Number Theory Section Summary: 10.1-2
Mersenne and Perfect Numbers

1. Summary

Father Marin Mersenne (1588-1648) helped drive the scientists of his day to share their results, and pass around the scientific knowledge available at that time. Yet the French priest had interests of his own, including number theory. Some of the most famous primes are graced with his name.

2. Definitions

perfect number: a positive integer n equal to the sum of all positive divisors, excluding n itself. [Name bestowed by the Pythagoreans.]

e.g.

- $P_1 = 6 = 2^1(2^2 - 1)$,
- $P_2 = 28 = 2^2(2^3 - 1)$,
- $P_3 = 496 = 2^4(2^5 - 1)$,
- $P_4 = 8128 = 2^6(2^7 - 1)$, and
- $P_5 = 33550336 = 2^{12}(2^{13} - 1)$ (!)

Something funky happens!

Mersenne number: $M_n = 2^n - 1$, with $n \geq 1$. If M_n is prime, then it's called a **Mersenne prime**

The latest prime (as of today, a Mersenne prime) was found December 15, 2005. The 43rd Mersenne Prime, it is

$$2^{30,402,457} - 1$$

and has nearly 10 million digits. There's a prize of $100,000 for the first 10 million digit prime!

Last time I taught this course (one year ago), they'd just found the 42nd, as described in Science News: "On Feb. 18 [2005], the computer-based Great Internet Mersenne Prime Search (GIMPS) turned up the largest known prime number, whose formula is 2 to the 25,964,951st power minus 1. The new prime is a whopping 7,816,230 digits long, making it more than half-a-million digits longer than the previous record-holder. The number would completely fill 58 issues of Science News."). I like that analogy!

Mersenne had conjectured that M_p is prime for 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257, and composite for all other prime powers $<$ 257. Mersenne was wrong (five in the list are not prime, and he missed three others), as was dramatically demonstrated in 1903 by Frank Nelson Cole for the case of 67 (See story, p. 216).

3. Theorems

The test of a perfect number is if

$$\sigma(n) = 2n$$

Theorem 10.1: If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect, and every even perfect number is of this form.

Proof: $\Rightarrow$ Assume 2^k-1 prime, $k>1$, & consider $n = 2^{k-1}(2^k-1)$. Let's use our tester σ:

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

& since $\gcd(2^{k-1}, 2^k-1) = 1$,

$$\sigma(n) = \sigma(2^{k-1})\,\sigma(2^k-1)$$
$$= \left(\frac{2^{k-1+1}-1}{2-1}\right)(2^k-1+1)$$
$$= (2^k-1)\,2^k = 2\cdot 2^{k-1}(2^k-1)$$
$$= 2n \quad \checkmark$$

$\Leftarrow$ Assume n is an even perfect number. Then we can write

$$n = 2^{k-1} m, \quad \text{where } m \text{ is odd.}$$

& we know that

$$\sigma(n) = 2n. \qquad k \geq 2.$$

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

$$= \left(\frac{2^{k-1+1} - 1}{2-1} \right) \sigma(m)$$

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

$$= 2^k m$$

So $(2^k - 1)$ divides $2^k m$, but $\gcd(2^k-1, 2^k) = 1$,

so $$2^k - 1 \mid m.$$

$$\therefore \quad m = (2^k - 1) X$$

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

$$\therefore \quad \sigma(m) = 2^k X$$

$$\geq m + X = (2^k - 1) X + X$$

$$= 2^k X$$

So in fact $\sigma(m) = m + X$

$\therefore X = 1$, & m is prime : $\sigma(m) = m + 1$

$\therefore \quad m = 2^k - 1$, & $n = 2^{k-1}(2^k - 1)$

4. Properties/Tricks/Hints/Etc.

Theorem 10.2: An even perfect number n ends in the digit 6 or 8; equivalently, either $n = 6 (\text{mod } 10)$ or $n = 8 (\text{mod } 10)$.

The proof of this result relies on a lemma, which is interesting:

Lemma: If $a^k - 1$ is prime ($a > 0$, $k \geq 2$) then $a = 2$ and k is also prime.

[As our author notes, ancients believe that $2^k - 1$ was always prime for k prime, but this is not the case: $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime (1536).]

