Relazione TdN1

- Lemma 1 (usato quasi da tutti, rigirato da una parte o dall'altra)

  Dato un primo $p \equiv 3 \pmod 4$ e due interi m ed n, se $p | m^2 + n^2$ allora $p|m$ e $p|n$.

  Si dimostra per LFT e sfruttando il fatto che $\frac{p-1}{2}$ è dispari:

  $$i^2 \equiv -j^2 \pmod p \rightarrow (i^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (j^2)^{\frac{p-1}{2}} \pmod p \rightarrow i \equiv -j \pmod p$$

  A questo punto si vede che $j^2 \equiv i^2 \equiv -j^2 \pmod p$ ma allora $2j^2 \equiv 0 \pmod{}$, quindi $p|j$ e $p|i$.

- Lemma 1.a

  Se r è un residuo quadratico modulo un primo $p \equiv 3 \pmod 4$, allora $-r$ non lo è.

  Infatti $m^2 \equiv r \pmod p$, se esistesse n t.c. $n^2 \equiv -r \pmod p$, allora avremmo $m^2 + n^2 \equiv 0 \pmod p$, con ovviamente $p \not| m, n$ assurdo per il Lemma 1. Corollario, usato da molti: -1 non è residuo quadratico modulo $p \equiv 3 \pmod 4$.

  Bonus question: dimostrare il Lemma 1.a, come ha fatto Kirill, con i generatori.

- Lemma 2 (usato solo da Borghese)

  Dati x e y coprimi e p primo dispari, l'MCD di $x - y$ e $p(x, y) = \frac{x^p - y^p}{x - y} = x^{p-1} + yx^{p-2} + \cdots + y^{p-1}$ è uguale a 1 o p.

  Per qualunque q primo che divida l'MCD vale $x \equiv y \pmod q$. Quindi modulo q $p(x, y) \equiv 0$ vale px^{p-1}. Ora, se q dividesse x, avremmo che $y \equiv x \equiv 0 \pmod q$ quindi x e y non sarebbero coprimi. Quindi $q \not| x$, e per $px^{p-1} \equiv 0 \pmod q$ segue che $q = p$ se q esiste, altrimenti $MCD = 1$. Si conclude infine ripetendo il ragiondamento modulo q^k tenendo presente che $q \not| x$ per dimostrare che potenze più alte di q non dividono l'MCD.

- Idea / puro fattore C / esercizio preparato apposta

  Tentando di trattare quel maledetto b^7, si trova $a^2 + 11^2 = b^7 + 2^7 = (b+2)(b^6 + 2b^5 + \cdots + 2^6)$

- Idea utile

  Se un numero è congruo a 3 modulo 4, ha dispari, e quindi almeno uno, fattori primi congrui a 3 modulo 4.

- Svolgimento

  Dall'equazione iniziale, si trova facilmente che a è pari e $b \equiv 1 \pmod 4$, quindi $b + 2 \equiv 3$. Segue che l'LHS ha almeno un fattore congruo a 3 modulo 4, che per il Lemma 1 è 11. Quindi l'unico fattore congruo a 3 modulo 4 di $b + 2$ è 11, e avrà nella scomposizione esponente dispari. Ma l'LHS è multiplo di 121, sempre per il Lemma 1, quindi anche $(b^6 + 2b^5 + \cdots + 2^6)$ è multiplo di 11, assurdo per il Lemma 2.

  Altri modi di concludere sono trovare che $b+2 \equiv 0 \pmod{11} \rightarrow b \equiv 9 \pmod{11}$ e calcolare modulo 11 $(b^6 + 2b^5 + \cdots + 2^6) \not\equiv 0$, oppure raccogliere e semplificare 121 e trovare che $c^2 + 1$ è multiplo di un primo $p \equiv 3 \pmod 4$, assurdo per il Lemma 1.a.