Lesson 25

Prime numbers

What is $\mathbb{Q}$?

$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}$ .... represent the same rational number

Idea : introduce an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$

$(a \quad b)$ for $\frac{a}{b}$

want $(a_1 \quad b_1) \; R \; (a_2 \quad b_2)$ to mean

$$\frac{a_1}{b_1} = \frac{a_2}{b_2}$$

iff $a_1 b_2 = a_2 b_1$

Rational numbers are congruence classes

i.e $0.5 = \left[\frac{1}{2}\right]_R = \left[\frac{2}{4}\right]_R = \left[\frac{3}{6}\right]_R \ldots$

Ex: $A = \mathbb{Z} \times \mathbb{Z} - \{0\}$

$(a_1, b_1) \; R \; (a_2, b_2) \iff a_1 b_2 = a_2 b_1$

Is R an equivalence relation?

(r) $(a\ b) \; R \; (a\ b)$ since $ab = ab$

(s) Suppose $(a\ b) \; R \; (c\ d)$ then $ad = bc$

so $bc = ad$ so $(c\ d) \; R \; (a\ b)$

(t) suppose $(a\ b) \; R \; (c\ d)$ and

$(c\ d) \; R \; (e\ f)$ then

$ad = bc$ and $cf = de$

so $adcf = bcde$ so $(a\ b) \; R \; (e\ f)$

describe equivalence classes

$$\frac{a}{b} \; R \; \frac{c}{d} \iff ad = bc$$

Equivalence classes of R are $\mathbb{Q}$

Functions on equivalence classes

$$f \qquad \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$$

$$f([a]_5) = [a+1]_5$$

well defined since if $b \in [a]_5$
then $[a+1]_5 = [b+1]_5$ i.e
$a+1 \equiv_5 b+1$

$$g \qquad \mathbb{Z}_5 \longrightarrow \mathbb{Z}$$

$$g([a]_5) = a+1$$

nonsense what is $g([0]_5)$? $\begin{matrix} 0+1 \\ 5+1 \\ -5+1 \end{matrix}$?

Note: in this lesson p denotes a prime number

Th: There are infinitely many prime numbers

Proof by contradiction assume $p_1, p_2, \dots, p_n$ are the only prime numbers; $z = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ is an integer > 1 therefore it has a prime factorization so it is divisible by p_L for some L, $1 \le L \le n$. so $z = p_L k$ for some $k \in \mathbb{Z}$ and $p_L k = p_1 \cdots p_L \cdots p_n + 1$ so $p_L (k - p_1 \cdots p_{L-1} p_{L+1} \cdots p_n) = 1$ so p_L div 1 impossible.

Important questions / algorithms

1) Given $n \in \mathbb{Z}^+$ decide if n is prime. Probabilistic algorithms exists. New (2002) deterministic polynomial time test.

2) Factor n. No polynomial time algorithm is known

3) How are primes distributed?
$\pi(n)$ = number of primes $\leq n$

Th: prime number theorem

$$\lim_{n \to +\infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1$$

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

Riemann hypothesis, if true gives bound on error $|\pi(n) - \mathrm{Li}(n)|$

Prime obsession by John Derbyshire

The music of primes by Marcus du Sautoy

Note : there are no primes between
$n! + 2$ and and $n! + n$
$n! + 2$, $n! + 3$, ... , $n! + n$ are all
composite (= not prime)

Bounded gaps between primes
has to do with the question :
are there infinitely many pairs of primes
of the form p, $p + k$ for a fixed k?
If $k = 2$ we call them twin primes
5, 7 11, 13 are twin primes

Special properties of $\mathbb{Z}_p$

1) What are the invertible elements of $\mathbb{Z}_p$? All non zero elements

2) Suppose $a \cdot b = 0$ in $\mathbb{Z}_p$ and $a \neq 0$
then a is invertible and
$a^{-1}(ab) = a^{-1} \cdot 0$ so
$b = 0$

3) Cancellation law
$ab = ac \wedge a \neq 0 \Rightarrow b = c$
holds in $\mathbb{Z}_p$

Th (Fermat's Little theorem)

Suppose $(a, p) = 1$ then $a^{p-1} \equiv 1 \bmod p$

Proof Consider $f: \mathbb{Z}_p \to \mathbb{Z}_p$

$f(x) = a \cdot x$

f is a bijection. (from Lesson 23)

and $f(0) = 0$ so

$f(1) f(2) \cdots f(p-1) = 1 \cdot 2 \cdot \cdots \cdot p-1$ in $\mathbb{Z}_p$

$f(1) f(2) \cdots f(p-1) \equiv_p 1 \cdot 2 \cdots (p-1)$

$a^{p-1} \; 1 \cdot 2 \cdot \cdots (p-1) \equiv_p 1 \cdot 2 \cdot \cdots (p-1)$

Can I cancel? Yes p is prime

so $(i, p) = 1$ for $1 \le i \le p-1$

so $a^{p-1} \equiv_p 1$

Compute $2^{36} \bmod 11$

11 is a prime so $2^{10} \equiv_{11} 1$.

$2^{36} = 2^6 \cdot (2^{10})^3 \equiv_{11} 64 \cdot 1 \equiv_{11} 9$