# Math 126 Number Theory

Prof. D. Joyce, Clark University

8 Feb 2006

**Due Today.** From page 35, exercises 1, 2.

**Due Friday.** From page 43, exercises 2, 3, 5, 6, 7.

**Due Wednesday.** From page 47, exercises 3–8, 10, 12.

**For next time.** Read section 3.1 on congruences.

**Last meeting.** Divisors of a number, their number and their sum. Multiplicative functions.

**Today.** Linear Diophantine equations. These are also called indeterminate linear equations. A linear Diophantine equation in two variables $x$ and $y$ is just a linear equation

$$ax + by = c$$

where $a$, $b$, and $c$ are constants, but we only consider integer solutions (positive, negative, or 0). In honor of Diophantus, when we only consider integer solutions, or when we only consider rational solutions, we call an equation a *Diophantine* equation. In a later chapter we'll look at quadratic and higher degree equations, but right now, we'll stick to linear equations.

There are two goals in solving a Diophantine equation. The weaker goal is to find any one solution. The stronger goal is to find all the solutions. In the case of a linear Diophantine equation, if you know one solution, that will help in finding all the rest.

**The hundred fowls problem.** Here's an old example, something called the hundred fowls problem. This famous problem is stated as follows. Roosters cost 5 coins each. Hens cost 3 coins each. Chicks are three for 1 coin. If 100 fowls are bought for exactly 100 coins, then how many of the three (roosters, hens, and chicks) are bought?

This problem can be solved by guessing an answer and adjusting your guess until you get it right. It doesn't take that long. But a better way is to use a bit of algebra. Let $x$ be the number of roosters bought, let $y$ be the number of hens bought, and let $z$ be the number of chicks bought. Then the problem can be stated in two equations in three unknowns, that is, a system of linear Diophantine equations.

$$\begin{aligned} x + y + z &= 100 \\ 5x + 3y + \tfrac{1}{3}z &= 100 \end{aligned}$$

There are various ways to solve this system. A standard method is to eliminate one of the variables to turn it into one equation in two unknowns.

Let's eliminate $z$. From the first equation, $z = 100 - x - y$, so the second equation becomes

$$5x + 3y + \tfrac{1}{3}(100 - x - y) = 100.$$

That simplifies first to

$$15x + 9y + 100 - x - y = 300$$

then to

$$14x + 8y = 200,$$

and finally to

$$7x + 4y = 100.$$

Now, we know that the greatest common divisor of 7 and 4 is 1, which we find using the Euclidean algorithm. And the steps in the Euclidean algorithm

give us a way to express 1 as a linear combination of 7 and 4. Since

$$\begin{aligned} 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

therefore

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 1 \cdot 7.$$

We can scale that up by a factor of 100 to get a solution of $100 = 7x + 4y$, namely

$$100 = 200 \cdot 4 - 100 \cdot 7.$$

Thus, $x = -100$ and $y = 200$ is a solution to the equation $100 = 7x + 4y$. Since $z = 100 - x - y$, therefore $z = 0$. Unfortunately, that doesn't directly help us with the hundred fowls problem, since $x$ can't be negative there. Nonetheless, what we've done generalizes to give us the first step to solving a linear Diophantine equation.

**How to find one solution.** We already know how to find a solution to the equation

$$ax + by = d$$

when $d = (a, b)$, the greatest common divisor of $a$ and $b$. That solution we can find using the Euclidean algorithm. So, if we want to find a solution to $ax + by = c$, and $d|c$, just take the solution we know for $ax + by = d$ and scale it up by a factor of $d/c$.

For example, back in an earlier section, the Euclidean algorithm gave us the greatest common divisor $(54, 21) = 3$, and the process gave us 3 as a linear combination of 54 and 21, namely $2 \cdot 54 + (-5) \cdot 21 = 3$. So, if we need to solve the equation $54x + 21y = 51$, since $51/3 = 17$, just scale up the solution $x = 2$, $y = -5$ by a factor of 17 to get $x = 34$, $y = -85$ as a solution to the equation $54x + 21y = 51$.

Thus, we can find one solution to the linear Diophantine equation $ax + by = c$ if the GCD $(a, b)$ divides $c$. On the other hand, if the GCD $(a, b)$ doesn't divide $c$, then there is no solution.

