Admin

- HW1 due tonight (10-6) @ 11:59 PM
  - Late submissions up to Monday @ 11:59 AM
  - * graded for correctness, and may be resubmitted
  - next for completion
- HW2 posted, due next Thursday
- Gradescope fixed?
- discord link on canvas

Regarding HW1 problem 3

This is hard.

Consider special cases and particular numbers.

For instance, analyze the proof that $\sqrt{2}$ is irrational.

Proof: Let $\sqrt{2} = \frac{p}{q}$ with p, q relatively prime integers.

Then $2 = \frac{p^2}{q^2}$

$$2q^2 = p^2$$

so $2 | p^2$. As 2 is prime, $2 | p$

Let $p = 2r$.

$$2q^2 = (2r)^2$$
$$= 4r^2$$

so $q^2 = 2r^2$, whence $2 | q^2$ so $2 | q$. □

But p, q were chosen to be coprime, contradiction.

??? Sure it works, but what does it mean? When I first saw this, it was just a random sequence of manipulations until you got lucky with a contradiction.

Here's a fake proof.

"Proof": Let $\sqrt{2} = \frac{p}{q}$. 2 appears $\frac{1}{2}$ a time on the left and an integer number of times on the right. Contradiction, as $\frac{1}{2} \notin \mathbb{Z}$. "□"

This is "morally" what the proof should be.

But we need to formalize.

Issue 1. We don't know how fractional exponents work. Is there a FTA for fractional exponents? This is unclear.

Solution. Clear the denominators in the exponent by squaring.

Here, $2 = \frac{p^2}{q^2}$. The left has 1 power of 2 and the right has an even power of 2. Contradiction? Note that $\frac{1}{2} \notin \mathbb{Z} \iff 1$ is not even, so this is the same moral idea

Issue 2. We don't know how FTA or divisibility works for rational numbers, only honest old integers.

Solution. Clear denominators to get $2q^2 = p^2$

Now we just have to analyze where the powers of 2 are.

Say $2^e \| q$ and $2^d \| p$

Then $2^{2e} \| q^2$ and $2^{2d} \| p^2$

and $2^{2e+1} \| 2q^2$

so in $2q^2 = p^2$, the LHS has $2e+1$ powers of 2 and the RHS has $2d$

By FTA, $2e+1 = 2d$. Can we find natural numbers d, e to make this true? No! The LHS is odd and the RHS is even. $\square$

Try some other examples, like $2^{1/3}$, $4^{1/3}$, $6^{1/2}$, $18^{1/2}$ to stretch this argument as far as possible and collect data for your conjectured characterization of when $n^{a/b}$ is rational, as well as a proof.

Euler products

Recall FTA:

Let $n \geq 1$. Then $n = \prod p_i^{e_i}$ uniquely, where p_i are distinct primes and $e_i \geq 1$.

Def. Let $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ for $s \in \mathbb{C}$

(Rmk. This converges absolutely for $\mathrm{Re}(s) > 1$ by a p test)

We will ignore issues of convergence and work purely formally.

Consider $(1 - 2^{-s})\zeta(s) = \zeta(s) - 2^{-s}\zeta(s)$

$$= \sum_{n \geq 1} \frac{1}{n^s} - \sum_{n \geq 1} \frac{1}{(2n)^s}$$

$$= \sum_{\substack{n \geq 1 \\ 2 \nmid n}} \frac{1}{n^s}$$

$$(1 - 3^{-s})(1 - 2^{-s})\zeta(s) = \sum_{\substack{n \geq 1 \\ 2 \nmid n}} \frac{1}{n^s} - \sum_{\substack{n \geq 1 \\ 2 \nmid n}} \frac{1}{(3n)^s}$$

$$= \sum_{\substack{n \geq 1 \\ 2,3 \nmid n}} \frac{1}{n^s}$$

1 2 3 4 (5) 6 7 8 9 10

(11) 12 (13) 14 15 16 (17) 18 (19) 20

Hence, $\left(\prod_{p \text{ prime}} (1-p^{-s})\right) \varphi(s) = 1$

So we arrive at the Euler product formula

$$\varphi(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

This can also be done in the reverse direction.

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} p^{-ks}$$

$$= (1+2^{-s}+2^{-2s}+2^{-3s}+\cdots)(1+3^{-s}+3^{-2s}+3^{-3s}+\cdots)$$
$$(1+5^{-s}+5^{-2s}+5^{-3s}+\cdots) \cdots$$

How do we expand such a product? For each component $\sum_{k=0}^{\infty} p^{-ks}$, pick one term $p^{-e_p s}$ for some $e_p \geq 0$. Multiply all these together $\prod p^{-e_p s}$ and sum over all choices of e_p.

