

The Euclidean Algorithm and Diophantine Equations

Donald Rideout, Memorial University of Newfoundland¹

Let $\mathbf{Z} = \{0, \pm 1, \pm 2, \dots\}$ denote the set of *integers*. For $a, b \in \mathbf{Z}$, $a \neq 0$, we say b is *divisible by an integer a* , or a *divides b* , or a is a *divisor of b* , and we write $a \mid b$, if $b = ac$, for some $c \in \mathbf{Z}$. Otherwise, we write $a \nmid b$. For example, $6 \mid 48$ since $48 = 6 \cdot 8$ and $-6 \mid 48$ since $48 = (-6)(-8)$. As an exercise, given integers a, b, c , $a \neq 0$, and $a \mid b$, $a \mid c$, prove that $a \mid (bx + cy)$ for any integers x and y .

Let $a, b \in \mathbf{Z}$, not both zero. We say $g \in \mathbf{Z}$ is a *greatest common divisor (gcd)* of a and b , and we write $g = (a, b)$, if

- (i) g is a common divisor of a and b , that is, $g \mid a$ and $g \mid b$.
- (ii) g is the greatest of the common divisors of a and b .

How do we find the gcd?

Method 1. (Elementary School) Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, where $\alpha_i \geq 0$ and $\beta_i \geq 0$. Then $g = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \dots p_r^{\min\{\alpha_r, \beta_r\}}$.

For example, if $a = 40 = 2^3 \cdot 5$ and $b = 225 = 3^2 \cdot 5^2$, then $a = 2^3 \cdot 3^0 \cdot 5^1$ and $b = 2^0 \cdot 3^2 \cdot 5^2$ so $g = 2^0 \cdot 3^0 \cdot 5^1 = 5$. There are real problems with this method since we are using the Fundamental Theorem of Arithmetic which says that every integer $n \geq 2$ can be factored uniquely into primes. This theorem is proved using an alternate method for finding gcd's and hence we have a problem with "circular reasoning." The above method is quite inefficient since we need to know the factorization of the number into primes, and for large numbers this is impractical.

The second method uses the Division Algorithm which states that if $a \neq 0$ and b is any integer, then there is an integer r such that $b = qa + r$ where $0 \leq r < |a|$. This is just the "Long Division" algorithm.

Method 2. This method finds the gcd by subtracting multiples of the larger number from the smaller, where we assume, without any loss of generality, that the numbers a and b are non-negative.

Theorem 1 *If $b = qa + r$, then $(a, b) = (a, b - qa) = (a, r)$.*

SUMMARY: Given any two integers, not both zero, subtracting a multiple of one number from the other changes the pair but not the gcd.

Before we prove this theorem, we give an example using the above result. Find $g = (679, 210)$. Using the theorem we have $(679, 210) = (679 - 3(210), 210) = (49, 210) = (49, 210 - 4(49)) = (49, 14) = (49 - 3(14), 14) = (7, 14) = (7, 14 - 2(7)) = (7, 0) = 7$.

¹Talk given at CMC Seminar, Waterloo, June 1997

Observe that we never needed to factor the numbers into primes! The Division Algorithm guarantees that the numbers get smaller until zero is reached.

Proof. Let $g = (a, b)$ and $g' = (a, b - qa)$. Then $g' \mid a$ and $g' \mid b - qa$, and hence $a = g'c$ and $b - qa = g'd$. Therefore $b = qa + g'd = qg'c + g'd = g'(qc + d)$, and hence $g' \mid b$. That is, g' is a common divisor of a and b , and by the definition of g , $g' \leq g$. A similar argument shows that $g \leq g'$ and hence $g = g'$. \square

The Division Algorithm can be used to show that there exist integers x_0 and y_0 such that

$$g = (a, b) = ax_0 + by_0.$$

Using the Division Algorithm, the sequence of computations showing that $7 = (679, 210)$ can be written as follows:

$$\begin{aligned} 679 &= 210(3) + 49 \\ 210 &= 49(4) + 14 \\ 49 &= 14(3) + 7 \\ 14 &= 7(2) + 0 \end{aligned}$$

where the sequence of remainders decrease to zero. This is an example of the more general Euclidean Algorithm.

