S25 MEDIUM N 1

Titolo nota 03/09/2025

- RADICI PRIMITIVE DELL'UNITÀ, POLINOMI CICLOTOMICI
- GENERATORI mod p, p^n
- LEMMA DI HENSEL
- LTE
- LEMMA DEL GUADAGNO DI UN PRIMO

POLINOMI CICLOTOMICI $\quad n \in \mathbb{Z}^+$

Def $\zeta \in \mathbb{C}$ è una radice primitiva n-esima dell'unità se

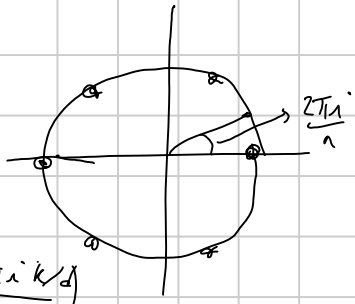
$$\zeta^n = 1 \quad \text{ma} \quad \zeta^k \neq 1 \ \ \forall 1 \le k < n$$

Sono della forma $\zeta = \zeta_n^k$ $\quad \zeta_n = \exp\left(\frac{2\pi i}{n}\right) = e^{\frac{2\pi i}{n}}$

con $(k,n)=1$ (altrimenti $d|k, d|n$)

$$\zeta_n^k = \exp\left(\frac{2\pi i k}{n}\right) = \exp\left(\frac{2\pi i k/d}{n/d}\right)$$

$\to$ radice n/d-esima



Def Per $n \in \mathbb{Z}^+$ l'n-esimo polinomio ciclotomico

$$\Phi_n(x) = \prod_{\substack{\alpha \text{ rad. prim. } n\text{-esima di } 1}} (x-\alpha) = \prod_{\substack{0 \le k < n \\ (k,n)=1}} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

Es: $\Phi_1(x) = x-1$

$\Phi_2(x) = x+1$

$\Phi_3(x) = \left(x - e^{\frac{2\pi i}{3}}\right)\left(x - e^{\frac{4\pi i}{3}}\right)$
$= x^2 + x + 1$

$\Phi_4(x) = (x-i)(x+i)$

Oss $\deg \Phi_n = \left|\{0 \le k < n \mid (k,n)=1\}\right| = \varphi(n)$

Lemma $\prod_{d|n} \Phi_d(x) = x^n - 1$

Dim Le radici di RHS sono $\{\zeta_n^k \mid 0 \le k < n\}$

Le radici del LHS è $\bigcup_{d|n} \{\zeta_d^j \mid 0 \le j < d, (j,d)=1\} = \bigcup_{d|n} \{\zeta_n^{\frac{n}{d}j} \mid 0 \le j < d, (j,d)=1\}$

$\zeta_d = \zeta_n^{n/d} = \exp\left(\frac{2\pi i \cdot \frac{n}{d}}{n}\right)$

$$= \bigcup_{d|n} \left\{\zeta_n^k \mid 0 \le k < n \ \ (k,n) = n/d\right\} = \left\{\zeta_n^k \mid 0 \le k < n\right\}$$

$\Rightarrow$ segue l'uguaglianza dei due polinomi (monici) $\square$

Cor $\quad n = \sum_{d \mid n} \varphi(d)$

Φ_n soddisfano ricorsivamente: $\Phi_1(x) = x - 1$

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)} \in \mathbb{Z}[x]$$ pol. a coeff. interi

---

Es $\quad P_n(x) = 1 + x + \cdots + x^{n-1} \qquad F_n(x) = P_1(x) P_2(x) \cdots P_n(x)$

$$\frac{F_{m+n}(x)}{F_m(x) F_n(x)} \in \mathbb{Z}[x]$$

Dim $\quad P_n(x) = \frac{x^n - 1}{x - 1} \qquad F_n(x) = \prod_{1 \le k \le n} \frac{x^k - 1}{x - 1} = \frac{1}{(x-1)^n} \prod_{k \le n} \prod_{d \mid k} \Phi_d(x) =$

$$\frac{1}{(x-1)^n} \prod_{1 \le d \le n} \prod_{\substack{d \le k \le n \\ d \mid k}} \Phi_d(x) = \frac{1}{(x-1)^n} \prod_{d \le n} \Phi_d(x)^{\lfloor n/d \rfloor}$$

$$\Rightarrow \frac{F_{m+n}(x)}{F_m(x) F_n(x)} = \frac{\cancel{1/(x-1)^{m+n}} \prod \Phi_d(x)^{\lfloor \frac{m+n}{d} \rfloor}}{\cancel{(x-1)^m} \cdot \cancel{(x-1)^n} \prod \Phi_d(x)^{\lfloor m/d \rfloor} \cdot \prod \Phi_d^{\lfloor n/d \rfloor}} = \prod_{1 \le d \le m+n} \Phi_d(x)^{\lfloor \frac{m+n}{d} \rfloor - \lfloor \frac{m}{d} \rfloor - \lfloor \frac{n}{d} \rfloor}$$

