HELLO

$$a^2+b^2=c^2+d^2$$

PROBLEM 47

$$x^3-9=y^2 \qquad x^3=y^2+9$$

if y is odd then x is even but then

$$y^2+9\equiv 2 \pmod 4, \quad x^3\equiv 0 \pmod 4$$

So y is even. Therefore $y^2+9\equiv 1 \pmod 4$, so

$$\underset{x^3}{\overset{\shortparallel}{y^2+9}}\equiv 1 \pmod 4$$

$x\equiv 1 \pmod 4$. but

$$\boxed{y^2+1=x^3-\underset{2^3}{\overset{\shortparallel}{8}}}$$

so

$x-2 \mid y^2+1^2$, but $x-2\equiv 1-2\equiv 3 \pmod 4$

YIN

Scanned with CamScanner

$\boxed{48}$ Prove that n is sum of 2 squares of integers $\Longleftrightarrow$ is sum of 2 squares of rationals. ②

if $n = \underset{\mathbb{Z}}{\underset{\cap}{a^2}} + \underset{\mathbb{Z}}{\underset{\cap}{b^2}} \Rightarrow n = \underset{\mathbb{Z} \subseteq \mathbb{Q}}{\underset{\cap}{a^2}} + \underset{\mathbb{Z} \subseteq \mathbb{Q}}{\underset{\cap}{b^2}}$.

We can assume that $n = q_1^2 + q_2^2$, $q_1, q_2 \in \mathbb{Q}$

also $q_1 = \frac{a}{b}$, $q_2 = \frac{c}{b}$, $a, b, c \in \mathbb{Z}$.

$\left(\frac{1}{7}, \frac{3}{5} \rightarrow \frac{5}{35}, \frac{21}{35} \right)$

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{b}\right)^2 = \frac{a^2 + c^2}{b^2} \Rightarrow$$

$$\boxed{n \cdot b^2 = a^2 + c^2} \Rightarrow n = x^2 + y^2 \ ?$$

Scanned with CamScanner

Problem 49 Prove that

$$\frac{x^2+1}{y^2-5} \notin \mathbb{Z} \quad \text{where} \quad x, y > 2.$$

3

- if y is even, then $y^2-5 \equiv 3 \pmod 4$, so

$$y^2-5 \nmid x^2+1. \quad p \mid x^2+1 \Rightarrow p \mid x, \; p \mid 1$$

if y is odd then $y^2-5 \equiv 0 \pmod 4$ so $4 \mid y^2-5$, so

$$4 \mid x^2+1 \Rightarrow \text{impossible} \quad \boxed{x^2 \not\equiv 0 \text{ or } 3 \bmod 4}$$

$$\lightning$$

$$y^2-5 \nmid x^2+1$$

Scanned with CamScanner

<u>Theorem</u>
(Monday)

$$n = x^2 + y^2 \iff v_p(n) \text{ is even when } p \equiv 3 \pmod 4$$

$$n \cdot b^2 = a^2 + c^2$$

Take any prime $p \mid n$ s.t. $n \equiv 3 \pmod 4$. Then

$$v_p(n \cdot b^2) = v_p(a^2 + c^2)$$

$$\parallel$$

$$v_p(n) + \underbrace{2 \cdot v_p(b)}_{\text{even}} = \underbrace{v_p(a^2 + c^2)}_{\text{even by Theorem}}$$

so $v_p(n)$ is even $\Rightarrow$ by theorem $n = x^2 + y^2$ $\blacksquare$

Scanned with CamScanner

50] We know that $p = 4k+1 \Rightarrow p = a^2+b^2$, you need to prove that if $p = a^2+b^2 = c^2+d^2$ then

$$\{a,b\} = \{c,d\}.$$

5

HINT! In november camp 2018, we had the following lemma

<u>Lemma</u> (4 number lemma) if integers $ab = cd$ then $a = kl$, $b = mn$, $c = km$, $d = nl$ for some k, l, m, n, integers.

$$a^2+b^2 = c^2+d^2, \quad a,b,c,d > 0$$

$$x^2 = (|x|)^2$$

$$a^2 - c^2 = d^2 - b^2$$

$$\underset{A}{(a-c)}\underset{B}{(a+c)} = \underset{C}{(d-b)}\underset{D}{(d+b)}$$

Scanned with CamScanner

$$a^2 - c^2 = d^2 - b^2 \qquad P = a^2 + b^2 = c^2 + d^2$$

$$\parallel$$

$$(a-c)(a+c) = (d-b)(d+b)$$

6

$$a - c = mn, \quad a + c = pq, \quad d - b = mp, \quad d + b = nq$$

$$\begin{cases} a - c = mn \\ a + c = pq \\ d - b = mp \\ d + b = nq \end{cases} \quad \begin{array}{l} \Rightarrow a = \dfrac{mn + pq}{2} \\ \\ \Rightarrow b = \dfrac{nq - mp}{2} \end{array}$$

