *Let $d = (a, b)$. Then*

1. $(a,\ b) = a$ *if and only if* $a|b$.
2. $1 \leq d \leq \min\ \{\ a,\ b\ \}$.
3. *If* $c|a$ *and* $c|b$*, then* $\left(\dfrac{a}{c},\ \dfrac{b}{c}\right) = \dfrac{d}{c}$.
4. *For all integers* n*, we have* $(an,\ bn) = n\,(a,\ b)$.

Proofs

Example: If $d|a$ and $d|b$, show that $d|(ax + by)$ for all integer values of x, y.

Greatest Common Divisor

Theorem

If $d = (a,\ b)$, then there exist integers x_0 and y_0 such that $d = ax_0 + by_0$, i.e. the greatest common divisor of a and b is expressible as a linear combination of the two integers.

Corollary

If $a,\ b$ are integers which are not both zero, then the set

$$T = \{\ ax + by \mid x,\ y \in \mathbb{Z}\ \}$$

is precisely the set of all multiples of $d = (a,\ b)$.

Relatively Prime

Definition

Two integers *a* and *b* which are not both zero are said to be **relatively prime** if $(a,\ b) = 1$.

Example

Let $a = 14$ and $b = 15$. The positive divisors of $a = 14$ are: 1, 2, 7, 14. On the other hand, the positive divisors of $b = 15$ are : 1, 3, 5, 15. This shows that the only common positive divisor and hence the greatest common divisor of *a* and *b* is 1, and so the given numbers ar relatively prime.

Relatively Prime

Corollary

If $(a,\ b) = d$*, then* $(a/d,\ b/d) = 1$*.*

Example

The above corollary states that if we divide *a* and *b* by their gcd, then the quotients will already be relatively prime. As an example, consider $(36,\ 28) = 4 = d$. If we divide 36 and 24 by $d = 4$, we get 9 and 7, respectively. it is clear that (9, 7) = 1, so 9 and 7 are relatively prime.

Corollary

If $a|c$ *and* $b|c$*, and if* $(a,\ b) = 1$*, then* $ab|c$*.*

Relatively Prime

Theorem

Let $a, \ b$ be two integers which are not both zero. Then $(a, \ b) = 1$ if and only if there exist positive integers x and y such that $1 = ax + by$.

Example

In the earlier example, we showed that $(14, \ 15) = 1$, so we should be able to express 1 as a linear combination of 14 and 15. Clearly, the required linear combination is

$$1 = 1(15) + (-1)(14)$$

Relatively Prime

Example

Show that for any positive integer a, we have $(2a+1,\ 9a+4)=1$. *Solution:*
Observe that because of the previous Theorem, it is sufficient to show that 1 can be expressed as a linear combination of $2a+1$ and $9a+4$. We can write

$$1 = 9(2a+1) + (-2)(9a+4)$$

and hence $(2a+1,\ 9a+4)=1$.

Relatively Prime

Theorem

(*Euclid's Lemma) If* $a|bc$ *and* $(a,\ b) = 1$*, then* $a|c$.

Remark

The above theorem says that if an integer a divides a product bc and it does not have any common factor other that 1 with b, then a must divide the second factor c.

Example

Let $a = 4$ and $bc = 72 = 9(8)$ with $b = 9$ and $c = 9$. Since $(a,\ b) = (4,\ 9) = 1$, we have $a|c = 4|8$.

The next theorem gives an alternative set of conditions in order for a positive integer *d* to be the greatest common divisor of two or more integers. The second condition says that *d* must be be the biggest among the common divisors of the given integers.

Theorem

Let $a,\ b \in \mathbb{Z}$ such that a and b are not both zero. Then $d = (a,\ b)$ if and only if the following conditions are satisfied:

1. $d|a$ *and* $d|b$
2. *If c is a positive integer such that* $c|a$ *and* $c|b$*, then* $c|d$.

Exercises

1. If $a|b$ and $a|c$, then $a^2|bc$.
2. The sum of the squares of two odd integers can not be a perfect square, i.e. if x and y are both odd, then there is no perfect square z^2 such that $x^2 + y^2 = z^2$.
3. Verify that for any integer a, we have $3|a(a+1)(a+2)$.
4. Show that for any integer a, we have $(5a+2, 7a+3) = 1$.
5. If a and b are integers which are not both zero, prove that $(2a-3b,\ 4a-5b)$ divides b.
6. If $(a,\ b) = (a,\ c) = 1$, prove that $(a,\ bc) = 1$.
7. If a and b are both odd integers, prove that $16|(a^4 + b^4 - 2)$.

Euclidean Algorithm

We have discussed some properties of the greatest common divisor. One of these is that the *gcd* of two integers is always expressible as a linear combination of the given integers. However, this is not very easy to do when the integers are big. In this section, we will present another method for determining the gcd. It also shows how the gcd can be expressed as a linear combination of the given integers. We begin with the following lemma, which is the basis for the proof of the main procedure.

Euclidean Algorithm

Lemma

If $a = bq + r$, then $(a,\ b) = (b,\ r)$.

