Thursday, November 7

Some miscellany involving the sum-of-divisors function $\sigma(n) = \sum_{d \mid n} d = id * 1$.

The ancient Greeks classified numbers n as abundant, perfect, or deficient depending on whether the sum of the proper divisors of n was greater than, equal to, or less than n. In particular n is perfect when

$$n = \sum_{\substack{d \mid n \\ d < n}} d = \sigma(n) - n \Leftrightarrow \sigma(n) = 2n.$$

For example, $6 = 1+2+3$ and $28 = 1+2+4+7+14$ are perfect; the next two perfect numbers are 496 and 8,128.

Note that σ is multiplicative and that

$$\sigma(p^r) = p^r + p^{r-1} + \cdots + p^2 + p + 1 = \frac{p^{r+1}-1}{p-1}.$$

Therefore n is perfect if and only if

$$2 = \frac{\sigma(n)}{n} = \prod_{p^r \| n} \frac{p^{r+1}-1}{p^r(p-1)}.$$

Let's factor the first four perfect numbers:

$6 = 2 \cdot 3 = 2^1(2^2-1)$

$28 = 4 \cdot 7 = 2^2(2^3-1)$

$496 = 16 \cdot 31 = 2^4(2^5-1)$

$8{,}128 = 64 \cdot 127 = 2^6(2^7-1)$.

Theorem: If $q = 2^p - 1$ is prime, then $n = 2^{p-1} q = 2^{p-1}(2^p-1)$ is perfect.

Remarks: If $2^k - 1$ is prime, then k has to be prime, since if $k = cd$ then

$$2^{cd} - 1 = (2^d - 1)(2^{(c-1)d} + 2^{(c-2)d} + \cdots + 2^{2d} + 2^d + 1).$$

But k prime is not sufficient: $2^{11} - 1 = 23 \cdot 89$.

Primes of the form $2^p - 1$ are called

Mersenne primes. $[q = 2^p - 1]$

Proof 1: The divisors of $n = 2^{p-1}q$ are

$1, 2, 2^2, \ldots, 2^{p-1}$; $q, 2q, 2^2q, \ldots, 2^{p-1}q$;

and these add to $2^p \cdot q = 2n$.

(complete list since q is prime)

Proof 2: $\sigma(n) = \sigma(2^{p-1}q) = \sigma(2^{p-1})\sigma(q)$

$$= \frac{2^p - 1}{2-1}(q+1) = (2^p - 1)2^p = 2n. \quad //$$

Converse is almost true:

Theorem: If n is an even perfect number, then there exists a prime p with $q = 2^p - 1$ also prime such that $n = 2^{p-1}q$.

Proof: Write $n = 2^{k-1}m$ where $k \geq 2$ and m is odd. Since n is perfect,

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1}m)$$
$$= \sigma(2^{k-1})\sigma(m)$$
$$= (2^k - 1)\sigma(m).$$

Then $(2^k - 1) \mid 2^k m$; since $(2^k - 1, 2^k) = 1$, we deduce that $(2^k - 1) \mid m$. Write $m = (2^k - 1)\ell$, so that

$$2^k(\cancel{(2^k-1)}\ell) = \cancel{(2^k-1)}\sigma(m)$$

$$2^k \ell = \sigma(m).$$

Note that m and ℓ are distinct divisors of m (since $k \geq 2$?); thus

$$2^k \ell = \sigma(m) \geq m + \ell = (2^k - 1)\ell + \ell = 2^k \ell.$$

We conclude that $\sigma(m) = m + \ell$; in particular, m has only two divisors (m and ℓ), so m is prime. Since $m = (2^k - 1)\ell$, we conclude that $\ell = 1$; and $2^k - 1$ is prime $\Rightarrow k$ is prime. //

We've just proved a 1-to-1 correspondence between Mersenne primes $2^p - 1$ and even perfect numbers $2^{p-1}(2^p - 1)$.

- We know 52 Mersenne primes: $p = 2, 3, 5, 7, 13, \ldots, 136{,}279{,}841$.
- There's a specific primality test for numbers of the form $2^p - 1$. — much faster (hence can find larger primes).
- Conjecture: There are infinitely many Mersenne primes / even perfect numbers.
- Conjecture: There are no odd perfect numbers.

Diophantine approximation: the topic of finding rational numbers a/b near given real numbers x ("near" in terms of the denominator b).

Example: Let's prove that $e = \sum_{n=0}^{\infty} \frac{1}{n!} \approx 2.71828$ is irrational.

