Lecture 11
Jan. 28th, 2015

four digits of 2^{1000}
2^{1000} mod $10000 = 10^4 = 2^4 \times 5^4$
$2^{1000} \equiv 0 \bmod 2^4$
$2^{1000} \equiv 1 \bmod 5^4$

Mersenne Prime: prime of form 2^P-1, p prime.
As of 2013, biggest Mersernne Prime is $2^{57885161}-1$

Fermat prime: prime of the form $F_n = 2^{2^n}+1$

$$F_1 = 2^{2^1}+1 = 5,\ F_2 = 2^{2^2}+1 = 17,\ F_3 = 65537,\ F_4 = 641 \times 6700417$$

· Given height, the number of possible binary trees is a Fermat prime.
F_n-gon can be constructed only by ruler & compasses.

Chapter 15 Perfect Numbers

$6 = 1+2+3 \Rightarrow$ sum of divisors of 6 other than 6 itself.
$10 > 1+2+5 = 8$
$28 = 1+2+4+7+14$

A perfect number is a number that is equal to the sum of proper divisors.

Euclid's Perfect number formula:
If 2^P-1 is a prime (Mersenne Prime), then $2^{P-1}(2^P-1)$ is a perfect number.

Check: $3 = 2^2-1$, $2 \times 3 = 6$
$7 = 2^3-1$, $2^2 \times 7 = 28$
$31 = 2^5-1$, $2^4 \times 31 = 496$

Proof: Let $q = 2^P-1$ prime
Check $2^{P-1}q$ is a perfect number
proper divisors of $2^{P-1}q$: $1, 2, 2^2, \dots, 2^{P-1}, q, 2q, 2^2q, \dots, 2^{P-2}q$

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

$$1+2q+\dots+2^{P-2}q = q(1+2+\dots+2^{P-2}) = q\frac{2^{P-1}}{2-1} = (2^{P-1}-1)q$$

So the sum of proper numbers $= 2^{P-1}q$

Using a big Mersenne Prime, we can generate a big perfect number
$2^{57885161}(2^{57885161}-1)$ is a perfect number.

Question: Does Euclid's perfect number formula describe all perfect number?

Euler's perfect number theorem:
If n is an even perfect number, then $n = 2^{P-1}(2^{P-1}-1)$ with 2^P-1

Odd perfect number? Are there any odd perfect number? Don't know, checked up to 10^{300}

$\sigma(n)$ = sum of all divisors of n (including 1 & n)
sigma

$\sigma(6)=1+2+3+6=12$
$\sigma(8)=1+2+4+8=15$

p prime
$\sigma(p)=1+p$
$\sigma(p^k)=1+p+\cdots+p^k=\frac{p^{k+1}-1}{p-1}$

For $\sigma(n)$ if n is a perfect number $\Leftrightarrow$ $\sigma(n)=2n$
$\sigma(n)$ is multiplicative, like $\phi(mn)=\phi(m)\phi(n)$, if $\gcd(m,n)=1$

Similarly, $\sigma(mn)=\sigma(m)\sigma(n)$ if $\gcd(m,n)=1$
$\sigma(15)=\sigma(3\times5)=1+3+5+15=24=\sigma(3)\sigma(5)=(3+1)(5+1)$
divisors of $15=3\times5$: $1,3,5,15$

Partial Proof:
p,q prime and $p\neq q$
$\sigma(pq)=1+p+q+pq=(1+p)(1+q)=\sigma(p)\sigma(q)$
$\gcd(m,n)=1$
mn
Divisor of m: $a_1,a_2,\cdots,a_k$
Divisor of n: $b_1,b_2,\cdots,b_l$
Claim: Divisor of mn are a_ib_j, $i=1,\cdots,k$, $j=1,\cdots,l$
Proof: Since n is even, write $n=2^k m$, m odd, $k\geq1$
$\sigma(n)=\sigma(2^k)\sigma(m)=\frac{2^{k+1}-1}{2-1}\sigma(m)=2^{k+1}\sigma(m)$?
$2^{k+1}\mid\sigma(m)$

$\sigma(m)=2^{k+1}c$
$(2^{k+1}-1)2^{k+1}c=2^{k+1}m$
$m=(2^{k+1}-1)c$

Claim: $c=1$
Suppose $c>1$, then m is divided by $1,c,m$
$\sigma(m)\geq1+c+m=1+c+(2^{k+1}-1)c=1+2^{k+1}c=1+\sigma(m)$ contradiction

So $m=2^{k+1}-1$
$\sigma(m)=2^{k+1}=m+1$ The only divisors of m are $1,m$
So m is prime.
So $n=2^{p-1}(2^p-1)$, 2^p-1 is a prime.