The Linear Combination Implied By the Euclidean Algorithm Using a TI84-CE Program

Timothy W. Jones

Abstract

The Euclidean Algorithm finds the greatest common divisor (GCD) of two integers; it also gives a way to express the GCD as a integer linear combination of the two numbers. This latter feature is not easily done by hand. We present programs for the Euclidean Algorithm and give a fast and easy way to find the linear combination.

Introduction

The numbers less than and relatively prime to any positive integer is a group under multiplication [2, 3]. To show every element in say the group of integers less than 18 and relatively prime to it, call it $RP(\equiv_{18}, *)$ is a group under multiplication modulo 18 requires that each of the classes given by $\{1, 5, 7, 11, 13, 17\}$ has an inverse.[1] If $A \in RP(\equiv_{18}, *)$ then

$$GCD(A, 18) = 1$$

is a given. Expressing A as a linear combination yields $AX + 18Y = 1$. Is X in a relatively prime class? If it shares a factor with 18, say $X = 3R$, then $A3R + 18Y = 1$ forces $3|1$, a contradiction. So yes, A has an inverse in $\in RP(\equiv_{18}, *)$, if we can find these X and Y values.

Abstract Algebra books prove the Euclidean Algoithm and they show in theory that X and Y exist. Schaum's Outline for Abstract Algebra [1] shows how to find the actual X and Y in

$$758X + 242Y = GCD(758, 242) = 2 \text{ and } 726X + 275Y = 11$$

[1] We reference classes with the smallest positive element in the class.

using the Euclidean Algorithm. It is difficult and hard to follow. It doesn't have to be. There is a easy trick using complex numbers that makes both hand calculations and computer programs much easier.

Ordered Pairs

Take the example of finding X and Y for 758 and 242. Suppose we have computed the sequence of $N = DQ + R$ given in Table 1. Our nomenclature: N, number; D, divisor; Q, quotient; and R, remainder. The quotients are in parenthesis in Table 1.

$758 = 242(3) + 32$	$758 - 242(3) = 32$
$242 = 32(7) + 18$	$242 - 32(7) = 18$
$32 = 18(1) + 14$	$32 - 18(1) = 14$
$18 = 14(1) + 4$	$18 - 14(1) + 4$
$14 = 4(3) + 2$	$14 - 4(3) = 2$
$4 = 2(2)$	$4 - 2(2) = 0$

Table 1: Euclid's Algorithm produces a decreasing sequence of remainders that must terminate in 0.

We are interested in the second column. Let $(1, 0)$ be 758 and $(0, 1)$ be 242. Then the first row, second column can be expressed as $(1, 0) - (0, 1)3 = (1, -3)$. We can then express the second row, second column with $(0, 1) - (1, -3)7 = (-6, 22)$. We are tracking how to express numbers using integer linear combinations of 758 and 242. Table 2 gives the translations to these ordered pairs.

We've crunched $X = 53$ and $Y = -166$. We can do a check with the dot product: $(758, 242) * (53, -166) = 2$ and 2 is the $GCD(758, 242)$.

The TI84 family of calculators does support lists. The only thing we need is a list of quotients. In the case of $(758, 242)$, this list can be created with the code $\{3, 7, 1, 1, 3\} \rightarrow L_1$. The calculator also supports complex numbers. Thus it can crunch $(8, -25) - (-15, 47)3$ easily with

$$(8 - 25i) - (-15 + 47i)3 = 53 - 166i.$$

$758 - 242(3) = 32$	$(1,0) - (0,1)3 = (1,-3)$
$242 - 32(7) = 18$	$(0,1) - (1,-3)7 = (-7,22)$
$32 - 18(1) = 14$	$(1,-3) - (-7,22)1 = (8,-25)$
$18 - 14(1) + 4$	$(-7,22) - (8,-25)1 = (-15,47)$
$14 - 4(3) = 2$	$(8,-25) - (-15,47)3 = (53,-166)$
$4 - 2(2) = 0$	$(-15,47) - (53,-166)2 = (-121,379)$

Table 2: The calculations of remainders are simplified by making them in terms of basis of the two given numbers.

Program for X and Y

We will assume that we have such a list of quotients for $(726, 275)$: $\{2, 1, 1, 1, 3\}$. Figure 1 gives a calculator program (and print out) that takes this list and generates the X and Y ordered pair for it. The complexity is much less than that of Schaum's Outline. Note: We make $1 + 0i$ our first number and $0 + 1i$ our second; the calculator doesn't support ordered pairs as such, but complex numbers are ordered pairs.

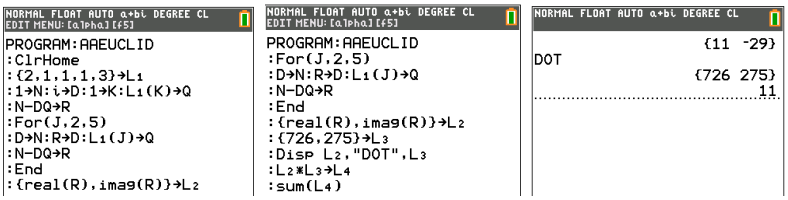

Figure 1: Left: The code gives R = 11-29i. The last line puts the two components into L_2. Middle: L_3 contains the start up numbers 726 and 275. Right: The dot product of $(11, -29)$ and $(726, 275)$ is 11, the GCD of 726 and 275.

The Euclidean Algorithm

Figure 2 gives a version of the Euclidean Algorithm that generates the list needed for the above X and Y program.

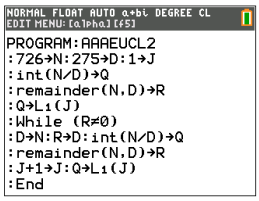

Figure 2: Code for generating the list of quotients needed for the X and Y program.

Conclusion

There is some minor tweaking that the program needs involving the dimensions of the L_1 list. These are nice challenges.

References

[1] Ayres, F., Jaisingh, L. (2004) *Schaums Outline of Abstract Algebra* 2nd ed., New York: McGraw-Hill.

[2] Birkoff, G., MacLane, S. (1977) *A Survey of Modern Algebra*, 4th ed. New York: Macmillan.

[3] Herstein, I.N. (1975) *Topics in Algebra*, 2nd ed., New York: Wiley.