$$(a^m - b^m,\ a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

$(a,b) = 1$

$p^\alpha \mid a^m - b^m$

$p^\alpha \mid a^n - b^n$

$a^m \equiv b^m \pmod{p^\alpha}$

$\Rightarrow \left(\frac{a}{b}\right)^m \equiv 1 \pmod{p^\alpha}$

$\mathrm{ord}_{p^\alpha}\left(\frac{a}{b}\right) \mid m$

$\mathrm{ord}_{p^\alpha}\left(\frac{a}{b}\right) \mid n$

$\mathrm{ord}_{p^\alpha}\left(\frac{a}{b}\right) \mid (m,n)$

$\left(\frac{a}{b}\right)^{(m,n)} \equiv 1 \pmod{p^\alpha}$

$\Rightarrow a^{(m,n)} \equiv b^{(m,n)} \pmod{p^\alpha}$

$a^{(m,n)} \equiv b^{(m,n)} \quad (p^\alpha) \qquad a^m \equiv b^m$

$\Rightarrow \quad m = (m,n) \cdot m' \qquad a^n \equiv b^n$

$n = (m,n) \cdot n'$

$a^{c^t} - b^{c^t}$ $\quad$ qt primi

$d^{c^t} \left(a_1^{c^t} - b_1^{c^t} \right)$

$\uparrow$

$a^{p_i^t} - b^{p_i^t} \qquad a - b$

$p_1, p_2, \dots, p_q$

dividono c

$\left(a^{p_i^t} - b^{p_i^t}, a^{p_j^t} - b^{p_i^t} \right) = a - b$

$p^x \mid n$ $\qquad a \equiv b \pmod{p}$

$\Rightarrow a^n \equiv b^n \pmod{p^x}$

$b = kp + a \longrightarrow b^n = (kp + a)^n =$

$= k^n p^n + nk^{n-1} p^{n-1} a + \dots + nkp a^{n-1} + a^n$

(divisibile per p^x)

z la max potenza di p:

$p^z \mid n$

$p^z \mid \binom{n}{j} p^j \Rightarrow p^{z-j} \mid \binom{n}{j}$

f la max potenza di p: $p^f \nmid j$

$\Rightarrow$ $\binom{n}{j+1} = \binom{n}{j} \cdot \frac{n-j}{j+1}$ $\qquad p^2 \mid \binom{n}{j}$

$p^{2-f} \mid \binom{n}{j}$ $\qquad p^{f_1} \mid j+1$

$p^{2-f_1} \mid \binom{n}{j+1}$

$p^f \mid \binom{n}{j} \cdot \frac{n-j}{j+1} = \binom{n}{j+1}$

p^{2-f} $\qquad p^f$

$1 \le e \le n$

$e^n \equiv 1 \quad (n)$

$e^n \equiv 1 \quad (p_1^\alpha)$ $\qquad p_1^\alpha \mid n$

$m_1 =$

$|\{e : e^n \equiv 1 \ (p^\alpha) \wedge 1 \le e \le p_1\}|$

$\frac{n \cdot m_1}{p_2}$ è che verifica la relazione tra 1 e n

p_2

$a \qquad a+p_1 \qquad a+2p_1 \quad \dots \quad a+(p_2-1)p_1$

$\frac{n \cdot m_1}{p_1} \cdot \frac{m_2}{p_2} \cdot \frac{m_3}{p_3} \cdots \qquad L(n) = \frac{n \cdot \prod m_i}{\prod p_i}$

$\phi(n) = \frac{n \cdot T(n)}{\prod p_i}$

$\phi(n) \mid L(n) \cdot T(n) = \frac{n \cdot \prod m_i \cdot T(n)}{\prod p_i}$

$\frac{n \cdot \boxed{\prod m_i} \cdot T(n)}{\prod p_i}$

$(n, T(n)) = 1 \Rightarrow m_i = 1 \quad \forall i$

$(n, \overline{\tau}(a)) = 1 \quad \Rightarrow p_i \nmid p_j - 1$

$a^h \equiv 1 \quad (p_1^\alpha) \Rightarrow \boxed{a^h \equiv 1 \quad (p_1)}$

$a \equiv 1 \quad (p_1)$

$w_1 = 1$

$\operatorname{ord}_{p_1} a \mid h$

$\operatorname{Ord}_{p_1} a \mid p_1 - 1$

$\Rightarrow \operatorname{ord}_{p_1} a = 1$

ES 2

$$f(x) = \frac{x^m - 1}{x - 1} = x^{m-1} + x^{m-2} + \dots + x + 1$$

$$\begin{pmatrix} 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$x^4 + x + 1$ *