OK?

$$p = a^2 + b^2 = \left(\frac{mn + pq}{2}\right)^2 + \left(\frac{nq - mp}{2}\right)^2 = \frac{(m^2 + q^2)(n^2 + p^2)}{4} \Rightarrow$$

$$\Rightarrow \quad 4 \cdot P = (m^2 + q^2)(n^2 + p^2) \Rightarrow P \mid m^2 + q^2, \text{ so}$$

$$n^2 + p^2 = 1, 2, 4$$

Scanned with CamScanner

$$p = a^2 + b^2 = c^2 + d^2$$

$$a^2 - c^2 = d^2 - b^2 \Rightarrow \underset{kl}{\underset{\parallel}{(a-c)}}\underset{mn}{\underset{\parallel}{(a+c)}} = \underset{km}{\underset{\parallel}{(d-b)}}\underset{ln}{\underset{\parallel}{(d+b)}}$$

7

$$\begin{cases} a-c = kl \\ a+c = \pm mn \\ d+b = \pm ln \\ d-b = \pm km \end{cases} \Rightarrow \quad a = \frac{kl+mn}{2}, \quad b = \frac{ln-km}{2} \Rightarrow$$

$$\Rightarrow \quad p = a^2+b^2 = \left(\frac{kl+mn}{2}\right)^2 + \left(\frac{ln-km}{2}\right)^2 = \frac{(k^2+n^2)(l^2+m^2)}{4}$$

$4p = (k^2+n^2)(l^2+m^2) \Rightarrow$ WLOG $p \mid k^2+n^2$, so

$l^2+m^2 \mid 4 \Rightarrow l^2+m^2 = 1, 2, 4$, if

$l^2+m^2 = 1 \rightsquigarrow$ some of l, m is $0 \Rightarrow$ 4

$l^2+m^2 = 4 \rightsquigarrow$ ~~l, m~~ no possible no

$l^2+m^2 = 2 \Rightarrow l, m = \pm 1$

Scanned with CamScanner

so $(a-c) = \pm(d-b)$
$(a+c) = \pm(d+b)$ $\Rightarrow$ $\{a, b\} = \{c, d\}$ $\boxtimes$

(8)

<u>Problem 51</u> there are infinitely many consecutive pairs:

$$(A, A+1)$$

A and $A+1$ has no divisor of the form $4k+3$.

For Abdulelah: Find all n such that $2^n - 1$ has a multiply of the form m^2+9.

$$2^n - 1 \mid m^2+9 \text{ for some } m.$$

<u>Problem 51</u> Omar: $p = 4k+1$, $(2^n, 2^n+1)$ when n is even

∞ (p^2, p^2+1) $(2^{\frac{n}{2}})^2+1^2$, $((n^2+1)^2, (n^2+1)^2+1)$

Scanned with CamScanner

Quadratic residues

Take a prime $\boxed{p>2}$, we are interested in solutions of the congruence $x^2 \equiv a \pmod{p}$ for fixed integer a. (a)

Definition • a is quadratic residue $\pmod{p}$ iff $\exists\, x \in \mathbb{Z}$ s.t

$$a \equiv x^2 \pmod{p}$$

For example 2 is quadratic residue modulo 7. Why

$$2 \equiv 3^2 \pmod{7}$$

• a is <u>not</u> quadratic residue iff it is <u>not</u> quadratic residue

For example

3 is not quadratic residue $\pmod{7}$

$$3 \equiv x^2 \pmod{7} \qquad 0, 1, 4, 2$$

Scanned with CamScanner

<u>Definition</u> (Legendre's symbol). Take prime p, and a - integer:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue} \\ -1 & \text{if } a \text{ is not quadratic residue} \\ 0 & \text{if } p \mid a. \end{cases}$$

(2)

so $\left(\frac{2}{7}\right) = 1$ because 2 is quadratic residue mod 7

$\left(\frac{3}{7}\right) = -1$ because 3 is not quadratic residue (mod 7)

$\left(\frac{14}{7}\right) = 0 \Leftarrow 7 \mid 14.$

$a \equiv x^2 \mod p$

Scanned with CamScanner

When we proved <u>step 1</u> in Fermat theorem about sum of squares.

