Review. Prime number theorem

Theorem 37. The gaps between primes can be arbitrarily large.

Proof. Indeed, for any integer $n > 1$,

$$n! + 2, \quad n! + 3, \quad \ldots, \quad n! + n$$

is a string of $n - 1$ composite numbers. Why are these numbers all composite!? □

Comment. Notice, however, how very large (compared to the gap) the numbers brought up in the proof are!

4 Diophantine equations

Diophantine equations are usual equations but we are only interested in integer solutions.

Example 38. Find the general solution to the diophantine equation $16x + 25y = 0$.

Solution. The non-diophantine equation $16x + 25y = 0$ has general solution $(x, y) = (25t, -16t)$ where the parameter t is any real number.

We need to figure out for which t this results in a solution where both coordinates $x = 25t$ and $y = -16t$ are integers. Obviously, t needs to be a rational number. Since $\gcd(16, 25) = 1$ the denominator of t must be 1, so that t must be an integer. In other words, the general solution to the diophantine equation $16x + 25y = 0$ is $(x, y) = (25t, -16t)$ where the parameter t is any integer.

Example 39. Find a solution to the diophantine equation $16x + 25y = 1$.

Solution. Since $\gcd(16, 25) = 1$, Bezout's theorem guarantees a solution, which we can find using the generalized Euclidean algorithm. Namely, in Example 19, we found that $-7 \cdot 25 + 11 \cdot 16 = 1$.

In other words, we have found the solution $x = 11$ and $y = -7$. In short, $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11 \\ -7 \end{bmatrix}$.

Are there other solutions? **Yes!** For instance, $x = -14$ and $y = 9$.

What is the **general solution**?

Solution. In the previous example we determined that the general solution to the corresponding **homogeneous (diophantine) equation** $16x + 25y = 0$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 25 \\ -16 \end{bmatrix} t$ where the parameter t is any integer.

We can add these solutions to any **particular solution** of $16x + 25y = 1$ to obtain the general solution to $16x + 25y = 1$. Therefore, the general solution is

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11 \\ -7 \end{bmatrix} + \begin{bmatrix} 25 \\ -16 \end{bmatrix} t = \begin{bmatrix} 11 + 25t \\ -7 - 16t \end{bmatrix},$$

where t is any integer.

Comment. Note that $t = -1$ results in $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11 - 25 \\ -7 + 16 \end{bmatrix} = \begin{bmatrix} -14 \\ 9 \end{bmatrix}$, another solution that we observed earlier.

Example 40. Find the general solution to the diophantine equation $16x + 25y = 3$.

Solution. It follows from the previous example that a particular solution is $\begin{bmatrix} x \\ y \end{bmatrix} = 3 \begin{bmatrix} 11 \\ -7 \end{bmatrix}$.

Hence, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 33 \\ -21 \end{bmatrix} + \begin{bmatrix} 25 \\ -16 \end{bmatrix} t = \begin{bmatrix} 33 + 25t \\ -21 - 16t \end{bmatrix}$.

Example 41. Find the general solution to the diophantine equation $6x + 15y = 10$.

Solution. This equation has no (integer) solution because the left-hand side is divisible by $\gcd(6, 15) = 3$ but the right-hand side is not divisible by 3.

Lemma 42. Let $a, b \in \mathbb{Z}$ (not both zero). The diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$.

Proof.
"$\Longrightarrow$" (the "only if" part): Let $d = \gcd(a, b)$. Then d divides $ax + by$. This implies that $d|c$.
"$\Longleftarrow$" (the "if" part): This is a consequence of Bezout's identity. $\square$

Note that we can therefore focus on diophantine equations $ax + by = c$ with $\gcd(a, b) = 1$.

(Otherwise, just divide both sides by $\gcd(a, b)$.)

Theorem 43. The diophantine equation $ax + by = c$ with $\gcd(a, b) = 1$ has the general solution

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + \begin{bmatrix} b \\ -a \end{bmatrix} t,$$

where $t \in \mathbb{Z}$ is a parameter, and x_0, y_0 is any particular solution.

How to find a particular solution? Since $\gcd(a, b) = 1$, we can find integers x_1, y_1 such that $ax_1 + by_1 = 1$ (this is Bezout's identity). Multiply both sides with c, to see that we can take $x_0 = cx_1$ and $y_0 = cy_1$.

Proof. First, let us consider the case of all real solutions. The general solution of $ax + by = c$ (which describes a line!) can be described as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} + \begin{bmatrix} b \\ -a \end{bmatrix} t$.

Since $\gcd(a, b) = 1$, this solution will be integers if and only if t is an integer. $\square$

Example 44. $56x + 72y = 2$ has no integer solutions (because $8|(56x + 72y)$ but $8 \nmid 2$).

Example 45. Find the general solution to the diophantine equation $56x + 72y = 24$.

Solution. We first note that this equation has an integer solution because 24 is a multiple of $\gcd(56, 72) = 8$.

To make our life easier, and to apply the theorem, we divide by 8 to get the equivalent equation $7x + 9y = 3$.

A solution to $7x + 9y = 1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$ (and we can always find such a solution using the Euclidean algorithm).

Therefore, a solution to $7x + 9y = 3$ is $\begin{bmatrix} x \\ y \end{bmatrix} = 3 \cdot \begin{bmatrix} 4 \\ -3 \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix}$.

In conclusion, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$.

Caution. Why would it be incorrect to state the general solution as $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 12 \\ -9 \end{bmatrix} + \begin{bmatrix} 72 \\ -56 \end{bmatrix} t$ for $t \in \mathbb{Z}$?

Armin Straub
straub@southalabama.edu