Rmk. If infinitely many $e_p \neq 1$ then $\prod p^{-e_p s} = 0$ as $\mathrm{Re}(s) > 1$

Hence, this becomes

$$\sum_{\substack{e_p \geq 0 \text{ for} \\ p \text{ prime s.t.} \\ \text{all but finitely} \\ \text{many } e_p = 0}} \left(\prod p^{e_p} \right)^{-s}$$

But $\left\{ (e_p)_p \;\middle|\; \begin{array}{l} e_p \geq 0 \text{ for} \\ p \text{ prime s.t.} \\ \text{all but finitely} \\ \text{many } e_p = 0 \end{array} \right\} \xrightarrow{\sim} \mathbb{Z}^{\geq 1}$

$$(e_p)_p \longmapsto \prod p^{e_p}$$

is exactly FTA!

Corollary. Consider $s = 1$ (OR, really take a limit as $s \to 1$ from the right)

$$\sum_{n \geq 1} \frac{1}{n} = \prod \frac{1}{1 - p^{-1}}$$

Hence, there are only many primes, as the harmonic series diverges!

may seem silly but this introduced complex analysis and the study of ζ into number theory.

For instance, we have a stronger result.

Thm. $\sum_{p \text{ prime}} \frac{1}{p}$ diverges

pf. Consider $\log(\zeta(s)) = \sum_p \log \frac{1}{1-\frac{1}{p}}$

Recall $\log\left(\frac{1}{1-x}\right) = \sum_{n \geq 1} \frac{x^n}{n}$

Thus, at $s=1$, we get, $\sum_p \sum_{n \geq 1} \frac{p^{-n}}{n}$

$= \sum_p p^{-1} + \underbrace{\sum_p \sum_{n \geq 2} \frac{p^{-n}}{n}}$

$\leq$

$\sum_p \frac{p^{-2}}{2} \sum_{n \geq 1} p^{-n}$

$=$

$\sum_p \frac{p^{-2}}{2} \frac{1}{1-p^{-1}}$

$=$

$\frac{1}{2} \sum_p \frac{1}{p(p-1)} \leq \frac{1}{2} \sum_k \frac{1}{k(k-1)}$

$< \infty$ by telescoping

OTOH $\varphi(\beta) = \sum \frac{1}{n}$ the harmonic series

Hence,

$$\log \sum_n \frac{1}{n} = \sum_p p^{-1} + C$$

for some constant C.

Thus, $\sum_p p^{-1}$ diverges.

In fact, we know that $\sum_n \frac{1}{n}$ diverges like $\log(x)$,

so $\sum_p p^{-1}$ diverges like $\log\log(x)$,

Recall that, by the prime number theorem, that $p_n \sim n \log n$. This result is consistent with that.

Further analysis of φ yields better and better estimates on the primes.

Quadratic residues

Recall $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv \bmod n$

where $a \equiv b \bmod n$ if $n \mid a-b$

i.e. $a-b \in n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

has n elements

By the HW 2 problem, we can perform arithmetic

$$\bar{a} + \bar{b} \overset{(def)}{=} \overline{a+b}$$

$$\bar{a} \cdot \bar{b} \overset{(def)}{=} \overline{ab}$$

in a reasonable fashion (i.e. $\mathbb{Z}/n\mathbb{Z}$ is a "commutative ring")

Def. m is a quadratic residue mod n if $x^2 = \bar{m}$ has a solution in $\mathbb{Z}/n\mathbb{Z}$,

i.e. if $\exists x \in \mathbb{Z}$ s.t. $x^2 \equiv m \bmod n$.

eg, what are quadratic residues mod 4?

$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{0}^2 = \bar{0}$

$\bar{1}^2 = \bar{1}$

$\bar{2}^2 = \bar{0}$

$\bar{3}^2 = \bar{9} = \bar{1}$

So the quadratic residues mod 4 are $\bar{0}$ and $\bar{1}$.

eg, everything in $\mathbb{Z}/2\mathbb{Z}$ is a square.

Thm. Let p be an odd prime. Then

$p = x^2 + y^2$ if and only if $p \equiv 1 \bmod 4$

pf. ($\Rightarrow$) x^2 and y^2 are quadratic residues mod 4 and are hence $\bar{0}$ or $\bar{1}$.

Thus, $\bar{x}^2 + \bar{y}^2 = \bar{0}$ or $\bar{1}$

but as p is prime, $4 \nmid p$, so

$p \equiv 1 \bmod 4$

($\Leftarrow$)???