Proof:

Let $a,\ b \in \mathbb{Z},\ \ a > 0$. By repeatedly applying the division algorithm, we can obtain a sequence of equations of the form

to $\mathrm{b} = \mathrm{q}_1 a + r_1,\ 0 \le r_1 < a$

$\mathrm{a} = \mathrm{q}_2 r_1 + r_2,\ 0 \le r_2 < r_1$

$\mathrm{r}_1 = q_3 r_2 + r_3,\ 0 \le r_3 < r_2$

$\vdots$

$\vdots$

$\mathrm{r}_{k-2} = q_k r_{k-1} + r_k,\ 0 \le r_k < r_{k-1}$

$\mathrm{r}_{k-1} = q_{k+1} r_k$

so that r_k is the last nonzero remainder. Then $(a,\ b) = r_k$. Moreover, $(a,\ b)$ can be expressed as a linear combination of a and b by eliminating the remainders $r_i,\ i = 1,\ 2,\ k-1$ from the above equations.

Euclidean Algorithm

By repeatedly applying the lemma, we get $(a,\ b) = (b,\ r) = (r,\ r_1) = (r_1,\ r_2) = \cdots = (r_{k-2},\ r_{k-1}) = (r_{k-1},\ r_k) = r_k$ since the last equation shows that r_{k-1} is a multiple of r_k and so r_k is their greatest common divisor.

Working our way backwards from the second to the last equation, we get

$$\begin{aligned} r_k &= r_{k-2} + (-q_k) r_{k-1} \\ &= \mathrm{r}_{k-2} + (-q_k)\{r_{k-3} + (-q_{k-1}) r_{k-2}\} \\ &= (\text{-}\mathrm{q}_k) r_{k-3} + r_{k-2}(1 + q_k q_{k-1}) \end{aligned}$$

We continue to eliminate the remainders in the sequence $r_{k-1},\ r_{k-2},\ r_{k-3},\ \ldots,\ r_1$ until r_k is expressed as a linear combination of a and b.

Example

Use the Euclidean algorithm to find (840, 504).
We obtain the following equations:

$$\begin{aligned} 840 &= (504)(1) + 336 \\ 504 &= (336)(1) + 168 \\ 336 &= (168)(2) + 0 \end{aligned}$$

so that the last nonzero remainder and hence the greatest common divisor is 168. To express 168 as a linear combination of 840 and 504, we have

$$\begin{aligned} 168 &= (504)(1) + (336)(-1) \\ &= (504)(1) + [(840)(1) + (504)(-1)](-1) \\ &= (840)(-1) + (504)(2) \end{aligned}$$

An immediate corollary to the theorem concerning the Euclidean Algorithm is stated as follows:

Corollary

If $c > 0$, then $(ca,\ cb) = c(a,\ b)$.

Least Common Multiple

Definition

Let $a,\ b$ be nonzero integers. A positive integer $m = [a,\ b]$ is called the **least common multiple** of a and b if it satisfies the following:

(a) $a|m$ and $b|m$

(b) If $a|c$ and $b|c$, where $c > 0$, then $m|c$

Example

Let $a = 12$ and let $b = 15$. The first few positive multiples of 12 are 12, 24, 36, 48, 60, 72, 84, 96, 108, 120 while the first few positive multiples of 15 are 15, 30, 45, 60, 75, 90, 105, 120. We see that 60 is the smallest common multiple of 12 and 15, and so we write [12, 15] = 60.

Least Common Multiple

The following theorem gives the basic properties of the least common multiple, aside from those included in the definition:

Theorem

Let $m = [a,\ b]$. Then we have

1. *If $a|n$ and $b|n$, then $m \leq n$.*
2. $[a,\ b] = b$ *if and only if* $a|b$.
3. $\max \{\ a,\ b\ \} \leq m \leq ab$.
4. *If $c|a$ and $c|b$, then $\left[\frac{a}{c},\ \frac{b}{c}\right] = \frac{m}{c}$.*
5. *For any positive integer n, we have $[an,\ bn] = n\,[a,\ b]$.*

Theorem

Let $a,\ b$ be positive integers. Then

$$(a,\ b)\,[a,\ b] = ab$$

An immediate consequence of Theorem **??** is the following corollary:

Corollary

Let a and b be positive integers. Then $[a,\ b] = ab$ if and only if $(a,\ b) = 1$.

Exercises

1. For each pair of integers, use the Euclidean algorithm to find the greatest common divisor of the numbers in the pair.
   1. 102, 402
   2. 231, 273
   3. 126, 621
   4. 104, 299
   5. 221, 273
   6. 185, 222
2. Use the Euclidean algorithm to obtain integers x and y satisfying the following:
   1. $(56,\ 72) = 56x + 72y$
   2. $(1769,\ 2378) = 1769x + 2378y$
3. Find all pairs of integers a and b such that $1 \leq a < b \leq 10$ and $(a,\ b) = 1$.
4. Find $[306,\ 657]$ using the equation given in Theorem **??**