Intermediate Math Circles
February 26, 2014
Diophantine Equations I

1. An introduction to Diophantine equations

A *Diophantine equation* is a polynomial equation that is intended to be solved over the integers.

$$\text{Eg.} \qquad x^2 = 4y^2, \qquad x = y + 2z^2, \qquad 2x^3 - y^2 = 1$$

- All coefficients in the equations are integers: $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$
- $x, y, z, \ldots$ are the variables and there can be any number of them in a given equation.
- We are interested in finding *integer* solutions to these equations.

For example: Given the equation $x = y + 2z^2$, can you find a triple (x, y, z) where x, y and z are integers that satisfy the equation? Can you find *all such triples*?

Famous examples:

1. $x^2 + y^2 = z^2$: Find positive integers (x, y, z) that satisfy this equation.
   - This is asking us to find *Pythagorean triples*!
   - One example is $(3, 4, 5)$ since $3^2 + 4^2 = 5^2$.
   - There are infinitely many solutions in the positive integers.
2. $x^3 + y^3 = z^3$: Find positive integers (x, y, z) that satisfy this equation.
   - There are *no solutions* in the positive integers!
3. *Linear Diophantine equations*: $ax + by = c$

2. Linear Diophantine Equations

A *linear Diophantine equation* is an equation of the form $ax + by = c$ where a, b and c are *fixed* (given) integers and we are *solving* for integers x and y.

$$\text{Eg.} \qquad 5x + 3y = 1 \qquad 12x + 6y = 4 \qquad 7x + (-2)y = 8$$

Can we find solutions to these equations with x and y being integers?

Example 1. Diophantus has \$2.55 in quarters and dimes. How many quarters and how many dimes does he have?

Solution. *Solve the equation* $25x + 10y = 255$ *with* x *and* y *integers.*

(In this case we should ensure that x *and* y *are not negative, for obvious reasons!)*

By guess and test, we come up with some possible solutions:

$$\begin{array}{ll} & x = 3 \text{ and } y = 18 \\ \text{or} & x = 5 \text{ and } y = 13 \\ \text{or} & x = 7 \text{ and } y = 8 \\ \text{or} & x = 9 \text{ and } y = 3 \end{array}$$

Are these all the integer solutions?

Example 2. A father's age is 4 less than twice that of his son, and the digits of the father's age (< 100) **are the reverse of the digits of the son's age. Find the two ages.**

Solution. *We can form a Diophantine equation as follows.*

Father's age: xy
Son's age: yx

Then the father's age is $10x + y$ *and the son's age is* $10y + x$ *and hence we need* x *and* y *to satisfy the equation*

$$\begin{aligned} 10x + y &= 2(10y + x) - 4 \\ 19y - 8x &= 4 \end{aligned}$$

We solve the equation $19y - 8x = 4$ *with* x *and* y *integers between* 1 *and* 9 *(inclusive).*

We find $x = 9, y = 4$ *and so the ages are* 94 *and* 49.

Are there any others solutions?

It is not always easy to find a solution to a linear Diophantine equation by trial and error.

For example, suppose we are asked to find an integer solution to the equation

$$1037x + 357y = 17.$$

Main Question for today: Given three integers a, b and c, how do you find a solution to $ax + by = c$ where x and y are integers?

Careful! There may not be an integer solution! Today we will determine conditions on a, b and c that guarantee an integer solution to the equation $ax + by = c$, and learn a method for finding such a solution, in the case where one exists.

When does a solution exist?

Are there any integer solutions to the equation $3x + 6y = 7$?

Suppose that we have two integers x and y satisfying the above equation. By dividing through by 3, we see that x and y must also satisfy the equation

$$x + 2y = \frac{7}{3}.$$

Since x and y are both integers, so is $x + 2y$, but $\frac{7}{3}$ is not! Therefore this second equation cannot hold. So the equation $3x + 6y = 7$ cannot have any integer solutions.

Conclusions?

The equation $ax + by = c$ has an integer solution only if any integer dividing both a and b also divides c.

