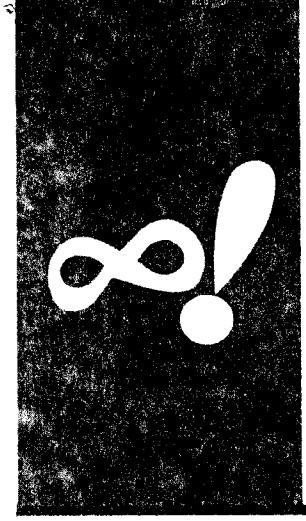

M·A·T·H·E·M·A·T·I·C·A·L R·E·C·R·E·A·T·I·O·N·S

Mathematical programming

Diophantine Equations

Finding whole-number solutions to equations

BY ROBERT T. KUROSAKA

A man buys some x's at $154 each and some y's at $69 each. If he spends a total of $5000, how many of each did he buy?

Although this problem appears to be from a first-year algebra text, we find that the techniques required are not usually found in a "mainstream" course in mathematics. The equation $154x + 69y = 5000$ has infinitely many solutions. However, assuming the man bought whole-number quantities, we want *integral* solutions (x,y) for the equation, and now we need a method for solving such equations.

DIOPHANTINE EQUATIONS

Equations of the form $ax + by = c$, for integral a, b, and c and integral solutions (x,y), are called Diophantine equations. No one is certain when or where Diophantus of Alexandria was born. Sources vary from "born about A.D. 50" to "flourished about A.D. 250." He is called "the father of algebra" having promoted algebraic notation and algebraic treatment of mathematical problems. Previously such work was done by "rhetorical algebra" or geometric proofs.

A variety of methods are available for solving Diophantine equations. One of these is modulo arithmetic, a powerful and fascinating concept that I may explore more closely in a future column.

A very simple method of solving our original problem comes to mind. Since the equation is equivalent to $y = (5000 - 154x)/69$, we can simply try consecutive values of x (from 1 to 32 only) until we get an integral value for y.

Since we are mathematically inclined, such an inelegant approach may not sit well with us. Rather, we may prefer to look for a method of solution based on general principles of mathematics. What can we say in general about integral solutions for an equation of the form $ax + by = c$?

First, we can readily see under what conditions the equation would have no solution. Consider the greatest common denominator (GCD) of a and b. We will call it d. If d is not a factor of c, the equation will have no integral solutions. Why? Since a/d is, by hypothesis, an integer and b/d is also one, the value $(a/d)x + (b/d)y$ will be an integer if x and y are integers. That is, the integers are *closed* under addition and multiplication. Thus, if c/d is not an integer, either x or y must not be an integer.

DIOPHANTUS MEETS EUCLID

This leads us to Euclid's algorithm, which was the subject of my last column in January (page 397). If we employ Euclid's algorithm to determine the GCD of a and b, we can immediately determine whether there are integer solutions to the Diophantine equation by dividing the GCD into c. But we can use Euclid's algorithm for much more than that. To see how, let us reexamine the algorithm with an eye toward solving Diophantine equations. Figure 1 outlines the way the Euclidean algorithm finds the GCD of 154 and 69. Their GCD is 1, meaning that the two numbers are relatively prime. Now, to begin our examination of the way to solve Diophantine equations, let's modify our original equation to $154x' + 69y' = 1$. That is, we will begin with the case where c is equal to the GCD.

In figure 2, I have rewritten the divisions of figure 1 as equations. In order to find integer values of x' and y' that solve the equation $154x' + 69y' = 1$, all I need to do is substitute $154 - 2(69)$ for 16 in equations 2 and 3 and $69 - 4(154 - 2(69))$ for 5 in equation 3. After collecting terms, I find that $1 = 13(154) - 29(69)$. Thus, $x' = 13$, $y' = -29$ will satisfy the equation $154x' + 69y' = 1$. We will call $(13, -29)$ the *basic solution* to $154x' + 69y' = 1$. Is it the *only* solution?

