Introduction to Number Theory Week 4 Handout

18/10/18

1 Introduction

Next week please hand in the solutions to the following exercises on Sheet 3: Q2(3), Q3, Q4(3), Q6. We will do the rest in class.

2 Comments on Sheet 1

2.1 General comments

- I only received homework from 5 people last week! It is very good practice for the exams for you to attempt the tutorial sheets (now and not a week before the exam!). A lot of the questions on the exams will be things from lecture notes and the tutorial sheets.
- I noticed a lot of people are writing down correct things but with little justification. An example is in Question 2 which I shall touch on below. You must always write down the reason for a correct statement else you will not get full marks!

2.2 Question 2

A lot of proofs for the first part of this question went along the following lines:

Proof. By Bézout's Lemma there exist $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} \gcd(ma, mb) &= uma + vmb \\ &= m(ua + vb) \\ &= |m| \gcd(a, b) \end{aligned}$$

□

The issue with this proof is that we are assuming that the u, v hypothesised to exist are dependent on ma and mb . It is not automatically true that $\gcd(a, b) = ua + vb$ **with the same u and v**. If you think about it, that is exactly what we are trying to prove! The reason why this is true requires further justification along the lines of $\gcd(ma, mb)$ is the smallest positive number of the form $uma + vmb$. Hence $|m| \gcd(a, b)$ is the smallest positive number of the form $ua + vb$.

3 A Hensel's Lemma example

Exercise. *Consider the polynomial $f(X) = X^3 + 1$. Find a solution to $f(X)$ modulo 8.*

Solution. We could just check every element of $\mathbb{Z}/8\mathbb{Z}$ (i.e $\mathbb{Z}_8$) but that's no fun. Let's use Hensel's Lemma to do it. The moral of Hensel's Lemma is as follows:

If we can find a solution modulo p^r, we might be able to find a solution modulo p^{r+1}

This process of creating new solutions in higher prime-power orders is called "lifting" - we'll see why at the end of this solution.

So lets lift from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/8\mathbb{Z}$ since its fairly easy: $\mathbb{Z}/4\mathbb{Z} = \{ [0]_4, [1]_4, [2]_4, [3]_4 \}$ so it's not too difficult to check each residue class. It turns out that

$$f(3) \equiv 0 \pmod 4$$

So we have a candidate solution modulo 4 to work with: $x_2 = 3$. We need to check that the derivative doesn't vanish at this number modulo the base prime which is 2 in this case. Our calculus kicks into gear and we get $f'(X) = 3X^2$ and

$$f'(3) = 3(3)^2 = 27 \equiv 1 \pmod 2$$

which is evidently not 0 so we can indeed apply Hensel's Lemma to this problem. The Lemma tells us that there exists an $x_3 \in \mathbb{Z}$ such that $f(3) \equiv 0 \pmod 8$ and $x_3 \equiv x_2 \pmod 4$. Explicitly, we have that

$$\begin{aligned} x_3 &= x_2 - f(x_r)u \\ &= 3 - 28u \end{aligned}$$

where u is an inverse of $f'(x_2) = 27$ modulo 2. That's just 1 so we get

$$x_3 = 3 - 28 = -25 \equiv 7 \pmod 8$$

Let's just make sure this does satisfy the properties we claim:

$$\begin{aligned} f(x_3) &= 7^3 + 1 = 344 \equiv 0 \pmod 8 \\ x_3 &= 7 \equiv 3 \pmod 4 \\ &= x_2 \end{aligned}$$

So $x_3 = 7$ is a solution. So why do we call this a lift anyway? Well, lets write out $x_2 = 3$ and $x_3 = 7$ in their base 2 expansions:

$$\begin{aligned} x_2 = 3 &= \phantom{1 \cdot 2^2 + {}} 1 \cdot 2^1 + 1 \cdot 2^0 \\ x_3 = 7 &= 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \end{aligned}$$

As you can see, x_3 is really just a sort of 'extension' of x_2: we've added another power of 2 to the expansion in this particular case - this is exactly what the property $x_3 \equiv x_2 \pmod{4 = 2^2}$ encodes.