We can rephrase this statement in a nicer way, using what is called the *greatest common divisor* of a and b.

3. Greatest Common Divisors

Definition (Division)**.** *We say that an integer d divides an integer e if there is some integer q such that $e = qd$. In other words, the quotient $\frac{e}{d}$ is equal to an integer. We call d a divisor of e.*

Definition (gcd)**.** *The greatest common divisor of a and b is the largest integer that divides both a and b. We write this integer as $gcd(a, b)$, "the gcd of a and b".*

One method for calculating $\gcd(a, b)$: Factor a and b and consider all divisors.

Examples. *Consider the following greatest common divisor calculations.*

- $\gcd(3, 6) = 3$
- $\gcd(15, 20) = 5$
- $\gcd(273, 182) = 91$
- $\gcd(11, 45) = 1$
- $\gcd(1037, 357) =?$
- $\gcd(187473, 171171) =?$

Example 3. Calculate gcd(273, 182).

Solution. *First, we factor the two integers to get*

$$273 = 3 \times 7 \times 13 \text{ and } 182 = 2 \times 7 \times 13.$$

Therefore the common divisors are $1, 7, 13$ *and* 91 $(= 7 \times 13)$*, and the greatest common divisor is* 91*.*

Note: *As* 1 *divides every integer, the gcd of two integers is always at least* 1*.*

Finding $\gcd(a, b)$ by factoring a and b may be difficult if a and b are large. It is possible to do, but it may be very time consuming.

Instead, we will use a method that does not require us to find a single divisor of either a or b. This method is called the *Euclidean algorithm*, which is basically repeated applications of the *division algorithm*.

The Division Algorithm:

Suppose that a and b are integers and $b > 0$. Then there exist unique integers q and r such that

$$a = qb + r$$

where $0 \leq r < b$. The integer q is called the *quotient*, r is called the *remainder*.

Examples. *Using the division algorithm.*

1. $a = 25$, $b = 7$ $\quad 25 = 3 \cdot 7 + 4 \quad (q = 3, r = 4)$
2. $a = 42$, $b = 7$ $\quad 42 = 6 \cdot 7 + 0 \quad (q = 6, r = 0)$
3. $a = 9$, $b = 6$ $\quad 9 = 1 \cdot 6 + 3 \quad (q = 1, r = 3)$
4. $a = -4$, $b = 6$ $\quad -4 = (-1) \cdot 6 + 2 \quad (q = -1, r = 2)$

FACT 1: If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.

Examples. *Using FACT 1.*

1. $25 = 3 \cdot 7 + 4$ $\quad \gcd(25, 7) = \gcd(7, 4) = 1$
2. $42 = 6 \cdot 7 + 0$ $\quad \gcd(42, 7) = \gcd(7, 0) = 7$
3. $9 = 1 \cdot 6 + 3$ $\quad \gcd(9, 6) = \gcd(6, 3) = 3$
4. $-4 = (-1) \cdot 6 + 2$ $\quad \gcd(-4, 6) = \gcd(6, 2) = 2$

How do we use FACT 1 to calculate greatest common divisors more efficiently?

Example 4. Calculate gcd(111, 52).

Solution. *Since* $111 = 2 \cdot 52 + 7$, *we have* $\gcd(111, 52) = \gcd(52, 7)$.

Since $52 = 7 \cdot 7 + 3$, *we have* $\gcd(52, 7) = \gcd(7, 3)$.

Since $7 = 2 \cdot 3 + 1$, *we have* $\gcd(7, 3) = \gcd(3, 1) = 1$.

We conclude that

$$\gcd(111, 52) = \gcd(52, 7) = \gcd(7, 3) = \gcd(3, 1) = 1.$$

This method is called the Euclidean algorithm.

The Euclidean Algorithm:

Input: A pair of positive integers (a, b).

Step 1. Arrange a and b so that $a \geq b$.

Step 2. Write $a = qb + r$ with $0 \leq r < b$ (*division algorithm*).