$x, y \in \mathbb{R} \quad \lfloor x + y \rfloor \ge \lfloor x \rfloor + \lfloor y \rfloor \quad (\Leftrightarrow \{x+y\} \le \{x\} + \{y\})$

GENERATORI

$m \in \mathbb{Z}^+ \qquad \mathbb{Z}/m\mathbb{Z} \qquad (\mathbb{Z}/m\mathbb{Z})^\times = \{ a \in \mathbb{Z}/m\mathbb{Z} \mid \exists\, b \in \mathbb{Z}/m\mathbb{Z} \;\; a \cdot b \equiv 1 \}$

$= \{ k \mid (k, m) = 1 \} \qquad |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$

$\bar{a} \in \mathbb{Z}/m\mathbb{Z} \qquad \operatorname{ord}_m(\bar{a}) = \min \{ l \mid a^l \equiv 1 \pmod m \}$

Pf $\quad a$ è generatore mod m se $(a, m) = 1 \;\; \operatorname{ord}_m(a) = \varphi(m)$, ovvero se

$$\{1, a, a^2, \ldots, a^{\varphi(m)-1}\} \equiv \{ k \mid (k, m) = 1 \} \bmod m$$

Thm $\quad$ Esiste una gen. mod m se e solo se $m = p^k, 2p^k, 2, 4 \qquad p \in \mathbb{P}, \; p \neq 2$

Dim [mod p] Se abbiamo $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, esso ha al più $\deg(f)$ radici

LEMMA #0

[Dipende dal fatto che $a, b \in \mathbb{Z}/p\mathbb{Z}$
$a \cdot b \equiv 0 \Rightarrow a \equiv 0 \vee b \equiv 0$]

[oss: $x^2 \equiv 1 \pmod 8$ ha 4 sol.]

$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times \quad a^{p-1} \equiv 1 \pmod p$ (FLT)

$\rightarrow f(x) = x^{p-1} - 1$ ha $p-1$ radici distinte

$$f(x) = x^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(x)$$

Ma, $\Phi_d(x)$ ha al più $\varphi(d)$ radici distinte, e quindi RHS ha al più $\sum_{d \mid p-1} \varphi(d) = p-1$ radici. Siccome vale l'uguaglianza con LHS

Segue che ogni $\Phi_d(x)$ ha esattamente $\varphi(d)$ radici ($d \mid p-1$) distinte

e inoltre $\Phi_d(a) \equiv 0 \Rightarrow \Phi_{d'}(a) \neq 0$ se $d, d' \mid p-1$ $d \neq d'$

In particolare $\Phi_{p-1}(x)$ ha $\varphi(p-1)$ radici distinte, che non sono radici di $\Phi_{d'}$ con $d' < p-1$, $d' \mid p-1$

$\Phi_{p-1}(a) \equiv 0 \rightarrow a^{p-1} \equiv 1 \ (p)$ Se valesse $a^{d'} \equiv 1 \ (p)$ con $d' < p-1$,

allora $\prod_{t \mid d'} \Phi_t(a) \equiv a^{d'} - 1 \equiv 0 \ (p) \Rightarrow \exists\, t \mid d' \mid p-1$ $\Phi_t(a) \equiv 0$ ↯ ($t \leq d' < p-1$)

$\Rightarrow a$ è radice primitiva $(p-1)$-esima, ovvero un generatore mod p. □

In particolare, ci sono esattamente $\varphi(p-1)$ generatori

mod p^k mod 2^k $k \geq 3$ non ci sono mod 8 $a^2 \equiv 1 \quad \forall a \in (\mathbb{Z}/8\mathbb{Z})^\times$

$\rightarrow \nexists\, a \ \operatorname{ord}_8(a) = 4 = \varphi(8)$

$p \neq 2$

oss $(a, p) = 1$ $a^d \equiv 1 \pmod{p^{k+1}} \Rightarrow a^d \equiv 1 \pmod{p^k}$

