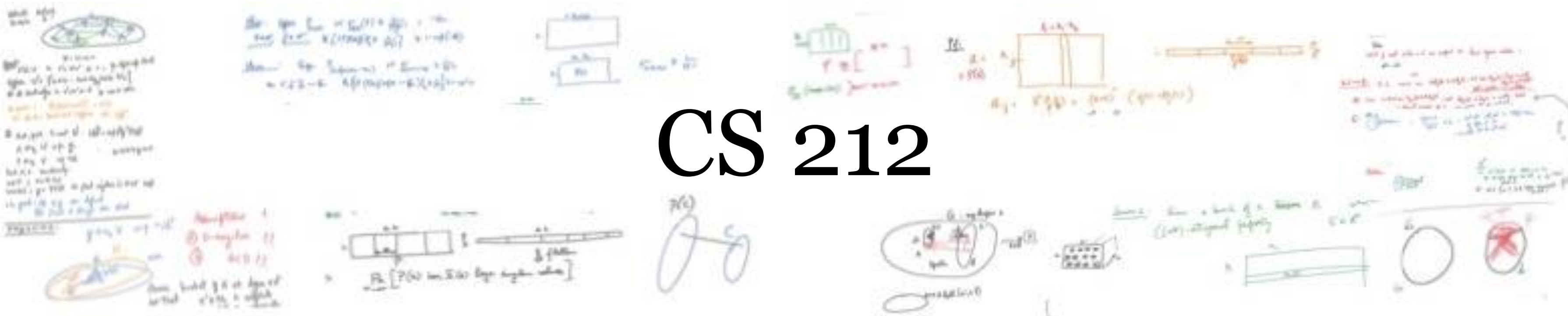


CS 212

Mathematical Foundations of Computer Science

Modular arithmetic

Announcements

- A practice exam will be posted.
- Solutions will be posted later in the week.
- Eric will hold office hours on Friday from 11 a.m. to 1 p.m. in Tech L158.

