Hello !

1) $x_1, x_2, \dots, x_n \geq 0$

$$x_1 + 2x_2 + \dots + n x_n \leq \binom{n}{2} + x_1 + x_2^2 + \dots + x_n^n$$

$$\binom{n}{2} = [1+2+\dots+n-1]$$

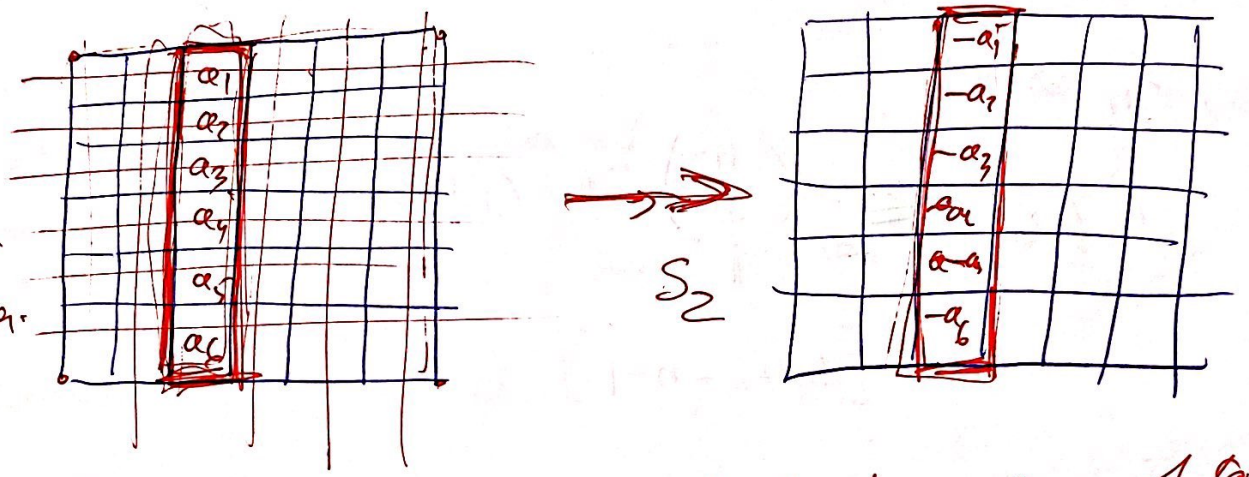
$$+\begin{cases} x_1 \geq x_1 \\ x_2^2 + 1 \geq 2x_2 \\ x_3^3 + 2 = x_3^3 + 1 + 1 \geq 3x_3 \\ x_4^4 + 3 = x_4^4 + 1 + 1 + 1 \geq 4x_4 \\ \vdots \\ x_n^n + n - 1 = x_n^n + \underbrace{1 + 1 + \dots + 1}_{n-1} \geq n \cdot \sqrt[n]{x_n^n \cdot \underbrace{1 \cdot 1 \cdots 1}_{n-1}} = n \cdot x_n \end{cases}$$

STATEMENT.

Skanowano w CamScanner

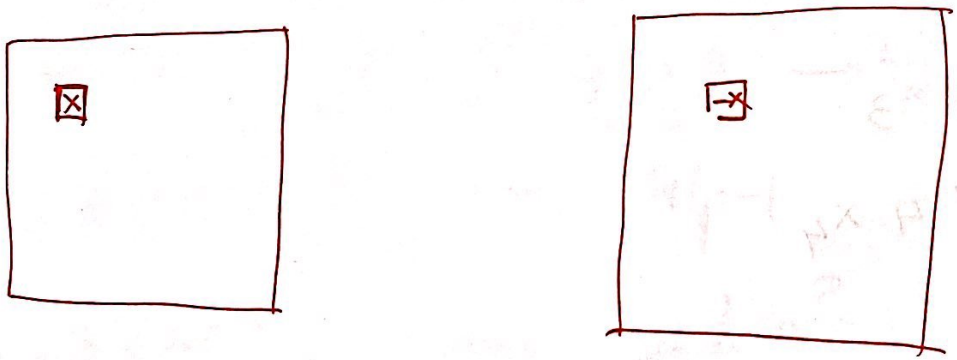
2) 2020×2020 table filled by reals

S - sum of all 2020^2 numbers.



$$\boxed{S_2 > S}$$

1 move is to change sign of numbers in 1 column or row.



$$2^{2020^2} < +\infty$$

Cannot make ∞ moves because S takes only finitely many values.

