11.7 Sum of divisor

Definition An integer $n \geq 2$ is a perfect number if n is the sum of its proper factors, i.e., factors strictly smaller than n.

Examples $6, 28, 496$. → $1+2+3=6$ → $1+2+4+7+14=28$

Questions Is there an odd perfect numbers?

Are there infinitely many even perfect numbers?

Definition A pair of integers $n, n+1$ are Ruth-Aaron pair if the sums of their prime divisors are equal.

Theorem (Erdös) There are infinitely many pairs of Ruth-Aaron pairs.

Crytology
RSA system
depends on number theory
$n = p \cdot q$ p, q prime

Math 214

Quiz on Thursday will cover material up to Homework 6.

Theorem Every integer $n \geq 2$ has a prime factor. If n is not a prime, then there is a prime factor of size not larger than $\sqrt{n}$.

Theorem If $n \in \mathbf{N}$ such that $n \neq k^2$ for some $k \in \mathbf{N}$, then $\sqrt{n}$ is irrational.

Theorem There are infinitely many prime numbers. ✓

Question There are infinitely pair of twin primes, i.e., $(p, p+2)$ pairs such that both p and $p+2$ are primes.

Example $(3,5), (5,7), (11,13)$.

~~1 2 3 4 ... 10~~
11 12 13 ... 20
⋮ ⋮ ⋮
91 ⋮ ~~100~~

→ Proof : If n is not a prime, then

$n = ab$ with $1 < a, b < n$.

So a or b is less than or equal to $\sqrt{n}$

∴ a or b has a prime factor of size less than or equal to $\sqrt{n}$. ☒

Math 214 Foundations of Higher Mathematics C.K. Li $[k]_n = \{nx+k : x \in \mathbb{Z}\}$

§8.5/8.6 Congruence Modulo n

We study properties of the partition $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ of the set Z.

Congruence Modulo n

Recall that for $n \in \mathbf{N}$ with $n > 1$, we have $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ with

$$[k] = \{nx + k : x \in \mathbf{Z}\}.$$

Two integers x, y lies in the same class if $x - y$ is divisible by n, and we write $x \equiv y \pmod{n}$.

Theorem Define a relation R on integers by xRy if $x \equiv y \pmod{n}$. Then

(a) For any $x \in \mathbf{Z}$, xRx. (Reflexive)

(b) For any $x, y \in \mathbf{Z}$, if xRy then yRx. (Symmetric)

(c) For any $x, y, z \in \mathbf{Z}$, if xRy, yRz, then xRz. (Transitive).

We say that R is an equivalence relation on Z. Note that $[x_1] = [x_2]$ if $x_1 R x_2$.

(a) Proof For any $x \in \mathbb{Z}$, xRx because ~~$x \equiv y$ for~~ $x \equiv x \pmod{n}$.

i.e., $x - x = n \cdot q$.

Which is true because

$x - x = 0 = n \cdot 0$

(b) If xRy in $\mathbb{Z}$, i.e., $x - y = nq$.

then $y - x = -nq = n(-q)$; $y \equiv x \pmod{n}$

then yRx.

(c) If xRy, yRz in $\mathbb{Z}$., i.e., $x - y = nq_1$
$y - z = nq_2$ $q_1, q_2 \in \mathbb{Z}$

Then $x - z = x - y + y - z = nq_1 + nq_2$.

~~xRz~~.

$\therefore x - z = n(q_1 + q_2)$

$\therefore x \equiv z \pmod{n}$

S a relation R on S.

R is symmetric iff:

$$(\forall x, y \in S)(xRy) \Rightarrow (yRx)$$

R is not symmetric iff:

$$(\exists\ x, y \in S) \sim (\text{If } xRy \text{ then } yRx)$$

i.e., $$(\exists\ x, y \in S)(xRy) \sim (yRx).$$

R is transitive:

$$(\forall\ x, y, z \in S \text{ such that } xRy, yRz)(xRz)$$

R is not transitive:

$$(\exists\ x, y, z \in S \text{ such that } (xRy), (yRz)) \sim (xRz)$$

(3) Consider xRy if $x > y$ on $\mathbb{Z}$.

Reflexive: Let $x = 1$, Then $x \not> x$.

$\therefore$ R is not reflexive.

Symmetric: Let $(x, y) = (2, 1)$.

Then $2 > 1$ i.e., xRy.

But $1 \not> 2$ i.e., it is not true that yRx

$\therefore$ R is not symmetric

Transitive: If xRy, yRz in $\mathbb{Z}$ i.e.,

$x > y$, $y > z$.

$\therefore$ $x > z$ So R is transitive

$\therefore$ xRz.

---

(1) Relations on $S = \{dog\}$

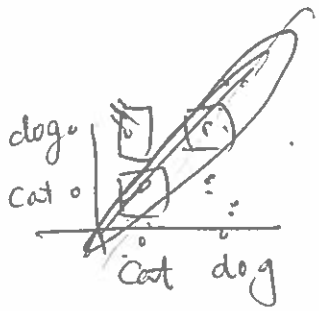
R_1. dog dog is not related

NOT reflexive no
Symmetric yes
Transitive yes

R_2 $dog R_2 dog$

reflexive yes
Symmetric yes
Transitive yes

~~Relations~~ Relations on $S = \{dog, cat\}$ ... R_{16}



	R_1	R_2	R_3
(cat, cat)	No	Yes	Yes
(cat, dog)	No	Yes	No
(dog, cat)	No	Yes	No
(dog, dog)	No	Yes	Yes

R	No	Yes	Yes
S	Yes	Yes	Yes
I	Yes	Yes	Yes

xRy means

$x=y=cat \rightarrow yRx$

$x=y=dog \rightarrow yRx$

If $|S| = n$ then there are $|S \times S| = n^2$ pairs.

& $\therefore$ 2^{n^2} relations

Every relation R on S corresponds to a subset of $S \times S$.

xRy, yRz

(1) $x = cat, y = cat, z = cat$

xRz ✓

(2) $x = dog, y = dog, z = dog$

xRz ✓