Number Theory

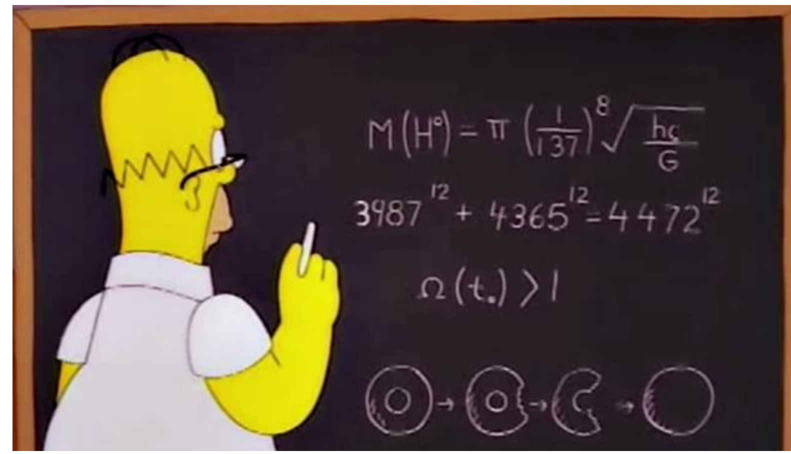
$x^2+y^2=z^2$

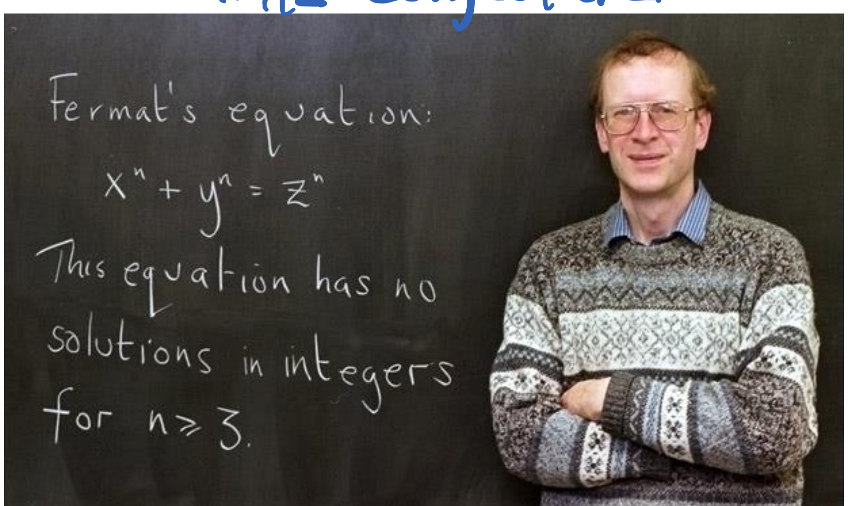
$x=3,\ y=4,\ z=5$

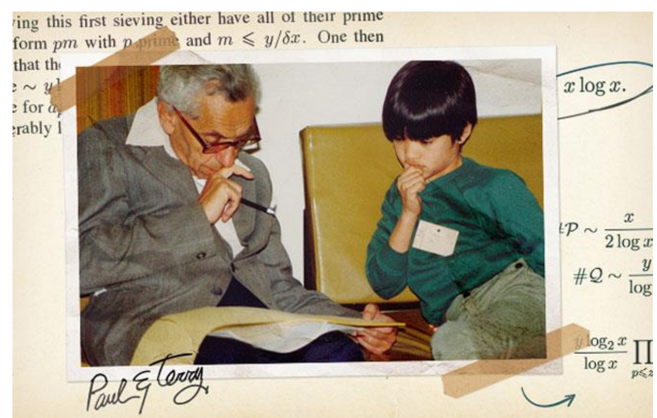
- Study of the structure in numbers.
- Long history (first area of math)
- Many Open Problems.

Twin prime conjecture

Collatz Conjecture







Basics

- Notation: $a|b$ means "a divides b" $ma=b$ for some $m \in \mathbb{Z}$

Fact: Given natural number n, natural number $d > 0$, then
$$n = qd + r \text{ such that } r \in \{0,1, \dots, d-1\}.$$

- q: quotient, r: remainder.

Simple Facts:

$ma=b$ $(km)a=kb$

- If $a|b$ then $a|\ kb$ for any integer k
- If $a|b$ and $a|c$ then $a|\ (b+c)$ and $a|\ (kb+\ell c)$ for integers k, ℓ

$ma=b$ $na=c$ $(m+n)a=b+c$

Prime numbers

Prime Numbers: p is a prime number iff

$$a \in \mathbb{N} \text{ and } a|p \quad \text{implies } a = p \;\; or \; a = 1.$$

Prime Numbers: special role in number theory.

Facts/ Theorems proved in class:

Thm 1: There are infinite prime numbers (contradiction proof)

Thm 2: Every natural number can be written as a product of primes and prime powers. (proved using Strong Induction)

GCD

Greatest Common Divisor: $gcd(12,30) = 6$

$GCD(a,b)$ = greatest $k \geq 1$ s.t. $k|a$ and $k|b$.

$12 = \underline{2} \cdot 2 \cdot \underline{3}$ $6 = 2 \cdot 3$

$30 = \underline{2} \cdot \underline{3} \cdot 5$

Least Common Multiple: $LCM(12,30) = 60$

$LCM(a,b)$ = smallest $k \geq 1$ s.t. a$|k$ and b$|k$.

$60 = 2 \cdot 2 \cdot 3 \cdot 5$

Fact: $LCM(a,b) \times GCD(a,b) = a \times b$

$12 \cdot 30 = 360 = 6 \cdot 60$

Properties of gcd(a,b)

$a, b = 2, 3$
$\gcd = 1 = 3 - 2$

$\{sa + tb \ : \ s, t$ are integers$\}$ is set of all integer combinations of a, b

Thm. $\gcd(a, b)$ is the smallest integer comb. of a, b that is positive

$a = l(\gcd(a,b))$

Proof. Let $m = sa + tb$ be the smallest integer combination

1) $\gcd(a, b) \leq m$: $m = s(l \gcd(a,b)) + t(k \gcd(a,b)) = (sl + kt) \cdot \gcd(a,b)$

also, $m > 0$

Recall $q, t \in \mathbb{Z} \Rightarrow qt \in \mathbb{Z}$

2) $m \leq \gcd(a, b)$: Will show $m |\ a$ and $m | b$. Let $a = qm + r$ with $r \in \{0,1,2 \ldots, m-1\}$. Hence $a = \underline{q(sa + tb)} + r$

$r = (1 - qs)a - qtb$

r is integer combo of a and b

So $r = 0$

So m divides both a and $b \Rightarrow m \leq \gcd(a,b)$

Properties of gcd(a,b)

- $\gcd(a, b)$ is smallest +ve integer combination of a, b (Thm)

- Every common divisor of a, b divides $\gcd(a, b)$
- $\gcd(ka, kb) = k \times \gcd(a, b)$

e.g. 4 and 15 are rel. prime

Relatively prime numbers a and b : gcd(a,b)=1. $\gcd(4, 15) = 1$

- $\gcd(a, b) = 1, \gcd(a, c) = 1 \Rightarrow \gcd(a, bc) = 1$
- $\gcd(a, b) = \gcd\big(b, remainder(a, b)\big)$

