University of Waterloo
Faculty of Mathematics

Centre for Education in
Mathematics and Computing

Intermediate Math Circles
November 18, 2009
Solving Linear Diophantine Equations

Diophantine equations are equations intended to be solved in the integers. For example, Fermat's Last Theorem is the statement that if $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has no solution in the integers, except the solutions with one of x, y, or z being 0.

It's too hard to try to understand <u>all</u> diophantine equations in one go, so we'll look at linear ones, like

$$7x + 3y = 4$$
or
$$10x + 4y = 12.$$

How can we find solutions to these with x and y being integers?

Example: Suppose that Bob has \$1.55 in quarters and dimes. How many quarters and how many dimes does he have? (There might be more than one solution!)

Solution: We're trying to solve $25x + 10y = 155$ with x and y integers (which shouldn't, in this case, be negative!). By trial-and-error we can find

$$\begin{array}{lll} & x = 1 & y = 13 \\ \text{or} & x = 3 & y = 8 \\ \text{or} & x = 5 & y = 3 \end{array}$$

$\square$

Example: A robot can move backwards or forwards with big steps (130 cm) or small steps (50 cm). Is there a series of moves it can make to end up 10 cm ahead of where it started? i.e., can we solve $130x + 50y = 10$?

Trial-and-error solution:

$$x = 2 \qquad y = -5$$

$$\longrightarrow\longrightarrow \qquad \text{2 big steps forward}$$

$$\longleftarrow\longleftarrow\longleftarrow\longleftarrow\longleftarrow \qquad \text{5 small steps back}$$

<u>OR</u> $\quad x = 7 \qquad y = -18$

There are many solutions. ☐

Main question: If a, b, and c are integers, the how can you find a solution to

$$ax + by = c$$

in integers?

Trick question! There might not be one!

For example, look at the equation

$$3x + 6y = 5$$

If we could find integers x and y for which that holds, then

$$x + 2y = \frac{5}{3}.$$

But $\frac{5}{3}$ is not an integer.

To figure out exactly when this sort of equation can be solved, we need some number theory.

If any integer divides both a and b, then

$$ax + by = c$$

can only have a solution if that integer also divides c.

Remember: an integer d "divides" another integer e if and only if $\frac{e}{d}$ is an integer.

The **"greatest common divisor"** of a and b is the largest integer that divides a <u>and</u> divides b. We write it as $\gcd(a, b)$.

For example:

$\gcd(3, 6) = 3$

$\gcd(10, 15) = 5$

$\gcd(3, 7) = 1$

1 divides everything, so $\gcd(a, b)$ is always at least 1.

$\boxed{\text{If } ax + by = c \text{ is going to have a solution, then } \gcd(a, b) \text{ needs to divide } c.}$

What's the best way to calculate $\gcd(a, b)$?

For small numbers a and b it's not too hard, but try calculating

$$\gcd(104723, 103093).$$

You can try to find all divisors, and see which ones divide both, but that could take all day!

Here's and interesting idea: If a number d divides a and b, and q is any integer, then d divides $a - qb$. Also, if e divides $a - qb$ and b, then e divides $a = (a - qb) + qb$. So for any integer q,

$$\gcd(a, b) = \gcd(b, a - qb).$$

Why is this useful?

Suppose we want to calculate

$$\gcd(73, 7)$$

This is the same as $\gcd(7, 73 - q \cdot 7)$ for <u>any</u> integer q. Like, for example, $q = 10$. So

$$\gcd(73, 7) = \gcd(7, 3) = 1$$

Example: $\gcd(117, 55) = ?$

Solution: $117 - 2 \cdot 55 = 7$, so

$$\gcd(117, 55) = \gcd(55, 7).$$

Now, $55 - 7 \cdot 7 = 6$, so

$$\gcd(55, 7) = \gcd(7, 6).$$

Again, $7 - 1 \cdot 6 = 1$, so

$$\gcd(7, 6) = \gcd(6, 1) = 1.$$

So $\gcd(117, 55) = 1$. $\square$

This is the "Euclidean algorithm" for calculating $\gcd(a, b)$.

