Solving Linear Diophantine's using a modular method

By: Om Patel

[1] - introduction

Diophantine equations are polynomial equations where we are only interested in the integer solutions. In particular, linear Diophantine equations are those which take the form: $ax + by = c$ such that $a, b, c \in \mathbb{Z}$ and if $gcd(a, b) | c \Rightarrow gcd(a, b) = \lambda = \gcd(a, b, c) \therefore a = \lambda\alpha, b = \lambda\beta, c = \lambda\gamma \therefore \lambda\alpha x + \lambda\beta y = \lambda\gamma \therefore \alpha x + \lambda\beta = \lambda\gamma \; where \; gcd(\alpha, \beta, \gamma) = 1 \Rightarrow gcd(\alpha, \beta) = 1$, then the equation has an infinite number of integer solutions in the form: $x = x_0 + kb$, $y = y_0 - ka$ where $k \in \mathbb{Z}$. Generally, these equations are solved using an extended Euclidian algorithm however through this essay I will be guiding you through how to solve these equations using modular arithmetic and particularly modular congruencies (Summarised from Wolfram MathWorld -https://mathworld.wolfram.com/DiophantineEquation.html).

Modular arithmetic is a way of working with numbers (generally integers) where we are concerned with the remainder of a number when divided by another number (generally one which is not a factor). Modular congruencies are a way of writing the fact that 2 integers have the same remainder when divided by the same number: $a \equiv$ b (mod n) meaning that a and b are integers which when divided by n have the same remainder. We can also rearrange to show that $(a - b) \equiv 0$ (mod n) meaning that (a-b) is a multiple of n. This can be shown algebraically by writing that $a = \alpha n + k \; and \; b = \beta$n + k (summarised from Wikipedia - https://en.wikipedia.org/wiki/Modular_arithmetic)

[2.1] – why the modular method

Looking at the linear Diophantine equation, $ax + by = c$, initially the normal method for solving this problem is using the Euclidian extended algorithm where we attempt to decompose the coefficients of x and y to be able to find a value for $gcd(a, b)$ by representing numbers in their remainder form and then we substitute backwards to achieve an equation in the form $ax + by = c$ where we have integer values of x and y however this method seems a bit unusual at first and may confuse you as to why this works however if we rephrase what we are doing in terms of modular arithmetic, gaining an intuition for where the general structure of x,y pairs for these beautiful equations.

[2.2] – the modular method

Given the equation in the form $ax + by = c \Rightarrow by = c - ax \therefore (c - ax)$must be a multiple of b. Since we know that $c - ax$ is a multiple of b we know that it will have a remainder of 0 when divided by b letting us set up the congruency that $(c - ax) \equiv 0 \; (mod \; b) \therefore c \equiv ax \; (mod \; b)$ giving us a congruency in mod b that we can work with to find x. We could use the extended

Euclidian algorithm to solve this congruency however in essence that is the same method as solving the linear Diophantine equation with the extended Euclidian algorithm, so instead we can work with the congruency given to try and isolate x: $ca^{-1} \equiv x\ (mod\ b)$ where a^{-1} is the inverse of a (mod b) such that $aa^{-1} \equiv 1\ (mod\ b)$, in essence the inverse of a is the modular arithmetic version of division. This means that now the only thing we have to find to solve this congruency is to find $a^{-1}\ (mod\ b)$ as we know what a and b are.

[2.3] – modular inverses

If we know that a and b are co-prime, such that $gcd(a,b) = 1$, we can utilise Euler's totient function and Eulers theorem where $\varphi(n)$ is the totient function that outputs the number of integers coprime to n in the range from 1 to n inclusive and Euler's theorem states that if $gcd(a,b) = 1$, then it holds that $a^{\varphi(b)} \equiv 1\ (mod\ b) \therefore\ a^{\varphi(b)-1} \equiv a^{-1} (mod\ b)$. However, if $gcd(a,b) \neq 1 \Rightarrow gcd(a,b) = \lambda = \gcd(a,b,c) \therefore a = \lambda\alpha, b = \lambda\beta, c = \lambda\gamma \therefore ax + by = c \Rightarrow \alpha x + \beta y = \gamma \therefore \beta y = \gamma - \alpha x\ \Longrightarrow (\gamma - \alpha x) \equiv 0\ (mod\ \beta) \therefore \gamma \equiv \alpha x\ (mod\ \beta) \Rightarrow\ x \equiv \gamma\alpha^{-1}\ (mod\ \beta)$ where we know that $gcd(\alpha,\beta) = 1$ meaning we can use Euler's totient function and Euler's theorem to find $\alpha^{-1}$and therefore x. we can compute large values of $\varphi(b)$ by using the fact that $\varphi(xy) =\ \varphi(x)\varphi(y)\frac{d}{\varphi(d)}$ where $d = gcd\ (x,y)$ and $\varphi(x^k) = x^k - x^{k-1}$ if x is prime and k ≥ 1. Using this fact, we can take the prime factor decomposition of b which we will write as $b = p_1^{a_1}p_2^{a_2} \dots p_{k-1}^{a_{k-1}}p_k^{a_k}$ ⇒ we can rewrite $\varphi(b)$ as $\varphi(p_1^{a_1}p_2^{a_2} \dots p_{k-1}^{a_{k-1}}p_k^{a_k}) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \dots \varphi(p_{k-1}^{a_{k-1}})\varphi(p_k^{a_k})$ as $gcd(p_i,p_j) = 1 \Rightarrow d = 1\ \therefore \varphi(d) = 1$.Therefore, we know that $\varphi(b) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_{k-1}^{a_{k-1}} - p_{k-1}^{a_{k-1}-1})(p_k^{a_k} - p_k^{a_k-1}) =\ p_1^{a_1}p_2^{a_2} \dots p_{k-1}^{a_{k-1}}p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_{k-1}}\right)\left(1 - \frac{1}{p_k}\right) = b\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_{k-1}}\right)\left(1 - \frac{1}{p_k}\right)$ which lets us work out the totient function of any integer by just working out all their unique prime factors and using the formula we derived above. (Ideas for finding a modular inverse using Euler methods taken from Medium post on Euler totient function and totient theorem - https://medium.com/@anilkumar78/euler-totient-function-totient-theorem-1b5104d00e65)

