Number Theory Homework.

1. The Euclidean algorithm and linear Diophantine equations.

By a ***Diophantine***[1] ***equation*** we mean a polynomial equation in two or more variables with integer coefficients and it is required to find integer solutions.

Here are examples:

$ax + by = c$ Where a, b and c are integers. This is the ***linear Diophantine equation.*** We will find all solutions to this equation in this section (when any exist).

$x^2 + y^2 = z^2$ The solutions to this are ***Pythagorean triples***. These are the side lengths of right triangles where the lengths of both legs and the hypotenuse have integral lengths. The best known example is the 3, 4, 5 triangle ($5^2 = 3^2 + 4^2$). We will find all Pythagorean triples during the course of the semester.

$x^n + y^n = z^n$ Where $n \geq 3$. This is the ***Fermat equation***. It was stated in 1637 by Fermat that this equation has no solution in positive integers. This became known as Fermat's Last Theorem and for a couple of centuries was the probably the most famous unsolved problem in mathematics. It was shown to be true by the British mathematician Andrew Wiles in 1994. An early notion of ideals in rings (we have seen ideals in the integers) was introduced by Ernst Kummer in the mid 1800s, to prove the result for a large number of integers n, for example all $n \leq 100$ other than 37, 59, and 67.

$x^2 - ny^2 = 1$ With n a positive integer that is not a perfect square and we look for nontrivial solutions (that is other than $x = \pm 1$ and $y = 0$). This is ***Pell's equation***. It has a solution for all such n, but they may not be easy to find. For example when $n = 60$ the smallest solution is $x = 31$ and $y = 4$ (which one can imagine finding by trial and error), but just change n by 1 to $n = 61$ the and smallest solution is $x = 1{,}766{,}319{,}049$ and $y = 226{,}153{,}980$ (which is be not going to be found by trial and error).

---

[1] Named after Diophantus of Alexandria who studied such equations in the 3rd Century AD.

Here we will just consider the linear Diophantine equation. We start with some examples that give an indication of when this equation has a solution.

$$3x + 4y = 19.$$

This has a solution $x = 1$, $y = 4$ (and from this solution we can construct infinitely many solutions $x = 1 + 4t$ and $4 - 3t$ where t is an integer.) On the other hand,

$$4x + 6y = 13$$

has no integral solutions, because if x and y are integers then the left side of the equation is even, but 13 is odd. As anther example

$$6x - 9y = 14$$

has no integral solutions as the left side is dividable by 3, but the right side is not. It turns out this problem of the left side of $ax + by = c$ having a divisor that the right side does not have is the only obstruction to the equation having integral solutions.

Theorem 1 (Solution to the linear Diophantine equation)**.** *If a, b, and c are integers with a and b both nonzero, then*

$$ax + by = c$$

has a solution if and only if

$$\gcd(a, b) \mid c.$$

If (x_0, y_0) is one solution, then the general solution[2] *is*

$$x = x_0 - \frac{bt}{\gcd(a, b)}, \qquad y = y_0 + \frac{at}{\gcd(a, b)}. \tag{1}$$

Remark 2. In the this theorem it is often convenient to use the following notation. Let

$$a' = \frac{a}{\gcd(a, b)}, \qquad b' = \frac{b}{\gcd(a, b)}.$$

Then the general solution is

$$x = x_0 - a't, \qquad y = y_0 + b't.$$

You will also often see the general solution written with t replaced by $-t$, that is

$$x = x_0 + a't, \qquad y = y_0 - b't.$$

This gives the same set of solutions, just listed in the reverse order. □

Problem 1. Prove Theorem 1 along the following lines. First show the easy direction, that is if $ax + by = c$ has a solution, then $\gcd(a, b) \mid c$.

In the other direction we assume that $\gcd(a, b) \mid c$ and show that the equation has a solution. To simplify notation set

$$d = \gcd(a, b).$$

[2]By "general solution" we mean that this gives all solutions.

We are assuming that $d \mid c$ and therefore there is an integer c' such that

$$c = dc'.$$

(a) Explain why there are integers x_1 and y_1 such that

$$ax_1 + by_1 = d. \tag{2}$$

Hint: Bézout's Theorem.