3) Find all primes p, q, r s.t $p^3 = p^2 + q^2 + r^2$

$3^3 = 3^2 + 3^2 + 3^2$

- if p, q, r are not multiples of 3

$p^3 = p^2 + q^2 + r^2 \equiv 1 + 1 + 1 \pmod 3 \Rightarrow p = 3$ ↯

so one number p, q, r is 3.

- Suppose $\boxed{p = 3}$ $\quad 27 = 9 + q^2 + r^2 \Rightarrow q^2 + r^2 = 18 \Rightarrow \underline{q = r = 3}$.

- WLOG $\boxed{r = 3}$ $\quad p^3 = p^2 + q^2 + 9 \rightsquigarrow 4 \mid p^2(p-1) = q^2 + 9 = q^2 + 3^2$

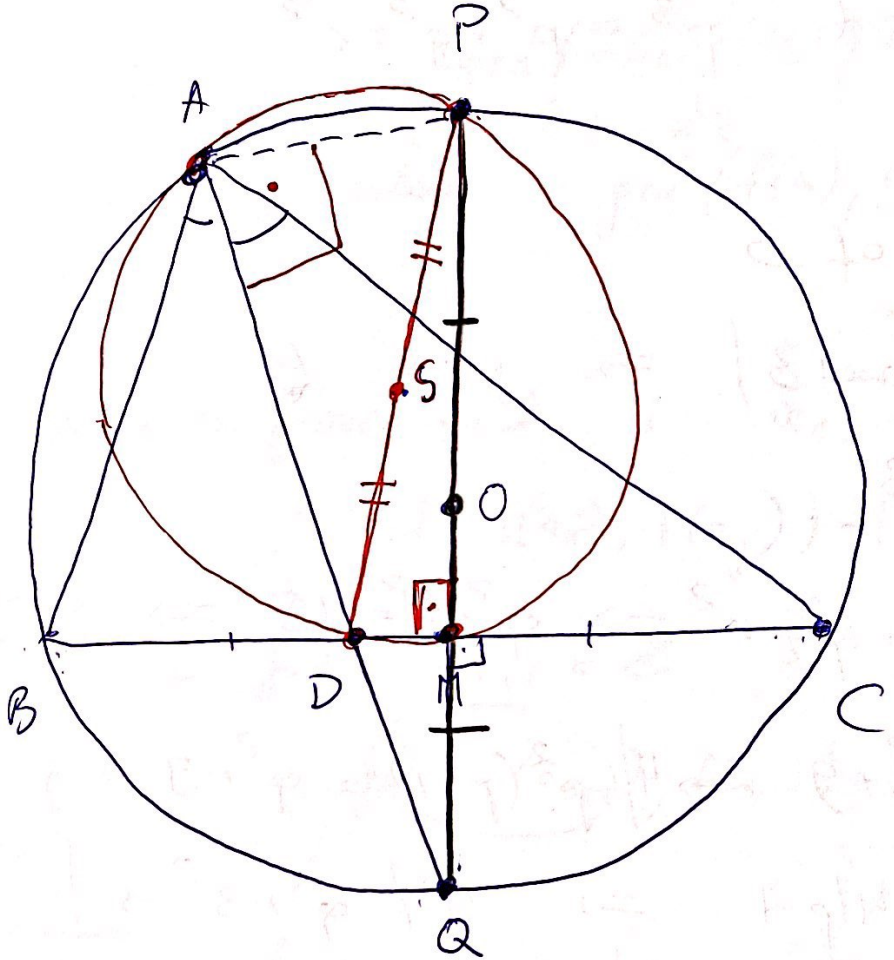
if $p \equiv 1 \pmod 4$ then $4 \mid p-1 \Rightarrow 4 \mid q^2 + 3^2 \Rightarrow \boxed{q^2 \equiv 3 \bmod 4}$

so $p \equiv 3 \pmod 4$, then $p \mid q^2 + 3^2 \Rightarrow p \mid q$ or $p \mid 3$ so

$\underline{p = q = 3}$ $\quad \underline{(3, 3, 3)}$.

