EXERCISES 319

Fermat & Mersenne primes

Fermat 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 $\begin{cases} 5^4\cdot 2^{28} + 2^{32} = 2^{28}(5^4+2^4) \\ 5^4\cdot 2^{28} - 1 = (5\cdot 2^7 - 1)(\dots) \end{cases}$ (a^4, b^4, $a-b$)

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

Fact some M_p's are prime, some not

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

Theorem (Euler) If $p \equiv 3\ (4)$ is a prime (≥ 7) & $2p+1$ prime then M_p composite

(div by $2p+1$)

Pf. Let $P = 2p+1$; $p = 4k+3 \Rightarrow P = 8k+7 \overset{*}{\Longrightarrow} 2^p = 2^{\frac{1}{2}(P-1)} \equiv 1 \pmod P$

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

Recall:

Def n called perfect if $\sigma(n) = 2n$ ($\sigma(n) = \sum_{d \mid n} d$, all pos 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 $\sigma(2^n P) = (2^n - 1)(P+1) = 2^{n+1}P \Rightarrow \square$

$\#\{x \in \mathbb{Z} \mid \frac{p}{2} < 2x < p\} =$

$= \#\{x \in \mathbb{Z} \mid \frac{p}{4} < x < \frac{p}{2}\} =$

$= \#\{x \in \mathbb{Z} \mid 2k + \frac{r}{4} < x < 4k + \frac{r}{2}\}$ ($p = 8k+r$)

$\equiv \#\{x \in \mathbb{Z} \mid \frac{r}{4} < x < \frac{r}{2}\} \pmod 2$

$-p/2$, 0, $p/2$, p

Indeed (in $[-\frac{p}{2}, \frac{p}{2}]$ coset rep mod p to $2, 4, \dots, p-1$)

Let $r_1, \dots, r_{\frac{p-1}{2}}$

Easy: $\{|r_1|, \dots, |r_{\frac{p-1}{2}}|\} = \{1, 2, \dots, \frac{p-1}{2}\}$

Take products $\Rightarrow (-1)^\mu \cdot 1 \times 2 \times \dots \times \frac{p-1}{2} = 2^{\frac{p-1}{2}} \times 1 \times 2 \times \dots \times \frac{p-1}{2}$ $\square$

(*) - define $\left(\frac{q}{p}\right)$; its multiplicativity

- Euler's th $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \pmod p$ ($p \geq 3$) [pf: enough for a prim root when both $= -1$]
- Gauss' lemma for 2 $\left(\frac{2}{p}\right) = (-1)^\mu$ where μ = # of members of set $2, 4, 6, \dots, p-1$ congr mod p to a neg # in $[-\frac{p}{2}, \frac{p}{2}]$
- Reciprocity for 2 $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$