(b) Let $x_0 = c'x_1$ and $y_0 = c'y_1$. Explain why (x_0, y_0) is a solution to the equation $ax + by = c$. *Hint:* Multiply both sides of 2 by c'.

So we have now shown $ax + by = c$ has a solution if and only if $d \mid c$.

We still need to find all solutions.

(c) Show that x and y given by equations (1) are solutions.

Now we just need to check that these give all solutions. Still using the notation $d = \gcd(a, b)$ write $a = a'd$, $b = b'd$. Let (x_0, y_0) be a solution of $ax + by = c$ and let (x, y) be any other solution.

(d) Explain why $\gcd(a', b') = 1$.

(e) Show

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

and use this to show

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

(f) Thus implies $b'(y - y_0) = -a'(x - x_0) =$ and therefore $a' \mid b'(y - y_0)$. Use this to show $a' \mid (y - y_0)$. *Hint:* We have a result that says if $\gcd(\alpha, \beta) = 1$ and $\alpha \mid \beta\gamma$, then $\alpha \mid \gamma$.

(g) As $a' \mid (y - y_0)$ there is an integer t such that $(y - y_0) = a't$. Plug this into $a'(x - x_0) + b'(y - y_0)$ to show $(x - x_0) = -b't$.

(h) Put this all altogether to get

$$x = x_0 - b't, \qquad y = y_0 + a't$$

which is just a rewritten form of the equations (1) for the general solution. Thus we have that every solution is of the required form and the proof is finished. □

The existence part of this can be generalized to more than two variables.

Proposition 3. *Let a, b, c be nonzero integers. Then for any integer d the Diophantine equation*

$$ax + by + cz = d$$

has a solution if and only if $\gcd(a, b, c) \mid d$.

Problem 2. Prove this along the lines of parts (a), (b), and (c) of the last problem. □

And of course we do not have to stop at three.

Problem 3. Show that if $a_1, a_2, \ldots, a_n$ are nonzero integers and $b \in \mathbb{Z}$, then the linear Diophantine equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

has a solution if and only if

$$\gcd(a_1, a_2, \ldots, a_n) \mid b.$$

□

This is all good from the theoretical point of view, but we would like an effective method for finding the solutions. Note the the proof above reduces solving $ax + by = c$ to finding a particular solution to the Bézout equation $ax + by = \gcd(a, b)$. We now show how the Euclidean algorithm can be used to find such solution in a effective manner.

Let $a = 116$ and $b = 248$ and we wish to find x_0 and y_0 with $116x_0 + 248y_0 = \gcd(116, 248)$. We divide a into b, take that remainder and divide that into a and keep that process up. (Here and in following calculations we put parenthesis around the numbers are currently the center of our attention. This is not for any mathematical reason, it is just a bookkeeping trick to hopefully make the calculations easier to follow.)

$$\begin{aligned} (248) &= 2(116) + (16) && \text{i.e.} && (16) &= (248) - 2(116) \\ (116) &= 7(16) + (4) && \text{i.e.} && (4) &= (116) - 7(16) \\ (16) &= 4(4) + (0) \end{aligned}$$

From this we see $\gcd(116, 248) = 4$. And we can work backwards through this to get

$$\begin{aligned} (4) &= (116) - 7(16) \\ &= (116) - 7\big((248) - 2(116)\big) \\ &= 15(116) - 7(248) \end{aligned}$$

and we therefore have that $x_0 = 15$ and $y_0 = -7$ is a solution to $116x + 248y = \gcd(116, 248) = 4$. To do a more complicated example consider finding the example of $\gcd(632, 2642) = 2$ from the last homework. As we are most interested in the remainders we will write the divisor algorithm in the form

$$(r) = (b) - q(a) \qquad \text{rather than} \qquad b = qa + r.$$

$$\begin{aligned} (114) &= (2642) - 4(632) \\ (62) &= (632) - 5(114) \\ (52) &= (114) - 1(62) \\ (10) &= (62) - 1(52) \\ (2) &= (52) - 5(10) \end{aligned}$$

