Hello !

1) $\boxed{p>2}$

$$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\dots\left(\frac{p-1}{p}\right)=0$$

- $\frac{p-1}{2}$ q. residuos and $\frac{p-1}{2}$ q. non residue mod p in $\{1,2,\dots,p-1\}$

$$\underbrace{\sum_{i\in QR}^{\frac{p-1}{2}}\left(\frac{i}{p}\right)}_{\underbrace{1+1+1\dots+}_{\frac{p-1}{2}}}+\underbrace{\sum_{j\in NQR}^{\frac{p-1}{2}}\left(\frac{j}{p}\right)}_{\underbrace{-1,-1\dots-1}_{\frac{p-1}{2}}}=\frac{p-1}{2}\cdot 1+\frac{p-1}{2}\cdot(-1)=0$$

$$\underline{\left(\frac{j}{p}\right)=-1}$$

Skanowano w CamScanner

2) $p \equiv 1 \pmod 4$

Sum of q.r. mod p is $\frac{p(p-1)}{4}$

k - q resoln the $p-k$ is also q.r.

$$\left(\frac{-k}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{k}{p}\right) \qquad \text{so} \left(\frac{p-k}{p}\right) = \left(\frac{-k}{p}\right) = \left(\frac{k}{p}\right)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$$

k is q.r. iff $p-k$ is q.r. too

$$p \equiv 1 \bmod 4 \Rightarrow \left(\frac{-1}{p}\right) = 1$$

$$-1 \equiv x^2 \pmod p \Leftrightarrow p \mid x^2+1$$

Fact $p \equiv 1 \bmod 4 \Rightarrow \exists\, n$ s.t. $p \mid n^2+1$

$\left(\frac{p-1}{2}\right)!$ Wilson

Skanowano w CamScanner

We prove k is QR iff $p-k$ is QR.

$a_1, a_2, \dots, a_{\frac{p-1}{2}} \rightarrow$ QR mod p in $\{1, 2, \dots, p-1\}$

$\frac{p-1}{4}$ pairs : $(a_i, \underbrace{p-a_i}_{a_j})$

in each pair the sum is $\boxed{a_i + p - a_i = p}$

Sum: $\boxed{\frac{p(p-1)}{4}}$

— $p > 3 \Rightarrow$ sum of all q. residues is divisible by p.

$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \pmod p$

so modulo p

Sum of QR $\equiv 1^2 + 2^2 + \dots + \left(\frac{p-1}{2}\right)^2 = \frac{p(p^2-1)}{24} \equiv 0$ mod p

$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Skanowano w CamScanner

$\underline{p = 4k+1}$

$p = a^2 + b^2$ for some a, b

Suppose a is odd.

Prove $\left(\frac{a}{p}\right) = 1$.

It is enough to prove that for any prime divisor $q \mid a$ $\left(\frac{q}{p}\right) = 1$.

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

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right)^{\alpha_1} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k} = \boxed{1}$$

Take $q \mid a$, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{2k \cdot \frac{q-1}{2}} = 1$ $\in \mathbb{Z}$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1$$

$$\left(\frac{p}{q}\right) = \left(\frac{a^2+b^2}{q}\right) = \left(\frac{a^2+b^2 \pmod q}{q}\right) \overset{(q \mid a)}{=} \left(\frac{b^2}{q}\right) = 1, \text{ so } \left(\frac{q}{p}\right) = 1$$

$\blacksquare$

Skanowano w CamScanner

3) $x_1 = 7, \quad x_{n+1} = 2x_n^2 - 1 \quad n \geq 1$

$2003 \nmid x_i$.

$\boxed{2003 \text{ is prime}}$

Suppose $2003 \mid x_{n+1}$

$2003 \mid 2x_n^2 - 1 \Rightarrow 2x_n^2 \equiv 1 \pmod{2003} \quad | \cdot 2$

$4x_n^2 \equiv 2 \pmod{2003}$

$\parallel$

$(2x_n)^2$

$\Rightarrow \left(\frac{2}{2003}\right) = 1$

$\lightning$

"2 is q.r. mod p iff $p \equiv \pm 1 \mod 8$"

$\left(\frac{2}{2003}\right) = (-1)^{\frac{2003^2-1}{8}} = -1$

Skanowano w CamScanner

p prime: Prove $\exists\, x \in \mathbb{Z}$ s.t. $p \mid x^2 - x + 3$ iff

$\exists\, y \in \mathbb{Z}$ s.t. $p \mid y^2 - y + 25$

$\exists_x \quad x^2 - x + 3 \equiv 0 \pmod{p}$ iff $\exists_y \quad y^2 - y + 25 \equiv 0 \pmod{p}$