(can be proven using Thm in last slide)

Euclid's Algorithm to find $\gcd(a, b)$

- The first algorithm (300 BC)

$GCD(a, b)$

0. If a=b, then return a

1. If $a < b$, swap a, b So we have $b < a$

2. $a' \leftarrow b$

3. $b' \leftarrow remainder(a, b)$

4. Return GCD(a', b')

Small modification: returns s, t satisfying $\gcd(a, b) = sa + t\,b$

5 mod 3 = 2

Modulo Arithmetic

$(a \; mod \; n)$ means the remainder when a is divided by n.

$$a \; (mod \; n) = r \;\Leftrightarrow$$
$a = dn + r$ for some integer d

$$\begin{array}{r@{\,}r|r}
 & & 4\;2 \\ \cline{3-3}
3\;1 & & 1\;3\;3\;1 \\
 & - & 1\;2\;4 \\ \cline{3-3}
 & & 9\;1 \\
 & - & 6\;2 \\ \cline{3-3}
 & & 2\;9
\end{array}$$

Congruence modulo n:

$a \equiv b \; (mod \; n)$ iff $n \mid (a - b)$

a and b have the same remainder when divided by n

$a = dn + r \qquad b = qn + r$

$a \equiv b \; (mod \; n)$ denoted by $a \equiv_n b$

Modulo Arithmetic is an equivalence relation

- Reflexive: $a \equiv_n a$
- Symmetric: $(a \equiv_n b) \Rightarrow (b \equiv_n a)$
- Transitive: $(a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c)$

Hence it is an equivalence relation (this defines residue classes).

$$\{\ldots, \underline{-3}, \underline{-2}, \underline{-1}, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \ldots\}$$ mod 3

$C_0 = \{\ldots, -3, 0, 3, \ldots\}$

$C_1 = \{\ldots, -2, 1, 4, \ldots\}$

$C_2 = \{\ldots, -1, 2, 5, \ldots\}$

Properties of Modular Arithmetic

b mod n + d mod n

- $a \equiv b \ (mod\ n),\ c \equiv d \ (mod\ n) \ \Rightarrow \ a + c \equiv b + d \ (mod\ n)$
- $a \equiv b \ (mod\ n),\ c \equiv d \ (mod\ n) \ \Rightarrow \ ac \equiv bd \ (mod\ n)$

This lets us do algebra with equivalence classes!

E.g. ~~Ite~~ Integers mod 2   Even and odd

Even + Even = Even

Even + Odd = Odd

Odd + Odd = Even

A Sample Proof

$a \equiv b \mod n$

$\Rightarrow a = q_1 n + r$

$b = q_2 n + r$

$c \equiv d \mod n$

$\Rightarrow c = q_3 n + r'$

$d = q_4 n + r'$

So $a + c \mod n \equiv (q_1 + q_3) n + r + r' \mod n \equiv r + r' \mod n$

$b + d \mod n \equiv (q_2 + q_4) n + r + r' \mod n \equiv r + r' \mod n$

Advantages of Residue Classes

$-2 \equiv 249 \mod 251$ $\qquad$ $-2 = (-1)251 + 249$

Why do we care about these residue classes?

Because we can replace any member of a residue class with another member when doing addition or multiplication mod n and the answer will not change

$504 = 2 \cdot 251 + 2$ remainder

Calculate: Does 251 divide 249 * 504 ? What is remainder?

$$249 \cdot 504 \mod 251 \equiv (249 \mod 251)(504 \mod 251)$$
$$\equiv (-2 \mod 251)(2 \mod 251)$$
$$\equiv (-2)2 \mod 251$$
$$\equiv -4 \mod 251 \equiv 247 \mod 251$$

An example of power of modulo arithmetic

$2^5 - 1 = 31 \quad 2^5 = 31 + 1$

$2^5 \bmod 31 \equiv 1 \bmod 31$

Calculate: What is remainder when 2^{1985} is divided by 31?

$$(2^{1985}) \bmod 31 \equiv (2^{5 \times 397}) \bmod 31$$

$$\equiv (2^5)^{397} \bmod 31$$

$$\equiv (2^5 \bmod 31)^{397}$$

$$\equiv (1 \bmod 31)^{397} \equiv 1 \bmod 31$$

Then remainder is 1

Inverse Modulo Primes

Thm. For any prime p, any $k \neq 0$ s.t. p $\nmid k$ i.e. p does not divide k, there exists unique inverse called $k^{-1}(mod\ p)$ i.e., $0 < k' < p$ such that $k' \cdot k \equiv 1\ (mod\ p)$

Pf. $\gcd(k, p) = 1$, hence there exists s, t satisfying $sk + tp = 1$