and we stop here as $2 \mid 10$. Now keep doing backward substations in this to get

$$\begin{aligned}
(2) &= (52) - 5(10) & &= (52) - 5\big((62) - (52)\big) \\
&= -5(62) + 6(52) & &= -5(62) + 6\big((114) - 1(62)\big) \\
&= 6(114) - 11(62) & &= 6(114) - 11\big((632) - 5(144)\big) \\
&= -11(632) + 61(114) & &= -11(632) + 61\big((2642) - 4(632)\big) \\
&= 61(2642) - 255(632)
\end{aligned}$$

Therefore $x_0 = 61$ and $y_0 = -255$ is solution to $ax + by = 2642x + 632y = 2$ and the general solution is

$$\begin{aligned}
x &= x_0 - \frac{b}{\gcd(a,b)}t = 61 - \frac{632}{2}t = 61 - 316t \\
y &= y_0 + \frac{a}{\gcd(a,b)}t = -255 + \frac{2642}{2}t = -255 + 1321t.
\end{aligned}$$

Example 4. Find all solutions to the Diophantine equation

$$324x - 142y = 30.$$

We start by using the Euclidean algorithm to find the greatest common divisor of 324 and -142.

$$\begin{aligned}
(40) &= (324) + 2(-142) \\
(18) &= (-142) + 4(40) \\
(4) &= (40) - 2(18) \\
(2) &= (18) - 4(4)
\end{aligned}$$

Thus $\gcd(324, -142) = 2$ and $2 \mid 30$, whence this Diophantine has a solution.

Now work backwards,

$$\begin{aligned}
(2) &= (18) - 4(4) & &= (18) - 4\big((40) - 2(18)\big) \\
&= -4(40) + 9(18) & &= -4(40) + 9\big((-142) + 4(40)\big) \\
&= 9(-142) + 32(40) & &= 9(-142) + 32\big((324) + 2(-142)\big) \\
&= 32(324) + 73(-142)
\end{aligned}$$

Therefore

$$324(32) - 142(73) = 2$$

Multiply this by 15 to get

$$324(15 \cdot 32) - 142(15 \cdot 73) = 15 \cdot 2,$$

that is

$$324(480) - 142(1095) = 30.$$

Thus $x_0 = 480$ and $y_0 = 1095$ is one solution to the equation. The general solution is then

$$x = 480 - \frac{-142}{2}t = 480 + 71t$$
$$y = 1095 + \frac{324}{2}t = 1095 + 162t$$

where t can be any integer. □

Example 5. A samll post office has only 13¢ and 17¢ stamps. How many ways can a postage of \$5.76 be done?

Let x be the number of 13¢ stamps and y the number of 17¢ stamps. Then the problem is equivalent to finding all solutions to the Diophantine equation

$$13x + 17y = 576$$

with $x \geq 0$ and $y \geq 0$. Clearly $\gcd(13, 17) = 1 \mid 576$ so there will be solutions in integers (which does not necessarily mean there are solutions in nonnegative integers). First use the Euclidean algorithm to find solutions to Bézout's equation.

$$(4) = (17) - (13)$$
$$(1) = (13) - 3(4).$$

and therefore

$$(1) = (13) - 4(4) = (13) - 3\big((17) - (13)\big) = 4(13) - 3(17).$$

Thus

$$13(4) + 17(-3) = 1.$$

Multiply by 576 to get

$$13(4 \cdot 576) + 17(-3 \cdot 576) = 13(2304) + 17(-1728) = 576.$$

This gives the pair $x_0 = 2304$ and $y_0 = -1728$ as one solution. The general solution is

$$x = 2304 - 17t, \qquad y = -1728 + 13t.$$

We are only interested in solutions that are nonnegative.

$$x = 2304 - 17t \geq 0 \qquad \Longrightarrow \qquad t \leq \frac{2304}{17} = 135.529\ldots$$