Let us write our equation in the general form again: $ax + by = c$. Now, let n be any integer and d be the GCD of a and b. If we add 0 to the left-hand side of the equation, we haven't changed it, so $ax + by + (nab/d -$

(continued)

Robert T. Kurosaka teaches mathematics in the Massachusetts State College system. He invites your correspondence c/o BYTE, POB 372 Hancock, NH 03449.

$nab/d) = c$. Rearranging, $ax + nab/d + by - nab/d = c$. Collecting terms, $a(x + nb/d) + b(y - na/d) = c$. So, once we have the basic solution for x and y, we can generate an infinite number of x's and y's that satisfy the equation by selecting any integer n, multiplying it by b/d, and adding it to the basic solution value of x while we multiply n by a/d and subtract it from the basic solution y. In the case of $154x' + 69y' = 1$, where the basic value of x' is 13, the basic value of y' is -29, and d is 1, any set of numbers (x'',y'') such that $x'' = 13 + n(69)$ and $y'' = -29 - n(154)$ will satisfy the equation.

So far, I have shown two things. First, if c is not a multiple of the GCD of a and b, there is no solution to the Diophantine equation. Second, if c equals the GCD of a and b, the Euclidean algorithm will provide a path for finding all integer solutions of x and y. But what if c is a multiple of the GCD of a and b?

We have let d equal the GCD of a and b. We will now introduce one last letter, e, such that $e = c/d$. Then, $c = de$. Since $ax' + by' = d$ and $c = de$, $e(ax' + by') = de = c$. Thus, $x = x'e$, $y = y'e$, and $a(x'e) + b(y'e) = c$. That is, to solve the equation $ax + by = c$, we solve the equation $ax' + by' = d$, find e such that $e = c/d$, and multiply x' by e and y' by e to find the basic solution of $ax + by = c$. Listing 1 (available for downloading from BYTEnet Listings at (617) 861-9764 or on disk [see page 358]) provides a BASIC program that prompts you to enter the Diophantine equation, checks to make sure that there are integer solutions, and then prints out the basic solutions for x and y, the GCD of a and b, and the parametric equations for obtaining all integer solutions to the Diophantine equation (see figure 3). Other than the Euclidean algorithm that was discussed last time, the program is just a lot of bookkeeping, so I won't bother discussing it here.

To find the GCD of 154 and 69 by the Euclidean algorithm:

1. Divide 154 by 69.

```
        2
   69 | 154
        138
        ---
         16
```

2. Divide the divisor by the remainder.

```
        4
   16 | 69
        64
        --
         5
```

3. Repeat step 2 until the remainder is 0.

```
        3
    5 | 16
        15
        --
         1
```

4. The GCD is the last nonzero remainder, or 1.

```
        5
    1 | 5
        5
        -
        0
```

Figure 1: *The Euclidean algorithm is illustrated with the numbers 154 and 69.*

Rewrite the divisions of figure 1 as equations:
1. $16 = 154 - 2(69)$
2. $5 = 69 - 4(16)$
3. $1 = 16 - 3(5)$

Substitute $154 - 2(69)$ for 16:
2. $5 = 69 - 4(154 - 2(69))$
3. $1 = 154 - 2(69) - 3(5)$

Substitute $69 - 4(154 - 2(69))$ for 5:
3. $1 = 154 - 2(69) - 3(69 - 4(154 - 2(69)))$

Collect terms to find the basic solution to $154x + 69y = 1$:
3. $1 = 13(154) - 29(69)$

Figure 2: *How to use the Euclidean algorithm to find basic solutions to Diophantine equations.*

Less Is More

What's that? The man in our starting problem didn't buy a negative number of x's or y's? Okay, we're almost done. For $154x + 69y = 5000$, $a = 154$, $b = 69$, $c = 5000$, $d = 1$, $e = 5000$, $x' = 13$, and $y' = -29$. Thus, $x = 13(5000)$, or 65,000, and $y = -29(5000)$, or $-145{,}000$. The parametric equation for all x solutions is $x = 65{,}000 + 69n$; for y, $y = -145{,}000 - 154n$. Since both x and y must be greater than 0, we can write $0 < 65{,}000 + 69n$ for x and $0 < -145{,}000 - 154n$ for y. Thus, $n > -65{,}000/69$ and $n < 145{,}000/(-154)$. Combining and simplifying, $-941.56 > n > -942.03$. Therefore, $n = -942$ and $x = 65{,}000 - 69(942)$, or 2, and $y = -145{,}000 + 154(942)$, or 68. Writing a program to handle inequalities is kind of a pain, so I'll leave that as an exercise for you (don't you wish *you* were a columnist?).