Theorem 2 *Given positive integers a and b , we have by the Division Algorithm the following equations*

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b, \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} + 0. \end{aligned} \tag{1}$$

The gcd of a and b is r_j , the last nonzero remainder in the division process. Values of x_0 and y_0 in $(a, b) = ax_0 + by_0$ can be obtained by eliminating the remainders r_{j-1}, \dots, r_2, r_1 from the set of equations.

We will not prove this theorem, but we will show how to use the theorem for the above example. From (1) we have:

$$\begin{aligned} 7 &= 49 - 14(3) \\ &= 49 - (210 - 49(4))(3) \\ &= 49(13) - 210(3) \\ &= (679 - 210(3))(13) - 210(3) \\ &= 679(13) + 210(-42). \end{aligned}$$

To find x_0 and y_0 such that $(a, b) = ax_0 + by_0$ it would be convenient to be able to work forward through the Equations (1). Let a and b be positive integers. Write

down the first two rows in the following table, and then add rows by the following rule. Obtain the i th row from the previous two rows by subtracting q_i times the $(i - 1)$ st row from the $(i - 2)$ nd row where $q_i = [r_{i-2}/r_{i-1}]$, the greatest integer in r_{i-2}/r_{i-1} . We will illustrate the method by choosing the above numbers $a = 679$ and $b = 210$.

1	0	a
0	1	b
c_1	d_1	r_1
c_2	d_2	r_2
\vdots	\vdots	\vdots
c_j	d_j	r_j
c_{j+1}	d_{j+1}	0

c_n	d_n	r_n
1	0	679
0	1	210
1	-3	49
-4	13	14
13	-42	7
-30	97	0

q_{n+1}
3
4
3
2

Hence

$$\begin{aligned} c_i &= c_{i-2} - q_i c_{i-1} \\ d_i &= d_{i-2} - q_i d_{i-1} \\ r_i &= r_{i-2} - q_i r_{i-1} \end{aligned}$$

where $c_{-1} = 1, d_{-1} = 0, r_{-1} = a, c_0 = 0, d_0 = 1$ and $r_0 = b$. The algorithm will terminate when $r_{j+1} = 0$. Then $(a, b) = r_j$ and each row (c_i, d_i, r_i) will satisfy the equation

$$ac_i + bd_i = r_i$$

and, in particular, $ac_j + bd_j = r_j = (a, b)$. How can this be proved? First, check the result for $i = -1$ and $i = 0$, and suppose that

$$\begin{aligned} r_{n-2} &= ac_{n-2} + bd_{n-2} \\ r_{n-1} &= ac_{n-1} + bd_{n-1} \end{aligned}$$

Then

$$\begin{aligned} ac_n + bd_n &= a(c_{n-2} - q_n c_{n-1}) + b(d_{n-2} - q_n d_{n-1}) \\ &= (ac_{n-2} + bd_{n-2}) - q_n(ac_{n-1} + bd_{n-1}) \\ &= r_{n-2} - q_n r_{n-1} \\ &= r_n. \end{aligned}$$

Note that we can find x_0 and y_0 simply by knowing the quotients q_i for $1 \leq i \leq j$ in Equations (1). The computations can be carried out very quickly. The numbers in the second last column are the required numbers. That is, $7 = 679c_3 + 210d_3 = 679(13) + 210(-42)$.