$\Rightarrow \operatorname{ord}_{p^k}(a) \mid \operatorname{ord}_{p^{k+1}}(a)$

a gen. mod $p^k \Rightarrow \operatorname{ord}_{p^k}(a) \mid \operatorname{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = (p-1)p^k$

$\varphi(p^k) = (p-1)p^{k-1} \Rightarrow \operatorname{ord}_{p^{k+1}}(a) = \begin{cases} (p-1)p^k \\ (p-1)p^{k-1} \end{cases}$

vorremmo quindi che $a^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$, cosicché a gen $\pmod{p^{k+1}}$

$k=1$ a è gen. mod p $\Rightarrow$ a è gen mod p^2 ✓

altrimenti, proviamo con $a+tp$ $\quad 0<t<p$

vogliamo che $1 \not\equiv (a+tp)^{p-1} = a^{p-1} + tp\cdot a^{p-2}\cdot\underbrace{(p-1)}_{\binom{p-1}{1}} + p^2(\cdots) \equiv a^{p-1} + tp(p-1)a^{p-2} \pmod{p^2}$

$p \nmid t(p-1)a^{p-2}$ siccome $a^{p-1} \equiv 1 \pmod p$ e $a^{p-1} \equiv 1 \pmod{p^2}$, aggiungendo un multiplo di p $t \not\equiv 0 \pmod p$, otteniamo $\underbrace{1 + (\not\equiv 0)\cdot p}_{\not\equiv 1 \pmod{p^2}} \pmod{p^2}$

$p>2$
$k>1$

a gen mod p^k $\quad a^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$

$(a+tp^k)^{(p-1)p^{k-1}} \equiv a^{(p-1)p^{k-1}} + a^{\cdots -1}\cdot tp^k\cdot(p-1)p^{k-1} + p^{2k}(\cdots) \pmod{p^{k+1}}$

$\equiv 0 \pmod{p^{k+1}}$ $\quad$ $k>1$

$\Rightarrow$ [a è gen. mod p^{k+1} $\leftrightarrow$ $a+tp^k$ lo è]

$a^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$

$\| \quad$ $0<t<p$

$1+tp^{k-1}$

$\pmod{p^{k+1}}$ $\quad \overset{?}{\not\equiv} a^{(p-1)p^{k-1}} \equiv (1+tp^{k-1})^p = 1 + \underbrace{p\cdot tp^{k-1}}_{t\cdot p^k} + t^2p^{2k-2}\underbrace{\binom{p}{2}}_{\frac{p(p-1)}{2}} + p^{3k-3}\cdots \equiv \pmod{p^{k+1}}$

$p \nmid t \quad \not\equiv 0 \pmod{p^{k+1}}$

$v_p(\ ) = 2k-2+v_p\left(\frac{p(p-1)}{2}\right) = 2k-2+1 = 2k-1 \geq k+1$ ✓

$p>2$ $\quad$ se $p=2$ $v_2\left(\frac{2\cdot 1}{2}\right) = 0$ NO

$v_p(\cdots) \geq 3k-3 \geq k+1$ ✓

$\Rightarrow a^{(p-1)p^{k-1}} \equiv 1 + tp^k \pmod{p^{k+1}}$ $\quad 0<t<p$

$\Rightarrow a^{(p-1)/p^{k-1}} \not\equiv 1 \pmod{p^{k+1}} \Rightarrow a$ è gen. mod p^{k+1} $\square$

ex $p, q \in \mathbb{P}$ $q > 2$ $\exists x$ $(x+1)^p \equiv x^p \pmod q$

$\Updownarrow$

$q \equiv 1 \pmod p$

Dim Se $\exists x \Rightarrow x \not\equiv 0, -1 \pmod q \Rightarrow x, x+1 \in (\mathbb{Z}/q\mathbb{Z})^*$

$\exists x \neq 0$ $(1+1/x)^p \equiv 1 \pmod q \iff \exists y$ $y^p \equiv 1 \pmod q$

$\left(\frac{x+1}{x}\right)^p$ (=) $q>$ (#) 1

g gen $\pmod q$ $y \equiv g^z \pmod q$ $y^p \equiv g^{pz}$

$\exists y$ (#) $y^p \equiv 1 \ (q) \iff \exists z$ (#) $\neq 0 \pmod{q-1}$ s.t. $g^{pz} \equiv 1 \ (q) \iff \exists z$ (#) $\neq 0 \ (q-1)$ $pz \equiv 0 \ (q-1)$