Mail Call

I have been receiving a lot of interesting mail recently. Professor Gernot

(continued)

Listing 1: A BASIC *program to solve Diophantine equations.*

```
10 '*************************************************
20 '*          DIOPHANTINE EQUATION SOLVER           *
30 '*                BY BOB KUROSAKA                 *
40 '*************************************************
50 CLS
60 PRINT "This program solves equations of the form AX + BY = C,"
70 PRINT "where A, B, C, X, and Y are all integer values."
80 PRINT :PRINT "Enter your equation as shown in the general form."
90 PRINT "For example, enter 154X + 69Y = 5000 or 154X-69Y = 5000."
100 PRINT "Do not enter negative coefficients with parentheses."
110 PRINT "That is, do NOT enter 154X + (-69Y) = 5000."
120 PRINT :PRINT "The program will not work properly for the degenerate case"
130 PRINT "where either A or B is 0."
140 PRINT :INPUT "Enter equation";EQUATION$.A$=EQUATION$
150 REM DEFINE A READABLE FUNCTION FOR DISCARDING LEFTMOST
    CHARACTERS.
160 DEF FNDROP.LEFT$(A$)=RIGHT$(A$,LEN(A$)-1)
170 REM PARSING ROUTINE
180 A=VAL(A$)
190 IF A=0 THEN A=1:IF LEFT$(A$,1)="-" THEN A=-1
200 A$=FNDROP.LEFT$(A$)
210 DISCARD$=LEFT$(A$,1)
220 WHILE DISCARD$<>"+" AND DISCARD$<>"-"
230       A$=FNDROP.LEFT$(A$)
240       DISCARD$=LEFT$(A$,1)
250 WEND
260 B=VAL(A$)
270 IF B=0 THEN B=1:IF DISCARD$="-" THEN B=-1
280 WHILE DISCARD$<>"="
290       A$=FNDROP.LEFT$(A$)
300       DISCARD$=LEFT$(A$,1)
310 WEND
320 A$=FNDROP.LEFT$(A$)
330 C=VAL(A$)
340 IF A<>INT(A) OR B<>INT(B) OR C<>INT(C) THEN PRINT "NOT A
                                    DIOPHANTINE EQUATION".GOTO 760
350 REM END OF PARSING ROUTINE
360 REM EUCLIDEAN ALGORITHM FOR FINDING GCD.
370 REM FIRST, INITIALIZE THE TERMS FOR THE ALGORITHM
380 IF ABS(A)>=ABS(B) THEN DIVIDEND=A:DIVISOR=B
390 IF ABS(A)<ABS(B) THEN DIVISOR=A:DIVIDEND=B:SWAP.XY$="YES"
400 REM USE 'FIX' INSTEAD OF 'INT' TO TRUNCATE RATHER THAN ROUND
    NEGATIVE #s.
410 QUOTIENT=FIX(DIVIDEND/DIVISOR)
420 REMAINDER=DIVIDEND-DIVISOR*QUOTIENT
430 REM X1=ONGOING COUNT OF X', Y1=ONGOING COUNT OF Y'. YOU
    CAN KEEP TRACK OF ALL ONGOING COUNTS BY USING ONLY THE
    PREVIOUS TWO VALUES FOR X' AND Y', SO WE NEED ONLY X1, X2, X3,
    AND Y1, Y2, Y3.
440 X1=1:Y1=-QUOTIENT
450 REM IF EITHER A OR B IS AN EVEN MULTIPLE OF THE OTHER, THEN
    EITHER X' OR Y' WILL EQUAL 1 WHILE THE OTHER EQUALS 0.
460 IF REMAINDER=0 THEN X2=0:Y2=1:GOTO 620
470 DIVIDEND=DIVISOR:DIVISOR=REMAINDER
480 QUOTIENT=FIX(DIVIDEND/DIVISOR)
490 REMAINDER=DIVIDEND-DIVISOR*QUOTIENT
500 X2=-QUOTIENT*X1:Y2=1-QUOTIENT*Y1
510 REM IF A GCD IS FOUND ON THE SECOND ITERATION OF THE
        EUCLIDEAN ALGORITHM, THEN X'=X1, Y'=Y1. IN ALL
        SUBSEQUENT CASES, X'=X2, Y'=Y2.
520 IF REMAINDER=0 THEN X2=X1:Y2=Y1:GOTO 620
```