Which implies $t \leq 135$ because t is an integer. Also

$$y = -1728 + 13t \geq 0 \qquad \Longrightarrow \qquad t \geq \frac{1728}{13} = 132.923\ldots$$

which implies $t \geq 133$. Thus $133 \leq t \leq 135$. So only the values $t = 133$, $t = 134$, and $t = 135$ give solutions to our problem. These give

$$(x, y) = (2304 - 17 \cdot 133, -1728 + 13 \cdot 133) = (43, 1)$$
$$(x, y) = (2304 - 17 \cdot 134, -1728 + 13 \cdot 134) = (26, 14)$$
$$(x, y) = (2304 - 17 \cdot 135, -1728 + 13 \cdot 135) = (9, 27)$$

for the number, x, of 13¢ stamps and, y, the number of 17¢ stamps. □

This suggests a more general problem. If a, b, and c are positive, are there conditions that guarantee that $ax + by = c$ has a nonnegative solution?

Proposition 6 (Sylvester, 1884)**.** *If a, b, and c be positive integers with $\gcd(a, b) = 1$ and $c \geq (a-1)(b-1)$. Then there are nonnegative integers x and y with*

$$ax + by = c.$$

This is sharp in the sense that if $c = (a-1)(b-1) - 1 = ab - a - b$ then the equation has no solution in nonnegative integers.

Proof. Let (x_0, y_0) be the an integral solution to $ax + by = c$. Then the general solution is

$$x = x_0 - bt, \qquad y = y_0 + at.$$

By the division algorithm we can choose t such that $x_1 := x_0 - bt$ satisfies $0 \leq x_1 \leq b - 1$. Let $y_1 = y_0 + at$. Then $ax_1 + by_1 = c$ and $x_1 \geq 0$. So it is enough to show $y_1 \geq 0$.

$$\begin{aligned} by_1 &= c - ax_1 \\ &\geq (a-1)(b-1) - ax_1 \\ &\geq (a-1)(b-1) - a(b-1) \\ &= (b-1)(a-1-a) \\ &= -(b-1). \end{aligned}$$

Divide by b

$$y_1 \geq -\frac{(b-1)}{b} = -1 + \frac{1}{b} > -1.$$

As y_1 is an integer this implies $y_1 \geq 0$. Therefore $ax + by = c$ has the nonnegative solution $(x, y) = (x_1, y_1)$.

For the second part of the Proposition, assume, towards a contradiction, that

$$ax + by = ab - a - b$$

has a solution with $x, y \geq 0$. Rewrite as

$$ab = a(x+1) + b(y+1).$$

This implies that $a \mid b(y+1)$ and as $\gcd(a, b) = 1$ this farther implies $a \mid (y+1)$. As $y \geq 0$ this yields that $(y+1) \geq a$. Likewise $b \mid a(x+1)$, $\gcd(a, b) = 1$ gives that $b \mid (x+1) \geq 1$ and $x \geq 0$ therefore gives $(x+1) \geq b$. This yields

$$ab = a(x+1) + b(y+1) \geq ab + ab = 2ab$$

the required contradiction. □

Problem 4. For the following pairs (a, b) of integers use the Euclidean algorithm to find integers x and y that solve the Bézout equation $ax + by = \gcd(a, b)$.

(a) $(a, b) = (16, 12)$ (b) $(a, b) = (8, -3)$ (c) $(a, b) = (-12, 10)$
(d) $(a, b) = (-21, -28)$ (e) $(a, b) = (653, 291)$ (f) $(a, b) = (741, -432)$
(g) $(a, b) = (-534, 972)$ (h) $(a, b) = (-548, -362)$. □

Problem 5. For the following linear Diophantine equation equations determine if they have solutions. If they do, give the general solution.

(a) $6x + 4y = 12$ (b) $6x - 4y = 12$ (c) $37x - 47y = 15$
(d) $432x - 974y = 3$ (e) $432x - 974y = 14$ (f) $31x + 19y = 102$
(g) $20x + 34y = 1$ (h) $21x + 34y = 1$ □

Problem 6. Find all nonnegative integral solutions to the following:

(a) $3x + 4y = 100$ (b) $12x + 18y = 204$ (c) $7x - 9y = 3$ □

1.1. **The linear Diophantine equation in three or more variables.** Under some conditions on the coefficients it is very easy to adapt what we have just done to finding the general solution to the linear Diophantine equation in three or more variables.