$\iff (p, q-1) \neq 1 \iff p \mid q-1$

LTE (LIFTING THE EXPONENT)

Def $n \in \mathbb{Z}$, $p \in \mathbb{P}$ $v_p(n) = \max\{k \in \mathbb{Z} \mid p^k \mid n\}$, $v_p(0) = \infty$

$v_p(x \cdot y) = v_p(x) + v_p(y)$

$v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

$= $ se $v_p(x) \neq v_p(y)$

$v_p(a^n - b^n) = ?$

LEMMA $p \in \mathbb{P}$ $a \neq b \in \mathbb{Z}$ $p \mid a-b$ $p \nmid a, b$ $n \geq 0$

$p \neq 2$ $\quad v_p(a^n - b^n) = v_p(a-b) + v_p(n)$

$p = 2$

se n è dispari $v_2(a^n - b^n) = v_2(a-b) + \cancel{v_2(n)}^{0}$

se n è pari $v_2(a^n - b^n) = v_2(a-b) + v_2(n) - 1 + v_2(a+b)$

$\longrightarrow$ se $4 \mid a-b \Rightarrow v_2(a^n - b^n) = v_2(a-b) + v_2(n)$

infatti se $n = 2m \Rightarrow a^2 \equiv b^2 \ (4) \Rightarrow$

$v_2(a^n - b^n) = v_2(a^{2m} - b^{2m}) = v_2(a^2 - b^2) + v_2(m)$

Dim Lifting the exponent nel caso più semplice

$$v_p(a^q-b^q)=v_p(a-b)+v_p(q)$$

$n=q\cdot n'$ ...

$$v_p(a^n-b^n)=v_p\left((a^{n'})^q-(b^{n'})^q\right)=$$

$$v_p(a^{n'}-b^{n'})+v_p(q)$$

$$\| $$

$$v_p(a-b)+\underbrace{v_p(n')+v_p(q)}_{=v_p(n)}$$

$q\neq p$

$$\frac{a^q-b^q}{a-b}=a^{q-1}+a^{q-2}b+\dots+b^{q-1}\equiv \underbrace{a^{q-1}+a^{q-1}+\dots+a^{q-1}}_{q}=q\,a^{q-1}\not\equiv 0\ (p)$$

$a\equiv b\ (p)$

$p=q$ $\quad a-b=p\cdot t$

$p\neq 2$

$$\frac{a^p-b^p}{a-b}=\sum_{i=0}^{p-1}a^i b^{p-1-i}=\sum_{i=0}^{p-1}b^{p-1-i}\cdot(b+pt)^i\equiv\sum_{i=0}^{p-1}b^{p-1}+b^{p-2}\cdot p\cdot t\left(\sum_{i=0}^{p-1}i\right)\quad \mathrm{mod}\,p^2$$

$$(b+pt)^i=b^i+i\cdot pt\cdot b^{i-1}+p^2(\dots)\equiv 0\ \mathrm{mod}\,p^2$$

$$\equiv p\cdot b^{p-1}+p\cdot t\cdot b^{p-2}\cdot\frac{p(p-1)}{2}\equiv p\cdot b^{p-1}\ (\mathrm{mod}\,p^2)$$

$p\neq 2$ $\qquad b^{p-1}\not\equiv 0\ (p)$

$$v_p\left(\frac{a^p-b^p}{a-b}\right)=1=v_p(p)$$

Se $p=2$ e $4\mid a-b$ $\to$ $2\,\|\,a+b$ $\qquad v_2(a+b)=1$

$$v_2\left(\frac{a^2-b^2}{a-b}\right)=v_2(a+b)=1=v_2(2)$$

□

VARIANTE DI LTE

$p\in\mathbb{P}$ $\quad p\mid a+b$ $\quad p\nmid ab$ $\qquad v_p(a^n+b^n)\overset{?}{=}v_p(a+b)+v_p(n)$

n dispari

$$v_3(2^3+1)=v_3(2+1)+v_3(3)$$

Dim Usiamo LTE per a e $-b$ $\quad (-b)^n=-b^n$

$$a^n+b^n=a^n-(-b)^n$$

(va bene pure nel caso $p=2$)

Ex Trova il max n^{esimo} t.c. $\qquad (2027\in\mathbb{P})$

$$2027^n\ \Big|\ 2026^{2027^{2028}}+2028^{2027^{2026}}+2027^{2026^{2028}}$$

ex $a \in \mathbb{Z}$ $a > 1$ $a_n = 1 + a + \dots + a^{n-1}$ $s \neq t \in \mathbb{Z}^+$

$(\forall p \in \mathbb{P} \quad p \mid s-t \Rightarrow p \mid a-1)$

$\Rightarrow \dfrac{a_s - a_t}{s-t} \in \mathbb{Z}$.