$x^2 + x + 1 \equiv (x^4 + x + 1)\, x$

$\equiv x^5 + x + 1$

$x^5 \equiv 1 \quad (f(x))$

$\mathbb{Z}_2^m$

$x^4 + x^2 \equiv x^4 + x + 1 + x^2 + x + 1 \equiv$

$\equiv x^4 + x^2 + 2x + 2 \equiv x^4 + x^2$

2^m

$$\begin{matrix} 0 \\ 1 \end{matrix} x^{m-1} + \begin{matrix} 0 \\ 1 \end{matrix} x^{m-2} \dots + \begin{matrix} 0 \\ 1 \end{matrix} x + \begin{matrix} a \\ 1 \end{matrix}$$

$$p(x) \equiv v_1 + v_2 + v_5 \cdots \equiv (v_{i_1} + v_{i_2} \cdots + v_{i_1} + v_{i_2} \cdots \equiv 0$$

$$\sum x_i x^i \quad \left(\sum x_i x^i\right) x \quad \cdots \left(\sum x_i x^i\right) x^{n-1}$$

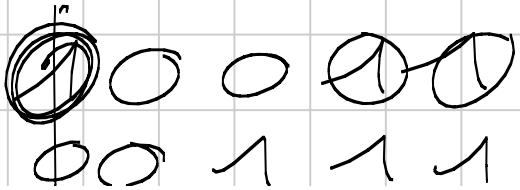
$$\left(\sum x_i x^i\right) \; q(x) \equiv 0 \qquad \left(f(x)\right)$$

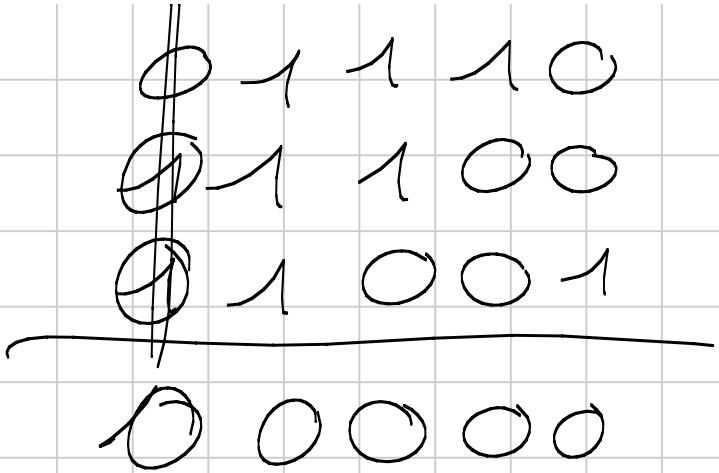
$$x^{n-1} + x^{n-2} + \cdots + 1$$

$$f(x) \nmid \sum x_i x^i$$

$$f(x) \mid q(x) \implies f(x) \equiv q(x)$$

$$q(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$$





$$\left(\sum x_i x^i\right) g(x) \equiv \sum x^i$$

Th. fondamentale delle funzioni simmetriche.

Qualunque polinomio simmetrico può essere scritto come polinomio nelle funzioni elementari $\sigma_{n,h}$ (h = grado, n = numero di variabili)

$\sigma_{3,1} = x_1 + x_2 + x_3$

$\sigma_{3,2} = x_1x_2 + x_1x_3 + x_2x_3$

$\sigma_{3,3} = x_1x_2x_3$

$$p(x,y) = x^3 + y^3 = (x+y)^3 - 3xy(x+y) = \underline{\sigma_{2,1}^3 - 3\sigma_{2,2}\sigma_{2,1}}$$