Example 7. Consider

$$5x + 2y + 3z = 12.$$

We rewrite this as

$$5x + 2y = 12 - 3z.$$

As $\gcd(5, 2) = 1 \mid (12 - 3z)$ for any value of z, this is solvable for x and y for any value of z. We see by inspection that

$$5(1) + 2(-2) = (1).$$

Multiply by $12 - 3z$ to get

$$(12 - 3z) + 2(-24 + 6z) = (12 - 3z).$$

Thus $(x_0, y_0) = (12 - 3z, -24 + 6z)$ is a particular solution to $5x + 2y = 12 - 3z$. Whence the general solution is

$$x = 12 - 3z - 2t, \qquad y = -24 + 6z + 5t$$

with $t \in \mathbb{Z}$. This can be made to look a bit more aesthetic by introducing a new variable s for z, that is set $z = s$ and writing the general solution to the original equation in the more symmetric form.

$$\begin{aligned} x &= 12 - 3s - 2t \\ y &= -24 + 6s + 5t \\ z &= s \end{aligned}$$

The condition that made this easy was $\gcd(5, 2) = 1$ so that $5x+2y = 12-3z$ has a solution for all z. □

Problem 7. Find the general solution to the following linear Diophantine equations.

(a) $13x + 5y + 2z = 100$.
(b) $6x + 4y + 5z = 98$. *Hint:* For this one you should start with either $4y + 5z = 98 - 6x$ or $6x + 5z = 98 - 4y$. Why is this? □

Consider the general linear Diophantine equation

$$ax + by + cz = d$$

in three variables. By Proposition 3 this has a solution if and only if $\gcd(a, b, c) \mid d$. If this is the case we can divide the equation through by $\gcd(a, b, c)$ and assume that $\gcd(a, b, c) = 1$. If there is a pair of the coefficients a, b, or c, say a and b, with $\gcd(a, b) = 1$, then we can rewrite the equation as $ax + by = d - cz$ and this will have a solution for all $z \in \mathbb{Z}$.

Example 8. Things are less straightforward if we have an equation such as

$$ax + by + cz = 6x + 10y + 15z = 23$$

where $\gcd(a, b, c) = 1$, so the equation is solvable, but $\gcd(a, b) = \gcd(6, 10) = 2$, $\gcd(b, c) = \gcd(10, 15) = 5$, and $\gcd(a, c) = \gcd(6, 15) = 3$. Thus moving one term to the right, say,

$$6x + 10y = 23 - 15z$$

gives an equation that is not solvable for all values of z, but only for those values where $\gcd(6, 10) = 2 \mid (23 - 15z)$. But $2 \mid (23 - 15z)$ if and only if z is odd. We can guarantee z is odd by setting $z = 2s + 1$ with $s \in \mathbb{Z}$. Then the equation becomes

$$6x + 10y = 23 - 15(2s + 1) = 8 - 30s.$$

Which has a solution for all integers s. We first need a solution to $6x+10y = \gcd(6, 10) = 2$. We could use the Euclidean algorithm, but in this case inspection shows

$$6(2) + 10(-1) = (2).$$

Multiply by $4 - 15s$ to get

$$6(8 - 30s) + 10(-4 + 15s) = (8 - 30s)$$

so that $x_0 = 8 - 30s$, $y_0 = -4 + 15s$ is a particular solution to his equation. Therefore the general solution to $6x + 10y = 23 - 15(2s + 1) = 8 - 30s$ is

$$x = 8 - 30s - 5t, \qquad y = -4 + 15s + 3t.$$

Whence the general solution to the original equation, $6x + 10y + 15z = 23$, is

$$\begin{aligned} x &= 8 - 30s - 5t \\ y &= -4 + 15s + 3t \\ z &= 1 + 2s \end{aligned}$$

□

Example 9. Here is a slightly more complicated example.