---

ex 1 $p = 2027$

$$v_p\left(\overbrace{(p-1)^{p^{p+1}} + (p+1)^{p^{p-1}}}^{S} + \overbrace{p^{(p+1)^{p+1}}}^{T} \right) = v_p(S)$$

car $v_p(S) < (p-1)^{p+1}$

$v_p\left(p^{(p-1)^{p+1}}\right) = (p-1)^{p+1}$

$S = \left((p-1)p^2\right)^{p^{p-1}} + (p+1)^{p^{p-1}}$ $\quad v_p(S) = v_p\left((p-1)p^2 + p+1\right) + v_p\left(p^{p-1}\right)$

$p \mid (p-1)p^2 + p + 1$ $\quad$ $\| \; p-1$

$v_p\left((p-1)^{p^2}+1\right) = v_p\left((p-1)+1\right) + v_p(p^2) = 3$

$\| \; 1$ $\quad \| \; 2$

$v_p(\dots + p) = v_p(p) = 1$

$v_p(S) = 1 + p - 1 = p < (p-1)^{p+1} \Rightarrow v_p(S+T) = v_p(S) = p$

$\| \; p2027$

---

ex $a_n = 1 + a + \dots + a^{n-1} = \dfrac{a^n - 1}{a-1}$ $\quad s > t > 0$ $\quad p \mid s-t \Rightarrow p \mid a-1$

$\dfrac{a_s - a_t}{s-t} \in \mathbb{Z} \Leftrightarrow \forall p \mid s-t \quad v_p(s-t) \leq v_p(a_s - a_t)$

$a_s - a_t = \dfrac{(a^s - y) - (a^t - y)}{a-1} = a^t \dfrac{a^{s-t} - 1}{a-1}$

$p \mid s-t \Rightarrow p \mid a-1$

$(p \neq 2)$ $\quad v_p\left(a^t \dfrac{a^{s-t}-1}{a-1}\right) = \underbrace{v_p(a)}_{(a,p)=1} \cdot t + v_p(a-1) + v_p(s-t) - v_p(a-1)$

$p = 2$ $\quad 2 \mid s-t \Rightarrow 2 \mid a-1$ $\quad v_2\left(\dfrac{a^{s-t}-1}{a-1}\right) = \underbrace{v_2(a+1)-1}_{\geq 0 \Leftarrow a \text{ impair}} + v_2(s-t) \geq v_2(s-t)$

LEMMA DEL GUADAGNO DI UN PRIMO

$a,b \in \mathbb{Z}^+$ $a>b>0$ $(a,b)=1$ $\forall n>1$ $\exists p \in \mathbb{P}$ $p \mid a^n - b^n$ $p \nmid a-b$

[a meno che $n=2$, $a+b=2^k$]

GENERALIZZAZIONE

(THM) ZSIGMONDY: Se $a>b>0$ $(a,b)=1$ $\forall n>1$ $\exists p \in \mathbb{P}$

$p \mid a^n - b^n$ $p \nmid a^k - b^k$ $\forall 1 \le k < n$

A MENO CHE $n=2$ $a+b=2^k$, $(a,b,n)=(2,1,6)$ $2^6-1=63$ $2^3-1=7$ $2^2-1=3$

Dim WLOG possiamo assumere $n=q \in \mathbb{P}$ $q \mid n$ $a^q - b^q \mid a^n - b^n$ (*)

Per quanto assumiamo che $p \mid a^q - b^q \Rightarrow p \mid a-b$

$p \mid a^q - b^q \Rightarrow p \mid a-b \underset{LTE}{\Rightarrow} v_p(a^q-b^q) = v_p(a-b) + v_p(q)$

$q \neq p$ $v_p(a^q-b^q) = v_p(a-b)$

$q = p$ $v_p(a^q-b^q) = v_p(a-b)+1$ $\Rightarrow \dfrac{a^q-b^q}{a-b} = q$

$$\frac{a^q-b^q}{a-b} = a^{q-1} + \dots + b^{q-1} > 1+1+\dots+1 = q \quad \lightning$$

Se $q=2$, c'è ancora un nuovo primo che divide $\frac{a^2-b^2}{a-b} = a+b$

e se abbiamo $p \mid a+b$ e $p \mid a-b \Rightarrow p \mid 2b \Rightarrow p=2$, ovvero $a+b=2^k$

Se $n=2^t$ $t>1$, basta usare il fatto che $4 \mid a^2-b^2$ e di nuovo LTE.