<u>Step 1</u> was For any prime $p \equiv 1 \pmod 4$ $\exists$ n such that

$p \mid n^2+1 \rightsquigarrow n^2 \equiv -1 \pmod p$ $\Leftarrow$

if $p = 4k+1 \Rightarrow \left(\frac{-1}{p}\right) = 1.$

<u>Exercus</u>

$-1 = \left(\frac{3}{5}\right)$, $-1 = \left(\frac{2}{11}\right)$, $\left(\frac{-1}{5}\right) = 1$

$3 \equiv x^2 \pmod 5$

$x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$0 \quad 1 \quad 4 \quad 4 \quad 1$

$4 = -1 \equiv x^2 \pmod 5$

$x = 2 \quad 4 \equiv -1 \pmod 5$

$2 \equiv x^2 \pmod{11}$

$81 = -7 = 2$

$x^2 = 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$0 \quad 1 \quad 4 \quad 9 \quad 5 \quad 3 \quad 3 \quad 5 \quad 9 \quad 4 \quad 1$

$x^2 \equiv 0, 1, 4$

$\neq \quad \neq \quad \neq 11$

$-1 \quad -1 \quad -1$

Scanned with CamScanner

$\left(\frac{a}{p}\right)$ is difficult by checking residue

$\boxed{p > 2}$

$\left(\frac{37}{1999}\right) \rightsquigarrow x^2 \equiv 37 \ (1999)$

1999 cases!

$\left(\frac{2}{11}\right) = -1$

$-1 \equiv 2^{\frac{11-1}{2}} \pmod{11}$

$2^5 \equiv -1 \pmod{11}$

$32 + 1$

Properties

- $\left(\frac{x^2}{p}\right) = \begin{cases} 1 & \text{if } p \nmid x \\ 0 & \text{if } p \mid x \end{cases}$

- $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ (Euler Criterion)

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

$\left(\frac{2}{11}\right) = -1$

$-1 = \left(\frac{2}{11}\right) \equiv 2^{\frac{11-1}{2}} \pmod{11}$

$\overset{\shortparallel}{32}$

Scanned with CamScanner

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

STEP 1

$p = 4k+1$ the $p \mid n^2+1$

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

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

For example if $p = 4k+1$ then

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

13

if $p = 4k+3$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} \equiv -1.$$

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

$$\left(\frac{a}{p}\right) = \left(\frac{a \pmod{p}}{p}\right)$$

Scanned with CamScanner

<u>Theorem</u> (Gauss's Reciprocity Law) For any odd different primes p, q we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

- There are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non residues in $\{1, 2, \dots, p-1\}$ mod p.

$p = 19$

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\begin{array}{cccccc} 1 & & 3 & 4 & 5 & 9 \\ \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow \\ 9 & & 5^2 \equiv 3 & 9 & 4^2 \equiv 5 & 9 \end{array}$$

q. r. $1, 3, 4, 5, 9 \rightarrow 5$

q nr. $2, 6, 7, 8, 10 \rightarrow 5$

Scanned with CamScanner

For example $814 = 2 \cdot 11 \cdot 37$

$$\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right) \cdot \left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right) = -1 \cdot -1 \cdot (-1) = -1$$

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

$$\left(\frac{11}{2003}\right) = \left(\frac{2003}{11}\right)^{=1} = (-1)^{\frac{11-1}{2} \cdot \frac{2003-1}{2}} = (-1)$$

$$\left(\frac{2003}{11}\right) = \left(\frac{2003 \pmod{11}}{11}\right) = \left(\frac{1^2}{11}\right) = 1$$

$$\left(\frac{11}{2003}\right) = -1$$

Scanned with CamScanner

$$\left(\frac{3\cdot 7}{2003}\right)\left(\frac{2003}{3\cdot 7}\right)^{-1} = (-1)^{\frac{37-1}{2}\cdot\frac{2003-1}{2}} = 1$$

$$\Downarrow$$

$$\left(\frac{2003}{37}\right) = \left(\frac{\overset{1998}{2003} \pmod{37}}{37}\right) = \left(\frac{5}{37}\right) = -1$$

$$\left(\frac{5}{37}\right)\left(\frac{37}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}} = 1$$

$$\left(\frac{37}{5}\right) = \left(\frac{37 \bmod 5}{5}\right) = \left(\frac{2}{5}\right) = -1 \Rightarrow$$

so

$$\left(\frac{37}{2003}\right) = -1 \qquad \text{so}$$

10

Scanned with CamScanner

Compute

$$\left(\frac{2020}{1013}\right) = \left(\frac{2020 \pmod{1013}}{1013}\right) = \left(\frac{-6}{1013}\right) = \pm$$

$$= \left(\frac{-1}{1013}\right) \cdot \left(\frac{2}{1013}\right)\left(\frac{3}{1013}\right)^{-1} = 1 \cdot (-1) \cdot (-1) = 1$$

$$\left(\frac{-1}{1013}\right) = (-1)^{\frac{1013-1}{2}} \cdot (-1)^{\frac{1013^2-1}{8}} = -1$$

odd

$$(-1)^{\frac{1013-1}{2}} = 1$$

even

$$\left(\frac{3}{1013}\right)\left(\frac{1013}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{1013-1}{2}} = 1$$

$$(-1)$$

$$\left(\frac{1013}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$$

Scanned with CamScanner