$$35x + 21y + 15z = 101.$$

Rewrite as

$$35x + 21y = 101 - 15z$$

This will have solution if and only if $\gcd(35, 21) = 7 \mid (101 - 15z)$. The idea is to let $z = 7s + r$ and choose r in such a way that $7 \mid (101 - 15z)$.

$$101 - 15z = 101 - 15(7s + r) = 101 - 15r - 105s.$$

If $r = 3$ this becomes

$$101 - 35z = 56 - 105s = 7(8 - 15s)$$

Letting $z = 7s + 3$ in $35x + 21y = 101 - 15z$ gives

$$35x + 21y = 7(8 - 15s).$$

To keep the numbers smaller divide by 7

$$5x + 3y = 8 - 15s.$$

A particular solution to

$$5x + 3y = 1$$

is $(-1, 2)$:

$$5(-1) + 3(2) = (1)$$

which we multiply by $8 - 15s$ to get

$$5(-8 + 15s) + 3(16 - 30s) = (8 - 15s).$$

which shows that $(x_0, y_0) = (-8, 15s, 16 - 30s)$ is a particular solution to $5x + 3y = 8 - 15s$. Therefore the general solution is

$$x = -8 + 15s - 3t, \qquad y = 16 - 30s + 5t.$$

Finally, getting back to the original problem, the general solution is

$$\begin{aligned} x &= -8 + 15s - 3t \\ y &= 16 - 30s + 5t \\ z &= 3 + 7s. \end{aligned}$$

□

We now outline why this method works. Starting with

$$ax + by + cz = d$$

with $\gcd(a, b, c) \mid d$. We move one variable to the right. To be concrete we move cz

$$ax + by = d - cz \tag{3}$$

For for a fixed z this will have a solution for x and y if and only if $\gcd(a, b) \mid (d - cz)$. Let $z = \gcd(a, b)s + r$ where s is a variable and we will choose r shortly. We want

$$d - cz = d - c(\gcd(a, b)s + r) = (d - cr) - c\gcd(a, b)s$$

to be divisible by $\gcd(a,b)$. This happens if and only if $\gcd(a,b) \mid (d-cr)$ which is equivalent to there being a u such that $(d-cr) = u\gcd(a,b)$ which can be rewritten as

$$cr + \gcd(a,b)u = d.$$

But $\gcd(c,\gcd(a,b)) = \gcd(a,b,c)$ and $\gcd(a,b,c) \mid d$. Whence by Theorem 1 there are $r = r_0$ and $u = u_0$, both integers, such that $cr_0 + \gcd(a,b)u_0 = d$, that is $(d - cr_0) = \gcd(a,b)u_0$. Combining this with some of the equations above

$$d-cz = (d-cr_0)-c\gcd(a,b)s = \gcd(a,b)u_0-c\gcd(a,b)s = \gcd(a,b)(u_0-cs)$$

and using this and $z = \gcd(a,b)s + r$ in (3) gives

$$ax + by = \gcd(a,b)(u_0 - cs)$$

which has a solution for all $s \in \mathbb{Z}$. Let $(x,y) = (x_0,y_0)$ be a particular solution solution to $ax + by = \gcd(a,b)$. Multiplying the equation $a(x_0) + b(y_0) = (\gcd(a,b))$ by $(u_0 - cs)$ shows $(x_0(u_0-cs), y_0(u_0-cs))$ is a particular solution to $ax+by = \gcd(a,b)(u_0-cs)$ and therefore the general solution to this equation is $x = x_0 - (u_0-cs)bt/\gcd(a,b)$, $y = y_0(u_0-cs) + a/\gcd(a,b)$ and finally the solution to the original equation is

$$\begin{aligned} x &= x_0(u_0 - cs) - \left(\frac{b}{\gcd(a,b)}\right)t \\ y &= y_0(u_0 - cs) + \left(\frac{a}{\gcd(a,b)}\right)t \\ z &= \gcd(a,b)s + r_0. \end{aligned}$$

Problem 8. Find the general solutions to the following Diophantine equations.

(a) $12x + 15y + 20z = 14$
(b) $21x - 14y + 10z = 6$
(c) $30x + 42y + 70z + 105w = 19$ □