$N = n + K$ $\quad n$ = variabili, K = grado

$N=1$

$N=2 \quad \begin{matrix} 1 & 1 \\ 2 & 0 \end{matrix}$

$N < m_1 + k_1$

$N+1 = m_1 + k_1$

$p(t_1, t_2 \dots, t_{m_1}) \quad$ di- grado k_1

$p(t_1, t_2 \dots, 0) = q(\sigma_{m_1-1,1}, \sigma_{m_1-1,2}, \dots \sigma_{m_1-1,m_1-1})$

$p(t_1, t_2 \dots, t_{m_1}) - q(\sigma_{m_1,1}, \sigma_{m_1,2}, \dots, \sigma_{m_1,m_1-1})$

$t_m = 0 \quad t_{m_1} \mid p - q$

$t_1 \mid p - q$

$\vdots$

$t_{m_1} \mid p - q$

$$\prod_{i=1}^{m_1} t_i \mid p - q$$

$$p - q = \sigma_{m_1, m_1} \cdot r(t_1, t_2 \dots t_{m_1})$$

m_1

$\sum_{\text{Sym}}$ α β a b ----

$k \Rightarrow k+1$ $\quad$ n divis. per almeno k primi

$$\underbrace{1 + d_2 + d_3 + \dots + d_k}_{\text{divisori distinti di } n} = n$$

Molt. per $n+1$

$$\underbrace{(n+1) + d_2(n+1) + \dots + d_k(n+1)}_{k+1 \text{ divisori distinti}} = n\,\underbrace{(n+1)}_{\text{qui c'è un primo che non c'era in } n}$$

$1 + n$

$1 + 2 + 3 = 6$ $\qquad$ $1 + 6 + 14 + 21 = 42$

(2) Hp $p^2 \mid 2^{p-1}-1$ $n \in \mathbb{N}$

Tesi $(p-1)(p!+2^n)$ ha almeno 3 primi

↑ Almeno c'è il 2

Oss. $p-1$ e $p!+2^n$ non hanno fattori in comune oltre al 2

Basta dim. che $p-1$ e $p!+2^n$ hanno un fattore oltre il 2, cioè non sono potenze di 2.

PER ASSURDO sia $p-1 = 2^k$ $p = 2^k+1$

Lemma importante: se 2^k+1 è un primo, allora $k = 2^m$

NUMERI DI FERMAT

$p = 2^{2^m}+1$ Hp $p^2 \mid 2^{p-1}-1$

$$\left(2^{2^m}+1\right)^2 \mid 2^{2^{2^m}}-1$$

$$2^{2^{2^m}}-1 = (2-1)(2+1)(2^2+1)\cdot(2^4+1)\cdot(2^8+1)\cdots$$

$2^{2^m}+1$ lo trovo qui

Basta dim che i fattori con il + sono rel. primi

<u>Lemma</u> Dato x intero $(x+1, x^n+1)$ ↗ 1 o 2 n pari

↘ $x+1$ n dispari

Nel nostro caso MCD (2 fattori) è $\frac{1}{2}$

$p \mid (x+1) \Rightarrow x \equiv -1 \ (p)$ essendo n pari

$p \mid (x^n+1) \qquad x^n+1 \equiv (-1)^n+1 \equiv 2 \ (p)$

— o — o —

2° caso Escludere $p! + 2^n = 2^k$

$p! = 2^a (2^b - 1)$ per opportuni a e b

sempre nell'Hp in cui $p^2 \mid (2^{p-1} - 1)$

Se no $120 = 128 - 8$

Sia $d = \mathrm{ord}_p(2)$ $\qquad p \| 2^b - 1$

$p^2 \mid 2^d - 1$ Se fosse così, avremmo che quando $p \mid 2^b - 1$, allora $p^2 \mid 2^b - 1$

Conseguenza: $\text{ord}_p 2 < \text{ord}_{p^2} 2$

Ora sappiamo che $p-1 = md$

$2^d - 1 = kp$ ← NON MULTIPLO DI p

$2^d = kp+1$

$p^2 \mid 2^{p-1} - 1$

$2^{p-1} - 1 = 2^{md} - 1$

$= (kp+1)^m - 1$

$= mkp + \cancel{1} \cancel{-1}$ (p^2) (NO p)

deve essere 0 mod p^2

m divisore di $p-1 \Rightarrow$ no p dentro.