The following short QuickBasic™ program computes the gcd and computes the numbers x_0, y_0 so that $g = ax_0 + by_0$.

```
PRINT "ENTER A AND B WITH B > 0" INPUT A, B
C1 = 1: C2 = 0: D1 = 0: D2 = 1: AA = A: BB = B
DO WHILE B > 0
  Q = INT(A / B): T = B: B = A
```

```
- Q * B: A = T T = C2: C2 = C1 - C2 * Q: C1 = T T = D2: D2 = D1 - D2 * Q:
D1 = T LOOP PRINT "THE GCD ="; A PRINT AA; "*" ; C1; "+" ; BB; "*" ; D1;
"=" ; A END
```

The Waterloo Maple software has several gcd programs. The best one for integers is `igcd` or `igcdex`. For example, `igcd(679, 210)`; gives the output 7, and `igcdex(679, 210, 's', 't');``s;t`; gives the output 7, 13, and -42 .

It is quite natural next to study the equation $ax + by = n$ and investigate the problem of finding *all* the integral solutions for any given $a, b, n \in \mathbf{Z}$. Such an equation is called a Diophantine equation in honour of the Greek mathematician Diophantus (4th century A.D.?) who first investigated the problem of finding integral solutions to equations, particularly the cases with more unknowns than equations. The next theorem is an important lemma needed to prove the next theorem (and also to prove the Fundamental Theorem of Arithmetic).

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

Proof. Since $(b, c) = 1$, there exists integers x and y such that $bx + cy = 1$. Multiplying by a we have $abx + acy = a$. Clearly c divides the left side of this last equation and hence c divides a . \square

Theorem 3 *If $(a, b) = 1$ and n is any integer, then $ax + by = n$ has a solution $x = x_0$ and $y = y_0$. Furthermore, all solutions are given by the equations*

$$\begin{aligned}x &= x_0 + bt \\y &= y_0 - at\end{aligned}$$

for all integral values of t .

Proof. Since $(a, b) = 1$, there exist integers x_1 and y_1 such that $ax_1 + by_1 = 1$. Then $x_0 = nx_1$ and $y_0 = ny_1$ is clearly a solution of $ax + by = n$ since

$$a(nx_1) + b(ny_1) = n \cdot 1.$$

Let x' and y' be another solution, then we have

$$ax' + by' = n$$

and

$$ax_0 + by_0 = n$$

so that

$$a(x' - x_0) + b(y' - y_0) = 0$$

and

$$a(x' - x_0) = -b(y' - y_0).$$

Since $(a, b) = 1$, provided $b \neq 0$ (note one of a or b is not zero, why?), it follows that $b \mid x' - x_0$ and therefore that $x' - x_0 = bt$ for some $t \in \mathbf{Z}$, or $x' = x_0 + bt$. Substituting bt for $x' - x_0$, we obtain

$$abt = -b(y' - y_0).$$

After cancelling b we have $y' = y_0 - at$.

We are finished if we check that $x = x_0 + bt, y = y_0 - at$ satisfy $ax + by = n$ for all integral values of the parameter t . \square

In general, if $(a, b) = g$ then $ax + by = n$ has a solution if and only if $g \mid n$. If $g \mid n$ then clearly the equations

$$\begin{aligned} ax + by &= n \\ \frac{a}{g}x + \frac{b}{g}y &= \frac{n}{g} \end{aligned}$$

have precisely the same solutions, and hence the theorem covers the general situation since g can be divided out.

Example. Solve the Diophantine equation $8x + 5y = 100$.

Solution 1. Since $8x = 5(20 - y)$ then $5 \mid 8x$, and hence $5 \mid x$ since $(5, 8) = 1$. Let $x = 5t$ for $t \in \mathbf{Z}$. Then $8(5t) + 5y = 100$ implies $8t + y = 20$. Hence, all solutions of $8x + 5y = 100$ are given by

$$\begin{aligned} x &= 5t \\ y &= 20 - 8t \end{aligned}$$

where t is any integer.

Solution 2. By inspection, $8(2) + 5(-3) = 1$ and, hence, a particular solution is $x_0 = 2(100) = 200$ and $y_0 = -3(100) = -300$. All solutions are of the form

$$\begin{aligned} x &= 200 + 5t \\ y &= -300 - 8t \end{aligned}$$

where t is any integer.

Example. Solve the Diophantine equation $69x + 111y = 9000$.

