Quiz:

(1) Express $\sigma_4(27)$ as $\frac{3^a - 1}{3^b - 1}$ for some integers a & b.

$$\sigma_4(27) = \sum_{d \mid 27} d^4 \qquad 27 = 3^3$$

(2) Suppose f is a multiplicative function and we are told:

$$f(2) = 4, \quad f(3) = 11, \quad f(4) = 3, \text{ and } \quad f(8) = 5.$$

Do we have enough information to compute $f(24)$?

- If so, compute it with a justification
- If not, explain why not.

$$\mathcal{D}(n) := \{ d \text{ is an positive integer} \mid d \text{ is a divisor of } n \}$$

$$\sigma_0(n) := \#\mathcal{D}(n) \qquad \sigma_k(n) := \sum_{d \in \mathcal{D}(n)} d^k$$

Prop. If $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\sigma_0(n) = (e_1 + 1) \cdots (e_r + 1)$$

$$\sigma_{\substack{k \\ (k \neq 0}}(n) = \frac{(p_1^{e_1+1})^k - 1}{p_1^k - 1} \cdot \cdots \cdot \frac{(p_r^{e_r+1})^k - 1}{p_r^k - 1}$$

Def. multiplicative means

$$f(mn) = f(m) \cdot f(n),$$

for any coprime positive integers m, n.

ANS:

(1) We have

$$\sigma_k(p^e) = \frac{p^{k(e+1)} - 1}{p^k - 1}$$

$27 = 3^3$

$k = 4 \quad p = 3 \quad e = 3$

$$= \frac{3^{4\cdot 4} - 1}{3^4 - 1} = \frac{3^{16} - 1}{3^4 - 1}$$

(a, b, c)

(2) Yes. Since $24 = 3 \cdot 8$ and $GCD(3, 8) = 1$

Multiplicativity of f implies

$$f(24) = f(3) \cdot f(8) = 11 \cdot 5 = 55.$$

Def. Let n be a positive integer.

- Say n is **perfect** if the sum of proper divisor of n equals n. Equivalently, $\sigma_1(n) = 2n$.

e.g. $6, 28, 496, 8128, 33\,550\,336, \cdots\cdots$

$= 1+2+3$ $= 1+2+4+7+14$

- Say n is **deficient** if $\sigma_1(n) < 2n$.

e.g. all primes are deficient $\sigma_1(p) = 1+p < 2p$

- Say n is **abundant** if $\sigma_1(n) > 2n$.

e.g. $12, 18, 20, 24, 30, 36, \cdots, 945, \cdots$

$\sigma_1(12) = 1+2+3+4+6+12$

Defn. A *Mersenne prime* is a prime number of the form

$$M_p = 2^p - 1 \qquad M_4 = 2^4 - 1 = 15 = 3 \cdot 5$$

e.g.: $M_2 = 2^2 - 1 = 3$ $M_3 = 2^3 - 1 = 7$ $M_5 = 2^5 - 1 = 31$ $M_7 = 2^7 - 1 = 127$

Prop.: If M_p is a prime number, then so is p.

proof: Toward a contradiction, suppose $p = ab$ $(1 < a, b < p)$.

Then $M_p = 2^{ab} - 1 = (2^a)^b - 1$ $\quad x = 2^a$

$$= (2^a - 1)\left((2^a)^{b-1} + \cdots + 2^a + 1\right)$$

$2^a - 1 > 1$

$(2^a)^{b-1} + \cdots + 2^a + 1 > 1$ since more than one term

$\sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}$

Contradict to M_p is prime ! (3)

The converse is false: $M_{11} = 2047 = 23 \cdot 89$ ~~prime~~

Thm (Euclid) If $M_p = 2^p - 1$ is a prime, then

$$N_p := 2^{p-1} M_p$$

is a perfect number.

proof.

$$\sigma_1(N_p) = \sigma_1(2^{p-1}) \cdot \sigma_1(M_p)$$

$$= \frac{2^p - 1}{2 - 1} \cdot (1 + M_p)$$

$$= \underbrace{(2^p - 1)}_{= M_p} \cdot 2^p$$

$$= 2 N_p$$

Open Questions:

- Are there infinitely many perfect numbers ?
- Are there infinitely many Mersenne primes ?

As of now (2022), only 51 Mersenne primes are found, the largest one of them is

$$M_{82\,589\,933} = 2^{82\,589\,933} - 1 \text{ (GIMPS 2018)}$$

www.mersenne.org.

Thm (Euler 1849)

ALL even perfect numbers arise from Mersene primes

If N is an even perfect number, then there is a prime p s.t

$$N = 2^{p-1}(2^p - 1)$$

Proof: Suppose N is an even perfect number.

Let $p := v_2(N) + 1$ & $q := \frac{N}{2^{p-1}}$ = product of odd prime powers in N

$\gcd(2^{p-1}, q) = 1$ by prime factorization of N.

