Lagrange gave a general solution in 1768 using continued fractions.

Let the smallest \( x, y \in \mathbb{Z} \) pair solving \( x^2 - dy^2 = 1 \) be called the fundamental solution.

Theorem (Don't use in homework) Let \( \frac{p_n}{q_n} \) be the \( n \)th convergent of \( \sqrt{d} \), \( \exists k \in \mathbb{N} \) such that \( (x, y) \) is the fundamental solution to \( x^2 - dy^2 = 1 \).

Proof: See chapter 8 of Baker.

Also note that we can show that if \( (x, y) \) is a fundamental solution then \( (x, y) \) is a solution iff \( x + y \sqrt{d} = \pm (x, y, \sqrt{d})^n \) for \( n \in \mathbb{Z} \).

Algebraic and Transcendental Numbers

A number \( \Theta \in \mathbb{R} \) is said to be algebraic of degree \( n \) if \( \Theta \) is the root of a polynomial with integer coefficients with smallest degree \( n \), \( p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), \( a_i \in \mathbb{Z} \).

Algebraic numbers form a ring.
So all $\frac{p}{q} \in \mathbb{Q}$ are algebraic with degree 1, since it is the root of $p(x) = qx - p$.

All $a + b\sqrt{d}$ with $d\in\mathbb{N}$ square-free and $a, b \in \mathbb{Q}$ are algebraic with degree 2 by the quadratic eq.

Cubic numbers that aren't algebraic are transcendental.

Most numbers are transcendental, as in there are countably many algebraic numbers and since $\mathbb{R}$ is uncountable, there are uncountably many transcendental numbers (algebraic numbers have Lebesgue measure 0).

In 1882 Lindemann proved Theorem: $\pi^\alpha$ is transcendental for all non-zero algebraic $\alpha \in \mathbb{C}$ shown in 1873 by Hermite.

So $e^{i\pi}$ is transcendental and since $e^{i\pi} = -1$, so $i\pi$.

So it is impossible to construct a square with the same area as a circle using a straight-edge and compass.
MORE GENERAL RESULTS ARE DUE TO WEIERSTRASS (1885) AND BAKER (1975) (AUTHOR OF THIS BOOK).

CAN FIND A MORE DIRECT PROOF OF THE TRANSCENDENCE OF e IN CHAPTER 6, USES CALCULUS.

(Also fun: e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, ...]
Euler did this. The proof is on the course website and isn't too hard to read, check it out.)
CHAPTER 2: FERMAT'S LAST THEOREM

THE KEY TO IMMORTALITY IS TO LEAVE CRYPTIC
NOTES IN STRANGE PLACES LIKE
"THE CASH IS BURIED UNDER A BIG W IN
SANTA ROSITA STATE PARK" IN A CAR WRECK OR
"I HAVE DISCOVERED A TRULY MARVELOUS PROOF
OF THIS, WHICH THIS MARGIN IS TOO NARROW TO
CONTAIN." IN THE MARGIN OF A BOOK

c. FERMAT, 1637

FERMAT'S LAST THEOREM [NOW WILES' THEOREM]
for n \in \mathbb{N} > 2, \ x^n + y^n = z^n \ has \ no \ solutions
in \ x, y, z \in \mathbb{Z}^+.

FERMAT DID PROVE THIS IN THE CASE WHERE n=4
USING AN INFINITE DESCENT ARGUMENT (SEE BOOK)
IT IS LIKELY HE THOUGHT THE ARGUMENT GENERALIZED
WHEN HE MADE THE COMMENT TO HIMSELF.

FROM THERE, ONE CAN SHOW THAT IF FERMAT'S
LAST THEOREM HOLDS FOR n=p, ODD PRIME WE
ARE DONE SINCE IF n=mp THEN A SOLUTION TO
x^m + y^m = z^m GIVES A SOLUTION TO (x^p)^p + (y^p)^p = (z^p)^p.
IT WAS PROVEN FOR \( p=3 \) (EULER), \( p=5 \) (DIRICHLET AND LEGENDRE, INDEPENDENTLY) AND \( p=7 \) (LAMÉ). SOPHIE GERMAINE DID \( p \leq 97 \) WHEN \( p \nmid x,y,z \), WHICH HELPED THE \( p=5,7 \) PROOFS.

IN 1847 LAMÉ ADDRESSED THE PARIS ACADEMY OF SCIENCES, SAYING HE HAD PROVEN FLT AND THANKED LIOUVILLE FOR THE ASSIST. LIOUVILLE TOOK THE STAGE AND SAID "UH... NO."

LAMÉ'S IDEA WAS TO FACTOR \( x^8 + y^8 = (x+y)(x^3+y^3)(x^3-y^3) \), WHERE \( \zeta_p = e^{2\pi i / p} \) IS A \( p \)TH ROOT OF UNITY AND USE THE RELATIVE PRIMENESS OF THE \( x+y \) TO CREATE AN INFINITE DESCENT ARGUMENT.

(WE USED AN INFINITE DESCENT ARGUMENT TO SHOW IF \( n=x^8+y^8 \), THEN THE PRIMES \( p \equiv 3 \pmod{8} \) DIVIDING \( n \) HAVE EVEN POWER)

LIOUVILLE COMMENTED THAT LAMÉ'S PROOF REQUIRED UNIQUE FACTORIZATION OF \( \mathbb{Z}[\zeta_p] \), WHICH HE DOUBTED.

TURNS OUT KUMMER SHOWED (THREE YEARS EARLIER, IN GERMANY) THAT \( \mathbb{Z}[\zeta_{p^3}] \) DOES NOT HAVE UNIQUE FACTORIZATION, BUT WAS WORKING ON A WAY AROUND IT WITH "IDEAL NUMBERS".
What does it mean not to have unique factorization?
Consider $\mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$
Consider $6 \in \mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
$2, 3, 1 \pm \sqrt{-5}$ are all irreducibles in $\mathbb{Z}[\sqrt{-5}]$.
$\mathbb{C}$ is irreducible in a ring, $R$, if $a | c$ for $a \in R$ means $a = uc$ where $u \in R$ is invertible. (like $1$)

Unique factorization happens when irreducibles are
prime, which means $p | ab \Rightarrow p | a$ or $p | b$
but $2$ is an irreducible in $\mathbb{Z}[\sqrt{-5}]$ that is
not prime, since $2 | (1 + \sqrt{-5})(1 - \sqrt{-5})$ but
$2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$

The fundamental theorem of arithmetic, that is
unique prime factorization, happens because
all irreducibles are prime in $\mathbb{Z}$ by the
the Euclidean algorithm (see the lemma on Day 2 of your lecture notes).

If you want to know more about number theory
over number fields ($\mathbb{Q}(\Theta)$ where $\Theta$ is algebraic)
take a course (or read a book) on algebraic
number theory.
Kummer's argument proved FLT for "regular primes", \( p \) primes that did not divide the class number of \( \mathbb{Z} \left[ \sqrt{5_p} \right] \).

Kummer's concept of "ideal numbers" were generalized by Dedekind in his construction of ideals. Hilbert and Noether made these into a thing.

**Elliptic Curves**

An elliptic curve is a curve of genus 1 with a specified base point, non-singular.

Given by the Weierstrass equation:

\[ E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

Where \( a_i \in K \), where \( K \) is a field that also satisfies other conditions like \( \bar{\mathbb{F}_p} \).

Under extra conditions, \( E \) can do a change of variables to rewrite the Weierstrass equations as:

\[ y^2 z = x^3 + ax z^2 + 1 z^3 \]