Step 1. If $p \mid x^2+y^2$ where $\gcd(x,y)=1$ then p is of the desired form,

The key is the following identity:

$$(x^2+y^2)(a^2+b^2) = (xa \pm yb)^2 + (xb+ya)^2$$

(cf. $|zw|^2 = |z|^2|w|^2$ for $z, w \in \mathbb{C}$)

cf. Cox's "primes of the form x^2+ny^2"

Lemma 1.4, pg 10

Step 2. Figure out when $p \mid x^2+y^2$ for $\gcd(x,y)=1$.

Def. Let $a \in \mathbb{Z}$ and p an odd prime. We define the Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and } a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a \text{ and } a \text{ is not a quadratic residue mod } p \end{cases}$$

Lemma. Let p be an odd prime not dividing an integer $n \neq 0$. Then $p \mid x^2+ny^2$ is solvable with $\gcd(x,y)=1$ iff $\left(\frac{-n}{p}\right)=1$.

($\Leftarrow$)

pf. Let $\left(\frac{-n}{p}\right)=1$, so that $-n$ is a quadratic residue mod p.

Then let $\bar{k}^2 = -\bar{n}$ in $\mathbb{Z}/p\mathbb{Z}$

so $\bar{k}^2 + \bar{n} = \bar{0}$

$\|$

$\bar{k}^2 + \bar{n}\,\bar{1}^2$

i.e. $p \mid k^2 + n\cdot 1^2$, and certainly $\gcd(k,1)=1$.

($\Rightarrow$) Let $p \mid x^2 + ny^2$ w/ $\gcd(x,y)=1$.

$\|$

$\bar{x}^2 + \bar{n}\bar{y}^2 = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$

If $\bar{y}=\bar{0}$ then $\bar{x}^2=\bar{0}$

(i.e. $p \mid y$) i.e. $p \mid x^2$ so $p \mid x$

so $\bar{x}=0$, i.e. $p \mid x$

But $\gcd(x,y)=1$. Hence, $\bar{y}\neq\bar{0}$

so $\gcd(y,p)=1$. By the Euclidean algorithm,

we can find $a,b \in \mathbb{Z}$ s.t. $ap+by=1$

$\Rightarrow b\bar{y}=\bar{1}$.

Hence, $\bar{x}^2 + \bar{n}\,\bar{y}^2 = \bar{0}$ (*)

and $\bar{b}\,\bar{y} = \bar{1}$

Multiply (*) by $\bar{b}^2$

$$\bar{x}^2\bar{b}^2 + \bar{n} = \bar{0}$$

$$-\bar{n} = \overline{xb}^2$$

$$\left(\frac{-n}{p}\right) = 1$$

□

Take $n = 1$. When is $\left(\frac{-1}{p}\right) = 1$?

i.e. when is -1 a quadratic residue mod p?

when $\bar{-1} = \bar{x}^2$ is solvable (cf. $i^2 = -1$ in $\mathbb{C}$)

Suppose such a solution $\bar{x}$ existed,

then $\bar{x}^4 = (\bar{x}^2)^2 = \overline{(-1)^2} = \bar{1}$.

Fermat's little theorem says

$$\bar{x}^{p-1} = \bar{1} \text{ in } \mathbb{Z}/p\mathbb{Z}$$

Suppose $p \not\equiv 1 \bmod 4$

As p is prime, this forces $p \equiv 3 \bmod 4$,

so write $p = 4k+3$.

$$\begin{array}{l} \bar{x}^{p-1} = \bar{1} \\ \| \\ \bar{x}^{4k+2} \\ \| \\ (\bar{x}^4)^k \bar{x}^2 \\ \| \\ \bar{x}^2 \end{array}$$

so $\bar{x}^2 = \bar{1}$, but we assumed that

$\bar{x}^2 = \bar{-1}$. As p is odd, $\bar{-1} \neq \bar{1}$.

Hence, we conclude $p \equiv 1 \bmod 4$ □

Thm (Quadratic reciprocity).

Let p, q be distinct odd primes.

Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

This, miraculously, connects $x^2 - p$ in $\mathbb{Z}/q\mathbb{Z}$ to $x^2 - q$ in $\mathbb{Z}/p\mathbb{Z}$

so for instance, it can be used in understanding when $p = x^2 + ny^2$

e.g. $p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8$

$p = x^2 + 3y^2 \iff p = 3$ or $p \equiv 1 \bmod 3$

(due to format)

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20$$

(conjectured by Euler)

Thm. Let $n \equiv 1, 2 \bmod 4$ be squarefree, $\exists f_n(x)$ an irreducible polynomial over $\mathbb{Z}$ s.t. $\forall p$ prime not dividing the discriminant of f_n,

$p = x^2 + ny^2 \iff \left(\frac{n}{p}\right) = 1$ and $f_n(x)$ has a root in $\mathbb{Z}/p\mathbb{Z}$

This is extremely hard and uses "higher reciprocity" via "class field theory" developed throughout the 20th century.