Es Dimostrare che esistono infiniti $n \in \mathbb{Z}^+$ t.c.

$$n^2 \mid 3^n + 2^n$$

Dim $1^2 \mid 3+2$ $5^2 \mid 3^5+2^5$ $v_5(3^5+2^5) = v_5(3+2) + v_5(5) = 2$

CLAIM esiste una famiglia di soluzioni a_n della forma

$a_n = p_n \cdot p_{n-1} \cdots p_1$ con $p_i \in \mathbb{P}$ $(a_0 = 1)$

p_i dispari $\quad a_{n+1} = p_{n+1} a_n$

p_i distinti $\quad p_n \mid 3^{a_{n-1}} + 2^{a_{n-1}} \quad \forall n \geq 1$

Assumiamo che $a_n^2 \mid 3^{a_n} + 2^{a_n} \mid 3^{a_{n+1}} + 2^{a_{n+1}}$

$\uparrow$ $2 \nmid p_{n+1}$

$q \mid 3^{a_n} + 2^{a_n} \Rightarrow$ (LTE) $v_q(3^{a_{n+1}} + 2^{a_{n+1}}) = v_q(3^{a_n} + 2^{a_n}) + v_q(p_{n+1})$

$\geq$?

$2 v_q(a_{n+1}) \longrightarrow \leq 2$

se $q \nmid a_{n+1}$, ovvero se $q \neq p_i$ $i \leq n+1$ ✓

se $q = p_i$ $\quad a_n^2 \mid 3^{a_n} + 2^{a_n} \mid 3^{a_{n+1}} + 2^{a_{n+1}}$

$a_n^2 = p_1^2 \cdots p_n^2$

quindi se $i \leq n$ ✓

se $i = n+1$, vogliamo che $v_{p_{n+1}}(3^{a_n} + 2^{a_n}) + v_{p_{n+1}}(p_{n+1}) \geq 2 v_{p_{n+1}}(a_{n+1})$

$v_{p_{n+1}}(p_{n+1}) = 1$, $\quad v_{p_{n+1}}(a_{n+1}) = 2$

$p_{n+1} \mid 3^{a_n} + 2^{a_n}$

Dobbiamo solo garantire che esista un tale primo, diverso dai $\{p_i\}_{i \leq k}$

VARIANTE DEL LEMMA SOPRA

$a > b > 0$ $\quad n$ dispari $\Rightarrow \exists\, p \in \mathbb{P}$ $\quad p \mid a^n + b^n \quad p \nmid a+b$

Attenzione $\quad 2^3 + 1 = 9 = (2^1+1)^2 = 3^2$

Dim: ci basta il caso $n = q \in \mathbb{P}_{>2}$ $\quad$ Per assurdo $p \mid a^n + b^n \Rightarrow p \mid a+b$

$v_p(a^q + b^q) = v_p(a+b) + v_p(q)$

$$\frac{a^q + b^q}{a+b} = q$$

$a \geq b$

$$a^{q-1} - a^{q-2}b + \dots + b^{q-1} > q$$

$$= a^{q-2}(a-b) + a^{q-4}b^2(a-b)$$

$$\geq 2^{q-2} + 2^{q-4} + \dots + 2 + 1 = 2 \cdot \frac{4^{\frac{q-3}{2}+1} - 1}{4-1} + 1 = \frac{2}{3}\left(4^{\frac{q-1}{2}} - 1\right) + 1$$

↯ $\quad q < \dots$ per q abbastanza grande

.... dopo un po' di conti si dovrebbe finire (ritrovare il caso speciale menzionato sopra) . □

Usando il lemma a basta prendere $p_{n+1} \mid 3^{2^n} - 2^{2^n}$ ma $= (3^{2^{n-1}})^{p_n} + (2^{2^{n-1}})^{p_n}$