Proof by contradiction: Assume $e = \frac{a}{b}$ with $b \geq 2$, $a \in \mathbb{N}$. Then $be \in \mathbb{N}$, and certainly $b!\,e \in \mathbb{N}$. Define

$$m = b!\,e - \sum_{n=0}^{b} \frac{b!}{n!} \in \mathbb{N},$$

and write

$$m = \sum_{n=b+1}^{\infty} \frac{b!}{n!} = \frac{1}{b+1} \sum_{n=b+1}^{\infty} \frac{(b+1)!}{n!}.$$

Note each summand is at most $\frac{1}{2}$ the previous summand; by induction,

$$\frac{(b+1)!}{(b+1+k)!} \leq \left(\frac{1}{2}\right)^k \frac{(b+1)!}{(b+1)!} = \left(\frac{1}{2}\right)^k.$$

So

$$m = \frac{1}{b+1} \sum_{k=0}^{\infty} \frac{(b+1)!}{(b+1+k)!} \leq \frac{1}{b+1} \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k = \frac{2}{b+1} < 1.$$

Thus $0 < m < 1 \Rightarrow$ contradiction. //

Template for proving a number x is irrational:

- By contradiction, suppose $x = \frac{a}{b}$;
- Do something clever to construct (from x, a, b) some integer m that's between 0 and 1.

Lemma: If $\frac{a}{b}, \frac{c}{d}$ are distinct rational numbers, then $\left|\frac{a}{b} - \frac{c}{d}\right| \geq \frac{1}{|bd|}$.

- Convention: we'll always write rational numbers with positive denominators (but not necessarily in lowest terms).

Proof: $\frac{a}{b} \neq \frac{c}{d} \Leftrightarrow ad - bc \neq 0$; hence

$$\left|\frac{a}{b} - \frac{c}{d}\right| = \left|\frac{ad-bc}{bd}\right| \geq \frac{1}{bd}. \quad //$$

Theorem (Dirichlet) Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. There exists $\frac{a}{b} \in \mathbb{Q}$ with $1 \leq b \leq n$ such that

$$\left|x - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}.$$

Remarks:

- Easier to prove $< \frac{1}{bn}$; but
- Best possible (take $x = \frac{1}{n+1}$).

Proof: Define the fractional part function $\{y\} = y - \lfloor y \rfloor$. Strategy: if $\{bx\}$ is close to 0 or 1, then x is close to $\frac{\text{some integer}}{b}$.

Consider the n numbers $\{x\}, \{2x\}, \ldots, \{nx\}$ and the $n+1$ intervals

$$\left[0, \tfrac{1}{n+1}\right), \left[\tfrac{1}{n+1}, \tfrac{2}{n+1}\right), \ldots, \left[\tfrac{n}{n+1}, 1\right).$$

Main argument: suppose 1 of these intervals contains two of these $\{jx\}, \{kx\}$ $(j \neq k)$. (WLOG, $1 \leq j < k \leq n$.) Then

$|\{kx\} - \{jx\}| < \frac{1}{n+1}$. Take $a = \lfloor kx \rfloor - \lfloor jx \rfloor$ and $b = k - j$; then $1 \leq b < n$ and

$$\left|x-\frac{a}{b}\right| = \left|\frac{(k-j)x}{k-j} - \frac{\lfloor kx\rfloor - \lfloor jx\rfloor}{k-j}\right|$$

$$= \left|\frac{\{kx\}-\{jx\}}{k-j}\right| < \frac{1}{n+1}\,\frac{1}{k-j}. \checkmark$$

We're done unless no interval contains 2 $\{kx\}$. In this case, either $\left[0, \frac{1}{n+1}\right)$ or $\left[\frac{n}{n+1}, 1\right)$ contains some $\{kx\}$.

- If $\{kx\} \in \left[0, \frac{1}{n+1}\right)$, choose $a = \lfloor kx\rfloor$ and $b = k$; then

$$\left|x-\frac{a}{b}\right| = \left|\frac{kx}{k} - \frac{\lfloor kx\rfloor}{k}\right| = \left|\frac{\{kx\}}{k}\right| < \frac{1}{n+1}\cdot\frac{1}{k}.$$

- If $\{kx\} \in \left[\frac{n}{n+1}, 1\right)$, choose $a = \lfloor kx\rfloor + 1$ and $b = k$:

$$\left|x-\frac{a}{b}\right| = \left|\frac{kx}{k} - \frac{\lfloor kx\rfloor+1}{k}\right| = \left|\frac{1-\{kx\}}{k}\right| < \frac{1}{n+1}\,\frac{1}{k}.$$

//