Skanowano w CamScanner

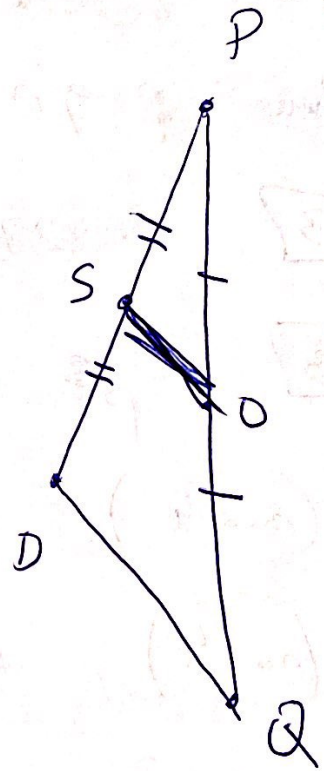
4)



M – midpoint of BC

S – circumcenter of ΔADM

Then $\underline{OS \parallel AD}$.



$\underline{SO \parallel DQ}$

Skanowano w CamScanner

29) $f \in \mathbb{Z}[x]$ $\quad \gcd(f(a), f(b)) = 1 \Rightarrow \exists$ set S s.t

$|S| = +\infty$ of integers $\quad \gcd(f(u), f(v)) = 1$. $\quad$ Polish Final 2004/3.

<u>Proof</u>

It suffices to prove that if $a_1, \dots, a_k$ integers s.t

$$\gcd(f(a_i), f(a_j)) = 1 \quad \text{for} \quad 1 \le i \ne j \le k$$

then we can find $a_{k+1} \in \mathbb{Z}$ s.t $\quad a_{k+1} \ne a_i$

$$\gcd(f(a_{k+1}), f(a_i)) = 1 \quad \text{for any} \quad i \in \{1 \dots k\}.$$

a, b, c

$$\begin{cases} a_{k+1} \equiv a_1 \pmod{\boxed{f(a_2)}} \\ a_{k+1} \equiv a_2 \pmod{\boxed{f(a_3)}} \\ a_{k+1} \equiv a_3 \pmod{\boxed{f(a_4)}} \\ \vdots \\ a_{k+1} \equiv a_{k-1} \pmod{\boxed{f(a_k)}} \\ a_{k+1} \equiv a_k \pmod{\boxed{f(a_1)}} \end{cases}$$

By CRT I can find such a_{k+1}

$f(a_{k+1}) \equiv f(a_i) \mod f(a_{i+1})$

$1 \le i < k$

$(a - b \mid f(a) - f(b))$

Skanowano w CamScanner

$$f(a_{k+1}) \equiv f(a_i) \pmod{f(a_{i+1})} \qquad 1 \le i < k$$

$$f(a_{k+1}) \equiv f(a_k) \pmod{f(a_1)}$$

Euclid Algorithm

so

$$\boxed{\gcd\left(f(a_{k+1}), f(a_{i+1})\right) = \gcd\left(f(a_i), f(a_{i+1})\right) = 1}$$

and similarly

$$\gcd\left(f(a_{k+1}), f(a_1)\right) = \gcd\left(f(a_k), f(a_1)\right) = 1.$$

Recall $(a,b)=1 \Rightarrow$ in arithmetic progression $\{an+b\}$ $\exists$ infinitely many pairwise coprime numbers

Easy consequence of Dirichlet theorem $(a,b)=1$ the there exists infinitely many primes of the form $an+b$

Problem 31

For any $n \geq 0$ there are pairwise coprime $k_0, k_1 \dots k_n > 1$ s.t.

$$k_0 k_1 \cdots k_n - 1 = t(t+1) = f(t) \qquad t^{2010} + t^{942} - 16$$

$$k_0 k_1 \cdots k_n = \boxed{t^2+t+1}$$

Prove ~~t^2+t+1~~ there are infinitely many t's s.t

t^2+t+1 has at least $n+1$ prime divisors.