<u>Step 1</u>: Arrange things so that $a \geq b$.

<u>Step 2</u>: Write $a = qb + r$, with $0 \leq r < b$.

<u>Step 3</u>: If $r = 0$, then b divides a, so $\gcd(a, b) = b$. STOP!
If <u>not</u> then $\gcd(a, b) = \gcd(b, r)$.

<u>Step 4</u>: Repeat to calculate $\gcd(b, r)$.

Since the numbers get smaller at every stage, you eventually get an answer.

Example: Calculate gcd(129, 48).

Solution:

$$\begin{aligned}
129 &= 2\cdot 48+33,\ \text{so} && \gcd(129,\ 48)=\gcd(48,\ 33)\\
48 &= 1\cdot 33+15,\ \text{so} && \gcd(48,\ 33)=\gcd(33,\ 15)\\
33 &= 2\cdot 15+3,\ \text{so} && \gcd(33,\ 15)=\gcd(15,\ 3)\\
15 &= 5\cdot 3+0,\ \text{so} && \gcd(15,\ 3)=3\\
&\text{We have} && \gcd(129,\ 48)=3.
\end{aligned}$$

□

Example: Is there a solution to

$$129x+48y=4?$$

Solution: NO! Because gcd(129, 48) = 3, which doesn't divide 4. □

So, we know how to show (sometimes) that $ax+by=c$ has <u>no</u> solution, but if it <u>does</u> have a solution, is there a clever way to find one?

For example, can we find a solution to

$$117x+55y=1?$$

(Remember that gcd(117, 55) = 1).

We found that

$$\begin{aligned}
117-2\cdot 55&=7\\
55-7\cdot 7&=6\\
7-1\cdot 6&=1\\
6-1\cdot 6&=0
\end{aligned}$$

Let's rearrange this:

$$\begin{aligned}
1&=\underline{7}-1\cdot\underline{6}\\
6&=\underline{55}-7\cdot\underline{7},\ \text{so}\\
1&=\underline{7}-1\cdot(\underline{55}-7\cdot\underline{7})\\
&=8\cdot\underline{7}-1\cdot\underline{55}\\
\text{But } 7&=\underline{117}-2\cdot\underline{55},\ \text{so}\\
1&=8\cdot(\underline{117}-2\cdot\underline{55})-1\cdot\underline{55}\\
&=8\cdot\underline{117}-17\cdot\underline{55}
\end{aligned}$$

So one solution to $117x+55y=1$ is $x=8$, $y=-17$.

This always works, and gives us a way to find a solution to $ax+by=c$ <u>if</u> $c=\gcd(a,\ b)$.

Example: Find a solution to $4389x + 2919y = 21$.

Solution: We can only do this if we happen to have $\gcd(4389, 2919) = 21$.

$$\begin{aligned}4389 &= 1 \cdot 2919 + 1470\\ 2919 &= 1 \cdot 1470 + 1449\\ 1470 &= 1 \cdot 1449 + 21\\ 1449 &= 69 \cdot 21 + 0\end{aligned}$$

So $\gcd(4389, 2919) = 21$

$$\begin{aligned}21 &= \underline{1470} - 1 \cdot \underline{1449}\\ &= \underline{1470} - 1 \cdot (\underline{2919} - 1 \cdot \underline{1470})\\ &= 2 \cdot \underline{1470} - 1 \cdot \underline{2919}\\ &= 2 \cdot (\underline{4389} - 1 \cdot \underline{2919}) - 1 \cdot \underline{2919}\\ &= 2 \cdot \underline{4389} - 3 \cdot \underline{2919}\end{aligned}$$

So one solution is $x = 2$, $y = -3$. $\square$

What about solving $ax + by = c$ when c is <u>not</u> $\gcd(a, b)$?