**How to find the rest of the solutions.** There is a standard technique in mathematics to find all the solutions to an equation—whether it be a Diophantine equation or a differential equation or whatever kind of equation—first find one solution to an equation, which we can call a *particular solution*, then find the rest of the solutions in terms of the particular solution.

Suppose we want to find all the solutions to the Diophantine equation

$$ax + by = c$$

and we've already found one solution $x = x_0$, $y = y_0$ using the Euclidean algorithm. Then we know that $ax_0 + by_0 = c$. Subtract the equation $ax_0 + by_0 = c$ from the equation $ax + by = c$ to get the equation

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

Introduce new variables $X$ and $Y$, and let $X = x - x_0$ and $Y = y - y_0$ so that the equation reads

$$aX + bY = 0.$$

This is a simpler equation because the constant $c$ doesn't appear in it. In fact, it's a homogeneous equation. A *homogeneous equation* is one in which all the terms have the same degree, in this case, they're all degree 1. In general, homogeneous equations are easier to work with than nonhomogeneous equations. In this case, we can easily solve the Diophantine equation $aX + bY = 0$ Let $d = (a, b)$, and divide by $d$ to get the equation $\frac{a}{d}X + \frac{b}{d}Y = 0$. Let $a' = a/d$ and $b' = b/d$, so that we need to solve the equation $a'X + b'Y = 0$ where $a'$ and $b'$ are relatively prime. The solutions are $(X, Y) = (b't, -a't)$ where $t$ is an any integer. We'll call $t$ a *parameter* in the solution. Then our final solution is

$$\begin{aligned} (x, y) &= (X + x_0, Y + y_0) \\ &= (b't + x_0, -a't + b_0) \\ &= (\tfrac{b}{d}t + x_0, -\tfrac{a}{d}t + y_0). \end{aligned}$$

For an example, consider the equation

$$54x + 21y = 51.$$

We've already found one particular solution $(x_0, y_0) = (34, -85)$. Now, since $(a, b) = (54, 21) = 3 = d$, therefore, the general solution is

$$\begin{aligned}(x, y) &= (\tfrac{b}{d}t + x_0, -\tfrac{a}{d}t + y_0) \\ &= (\tfrac{21}{3}t + 34, -\tfrac{54}{3}t + 85) \\ &= (7t + 34, -18t + 85)\end{aligned}$$

where $t$ is any integer.

We can summarize this investigation as a theorem.

*Theorem.* Let $a$ and $b$ be nonzero integers with greatest common divisor $d = (a, b)$. Then the Diophantine equation

$$ax + by = c$$

has a solution if and only if $d|c$. In that case, if $(x, y) = (x_0, y_0)$ is one solution, then all the other solutions are of the form

$$(x, y) = (x_0 + \tfrac{b}{d}t, y_0 - \tfrac{a}{d}t)$$

where $t$ is any integer.

**Back to the hundred fowls.** We found one solution to the Diophantine equation $100 = 7x+4y$, namely, the particular solution $x = x_0 = -100$ and $y = y_0 = 200$. We need to find the rest so that we can find one where $x$, $y$, and $z$ are all positive. According to the theorem we just proved, the rest of the solutions are of the form

$$(x, y) = (x_0 + \tfrac{b}{d}t, y_0 - \tfrac{a}{d}t)$$

where $d = (a, b) = (7, 4) = 1$ and $t$ is any integer, so

$$(x, y) = (-100 + 4t, 200 - 7t)$$

And since $z = 100 - x - y$, therefore

$$\begin{aligned}z &= 100 - (-100 + 4t) - (200 - 7t) \\ &= 3t.\end{aligned}$$

Now, since the problem requires that each of $x$, $y$, and $z$ be nonnegative (and positive would be even better), we need to find $t$ so that each of $-100+4t$, $200 - 7t$, and $3t$ is nonnegative.

In order that $-100 + 4t$ be nonnegative, $t$ needs to be greater than or equal to 25. In order that $200 - 7t$ be nonnegative, $t$ needs to be less than 28. And in order that $3t$ be nonnegative, $t$ needs to be greater than or equal to 0. Thus, $t$ has to be in the range

$$25 \le t \le 28.$$

That gives us the four solutions to the hundred fowls problem.

| $t$ | $x$ | $y$ | $z$ |
|---|---|---|---|
| 25 | 0 | 25 | 75 |
| 26 | 4 | 18 | 78 |
| 27 | 8 | 11 | 81 |
| 28 | 12 | 4 | 84 |