$\boxed{P(X) = X^2+X+1}$

$\exists t$

$\geq n+1$

$$t^2+t+1 = \underbrace{\boxed{p_1^{\alpha_1}}}_{k_0} \underbrace{\boxed{\cdots}}_{k_1} \underbrace{\boxed{p_{n+1}^{\alpha_k} \; q_1^{\beta_1} \cdots q_\omega^{\beta_\omega}}}_{k_n}$$

But $f \in \mathbb{Z}[X]$ n, k there is a s.t

$f(a), f(a+1) \dots f(a+n-1)$ has at least k distinct prime divisors

APMO 2009

Prove that for any positive integer k, there exists an arithmetic progression

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_k}{b_k}, \quad a_i \in \mathbb{Q}$$

s.t. $\gcd(a_i; b_i) = 1$, $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ are all distinct.

$k \geq 2$ take primes

$$k < p_k < \dots < p_2 < p_1, \quad N = p_1 p_2 \cdots p_k.$$

$$\begin{cases} x \equiv -1 \pmod{p_1} \\ x \equiv -2 \pmod{p_2} \\ \vdots \\ x \equiv -k \pmod{p_k} \end{cases}$$

By CRT $\exists!$ such x mod N

$$\boxed{x > N^2}$$

Skanowano w CamScanner

$$\frac{x+1}{N}, \frac{x+2}{N}, \dots, \frac{x+k}{N} \leftarrow \underline{\text{arithmetic progression}}$$

$\frac{1}{N}$

$p_i \mid x+i$ not divisible by p_j for $j \neq i$ (Why?)

$p_i, p_j \mid x+i$ $\quad p_j \mid x+j \Rightarrow p_j \mid |i-j|$ but

$$|i-j| < k < p_j \quad ↯$$

$$a_i = \frac{x+i}{p_i} \in \mathbb{Z} \qquad b_i = \frac{N}{p_i} = \prod_{k \neq i} p_k \in \mathbb{Z}.$$

$$\frac{x+i}{N} = \frac{a_i}{b_i}, \quad \gcd(a_i, b_i) = 1$$

<u>Moreover</u> for $j > i$

$$a_j = \frac{x+j}{p_j} > \frac{x+i}{p_j} > \frac{x+i}{p_i} = a_i \quad \text{so } a_i \neq a_j$$

Skanowano w CamScanner

$$a_i = \frac{x+i}{p_i} > \frac{N^2}{p_i} > N > \frac{N}{p_j} = b_j \quad \text{for all } i, j$$

$(x > N^2)$ $\quad (N = \prod p_i)$

a_i and b_j are different

$$b_i \neq b_j$$

$$\frac{N}{p_i} \neq \frac{N}{p_j}$$

$\boxed{2^{nd} \text{ solution}}$

$k \geq 2$

$$\frac{(k!)^2+1}{k!}, \quad \frac{(k!)^2+2}{k!}, \quad \ldots \quad \frac{(k!)^2+k}{k!}$$

$$a_i = \frac{(k!)^2+i}{i} \qquad b_i = \frac{k!}{i} \qquad \text{gcd}(a_i, b_i) = 1$$

$$b_i \neq b_j$$

$j > i$

$$\boxed{a_i} = \frac{(k!)^2+i}{i} > \boxed{a_j} = \frac{(k!)^2+j}{j} > \frac{k!}{i} = \boxed{b_i} > \boxed{b_j} = \frac{k!}{j} \quad \text{and different}$$

Skanowano w CamScanner

4) Find all positive integer n s.t. there is m s.t

$$\boxed{2^n - 1 \mid m^2 + 9}$$

<u>Proof</u> <u>$n=1$</u> ✓ Assume $n \geq 2$ and $\underline{2^n - 1 \mid m^2 + 9} = m^2 + 3^2$ so

