Lecture 1
Instructor : Henry Kim

solutions to Pythagorean tripples :

$$a^2+b^2=c^2$$

$a=st$
$b=\frac{s^2-t^2}{2}$ where s, t are odd integers.
$c=\frac{s^2+t^2}{2}$

. . . .

what about $a^n+b^n=c^n$, $n\geq 3$ integer solutions? ∞
Fermat's last theorem
A. Wiles solved this. (with Elliptic curves)

Primes . 2, 3, 5, 7, 11, 13, 17, 19, ⋯
Primes of the form $3x+1$, x int.
Which primes are sum of two squares? $p\equiv 1 \mod 4$
$5=1^2+2^2$
twin prime conjecture: (3, 5), (11, 13), (17, 19), ⋯ ∞ (still unsolved)

Primes of the form n^2+1, $n\in\mathbb{Z}$ (unsolved)

In 1903:
$$2^{67}-1 = 147573952589676412927$$
$$=193707721 \times 761838257287$$
primes

"factoring"
idea of RSA

prime # thm: (approx) $\pi(x)=\frac{x}{\log x}$

$\pi(x)=\sum_{p<x} 1$
(# of primes less than x)

and $Li(x)=\int_2^x \frac{dt}{\log t}$ (best approx to $\pi(x)$ so far)

Chapter 2.
$a^2+b^2=c^2$ integer solutions
if with common factor, $(da')^2+(db')^2=(dc')^2$
$a'^2+b'^2=c'^2$
so we can assume a, b, c have no common factors
we call such (a, b, c) primitive Pythagorean triples.

If a, b are both even, c is even. $\Rightarrow$ have common factor 2 $\Rightarrow$ impossible
If a, b are both odd, $a=2x+1$, $b=2y+1$, $x, y\in\mathbb{Z}$
$a^2+b^2=4x^2+4y^2+4x+4y+2$ is even
c^2 even $\Rightarrow c$ even
so we write $c=2z = 2x^2+2y^2+2x+2y+1$ which is odd ($\Rightarrow\Leftarrow$)
So we can assume a is odd, b is even, $\Rightarrow c$ is odd

$$a^2 = c^2 - b^2 = (c+b)(c-b)$$

claim $c+b$, $c-b$ have no common factors ($c+b$, $c-b$ are relatively prime/coprime)

Proof by contradiction.

Suppose d divides both $c+b$ & $c-b$

d divides $c+b+c-b = 2c$ and $c+b-(c-b) = 2b$

$d \mid a^2 \Rightarrow d$ is odd

(a,b,c) have no common factor

$\Rightarrow d = 1$

Unique factorization of integer $\rightarrow$ to be learned in §7

$$a^2 = (c+b)(c-b) \Rightarrow c+b = s^2, \quad c-b = t^2$$

($s > t \geq 1$, s and t are both odd, with no common factor)

so $c = \frac{s^2+t^2}{2}$, $b = \frac{s^2-t^2}{2}$, $a = st$