Family 48 Problem Set 2

Rithvik Reddy

June 29th 2020

1 Introduction

Ok, so this is the second problem set. It will mostly be an extension of Extra Problem Set 1 but there wil be some other things which are more number-theory focused.

First, let's start off with a simple one,requiring just some obvious algebraic manipulations

Problem 1. *Prove that e is not an algebraic number of degree 2, i.e there exists no degree 2 polynomial $f \in \mathbb{Z}[x]$ such that $f(e) = 0$.*

We know that e is irrational, however even the stronger result that e is transcendental is true. Remember how I talked about how the degree of an algebraic number is a 'measure' of its irrationality, well transcendental means that the number is 'too irrational to be measured' whatever that means I promised a proof of transcendentality of e last time so I'll do that now.

2 e is transcendental

Before moving on, let's recall what we did in Extra Problem Set 1, we proved the following theorem(which is known as Liouville's theorem):

Theorem 1. *If α is a real algebraic number of degree n there exists a constant $c(\alpha)$ such that for all rationals $\frac{p}{q}$ with $(p, q) = 1$,*

$$\mid \alpha - \frac{p}{q} \mid > \frac{c(\alpha)}{q^n} \tag{1}$$

We can keep this result in mind for now, it might prove useful later on. If α is an irrational number, then a simple calculation using the pigeonhole principle allows us to get the following approximation.

Theorem 2. *Let $\alpha \in \mathbb{R}$ be irrational. Then there exists infinitely many rationals $\frac{p}{q}$ such that $\mid \alpha - \frac{p}{q} \mid < \frac{1}{q^2}$*

Proof. Consider the $n + 1$ numbers $1, \{frac(k\alpha) | 1 \leq k \leq n\}$ where $frac(x)$ is the fractional part of the number(in other words $frac(x) = x - \lfloor x \rfloor$ for $x > 0$ and $x - \lceil x \rceil$ for $x \leq 0$).

By the pigeonhole principle, 2 of these numbers must lie in some subinterval of $(0, 1]$ of the form $(\frac{i}{n}, \frac{i+1}{n})$ where $0 \leq i \leq n - 1$. The size of each of these intervals is $\frac{1}{n}$. In other words, there exists q, q' such that $frac(q\alpha), frac(q'\alpha)$ lie in the same subinterval. So, the difference satisfies $\mid \alpha(q - q') - p \mid < \frac{1}{n}$ for some integer p.Dividing by, we get

$\mid \alpha - \frac{p}{|q-q'|} \mid \leq \frac{n}{|q-q'|}$

But $|q - q'| = q_1$ for some $1 \leq q_1 \leq n$ so

$\mid \alpha - \frac{p}{q_1} \mid \leq \frac{1}{q_1^2}$

Infinitely many of these distinct $\frac{p}{q}$ must exist else $|\alpha - \frac{p}{q}|$ would have a minimum which is a contradiction(why?)

One of the first examples of transcendentality was $\sum\limits_{n=0}^{\infty} 10^{-n!}$, proven, I think by Liouville.

The above theorem shows that this famous theorem of Siegel-Roth is the 'best possible'.

Theorem 3. *Let α be irrational and algebraic. Then, there exist only finitely many solutions to*

$$\mid \alpha - \frac{p}{q} \mid < \frac{1}{k^{2+\epsilon}} \tag{2}$$

for any $\epsilon > 0$

As we have stated before, e is transcendental. I've attached a proof in the github repo which uses classic Hermite techniques to do so. It requires nothing more than some knowledge of calculus.One of the lines uses the fact that $p!$ grows faster than e^p, that is $\lim_{p\to\infty} \frac{e^p}{p!} \to 0$. □

Try and do this problem

3 More stuff on primitive roots

We've proven that U_p has a primitive root. Use that to prove the following results that I discussed in the meetings.

Problem 2. *If $d|p-1$, prove that there are exactly $\phi(d)$ elements of order d in $Z_p^\times$*

Problem 3. *Prove Euler's theorem and submit that in place of the required FLT proof in Problem Set 10.*

Now, we're going to see how even $\mathbb{Z}_{p^2}^\times$ has a primitive root or generator.

Problem 4. *Prove that $\mathbb{Z}_{p^2}^\times$ has a primitive root for prime p.*

Here is a sketch of how to prove it.

Proof. The proof holds true for $p = 2$ which can be quickly verified separately. We'll assume now that p is an odd prime. First let s be a primitive root $modp$ and then study the order of s $modp^2$, say $ord_{p^2}(s) = n$, then $s^n = 1 \pmod{p^2} \Rightarrow s^n = 1 \pmod{p}$. Use the facts about orders that we already know and show that either s is also a primitive root $modp^2$ or $s + p$ is a primitive root. $\square$

You can generalize but it is a little hard.

Problem 5. ** Prove that $\mathbb{Z}_{p^k}^\times$ has a primitive root.*