$2^n - 1$ cannot have a prime divisor $p > 3$ $p \equiv 3 \pmod 4$

if n has odd divisor $d > 1$ then

$$\underline{2^d - 1 \mid 2^n - 1} \quad \left(\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1 \right)$$

so

$$2^d - 1 \mid m^2 + 9 = m^2 + 3^2 \quad \text{but} \quad \underbrace{2^d - 1}_{3 \bmod 4} \equiv -1 \bmod 4$$

$$\cancel{2^{2k+1} \equiv 2 \bmod 3}$$

$$\cancel{2^{2k+1} - 1 \equiv 1 \bmod 3}$$

$$3 \nmid 2^d - 1$$

$$\Longrightarrow \boxed{n = 2^k}$$

Skanowano w CamScanner

I will prove that if $n = 2^k$ then I can find m s.t.

$$2^n - 1 \mid m^2 + 9$$

$$2^n - 1 = \overset{(2-1)}{(2+1)}(2^2+1)(2^4+1)\cdots(2^{2^{k-1}}+1)$$

$(2-1)(2+1) = 2^2 - 1$

$(2^2-1)(2^2+1) = 2^4 - 1 \ldots$

~~take~~ take $m = 3a$, $2^n - 1 \mid 9a^2 + 9 = 9(a^2+1)$

I need to find a s.t. $2^n - 1 \mid a^2 + 1$

$\gcd\left(2^{2^i}+1,\ 2^{2^j}+1\right) = 1$. Why? $j > i$

d - common divisor of $2^{2^i}+1$, $2^{2^j}+1$ d is odd

$2^{2^i} \equiv -1 \mod d$ $\quad \left(2^{2^i}\right)^{2^{j-i}} \equiv (-1)^{2^{j-i}} = 1 \mod d$

$-1 \equiv 2^{2^j} = 1 \mod d$ ↯

Skanowano w CamScanner

By CRT

$$a \equiv 2^{2^{i-1}} \pmod{2^{2^i}+1} \quad \text{for } i = 1 \dots k-1$$

IMO 1999 Shortlist

then

$$a^2+1 \equiv 0 \mod (2^{2^i}+1)$$

$$\parallel$$

$$(2^{2^{i-1}})^2+1 = 2^{2^i}+1 \equiv 0 \mod (2^{2^i}+1)$$

so

$$\prod (2^{2^i}+1) \mid a^2+1$$

$$\boxed{m! = 3g}$$

$$(2+1)(2^2+1) \dots (2^{2^{k-1}}+1) \mid a^2+1$$

$$\parallel$$

$$2^n-1 = 2^{2^k}-1 \mid a^2+1 \rightsquigarrow 2^n-1 \mid 9a^2+9 = m^2+9$$

done.

Skanowano w CamScanner

Quadratic residues

Assume $p > 2$

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

$p = 3$

$x^2 \equiv 1 \pmod{3} \rightsquigarrow x = 1$

$x^2 \equiv -1 \pmod{3} \rightsquigarrow$ no such x.

$-x$

Definition Let $p > 2$ odd prime. Then a is $\boxed{\text{quadratic residue}}$ iff $\exists\, x$ s.t. $x^2 \equiv a \pmod{p}$

a is $\boxed{\text{quadratic nonresidue}}$ iff is not quadratic residue

1 is q.r. -1 is not q.r. modulo 3.

Definition (Legendre Symbol)

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

Skanowano w CamScanner

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

$$3 \equiv x^2 \mod 5$$

$x = 0, 1, 2, 3, 4$

$0, 1, 4, 4, 1$

$$\left(\frac{-1}{7}\right) = -1$$

$$-1 \equiv x^2 \mod 7$$

$$7 \mid x^2 + 1 \rightsquigarrow 7 \mid x \wedge 7 \mid 1 \quad ↯$$

$$\cancel{\left(\frac{673}{2017}\right)} = \left(\frac{a}{p}\right)$$

$$\left(\frac{a}{p}\right) \qquad x^2 \equiv a \mod p$$

$\{1, 2, \ldots,$

$1, 2, \boxed{3}, 4, \boxed{5}, \boxed{6}$

$$3^2 \equiv 2 \mod 7$$

Skanowano w CamScanner

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

2) there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues in set $\{1, 2, \dots, p-1\}$ modulo p.