Lemma x intero, p primo

$$\left(x-1, \frac{x^p-1}{x-1}\right) \mid p$$

Inoltre, se è p, allora $\dfrac{x^p-1}{x-1} \equiv p \mod p^2$

Esempio x^2+x+1 $\qquad \left(x-1, x^2+x+1\right) = \begin{cases} 1 \\ 3 \end{cases}$

Se $x^2+x+1 \equiv 0 \ (3)$, allora $x^2+x+1 \equiv 3 \ (9)$

$q \mid x-1$

$q \mid x^{p-1}+x^{p-2}+\dots+x+1$

$x \equiv 1 \ (q)$

$\underbrace{1+\dots+1}_{p \text{ fattori}} \equiv p \ (q)$

$\Rightarrow p = q$

Se $x^{p-1} + x^{p-2} + \dots + x + 1$ è multiplo di p

Se $x \equiv 1 \ (p)$ $\quad x = kp + 1$

$$x^{p-1} + x^{p-2} + \dots + x + 1 =$$

$$= (kp+1)^{p-1} + (kp+1)^{p-2} + \dots + (kp+1) + 1$$

$$= kp(p-1) + 1 + kp(p-2) + 1 + \dots + (kp+1) + 1$$

p addendi

$$p + kp\left(1 + 2 + \dots + (p-1)\right) \equiv p + \frac{kp(p-1)}{2}$$

se $p > 2$ si GUADAGNA

$x^{p-1} + x^{p-2} + \dots + x + 1$ multiplo di p

$\Downarrow$

$x \equiv 1 \quad (p)$

$\Downarrow$

$x^p - 1 \equiv 0 \quad (p)$

$\Downarrow$

$x - 1 \equiv 0 \quad (p)$

$$2^{m} + m \equiv 0 \quad (p)$$

$$m = (p-1)K + h$$

$$2^{(p-1)K+h} + (p-1)K + h \equiv 2^{h} + (p-1)K + h \equiv 0 \quad (p)$$

$h = 0 \qquad 1 + (p-1)K \equiv 0 \quad (p)$

$$2^{M} + M \equiv 0 \quad (p^2)$$

$$M = \varphi(p^2) \cdot K + h = p(p-1)K + h$$

$$2^{p(p-1)K+h} + p(p-1)K + h \equiv 0 \quad (p^2)$$

$$2^{h} + h \equiv 0 \quad (p)$$

$$\beta p + p(p-1)K \equiv 0 \quad (p^2)$$

$B - K \equiv 0 \quad (p) \qquad B \equiv K \quad (p)$

Voglio dimostrare che, dato che ho trovato m per $\frac{n}{p}$, lo trovo per n, dove $p = \max$ primo che divide n.

$2^M + M \equiv 0 \quad (nq) \qquad n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$M = m + \phi(nq) \cdot p_1 \cdots p_k \, K \qquad \phi(nq) = \phi n \, \phi q$

$2^m + m + (p_1 - 1) \cdots (p_k - 1) \, p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot (q-1) \cdot K \equiv 0 \quad (nq)$

$2^m + m \equiv B n \quad (nq)$

$2^m + m + \underbrace{(p_1 - 1) \cdots (p_k - 1) \, p_1^{\alpha_1} \cdots p_k^{\alpha_k} (q-1)}_{Q} K \equiv 0 \quad (n)$

$$2^m + m + QK \equiv 0 \quad (q)$$

$$K \equiv (-2^m - m)\, Q^{-1} \quad (q)$$

$$M = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q^{\alpha}$$

$$M = m + \phi(Mq)\, p_1 \cdots p_k q^K$$

$$2^M + M \equiv 2^m + m + (p_1 - 1) \cdots (p_k - 1)(q-1) p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot q^{\alpha} K \equiv 0 \quad (Mq)$$

$$2^m + m \equiv 0 \quad (p_1^{\alpha_1} \cdots p_k^{\alpha_k} q^{\alpha})$$

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$BQ + QQK \equiv 0 \qquad (q^{\alpha+1})$$

$$K \equiv -BQ^{-1} \quad (q)$$

p $p=2$ 2^k

Il passo base è $n=2^k$. Basta scegliere $m : 2^k$.

$2^m + m \equiv 0 \quad (n)$

$2^m + m \equiv a \quad (n)$