In-person office hours:

- Wednesday 4-5 at 215 Huron 10^{th} floor lounge

or HU 1009

- or by appointment

- $\sqrt{2}$ is not a rational number

Assume $\sqrt{2}$ is rational. $\Rightarrow \sqrt{2} = \frac{a}{b}$ for some positive integers a, b.

$\sqrt{2} = \frac{a}{b} \Rightarrow b\sqrt{2} = a \Rightarrow 2b^2 = a^2$.

Say a and b have prime factorizations $a = 2^x \cdot \ldots\ldots$ and $b = 2^y \cdot \ldots\ldots$

$\Rightarrow 2b^2 = 2^{2y+1} \cdot \ldots\ldots$ and $a^2 = 2^{2x} \cdot \ldots\ldots$

$\Rightarrow 2y + 1 = 2x$, contradiction.

Notation: We write $p^e \| a$ if $p^e | a$ but $p^{e+1} \nmid a$

fully divides

(p^e is the highest power of p contained in a)

- $p^\alpha \| a$ and $p^\beta \| b \Rightarrow p^{\alpha+\beta} \| ab$, $p^{\alpha-\beta} \| \frac{a}{b}$.

Exercise: If $p^\alpha \| a$ and $p^\beta \| b$ and $\alpha < \beta$, then $p^\alpha \| a+b$. (If $\beta < \alpha$, then $p^\beta \| a+b$. If $\alpha = \beta$, $p^\alpha \mid a+b$ but not necessarily $p^\alpha \| a+b$).

$4 \cdot 9$

Questions: Suppose $(a,b) = 1$ and ab is a square. What can we say further about a and b?

$(a,b) = 1 \Rightarrow$ They have different prime factors.

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ and $b = p_{k+1}^{\alpha_{k+1}} \cdot \ldots \cdot p_{k+\ell}^{\alpha_{k+\ell}}$

$\Rightarrow ab = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{k+\ell}^{\alpha_{k+\ell}}$ is a square

$\Rightarrow \alpha_1, \alpha_2, \ldots, \alpha_{k+\ell}$ are all even.

$\alpha_1, \alpha_2, \ldots, \alpha_k$ even $\Rightarrow$ a is a square

$\alpha_{k+1}, \ldots, \alpha_{k+\ell}$ even $\Rightarrow$ b is a square

Can generalize: If $a_1, a_2, \ldots, a_k$ are mutually coprime and $a_1 a_2 \ldots a_k$ is an m^{th} power of an integer, then so are all of $a_1, a_2, \ldots, a_k$.

Exercise: $n(n+1)$ is never a square, $n \geq 1$.

Theorem: There are infinitely many primes.

Proof: Suppose not and say $p_1, p_2, \dots, p_n$ are all the primes. Consider $m = p_1 p_2 \cdots p_n + 1$.

- m cannot be a prime. Because m is larger than all of the "finitely many" primes $p_1, p_2, \dots, p_n$ $\Rightarrow$ m composite

This part was unnecessary

$\Rightarrow$ m has a prime divisor, say $p_i \mid m$

- $p_i \mid m$ and $p_i \mid p_1 p_2 \cdots p_n$ $\Rightarrow$ $p_i \mid m - p_1 p_2 \cdots p_n$

$\Rightarrow$ $p_i \mid 1$, contradiction.

Integers have one the forms: $4k, 4k+1, 4k+2, 4k+3$

Are there infinitely many primes for each form?

- $4k$: no because there is no prime divisible by 4.

- $4k+2$: no because there is no prime divisible by 2, except $p = 2$.

Dirichlet's Theorem: There are infinitely many primes of the form $ak + b$ if and only if $(a, b) = 1$.

We can give a proof for $4k+3$, but a general proof is beyond our level.

Lemma: We cannot have the form $4k+3$ by multiplying $4k$, $4k+1$, $4k+2$.

$4k \cdot 4\ell = 4m$ $\qquad (4k+1)\cdot(4\ell+1) = 4m+1$

$4k \cdot (4\ell+1) = 4m$ $\qquad (4k+1)\cdot(4\ell+2) = 4m+2$

$4k \cdot (4\ell+2) = 4m$ $\qquad (4k+2)\cdot(4\ell+2) = 4m.$

Infinitely many primes $4k+3$:

Proof: Suppose $3 = p_1$, $7 = p_2$, $p_3, \ldots, p_n$ are all the primes of the form $4k+3$.

$m = 4\, p_1 p_2 \cdots p_n - 1$.

- m is of the form $4k+3$

$m = 4(p_1 p_2 \cdots p_n - 1) + 3$

- m has a prime divisor of the form $4k+3$, by the lemma.

- Say $p_i \mid m$.

$p_i \mid 4\, p_1 p_2 \cdots p_n \Rightarrow p_i \mid 1$, contradiction.

- Pay attention to the differences between the two proofs.

- Why the same argument doesn't work for $4k+1$?