By perfectness,

$$2^p \cdot q = 2N = \sigma_1(N)$$

$$= \sigma_1(2^{p-1} \cdot q)$$

$$= \sigma_1(2^{p-1})\,\sigma_1(q)$$

$$= \frac{2^p - 1}{2-1}\,\sigma_1(q) = (2^p - 1)\,\sigma_1(q)$$

$$\sigma_1(q) = \frac{2^p \cdot q}{2^p - 1} \quad \text{is an integer.}$$

$$= q + \frac{q}{2^p - 1}$$

Hence $\frac{q}{2^p - 1}$ is an integer d and moreover a divisor of q.

On the other hand:

$\sigma_1(q)$ = sum of divisors of q

$= q + d +$ other divisors

has to be zero

Namely, there are only two divisors of q.

So q is a prime number!

And we have $d=1$.

Hence $q = 2^p - 1$ a Mersenn prime! and $n = 2^{p-1}(2^p - 1)$.

Even perfect numbers $\leftrightsquigarrow$ Mersenne primes

Open Questions:

- Is there any odd perfect numbers?

Ch.3 Rational Numbers

Defn: A **rational number** is a number, which equals $\frac{a}{b}$ for some integers a, b and $b \neq 0$. "ratio"

(v.s. A **fraction** is an expression $\frac{a}{b}$, where a, b are integers. When $b=0$, this fraction represents No numbers)

E.g. $\frac{5}{3}$ & $\frac{15}{9}$ are different fractions, but they give the same number.

Notation: $\mathbb{Q}$ set of rational numbers. $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$ whenever $c \in \mathbb{Z} \setminus \{0\}$

Defn. Say a fraction $\frac{a}{b}$ is **reduced** if $GCD(a,b)=1$ & $b>0$.

E.g. $\frac{-2}{3}$ ✓ $\frac{2}{-3}$ ✗ $\frac{2}{4}$ ✗

Thm. Any rational number has a unique reduced fraction representation.

Pf: Suppose the rational number is represented by the fraction $\frac{a}{b}$.

We may assume $b>0$, since $\frac{a}{b}=\frac{-a}{-b}$.

If a,b coprime, ✓ If not, let $a = c\cdot GCD(a,b)$, $b = d\cdot GCD(a,b)$

Then $\frac{a}{b}=\frac{c}{d}$ & $GCD(c,d)=1$.

Suppose $\frac{c'}{d'}$ is another reduced fraction representing the rational number.

Then $\frac{c}{d} = \frac{c'}{d'}$ $(\Rightarrow cd' = c'd)$ and $d, d' > 0$.

$d \mid c'd = cd'$ + $GCD(c, d) = 1 \Rightarrow d \mid d'$

Similarly, $d \mid d'$. But both d & d' are positive integers.

By antisymetric property of $\cdot|$, $d = d'$. Then $c = c'$. ∎

Prop. Any nonzero rational number α has a unique prime factorization:

$$\alpha = \pm 2^{e_2} \cdot 3^{e_3} \cdot \dots \cdot p^{e_p} \cdot \dots$$

$\pm$ + or −, a sign.

$e_p \in \mathbb{Z}$ and Only finitely many e_p are non-zero.

Pf: (Existence)

Let $\frac{a}{b}$ be the reduced fraction representing α.

Then $$\alpha = \frac{a}{b} = (\text{sign of } a) \cdot \frac{|a|}{b}$$

$$= (\text{sign of } a) \cdot \frac{\text{product of } p^{v_p(|a|)}}{\text{product of } p^{v_p(b)}}$$

($v_p(|a|)$: exponent of p in the prime factorization of $|a|$)

$$= (\text{sign of } a) \cdot \text{product of } p^{e_p},$$

where $e_p = v_p(|a|) - v_p(b)$.

(Uniqueness:)

Suppose $\alpha = \pm 2^{f_2} \cdot 3^{f_3} \cdot \dots \cdot p^{f_p} \cdot \dots$ is another prime factorization.

($\pm$: a sign.)

let $P_+ = \{ p \text{ is prime} \mid f_p > 0 \}$

$P_- = \{ p \text{ is prime} \mid f_p < 0 \}$

"$\prod$" read as "the product of"

define $c = \pm \cdot \prod_{p \in P_+} p^{f_p}$ and $d = \prod_{p \in P_-} p^{-f_p} > 0$

$\mathrm{GCD}(c, d) = 1$

Then $\frac{c}{d}$ is a reduced fraction and $\alpha = \frac{c}{d}$. $\left(\alpha = \frac{a}{b}\right)$

Then $\pm$ = sign of a, $|c| = |a|$, and $d = b$.

(by the theorem/uniqueness of reduced fraction representation) $a = c$, $b = d$

Then the uniqueness of prime factorization for positive integers shows

$p \in P_+ \Rightarrow f_p = v_p(|a|) = e_p$

$p \in P_- \Rightarrow f_p = v_p(b) = e_p$

$p \notin P_+ \cup P_- \Rightarrow f_p = 0 = e_p$

Next Quiz :

Find the reduced fraction representation of the following rational number and give its prime factorization.

$$-1.56$$

- For *Mersenne primes*, see https://primes.utm.edu/mersenne/ and https://www.mersenne.org/.
- Please prepare the above quiz for next meeting.
- Please read pp. 75–85 of the textbook for next lecture.