Step 3. If $r = 0$ then stop! If $r > 0$ then go back to Step 1, this time with the pair (b, r).

Output: The last non-zero remainder r *if such an* r *exists, or else output* b.

Let's convince ourselves that this procedure will always output $\gcd(a, b)$.

Example 5. Calculate $\gcd(481, 1053)$ using the Euclidean algorithm.

Solution. *Here we apply the Euclidean algorithm to the pair* $(481, 1053)$*. We will keep track of what is happening with the gcd calculation on the right hand side.*

As $481 < 1053$*, set* $a = 1053$ *and* $b = 481$	$\gcd(481, 1053) = \gcd(1053, 481)$
Write $1053 = 2 \cdot 481 + 91$ $\quad (r = 91)$	$\gcd(1053, 481) = \gcd(481, 91)$
Write $481 = 5 \cdot 91 + 26$ $\quad (r = 26)$	$\gcd(481, 91) = \gcd(91, 26)$
Write $91 = 3 \cdot 26 + 13$ $\quad (r = 13)$	$\gcd(91, 26) = \gcd(26, 13)$
Write $26 = 2 \cdot 13 + 0$ $\quad (r = 0)$	$\gcd(26, 13) = \gcd(13, 0) = 13$

The output is 13*, last non-zero remainder. From the gcd equalities on the right hand side we see that* $\gcd(481, 1053) = \gcd(13, 0) = 13$.

Example 6. Calculate $\gcd(78, 26)$ using the Euclidean algorithm.

Solution. *We have* $78 < 26$ *so we write* $78 = 3 \cdot 26 + 0$ *and so* $r = 0$*. Since there are no non-zero remainders, we output* $b = 26$.

This always happens if one of the integers divides the other.

Remarks.

1. Since $a \leq b$ and $r < b$, the integers get smaller after each iteration of the division algorithm, and so this procedure must eventually stop. Can you convince yourself that you will always reach a remainder of zero, and that the output will always be $\gcd(a, b)$?

2. To use the algorithm you do not need to keep track of the various gcd calculations on the right, but it is a good idea! You may not need to run the algorithm the whole way through: Once you see a "gcd calculation" that you can do in quickly in your head, you can stop and use that answer.

Exercise Set 1:

1. Calculate $\gcd(56, 287)$ by
   (a) factoring 56 and 287.
   (b) the Euclidean algorithm.
2. Use the Euclidean algorithm to calculate $\gcd(264, 671)$.
3. Use the Euclidean algorithm to calculate $\gcd(2233, 2549)$.
4. Use the Euclidean algorithm to calculate $\gcd(7826, 6279)$.
5. Use the Euclidean algorithm to calculate $\gcd(187473, 171171)$.

Answers:

1. (a) $56 = 2^3 \cdot 7$ and $287 = 7 \times 41$ and so $\gcd(56, 287) = 7$.
   (b) $287 = 5 \cdot 56 + 7$
   $56 = 8 \cdot 7 \ + 0$ and so $\gcd(56, 287) = 7$.
2. $\gcd(264, 671) = 11$.
3. $\gcd(2233, 2549) = 1$.
4. $\gcd(7826, 6279) = 91$.
5. $\gcd(187473, 171171) = 8151$.

4. The Euclidean algorithm and linear Diophantine equations

Example 7. Find integers x and y such that $1037x + 357y = 17$.

Solution. *The Euclidean algorithm gives:*

$$\begin{aligned} 1037 &= 2 \cdot 357 + 323 && (1)\\ 357 &= 1 \cdot 323 + 34 && (2)\\ 323 &= 9 \cdot 34 + 17 && (3)\\ 34 &= 2 \cdot 17 + 0 && (4) \end{aligned}$$

and so we have $\gcd(1037, 357) = 17$. *Notice that this our value of c in the equation. We can exploit this fact by tracing our steps in the Euclidean algorithm and working backwards as follows.*

From (3): $17 = 323 - 9 \cdot 34$

Substituting for 34 using (2): $17 = 323 - 9 \cdot (357 - 1 \cdot 323)$

Simplifying: $17 = 10 \cdot 323 - 9 \cdot 357$

Substituting for 323 using (1): $17 = 10 \cdot (1037 - 2 \cdot 357) - 9 \cdot 357$

Simplifying: $\mathbf{17 = 10 \cdot 1037 - 29 \cdot 357}$

So one solution is $\boldsymbol{x = 10}$, $\boldsymbol{y = -29}$. *Check!*

Conclusions? If $c = \gcd(a, b)$, then $ax + by = c$ has an integer solution.