Proof: (of lemma): Assume a^k-1 is prime.

$$a^k - 1 = (a-1)(\underbrace{a^{k-1} + \dots + a + 1}_{\text{geometric series}})$$

$$\left(a^{k-1} + \dots + a + 1 = \frac{a^k-1}{a-1} \right)$$

$\therefore$ because a^k-1 is prime, one of the factors is 1.

$$a - 1 = 1 \quad \text{or} \quad \underbrace{a^{k-1} + \dots + a + 1}_{>1} = 1$$

$$\therefore \quad a - 1 = 1 \Rightarrow \boxed{a = 2}$$

Now suppose that $k = r \cdot s$, $r, s > 1$: then

$$2^k - 1 = 2^{r \cdot s} - 1 = (2^r)^s - 1$$
$$= \underbrace{[2^r - 1]}_{>1} \underbrace{[(2^r)^{s-1} + \dots + 2^r + 1]}_{>1}$$

contradiction: one of the factors has to be 1.

$\therefore$ k is prime.

Proof of the Theorem: by cases

Let n be an even perfect number:

$$n = 2^{k-1}\underbrace{(2^k-1)}$$

prime, & k is prime
(by the lemma).

So k has one of the forms $2, 4j+1, 4j+3$.

By cases:

Let $k=2$

$$n = 2^{2-1}(2^2-1) = 6 \quad \checkmark \qquad (\equiv 6 \pmod{10})$$

Let $k = 4j+1$

$$\begin{aligned} n &= 2^{(4j+1)-1}\left(2^{4j+1}-1\right) \\ &= 2^{4j}\left(2\cdot 2^{4j}-1\right) \\ &= (16)^j\left(2\cdot(16)^j-1\right) \\ &= 2\cdot(16)^{2j} - (16)^j \equiv 2\cdot 6 - 6 \equiv 6 \pmod{10} \end{aligned}$$

What is $16^\ell \pmod{10}$? $\underline{\underline{6}}$ $\quad \ell \geq 1$

Proof by induction:

Base: $16 \equiv 6 \pmod{10}$ $\checkmark$

$\Rightarrow$: Assume $16^\ell \equiv 6 \pmod{10}$;

Then

$$\begin{aligned} 16^{\ell+1} &\equiv 16^\ell \cdot 16 \equiv 6\cdot 16 \\ &\equiv 96 \equiv 6 \pmod{10} \quad \checkmark \end{aligned}$$

QED

Let $k = 4j+3$:

$$n = 2^{(4i+3)-1}\left(2^{(4i+3)} - 1\right)$$

$$= 2^2\, 16^i\left(8 \cdot 16^i - 1\right)$$

$$= 32(16^i) - 4\, 16^i$$

$$\equiv 32 \cdot 6 - 4 \cdot 6$$

$$\equiv 12 \cdot 4 - 4 \cdot 4$$

$$\equiv 48$$

$$\equiv 8 \pmod{10}$$

#2a, p 214

No power of a prime can be a perfect number.

By contradiction, assume $n = p^k$ is perfect, so $\sigma(n) = \sigma(p^k) = 2n$

$$= 2p^k$$

$$\sigma(p^k) = \boxed{\frac{p^{k+1} - 1}{p-1} = 2p^k}$$

$$p^{k+1} - 1 = 2p^k(p-1)$$

$$0 = p^{k+1} - 2p^k + 1$$

$$0 = \underbrace{p^k \underbrace{(p-2)}_{\geq 0} + 1}_{> 0}$$

$p \geq 2$

contradiction

Hence no perfect # can be a power of a prime.

#3 If n is a perfect #, prove that

$$\sum_{d|n} \frac{1}{d} = 2$$

If d is a divisor of n, then $\exists\, d'$ /

$$d \cdot d' = n \quad ; \qquad \frac{1}{d} = \frac{d'}{n}$$

Hence

$$\sum_{d|n} \frac{1}{d} = \sum_{d'|n} \frac{d'}{n} = \frac{1}{n} \boxed{\sum_{d'|n} d'} = \frac{1}{n} \sigma(n)$$

$$= \frac{1}{n} \cdot 2n = \underline{\underline{2}}$$

#7. No proper divisor of perfect n can be perfect [Hint: Use #3!]

know:

$$\sum_{d|n} \frac{1}{d} = 2$$

Let δ be a perfect proper divisor of n, $\delta < n$. & $\delta | n$

$$\sum_{d|\delta} \frac{1}{d} = 2 \qquad (\text{by } \#3)$$

$$\text{But } 2 = \underbrace{\sum_{d|\delta} \frac{1}{d} < \sum_{d|n} \frac{1}{d}}_{\text{(since every term in the first sum is in the second, but the 2nd has more)}} = 2 \qquad \text{Contradiction.}$$