Solution. Since $(69, 111) = 3(23, 37) = 3$, we solve the equivalent equation $23x + 37y = 3000$. Since $23(-8) + 37(5) = 1$ then a particular solution is $x_0 = -8(3000) = -24,000$ and $y_0 = 5(3000) = 15,000$. All solutions are of the form

$$\begin{aligned} x &= -24000 + 37t \\ y &= 15000 - 23t \end{aligned}$$

where t is any integer.

Problems.

1. Find, if possible, the complete solution to the following Diophantine equations.

$$\begin{array}{lll} \text{(i)} & 28x + 35y = 60 & \text{(ii)} \quad 21x + 15y = 9 & \text{(iii)} \quad 343x + 259y = 658 \\ \text{(iv)} & 14x + 9y = 1000 & \text{(v)} \quad 12x + 57y = 423 & \text{(vi)} \quad 11x - 12y = 13. \end{array}$$

Now find all the positive solutions, if any, of each of the above equations.

2. A customer has a large quantity of dimes and quarters. In how many different ways can he pay exactly for an item that is (i) worth \$3.49 or (ii) worth \$2.65?
3. When a man cashed a cheque, the clerk mistook the number of cents for the number of dollars, and vice versa. After spending 68 cents, the man discovered that he still had precisely twice as much money as the amount for which the cheque was originally written. What is the smallest amount for which the cheque could have been written?
4. A certain course has 120 students of whom 86 faithfully attended classes while 34 did not. The instructor would like to assign the same final integral mark to each student in the first group (i.e., those who attended classes) and a second lower integral mark to each of the students in the other group. In addition, the instructor would like the class average to be exactly 70. What mark should the instructor assign?
5. The Smiths run a restaurant which charges a flat fee of \$11.00 per adult and \$7.00 per child. At the end of an evening the total in the cash register is \$657.00. What is the smallest number of people who could have dined that day? largest number?
6. An oil company has a contract to deliver 100,000 litres of gasoline. Their tankers can carry 2,400 litres, and they can attach one trailer carrying 2,200 litres to each tanker. All the tankers and trailers must be completely full on this contract, otherwise, the gas would slosh around too much when going over some rough roads. Find the least number of tankers required to fulfill the contract. Each trailer, if used, must be pulled by a full tanker.
7. A man purchased at a post office some one-cent stamps, three-quarters as many two's as one's, three-quarters as many five's as two's, and five eight-cent stamps. He paid for them with a single bill, and there was no change. How many stamps of each kind did he buy? (Assume there are 1(loonie?), 2, 5, 10, 20, 50, 100, 1000, and 10000 dollar bills.)

Solutions.

1. (i) no solution (ii) $x = -6 + 5t$, $y = 9 - 7t$, $t \in \mathbf{Z}$; no positive solutions.
 (iii) $x = -282 + 37t$, $y = 376 - 49t$, $t \in \mathbf{Z}$; no positive solutions.
 (iv) $x = 2000 + 9t$, $y = -3000 - 14t$, $t \in \mathbf{Z}$. There are eight positive solutions:

x	2	11	20	29	38	47	56	65
y	108	94	80	66	52	38	24	10

- (v) $x = 705 + 19t$, $y = -141 - 4t$, $t \in \mathbf{Z}$. There are two positive solutions:
 $(x, y) = (2, 7)$ and $(21, 3)$.

2. (i) no solution
 (ii) If $x =$ the number of dimes and $y =$ the number of quarters, then the five possible ways are given in the table:

x	4	9	14	19	24
y	9	7	5	3	1

($x = -106 + 5t$, $y = 53 - 2t$, $t \in \mathbf{Z}$ is the general solution of $10x + 25y = 265$.)

3. \$10.21
4. 87% and 27%
5. smallest number = 63; largest number = 91.
6. The least number of tankers is 27.
7. 18,816 ones, 14,112 twos, 10,584 fives, and 5 eights. (Ross Honsberger in his book *Mathematical Morsels* entitles this problem "A Mathematical Joke".)