(continued)

```
530 REM THE FIRST TWO ITERATIONS ARE THE ONLY ONES THAT DO NOT
        FOLLOW THE PATTERN: X(N) = X(N - 2) - QUOTIENT*X(N - 1),
        Y(N) = Y(N - 2) - QUOTIENT*Y(N - 1).
540 WHILE REMAINDER < > 0
550       DIVIDEND = DIVISOR:DIVISOR = REMAINDER
560       QUOTIENT = FIX(DIVIDEND/DIVISOR)
570       REMAINDER = DIVIDEND - DIVISOR*QUOTIENT
580       IF REMAINDER = 0 THEN 610
590       X3 = X1 - QUOTIENT*X2:Y3 = Y1 - QUOTIENT*Y2
600       X1 = X2:X2 = X3:Y1 = Y2:Y2 = Y3
610 WEND
620 REM CALCULATE BASIC SOLUTION FOR AX + BY = C FROM GCD
        RESULTS, WHICH HAVE PROVIDED AX' + BY' = D BASIC
        SOLUTION.
630 D = DIVISOR:E = C/D
640 IF C/D < > INT(C/D) THEN PRINT "NO INTEGER SOLUTIONS.":GOTO 760
650 IF SWAP.XY$ = "YES" THEN SWAP X2,Y2
660 PRINT "The basic solution to the Diophantine equation,"
670 PRINT EQUATION$;"    is:"
680 PRINT "X = ";X2*E:PRINT "Y = ";Y2*E
690 PRINT "The GCD of ";A;" and ";B;" is:";ABS(D)
700 PRINT "The parametric equations for all integer answers is:"
710 PRINT "X = ";X2*E;:IF B/D>0 THEN PRINT " +";
720 PRINT B/D;"N,       and"
730 PRINT "Y = ";Y2*E;:IF A/D<0 THEN PRINT " +"; ELSE PRINT " -";
740 PRINT ABS(A/D);"N"
750 PRINT "for all integer values N."
760 END
```

```
This program solves equations of the form ax + by = c, where a, b, c, x, and y
are all integer values.

Enter your equation as shown in the general form. For example, enter 154x + 69y
= 5000 or 154x - 69y = 5000. Do not enter negative coefficients with
parentheses. That is, do not enter 154x + (-69y) = 5000.

The program will not work properly for the degenerate case where either a or b is
0.

Enter equation? 74x+85y=1
The basic solution to the Diophantine equation,
74x+85y=1 is
x = -31
y = 27
The GCD of 74 and 85 is 1.
The parametric equations for all integer answers are
x = -31 + 85n and
y = 27 - 74n
for all integer values n.
```

Figure 3: *A screen dump of the program in listing 1 solving a Diophantine equation.*

Metze of the University of Illinois at Urbana-Champaign stunned me with this concept: Use ϕ, the Golden Mean, as a number base. (I will wait while you catch your breath.)

The system uses the digits 0 and 1 and is based on the identity $\phi^2 = \phi + 1$. In order to get a feel for what he has to say, we should take a brief excursion into another way of using the Euclidean algorithm: representing numbers as continued fractions. Figure 4a shows how to represent 154/69 as a continued fraction. You just collect all the quotients from the Euclidean algorithm (2, 4, 3, 5) and stack them as shown in the figure. Any rational number can be expressed as a finite continued fraction. Now, $\phi = (1 + \sqrt{5})/2$, and $\sqrt{5}$ is irrational. Its continued fraction will be infinite but regular (see figure 4b). When we "add" the continued fractions for 1/2 and $\sqrt{5}/2$, we get the continued fraction for ϕ in figure 4c. ϕ turns out to be the simplest continued fraction, $(\overline{1})$. Back to Professor Metze.