$p > 2$ key

$4x^2 - 4x + 12 \equiv 0 \pmod{p}$

$(2x-1)^2 + 11 \equiv 0 \pmod{p}$ iff $\exists_y \quad 4y^2 - 4y + 100 \equiv 0 \pmod{p}$

$(2y-1)^2 \equiv -99 \pmod{p}$

$\downarrow$ QR $\qquad\qquad$ $\downarrow$ QR

$\left(\frac{-11}{p}\right) = 1$ iff $\left(\frac{-99}{p}\right) = 1$

$$\left(\frac{-99}{p}\right) = \left(\frac{-11}{p}\right) \cdot \left(\frac{9}{p}\right) = \left(\frac{-11}{p}\right) \cdot \underbrace{\left(\frac{3^2}{p}\right)}_{=1} = \left(\frac{-11}{p}\right)$$

$\blacksquare$

Skanowano w CamScanner

2^n+1 has no prime divisor of the form $\underline{8k-1}$.

$$2^n \equiv -1 \pmod{p}$$

$p = 8k-1$

<u>Next problem</u>:

$6 \mid p+1$, $p \mid a+b+c$, $p \mid a^4+b^4+c^4$ for some integers a, b, c.

Prove $p \mid a$, $p \mid b$, $p \mid c$.

- n is even $n = 2k$

$$2^{2k} \equiv -1 \pmod{p} \Rightarrow \underset{\substack{\uparrow \\ \text{square}}}{(2^k)^2} \equiv -1 \pmod{p} \rightsquigarrow \left(\frac{-1}{p}\right) = 1$$

$$(-1)^{\overset{\overset{8k-1-1}{\shortparallel}}{\frac{p-1}{2}}} = (-1)^{4k-1} = -1$$

$\lightning$

$2^n \equiv -1 \pmod p$ $\qquad$ $\underline{p = 8k-1}$.

n isod

$n = 2k+1$

$$2^{2k+1} \equiv -1 \pmod p \cdot 2$$

$$\left(2^{k+1}\right)^2 \equiv -2 \pmod p \implies \left(\frac{-2}{p}\right) = 1$$

$\uparrow$

squre

" $\left(\frac{-2}{p}\right) = 1$ iff $\quad p \equiv 1, 3 \mod 8$

<u>Baltic Way 2010</u>

Sypopne $\quad p \mid a \qquad 6 \mid p+1, \quad p \mid a+b+c$

$p \mid a^4+b^4+c^4$

$$\begin{cases} c \equiv -(a+b) \pmod p \\ c^4 \equiv -(a^4+b^4) \pmod p \end{cases} \qquad (a+b)^4 + a^4 + b^4 \equiv 0 \pmod p$$

$$\| \qquad 2(a^2+ab+b^2)^2$$

$$(a+b)^4 = (-a+b)^4 \equiv c^4 \equiv -(a^4+b^4) \pmod p$$

Skanowano w CamScanner

$$2(a^2+ab+b^2)^2 \equiv 0 \pmod{p} \implies \boxed{p \mid a^2+ab+b^2}$$

$$a^2+ab+b^2 \equiv 0 \pmod{p} \quad | \cdot 4$$

$$4a^2+4ab+4b^2 \equiv 0 \pmod{p}$$

$$\parallel$$

$$(2a+b)^2+3b^2 \equiv 0 \pmod{p}$$

$$(2a+b)^2 \equiv -3b^2 \pmod{p} \implies$$

if $p \nmid b$ then

$$\left(\frac{-3}{p}\right) = 1$$

iff

$$(p \equiv 1 \mod 6)$$

$$6 \mid p+1$$

← empty

↯

Clear?

Suppose $\boxed{p \nmid b}$

$$\left(\frac{-3b^2}{p}\right) = 1$$

$$\parallel$$

$$\left(\frac{-3}{p}\right) \cdot \left(\frac{b^2}{p}\right) = \left(\frac{-3}{p}\right)$$

$$\parallel$$

$$1$$

$\boxed{p \mid b}$

$p \mid a$, $p \mid c$

Skanowano w CamScanner

Theorem (Let c be integer which is not a ~~pri~~ square!

then there is prime p s.t $\left(\frac{c}{p}\right) = -1$.

Proof c, WLOG $c = p_1 p_2 \cdots p_n$ for some primes (Why?)

