Introduction to Number Theory Week 2 Handout

04/10/18

1 Introduction

Tutor Name: Alexandre (Alex) Daoud (S5.13)
Email: alexandre.daoud@kcl.ac.uk
Tutorial Group: 02_JT
Tutorial Website: `http://p-adic.com/teaching/ccm224_1819`

2 Handing in Sheet 1

I will mark your answers to the following questions once you hand them in next week:

- Q1 (3), Q2, Q4, Q5

The rest (except 6) we will have a look at today in class.

3 A practice Linear Diophantine Equation

We will have a look at the following Exercise today (as practice for Exercise 5):

Exercise. *Consider the linear Diophantine equation*

$$28x + 49y = 14$$

State whether or not this equation has an integer solution $(x, y) \in \mathbb{Z}^2$*. If not, state a reason for why. If so then find a closed form for all its integer solutions.*

Solution. Theorem 1.13 from lectures tells us that this equation has integer solutions if and only 14 is a multiple of $\gcd(28, 49)$. Staring at these numbers hard enough, we realise that $\gcd(28, 49) = 7$ so indeed this equation has integer solutions.

Theorem 1.13 also tells us how we should find a closed form for these solutions. We must first apply the Euclidean algorithm forwards then backwards to 28 and 49 in order to find two integers u and v such that

$$28u + 49v = 7$$

So let's do that:

$$\begin{aligned} 49 &= 1 * 28 + 21 \\ 28 &= 1 * 21 + 7 \\ 21 &= 3 * 7 + 0 \end{aligned}$$

Now reversing the algorithm gives

$$\begin{aligned} 7 &= 28 - 1 * 21 \\ 7 &= 28 - 1 * (49 - 1 * 28) \\ 7 &= 28 - 1 * 49 + 1 * 28 \\ 7 &= 2 * 28 - 1 * 49 \end{aligned}$$

So $u = 2$ and $v = -1$. Hence the solutions to the equation are given by $(x_n, y_n)_{n\in\mathbb{Z}}$ where

$$x_n = \frac{14}{7}(2) + \frac{49}{7}n$$
$$x_n = 4 + 7n$$

$$y_n = \frac{14}{7}(-1) - \frac{28}{7}n$$
$$y_n = -2 - 4n$$

and we are done! (Make sure to check that these solutions indeed work!)

4 Detailed solution to Question 3

Exercise. *Let $a > b > 1$ be integers.*

1. *Consider the first two steps of the Euclidean algorithm for computing* $\gcd(a, b)$*:*

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$

   Show that $r_2 < \frac{b}{2}$.

2. *Let $\lambda(a, b)$ be the number of steps taken by the Euclidean algorithm for computing* $\gcd(a, b)$ *- more precisely, we let $\lambda(a, b) = n$ where r_n is the first zero remainder in the Euclidean algorithm.*
   Show that $\lambda(a, b) \leq \lceil \frac{\log b}{\log 2} \rceil$.

Solution. We shall prove Part 1 and the link between Part 1 and Part 2 via the following claim:

Claim. Let $n \in \mathbb{N}$ and denote by r_n the n^{th} remainder given by the Euclidean algorithm. Then

$$r_{2n} < \frac{b}{2^n}$$

Proof. We prove the claim by induction on n. First assume that $n = 1$. We need to show that $r_2 < \frac{b}{2}$. By Theorem 1.2 in the notes, we know that $r_2 < r_1$. Hence if $r_1 \leq \frac{b}{2}$ then we are done. So let's assume that $r_1 > \frac{b}{2}$. Then

$$r_2 = b - q_2 r_1$$
$$< b - \frac{b}{2}$$
$$< \frac{b}{2}$$

and so the claim is proven when $n = 1$. Now assume, given an arbitrary $n \in \mathbb{N}$, we have that $r_{2n} < \frac{b}{2^n}$. We need to show that $r_{2(n+1)} < \frac{b}{2^{n+1}}$. As before, Theorem 1.2 tells us that $r_{2n+2} < r_{2n+1}$ so if $r_{2n+1} \leq \frac{b}{2^{n+1}}$ then we are done. If not then $r_{2n+1} > \frac{b}{2^{n+1}}$. By the induction hypothesis we know that $r_{2n} < \frac{b}{2^n}$. Putting it all together, we get

$$r_{2(n+1)} = r_{2n+2} = r_{2n} - q_{2n+2} r_{2n+1}$$
$$< \frac{b}{2^n} - \frac{b}{2^{n+1}}$$
$$< \frac{b}{2^{n+1}}$$

which proves the claim. □

We are now in a position to finish the solution to Part 2. Let $n = \lceil \frac{\log b}{\log 2} \rceil$. Then $n \geq \frac{\log b}{\log 2}$. Doing some algebra, we find that $2^n \geq b$. But by the claim, we know that $r_{2n} < \frac{b}{2^n}$ and so

$$r_{2n} < \frac{b}{2^n} \leq 1$$

Now, Theorem 1.2 says that $r_{2n} \geq 0$ so, necessarily, $r_{2n} = 0$. We can thus be assured that after at most $2n$ steps, the Euclidean algorithm is guaranteed to have terminated. In other words, $\lambda(a, b)$ can be no larger than $2n = 2\lceil \frac{\log b}{\log 2} \rceil$.