[2.4] – finishing the solution

Now that we can find a solution for x, which we will call x_0, we can substitute back into the equation for y in terms of x ($y = -\frac{a}{b}x + \frac{c}{b}$ or $y = -\frac{\alpha}{\beta}x + \frac{\gamma}{\beta}$) and find a corresponding y value, which we will call y_0 where $y_0 = -\frac{ax_0+c}{b}\ or\ y_0 = -\frac{\alpha x_0+\gamma}{\beta}$, which satisfies the equation $ax + by = c$ however, since the solution was calculated from the modular congruency it is not the only solution as there are infinitely many integers that have the same remainder when divided by an integer, for example, both 4 and 7 have remainder 1 when divided by 3. Since when we found x we used mod b or mod β, our answers for x take the form of either $x = x_0 + bk\ or\ x = x_0 + \beta k$ where $k \in \mathbb{Z}$ depending on whether we had to simplify the original equation or not. Using these expressions for x, we can now find the corresponding infinite list of y values which take the form of $y = -\frac{a(x_0+bk)+c}{b} = -ak - \frac{ax_0+c}{b} = x_0 - ak$ or $y = x_0 - \alpha k$ depending on whether we had to simplify the original equation or not.

[2.5] – why simplification always works

For equations $a_1x + b_1y = c_1$ where $gcd(a_1, b_1) \neq 1$ we can assign this divisor a variable such as ω where $\omega = gcd(a_1, b_1)$ therefore using properties of linear Diophantine equations we can state that $\omega | c_1$ hence all 3 integers in the original equation can be written as a product of ω where $a_1 = \omega a_2, b_1 = \omega b_2, c_1 = \omega c_2$ meaning we can divide the initial equation by ω to get the equation $a_2x + b_2y = c_2$ (previously I referred to these values as α, β, γ to save me from having to use subscripts) where the $gcd(a_2, b_2) = 1 = gcd(a_2, b_2, c_2)$ as $gcd(a_2, b_2)$ must divide $c_2$making it a divisor and since the largest divisor of a_2, b_2 is also a divisor of c_2, then it means that the largest divisor of all 3 terms is the same as just that of a_2, b_2. Now since we have an equation in the form $ax + by = c$ where $gcd(a, b) = 1$ which means that we can utilise our Euler's totient function and Euler's theorem as we have satisfied the key quality which we required (gcd = 1) which is why we are able to always use this method even if initially the gcd doesn't equate to 1 at first glance.

[3] – an example to consolidate

Take the equation 21x + 15y = 69, we can see immediately that the gcd(21, 15) is not 1 but in fact is 3 and similarly with the gcd(21, 15, 69) has the same value of 3 meaning that we can divide the equation by 3 to achieve a new equation of 7x + 5y = 23, where both gcds are now 1 meaning we can now begin without modular method. We can say that 5y = 23 – 7x showing us that 23 – 7x is a multiple of 5 letting us set out modular congruency $23 - 7x \equiv 0 \ (mod\ 5) \implies$ $23 \equiv 7x \pmod 5$ meaning $23(7^{-1}) \equiv x \pmod 5$ where $7^{-1} \bmod 5 = 7^{\varphi(5)-1}$ *where* $\varphi(5) = 5(1 - \frac{1}{5}) = 4$ hence $7^{-1} = 7^{4-1} = 7^3 = 343 \bmod 5 = 3$ hence $x \equiv 23(3) \pmod 5 \implies x \equiv 4 \pmod 5$ meaning $x = 4 + 5k$ where $k \in \mathbb{Z}$ which means that $x_0 = 4$ and since $y = \frac{23-7x}{5}$, $y_0 = -1$ hence $y = \frac{23-7(4+5k)}{5} = \frac{23-28-35k}{5} = \frac{-5-35k}{5} = -1 - 7k$ which gives us our general set of solutions for x and y which satisfy the original equation and also fit the generalised formula we had derived across the previous sections.