$c = p^2 \cdot c_2$ $\qquad p_1 < p_2 < \cdots < p_n$

$\left(\frac{c}{q}\right) = \left(\frac{c_2}{q}\right)$

- ~~[illegible]~~ $p_1 > 2$ Take $r_1, r_2, \ldots, r_n$ such that

$$\left(\frac{r_1}{p_1}\right) = -1 \qquad \left(\frac{r_2}{p_2}\right) = \left(\frac{r_3}{p_3}\right) = \cdots = \left(\frac{r_n}{p_n}\right) = 1$$

$p = Ak + p$

$\boxed{p = p_1 p_1 \cdots p_n \cdot 4 - k + \text{small}}$

$$\begin{cases} p \equiv r_1 \pmod{p_1} \\ p \equiv r_2 \pmod{p_2} \\ \vdots \\ p \equiv r_n \pmod{p_n} \\ p \equiv 1 \pmod{4} \end{cases}$$

By CRT there is such integer $\boxed{p}$.

By Dirichlet I can assume p is prime.

$\{am+b\}$ ∞ primes

$(a,b) = 1$

Skanowano w CamScanner

$$\left(\frac{p}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = \begin{cases} -1 & \text{if } i = 1 \\ 1 & \text{if } 2 \le i \le n \end{cases}$$

$p = 4k+1$

$(p \equiv r_i \pmod{p_i})$

Gauss law:

$$\left(\frac{p_i}{p}\right)\left(\frac{p}{p_i}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{p_i-1}{2}} = (-1)^{2k\cdot\frac{p_i-1}{2}} = 1 \quad \in \mathbb{Z}$$

so $$\left(\frac{p_i}{p}\right) = \begin{cases} -1 & \text{if } i = 1 \\ 1 & \text{if } 2 \le i \le n \end{cases}$$

$$\left(\frac{c}{p}\right) = \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_n}{p}\right) = (-1)\cdot 1\cdot 1\cdots 1 = \underline{-1}.$$

- $\underline{p_1 = 2}$ Choose $\left(\frac{r_i}{p_i}\right) = 1$ for $2 \le i \le n$

Skanowano w CamScanner

Choose $\left(\frac{r_i}{p_i}\right) = 1$ for $2 \le i \le n$ $\qquad c = 2 \cdot p_2 \cdot p_3 \cdots p_n$.

$$(*) \begin{cases} p \equiv r_2 \pmod{p_2} \\ p \equiv r_3 \pmod{p_3} \\ \vdots \\ p \equiv r_n \pmod{p_n} \\ p \equiv 5 \pmod 8 \end{cases}$$

By CRT + DIRICHLET I can find prime p such that $(*)$

$$\left(\frac{p}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = 1 \quad \text{for } 2 \le i \le n, \qquad p \equiv 8k+5$$

$$\left(\frac{p}{p_i}\right)\left(\frac{p_i}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{p_i - 1}{2}} = (-1)^{(4k+2) \cdot \frac{p_i - 1}{2}} = 1 \qquad \frac{p_i - 1}{2} \in \mathbb{Z}.$$

so $\left(\frac{p_i}{p}\right) = 1$ for $2 \le i \le n$, so

$$\left(\frac{c}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p_2}{p}\right) \cdots \left(\frac{p_n}{p}\right) = \left(\frac{2}{p}\right) \cdot 1 \cdot \ldots \cdot 1 = \left(\frac{2}{p}\right) = -1 \quad \star$$

Skanowano w CamScanner

For any c - integer there are infinitely many primes p s.t

$$\boxed{\left(\frac{c}{p}\right) = -1}$$

if you want prove that integer A is square then.
it is enough to prove that $\left(\frac{A}{p}\right) = 1$ for sufficiently large prime p

for some M and $p > M$ $\left(\frac{A}{p}\right) = 1$, but

<u>Problem</u>

$a, b \in \mathbb{Z}$ such that $a \neq 0$ and

$$6a \mid 3 + a + b^2.$$

<u>Polis Final 2016</u>

Prove $a < 0$.

<u>Problem A(i)</u> n - integer. Prove that any prime divisor of $n^4 - n^2 + 1$ is of the form $12k+1$

Skanowano w CamScanner

$a, b \in \mathbb{Z}$, $a \neq 0$, $6a \mid 3 + a + b^2$. Prove $a < 0$.

$$3 + a + b^2 = 6a \cdot k$$

$$\underbrace{3 + b^2}_{>0} = \underset{\substack{\vee \\ 0}}{a}(6k - 1) \qquad k > 0$$

Suppose $a > 0$ so

$6k - 1$ has a prime divisor of the form $\overset{q}{\overset{\shortparallel}{6\ell + 5}}$ (why?)