3) <u>Euler criterion</u>

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

$\left(\begin{array}{l} a \equiv x^2 \\ a^{\frac{p-1}{2}} = x^{p-1} = 1 = \left(\frac{x^2}{p}\right) \end{array} \right.$ mod p.

4) $\left(\frac{x^2}{p}\right) = 1$ $\quad (x^2 \equiv y^2 \bmod p)$

5) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ for any a, b $(p > 2)$

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

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

Skanowano w CamScanner

8) (Theorem Gauss reciprocity law) for any odd p, q distinct primes

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

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

<u>Example</u>

$$\left(\frac{-12000}{821}\right) = \left(\frac{-12000 \bmod 821}{821}\right) = \left(\frac{315}{821}\right) =$$

$$= \left(\frac{5 \cdot 63}{821}\right) = \left(\frac{5 \cdot 9 \cdot 7}{821}\right) = \left(\frac{5}{821}\right)\left(\frac{7}{821}\right)\left(\frac{9}{821}\right)$$

$$\left(\frac{9}{821}\right) = \left(\frac{3^2}{821}\right) = 1$$

$$= 1 \cdot 1 \cdot 1 = \boxed{1}$$

Skanowano w CamScanner

You are left with

$$\left(\frac{5}{821}\right)\left(\frac{821}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{821-1}{2}} = (-1)^{820} = 1$$

$$\left(\frac{821}{5}\right) = \left(\frac{821 \bmod 5}{5}\right) = \left(\frac{1}{5}\right) = \left(\frac{1^2}{5}\right) = 1$$

so $\left(\frac{5}{821}\right) = 1$

$$\left(\frac{7}{821}\right)\cdot\left(\frac{821}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{821-1}{2}} = (-1)^{3\cdot 410} = 1$$

$2 \equiv 3^2 \bmod 7$

$$\left(\frac{821}{7}\right) = \left(\frac{821 \bmod 7}{7}\right) = \left(\frac{2}{7}\right) = 1$$

so

$$\left(\frac{7}{821}\right) = 1$$

Skanowano w CamScanner

Compute: $\left(\frac{600}{953}\right)$, $\left(\frac{2020^3}{953}\right)$, $\left(\frac{-7000}{757}\right)$

$$\left(\frac{600}{953}\right) = \left(\frac{2\cdot 3\cdot 10^2}{953}\right) = \left(\frac{2}{953}\right)\cdot\left(\frac{3}{953}\right)\cdot\underbrace{\left(\frac{10^2}{953}\right)}_{=1} = 1\cdot(-1)\cdot 1 = \boxed{-1}$$

$$\left(\frac{2}{953}\right) = (-1)^{\frac{953^2-1}{8}} = (-1)^{113526} = 1$$

$$\left(\frac{3}{953}\right)\left(\frac{953}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{953-1}{2}} = -1$$

$$\left(\frac{953}{3}\right) = \left(\frac{953 \bmod 3}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{3}{953}\right) = -1$$

Skanowano w CamScanner

$$\left(\frac{2020^3}{953}\right) = \underbrace{\left(\frac{2020^2}{953}\right)}_{=1}\left(\frac{2020}{953}\right) = \left(\frac{2020}{953}\right) = \left(\frac{2020 \bmod 953}{953}\right) = 1\cdot(-1)\cdot(-1) = \boxed{1}$$

$$= \left(\frac{114}{953}\right) = \left(\frac{2\cdot 3\cdot 19}{953}\right) = \left(\frac{2}{953}\right)\left(\frac{3}{953}\right)\left(\frac{19}{953}\right)$$

