

# EXERCISES 319

## Fermat & Mersenne primes

Fermat ~~primes~~ numbers  $F_n = 2^{2^n} + 1$ ,  $n \in \mathbb{N}$  [ $2^m + 1$  prime  $\Rightarrow m = 2^n$ ]

Mersenne numbers  $M_p = 2^p - 1$ ,  $p$  prime [ $2^m - 1$  prime  $\Rightarrow m$  prime]

Conj (Fermat)  $F_n$  are prime

Euler gave counterex  $F_5 = 2^{2^5} + 1 = 641 \times 6700417$

Pf:  $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$  divides  $\left\{ \begin{array}{l} 5^4 \cdot 2^{28} + 2^{32} = 2^{28}(5^4 + 2^4) \\ 5^4 \cdot 2^{28} - 1 = (5 \cdot 2^7 - 1)(\dots) \end{array} \right.$   
 so it divides their difference  $\square$

Fact nobody found a prime  $F_n$ ,  $n \geq 5$

Prop  $F_n \mid F_m - 2$  for  $m > n$ . (In partic  $(F_n, F_m) = 1$ ).

Pf:  $m = n+k \Rightarrow F_m - 2 = 2^{2^{n+k}} - 1 = (2^{2^n})^{2^k} - 1 = x^{2^k} - 1 = (x-1)(\dots)$   
 $\uparrow$   
 $x = 2^{2^n}$

Fact Some  $M_p$ 's are prime, some not

Conj(?)  $\exists \infty$  prime  $M_p$ 's.

Theorem (Euler) If  $p \equiv 3 \pmod{4}$  is a prime ( $\geq 7$ ) &  $2p+1$  prime then  $M_p$  composite.  
 Pf. Let  $P = 2p+1$ ;  $p = 4k+3 \Rightarrow P = 8k+7 \xrightarrow{*} 2^P = 2^{\frac{1}{2}(P-1)} \equiv 1 \pmod{P}$

$\Rightarrow P \mid M_p = 2^P - 1 > 2p+1 = P \Rightarrow M_p$  composite.

Recall:

Def  $n$  called perfect if  $\sigma(n) = 2n$  ( $\sigma(n) = \sum_{d|n} d$ , all div including  $1 \& n$ )

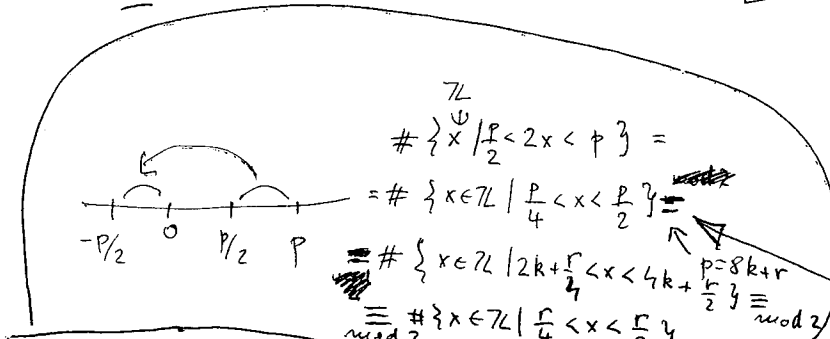
Ex 6, 28 perfect

Theorem (Euclid) If  $M_p = 2^p - 1$  prime then  $2^{p-1} M_p$  is perfect

Pf  $\sigma(2^{p-1} M_p) = 1 + 2 + \dots + 2^{p-1} + M + 2M + \dots + 2^{p-1}M = 2^p - 1 + (2^p - 1)M = (2^p - 1)(M+1) = M \cdot 2^p$

Converse (Euclid) Assume  $2^n P$  perfect. Then  $P = M_p$ ,  $n = p-1$ .

Pf  $\sigma(2^n P) = (2^{n+1} - 1)P = 2^{n+1}P \Rightarrow \square$



Indeed  
 Let  $r_1, \dots, r_{\frac{p-1}{2}} \equiv 1, 2, \dots, \frac{p-1}{2} \pmod{p}$   
 Easy: Take products  $\Rightarrow (-1)^k \cdot 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} = 2^{\frac{p-1}{2}}$

- \* - define  $\left(\frac{a}{p}\right)$ ; its multiplicativity
- Euler's th  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$  [pf: enough for a prim root when both  $\equiv -1$ ]
- Gauss' lemma for 2  $\left(\frac{2}{p}\right) = (-1)^M$  where  $M = \#$  of members of set  $2, 4, 6, \dots, p-1$
- Reciprocity for 2  $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$