$p_{n+1} \nmid 3^{2^{n-1}} + 2^{2^{n-1}}$. Quindi basta anche per ip. ind. $p_1 \cdots p_n \mid 3^{2^{n-1}} + 2^{2^{n-1}}$

(Prima base dell'induzione $a_0 = 1$ $a_1 = 5 = p_1$) . □

LEMMA DI HENSEL

$f(x) \in \mathbb{Z}[x]$ $\quad f(x) \equiv 0 \pmod{p}$ $\quad p \in \mathbb{P}$

$x_0 \in \mathbb{Z}/p^n\mathbb{Z}$ $\quad f(x_0) \equiv 0 \pmod{p^n}$ $\quad \wedge \quad f'(x_0) \not\equiv 0 \pmod{p}$

$\Rightarrow \underbrace{\exists!}_{\text{ESISTE UNICO}} \tilde{x}_0 \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ $\quad f(\tilde{x}_0) \equiv 0 \pmod{p^{n+1}}$ e $\tilde{x}_0 \equiv x_0 \pmod{p^n}$

[PROMEMORIA Dato $f(x) = \sum_{n=0}^{d} a_n x^n$ $\quad f'(x) = \sum_{n=0}^{d} a_n \cdot n \cdot x^{n-1}$]

[Un esempio in cui non possiamo applicare Hensel è $x^2 \equiv 1 \pmod{2^n}$
$f(x) = x^2 - 1$ $\quad f'(x) = 2x = 0$ $\quad x^2 - 1 \equiv 0 \pmod{8}$ ha 4 sol.
$x_0 = 1$ $\quad f'(x_0) \equiv 0$
$f(x) = x^2 \pmod{p^n}$]

Dim Partendo da x_0 a voglia $\tilde{x}_0 \equiv x \pmod{p^n}$, dobbiamo avere $\tilde{x}_0 = x_0 + t p^n$ $\quad t \in \mathbb{Z}/p\mathbb{Z}$. Vogliamo che $\exists! \, t \in \mathbb{Z}/p\mathbb{Z}$

$f(x_0 + t p^n) \equiv 0 \pmod{p^{n+1}}$

$f(x) = \sum_{k=0}^{d} a_k x^k$ $\quad f(x_0 + t p^n) = \sum_k a_k (x_0 + t p^n)^k =$

$= \sum_k a_k x_0^k + a_k \binom{k}{1} x_0^{k-1} t p^n + p^{2n}(\dots)$ $\quad p^{n+1} \mid p^{2n}$ $\quad n \geq 1$

$\equiv f(x_0) + \left(\sum a_k \cdot k x_0^{k-1}\right) \cdot p^n \cdot t \pmod{p^{n+1}}$

$f(x_0) + f'(x_0) \cdot t \cdot p^n \pmod{p^{n+1}}$

Ma sappiamo che $f(x_0) \equiv 0 \ (p^n)$ e $p \nmid f'(x_0)$

→ Dividiamo per p^n $\quad \frac{f(x_0)}{p^n} + t \cdot f'(x_0) \equiv 0 \pmod p$

$t \equiv -\frac{f(x_0)}{p^n f'(x_0)} \qquad \tilde{x}_0 \equiv x_0 - p^n \frac{f(x_0)}{p^n f'(x_0)} = x_0 - \frac{f(x_0)}{f'(x_0)}$

(METODO DI NEWTON)

es $f(x) = x^2 + 5 \equiv 0 \pmod{7^n}$

mod 7 → 3, −3 $\qquad f'(3) = 2 \cdot 3 = 6 \not\equiv 0 \ (7)$

$\qquad f'(-3) = 2 \cdot (-3) \equiv 1 \not\equiv 0 \ (7)$

$3 \rightsquigarrow 3 - \frac{14}{6} = 4/6 = 2/3 = 2 \cdot 33 = 17 \rightsquigarrow \ldots$

$-3 \rightsquigarrow -17 \rightsquigarrow \ldots$

oss il lemma di Hensel ci dice anche che è inutile sperare di trovare

Tutte le sol. di una diofantea della forma

$p^n = f(x)$ lavorando mod p^k.

Per esempio $7^n = x^2 + 5$, guardando l'eq. mod 7^k $(k \leq n)$

avremo sempre 2 sol.

In realtà in questo caso possiamo fare altri ragionamenti

→ (mod 3) $\quad 1^n \equiv x^2 - 1 \quad$ ⇒ NON CI SONO SOL.

$\equiv$ −1 / 0