We know that we need $\gcd(a, b)$ to <u>divide</u> c, so $\dfrac{c}{\gcd(a,\ b)}$ is an integer.

If $ax + by = \gcd(a,\ b)$, then

$$\begin{aligned}&a\left(x \cdot \frac{c}{\gcd(a,\ b)}\right) + b\left(y \cdot \frac{c}{\gcd(a,\ b)}\right)\\ =\ &\frac{c}{\gcd(a,\ b)} \cdot (ax + by)\\ =\ &c\end{aligned}$$

So just

1. Solve $ax + by = \gcd(a,\ b)$.
2. Multiply the x and y in the solution by $\dfrac{c}{\gcd(a,\ b)}$.

Example: Find a solution to $4389x + 2919y = 231$.

Solution: We know that $\gcd(4389, 2919) = 21$, so this is only going to work if 21 divides 231. It does!

$$\frac{231}{21} = 11, \text{ so}$$

1. Find a solution to $4389x + 2919y = 21$. We've done this: $x = 2$, $y = -3$.
2. Multiply by 11. So the <u>new</u> solution is $x = 22$, $y = -33$.

Check: $4389(22) + 2919(-33) = 231$. $\square$

So we now know that

$$ax + by = c$$

has a solution (in the integers) if and only if $\gcd(a,\ b)$ divides c, and we know how to find a solution if there is one.

How can we find more solutions?

Suppose x, y is a solution to $ax + by = c$.

For example, $x = 2$, $y = -5$ is a solution to

$$18x + 7y = 1$$

Notice that $x = 2 + 7$ and $y = -5 - 18$ is also a solution. In fact, if k is any integer,

$$x = 2 + 7k,\ \ y = -5 - 18k$$

is a solution, since

$$\begin{aligned} &18(2 + 7k) + 7(-5 - 18k) \\ &= 36 + 18 \cdot 7 \cdot k - 35 - 18 \cdot 7 \cdot k \\ &= 1 \end{aligned}$$

You can use this formula to describe <u>all</u> solutions to $18x + 7y = 1$.

In general, this works for any equation $ax + by = c$. If $x = x_0$, $y = y_0$ is one solution, then the full set of solutions is given by choosing integers k, and letting $x = x_0 + k \cdot e$, $y = y_0 - k \cdot f$, where

$$e = \frac{a}{\gcd(a,\ b)} \qquad\qquad f = \frac{b}{\gcd(a,\ b)}$$

Example: Write down a formula giving the solutions to

$$4389x + 2919y = 231$$

Solution: We already have one: $x = 22$, $y = -33$

$$\begin{aligned} \text{Now, } e &= \frac{a}{\gcd(a,\ b)} = \frac{4389}{21} = 209 \\ f &= \frac{b}{\gcd(a,\ b)} = \frac{2919}{21} = 139 \end{aligned}$$

So the solutions are exactly

$$\begin{aligned} x &= 22 + k \cdot 209 \\ y &= -33 - k \cdot 139 \end{aligned}$$

for all integers k.

Problems

1. Here's a little puzzle: start with the number 0, and at every step, you may add or subtract either the number 5 or the number 17 (that's four possible moves in total). Is it possible to eventually get to the number 1?

$$0 \xrightarrow{+17} 17 \xrightarrow{-5} 12 \longrightarrow \dots$$

2. Find the greatest common divisors:

   a) gcd(55, 20)
   b) gcd(318, 225)
   c) gcd(2009, 4182)
   d) gcd(43477, 35021)
   e) gcd(127146, 123456)
   f) gcd(422058756, 464963310)

3. Find a solution to each of the following diophantine equations, or explain where there is none:

   a) $55x + 20y = 5$
   b) $318x + 225y = 4$
   c) $2009x + 4182y = 820$
   d) $43477x + 35021y = 7$
   e) $127146x + 123456y = 12$
   f) $422058756x + 464963310y = 42$

4. For each of the above equations (except those that didn't have solutions!) write down a formula describing ALL solutions to the equations in terms of an integer k.