Example 8. Find integers x and y such that $1037x + 357y = 51$.

Solution. *Notice that* $51 = 3 \times 17$ *and so* 17 *divides* 51. *From the previous example, we have that*

$$1037 \cdot 10 + 357 \cdot (-29) = 17$$

and so multiplying the entire equation by 3 *gives*

$$\begin{aligned} 3\left(1037 \cdot 10 + 357 \cdot (-29)\right) &= 3\ (17)\\ 1037 \cdot \left(3 \cdot 10\right) + 357 \cdot \left(3 \cdot (-29)\right) &= 51\\ 1037 \cdot 30 + 357 \cdot (-87) &= 51 \end{aligned}$$

Since 17 *divides* 51, *we have a solution, namely* $\boldsymbol{x = 30}$, $\boldsymbol{y = -87}$. *Check!*

Conclusions? If $\gcd(a, b)$ divides c, then $ax + by = c$ has an integer solution.

Example 9. Find integers x and y such that $1037x + 357y = 10$.

Solution. *Suppose that we do have integers x and y satisfying the above equation. Since $17 = \gcd(1037, 357)$, we can factor it out of the left hand side of the equation:*

$$\begin{aligned} 1037x + 357y &= 10 \\ (17 \cdot 61)x + (17 \cdot 21)y &= 10 \\ 17\Big(61x + 21y\Big) &= 10 \end{aligned}$$

Since 17 does not divide 10, this last equality is impossible!

So no solution exists.

Conclusions? If $\gcd(a, b)$ does not divide c, then the equation $ax + by = c$ has no integer solutions.

Final Thoughts:

1. Using the Euclidean algorithm and working backwards we can *always* find integers x and y such that
$$ax + by = \gcd(a, b).$$

2. The equation $ax + by = c$ has an integer solution if and only if $\gcd(a, b)$ divides c.

   To find a solution: Once we have found x and y such that $ax + by = \gcd(a, b)$, we can multiply through by $\frac{c}{\gcd(a,b)}$ to get
$$\frac{c}{\gcd(a, b)} \cdot \Big(ax + by\Big) = \frac{c}{\gcd(a, b)} \cdot \Big(\gcd(a, b)\Big) = c$$
   Remember that $\frac{c}{\gcd(a,b)}$ is an integer! So we have $ax' + by' = c$ where
$$x' = x \cdot \frac{c}{\gcd(a, b)} \text{ and } y' = y \cdot \frac{c}{\gcd(a, b)}.$$

Exercise Set 2

Find an integer solution to the following linear Diophantine equations, or explain why one does not exist.

1. $105x + 39y = 3$
2. $132x + 52y = 6$
3. $273x + 462y = 21$
4. $3135x + 2093y = 1$
5. $5548x + 7391y = 57$

Possible Answers:

1. The pair $x = 3, y = -8$ is one (of many) solutions.
2. As $\gcd(132, 52) = 4$ and 4 does not divide 6, there are no integer solutions.
3. The pair $x = -5, y = 3$ is one (of many) solutions.
4. The pair $x = 930, y = -1393$ is one (of many) solutions.
5. We find that $x = 4, y = -3$ is a solution to the equation

$$5548x + 7391y = \gcd(5548, 7391) = 19.$$

As $57 = 3 \cdot 19$, the pair $x' = 3 \cdot 4 = 12, y' = 3 \cdot (-3) = -9$ is one (of many) solutions to the given equation.