$$\left(\frac{2}{953}\right) = (-1)^{\frac{953^2-1}{8}} = 1$$

$$\left(\frac{3}{953}\right) = -1$$

$$\left(\frac{3}{19}\right)\cdot\left(\frac{19}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{19-1}{2}} = -1$$

$$\left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = -1$$

$$\underbrace{\left(\frac{19}{953}\right)}_{=1}\boxed{\left(\frac{953}{19}\right)} = (-1)^{\frac{19-1}{2}\cdot\frac{953-1}{2}} = 1$$

$$\left(\frac{953}{19}\right) = \left(\frac{953 \bmod 19}{19}\right) = \left(\frac{3}{19}\right) = -1$$

Skanowano w CamScanner

$$\left(\frac{-7000}{757}\right) = \left(\frac{-1}{757}\right)\cdot\left(\frac{7}{757}\right)\cdot\left(\frac{2}{757}\right)\cdot\left(\frac{5}{757}\right)\cdot\left(\frac{10}{757}\right) = \underline{1}$$

$$\left(\frac{-1}{757}\right) = (-1)^{\frac{757-1}{2}} = 1 \qquad \left(\frac{2}{757}\right) = (-1)^{\frac{757^2-1}{8}} = -1 \qquad \left(\frac{10}{757}\right) = 1$$

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

$$\left(\frac{5}{757}\right)\left(\frac{757}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{757-1}{2}} = 1$$

$$\left(\frac{757}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$$\left(\frac{7}{757}\right)\left(\frac{757}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{757-1}{2}} = (-1)^{3\cdot 378} = 1$$

$$\left(\frac{757}{7}\right) = \left(\frac{1}{7}\right) = 1$$

Skanowano w CamScanner

Prove that

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

  $\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod 8$

  $\times$ $\left(\frac{3}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod{12}$

  $\left(\frac{-3}{p}\right) = 1$ iff $p \equiv 1 \pmod 6$

- $\times$ Suppose $\left(\frac{3}{p}\right) = 1 \implies p = \pm 1 \pmod{12}$

$$p = \pm 1 = 1$$

Take $p = 12k + 5$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = (-1)^{\frac{12k+5-1}{2}} = (-1)^{6k+2} = 1$$

$p \equiv 1$

$\cancel{1}$ mod 12

$\cancel{2}$

$\cancel{3}$

$\cancel{4}$ 11

5 1

$\cancel{6}$ 5

7 7

$\cancel{8}$

$\cancel{9}$

$\cancel{10}$

we need exclude

Skanowano w CamScanner

$p = 8k+7$

$$\frac{(8k+3)^2-1}{8} \qquad 8A+1$$

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

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 6$$

$$p = 1 \text{ or } -1 \bmod 6$$

$$p = 6k+5$$

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

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

$$\left(\frac{p}{3}\right) = \left(\frac{6k+5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Skanowano w CamScanner

so

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

$$\left(\frac{p}{3}\right) = \left(\frac{12k+5}{3}\right) = \left(\frac{12k+5 \pmod 3}{3}\right) = \left(\frac{2}{3}\right) = -1$$

so $\left(\frac{3}{p}\right) = -1$ ↯

$12k+7 = p$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{12k+7-1}{2}} = (-1)^{6k+3} = -1$$

$$\left(\frac{p}{3}\right) = \left(\frac{12k+7}{3}\right) = \left(\frac{1}{3}\right) = 1 \quad \text{so} \quad \left(\frac{3}{p}\right) = -1 \quad ↯$$

$\left(\frac{2}{p}\right) = 1$ iff $p = \pm 1 \pmod 8$

$p = \begin{matrix} 1 \\ \cancel{2} \\ 3 \\ \cancel{4} \\ 5 \\ \cancel{6} \\ 7 \end{matrix} \pmod 8$

$p = 8k+5$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8k+5)^2-1}{8}} =$$

$$= (-1)^{\left(\frac{64k^2+80k+24}{8}\right)} = (-1)^{8k^2+10k+3} = -1$$

Skanowano w CamScanner