One interesting letter suggested using the Golden Mean as a number base by employing the identity $\phi^2 = \phi + 1$.

The identity $\phi^2 = \phi + 1$ means that "100" = "011" in the ϕ-nary system, and these two patterns can be interchanged anywhere in a ϕ-nary number. For example, 10011 = 10100 (the rightmost "011" becomes "100"), and 1110 = 10010 (the leftmost "011" becomes "100"). That is, the final representation need not contain consecutive 1s.

You may want to try to construct an addition table in base ϕ, but some mental agility is required. Our first snag is "1 + 1." How do we "carry" in this system? Since 1 = 1.00 = 0.11 (remember the pattern switch?), we can proceed: 1 + 1 = 1.00 + 1.00 = 1.00 + 0.11 = 1.11, which can be rewritten as 10.01, and we have found "2"! You may wish to verify that 10.01 = 2, that is, that $\phi + \phi^{-2} = 2$. Similarly, we find "3" with 10.01 + 1.00 = 11.01, = 100.01, and so on. The representations grow rapidly in both directions.

There was a large and enthusiastic response to the "π, e, and All That"

(continued)

column (September 1985, page 409). Many readers requested the derivation of the complete permutations formula. Everyone found or already knew of the hiding place of ϕ in the Fibonacci sequence. Others demanded to know why $e^{i\pi} = -1$.

All who were interested in the approximation of π by the Buffon experiment agreed that my program was dishonest for its inclusion of $\pi/2$ in the program itself. Several readers offered alternative methods that avoided using π.

An impressive method for doing the Buffon experiment without using π involves calculating slopes for random pairs of points.

The most popular suggestion was the potshot method. There is a circular target inscribed on a square board. Random shots are fired at the board, and, assuming all shots hit the board, we count the number of shots that strike inside the circle. For longer and longer volleys, the ratio of the number of strikes inside the circle to the number of shots fired approaches $\pi/4$. Donald S. Higgins of St. Petersburg, Florida, offered the miniprogram in listing 2.

It turns out that I was lucky not to have adopted his method because the April 1985 *Scientific American* described it (among other simulations) in the "Computer Recreations" column by A. K. Dewdney.

Ellis Golub of Bryn Mawr, Pennsylvania, offered an impressive method. Select four random decimals and use them to form two random points: (x1,y1) and (x2,y2). Consider the slope of the line through these two points: SLOPE = (y2 – y1)/(x2 – x1). Then let PROJ = .25/SQR (SLOPE ^ 2 + 1), which is equivalent to my .25 * COS(ANGLE) but completely eliminates the use of trig functions and any mention of π. He also had a 25 percent reduction in running time.

In the next column, I will examine Pellian equations, which are of the form $x^2 - ny^2 = 1$, where n is a nonsquare integer and the solutions (x,y) are integral. Until then, keep those cards and letters coming. ■

(a)

The quotients of the Euclidean algorithm for the GCD of 154 and 69 are (2,4,3,5). The continued fractional representation of 154/69 is

$$154/69 = 2 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{5}}}$$

(b)

The continued fractional representation of $\sqrt{5}$ is

$$\sqrt{5} = 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}$$

(c)

The continued fractional representation of $\phi = (1 + \sqrt{5})/2$ is

$$\phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}$$

Figure 4: *The way of representing numbers as continuing fractions. (a) 154/69 as a continuing fraction; (b) the infinite continuing fraction for $\sqrt{5}$; (c) the simplest infinite continuing fraction, ϕ.*

Listing 2: *Donald Higgins's program to approximate π by the potshot method.*

```
5 REM Program to approximate pi by Donald S. Higgins, St. Petersburg, FL.
10 INPUT "TRIALS", N
20 FOR I = 1 TO N
30       X = RND(0)
40       Y = RND(0)
50       IF X*X+Y*Y < 1 THEN C = C + 1
60 NEXT I
70 PRINT "ESTIMATE OF PI =", 4*C/N
```