$4k + 3$

$$6k - 1 = \underbrace{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}_{6k+1} \qquad \underbrace{q_1^{\beta_1} \cdots q_\ell^{\beta_1}}_{6\omega + 5} \quad 6B + 1$$

$q \mid 3 + b^2$

so

$\underline{\beta_i \geq 1}$ $\qquad 6A + 1$

$3 + b^2 \equiv 0 \pmod{q}$

$(6\omega + 5)(6\omega + 5) = 6C + 1$

$\left(\frac{-3}{q}\right) \equiv 1$ $\underline{\text{iff}}$ $q \equiv 1 \pmod{6}$

Skanowano w CamScanner

$$p \mid n^4 - n^2 + 1 \implies p = 12k+1$$

$$n^4 - n^2 + 1 = (n^2-1)^2 + n^2 = (n^2+1)^2 - 3n^2$$

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

$$p \equiv (1 \bmod 4)$$

$$(n^2+1)^2 \equiv 3n^2 \pmod p \quad \Big| \cdot (n^{-1})^2 \bmod p$$

$$(n, n^2+1) = 1$$

$$\left((n^2+1)\cdot n^{-1}\right)^2 \equiv 3 \bmod p$$

$$\Downarrow$$

$$\underline{\left(\frac{3}{p}\right) = 1} \quad \text{if} \quad p \equiv \pm 1 \bmod 12$$

$$\Downarrow$$

$$p \equiv 1 \pmod{12}$$

Ex. 1 - 2.

Skanowano w CamScanner

$p = 1 \bmod 4 \implies p = a^2 + b^2$

$p \equiv 1 \pmod 3$

if $p \equiv 1 \pmod 3 \implies$ Yesterday Problem $\left(\frac{-3}{p}\right) = 1$ $\quad -3 = n^2 \pmod p$ for some n.

Thue Lemma: $(a, n) = 1$ then $\exists$

$0 < x, y \leq \sqrt{n}$ s.t. $ax \equiv \pm y \pmod n$

$-3 \equiv n^2 \pmod p$ so $(n, p) = 1$

therefore by Thue Lemma there are

$0 < x, y < \sqrt{p}$ $\in \mathbb{Z}$. s.t. $(nx)^2 \equiv (\pm y)^2 \pmod p$

$-3x^2 \equiv n^2x^2 \equiv y^2 \pmod p$ so $p \mid 3x^2 + y^2$ but

$0 < 3x^2 + y^2 < 3(\sqrt{p})^2 + (\sqrt{p})^2 = 4p$. SO

$3x^2 + y^2 \in \{p, 2p, 3p\}$.

Skanowano w CamScanner

1) Suppose

$$3x^2+y^2=p \Rightarrow p = 3x^2+y^2 = (y-x)^2 + (y-x)\cdot 2x + (2x)^2$$

$$A^2 + A\cdot B + B^2$$

2) $3x^2+y^2=2p \Rightarrow x, y$ have the same parity, in particula

$$4 \mid 3x^3+y^2 \Rightarrow 4 \mid 2p \Rightarrow 2 \mid p \quad ↯$$

3) $3p = 3y^2+x^2 \Rightarrow 3 \mid x \Rightarrow x = 3x_1 \Rightarrow$

$$3p = 3y^2+9x_1^2 \Rightarrow p = y^2+3x_1^2$$

$$\downarrow$$

Cas 1

so $p = C^2+CD\cdot D^2$

Conclusion: if $p \equiv 1 \pmod 3$ then

$$p = A^2+AB+B^2 \text{ for some } A, B.$$

Ex. $7 = 2^2+2\cdot 1+1^2$.

Skanowano w CamScanner

$p>2$, $\boxed{p = x^2+xy+y^2}$ for some x, y.

$p=3 \rightsquigarrow$ $\underline{x\ y = 1}$

$$p \mid 4x^2+4xy+4y^2 = (2x+y)^2 + 3y^2$$

$$\Downarrow$$

$$\left(\frac{-3}{p}\right) = 1 \rightsquigarrow p \equiv 1 \pmod 3$$

$$\boxed{p = x^2+xy+y^2 \text{ iff } p=3 \text{ or } p \equiv 1 \bmod 3}$$

<u>What NOW</u> Deadline will be Sunday <u>23:59.</u>

Skanowano w CamScanner