$$\left(\frac{600}{953}\right) = \left(\frac{2^3 \cdot 3 \cdot 5^2}{953}\right) \overset{\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)}{=} \left(\frac{2^{3}}{953}\right)\left(\frac{3}{953}\right)\underbrace{\left(\frac{5^2}{953}\right)}_{1} =$$

$2^3 = 2^2 \cdot 2$

prime

$$= \left(\frac{2}{953}\right)\left(\frac{3}{953}\right) = \left(\frac{3}{953}\right) \overset{\text{Finally}}{=} \boxed{-1}$$

1

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

$$\frac{p^2-1}{8}$$

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

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

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

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

Scanned with CamScanner

$$\left(\frac{2020^3}{953}\right) = \underbrace{\left(\frac{2020^2}{953}\right)}_{=1}\left(\frac{2020}{953}\right) = \underbrace{\left(\frac{2020}{953}\right)}_{=1} \overset{\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)}{=} \underbrace{\left(\frac{114}{953}\right)}_{=-1}$$

$$= \left(\frac{114}{953}\right) = \left(\frac{2\cdot 3\cdot 19}{953}\right) = \underbrace{\left(\frac{2}{953}\right)}_{=1}\underbrace{\left(\frac{3}{953}\right)}_{=-1}\underbrace{\left(\frac{19}{953}\right)}_{=-1} = 1$$

Full

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

$$-\left(\frac{3}{953}\right) \overset{\text{Previous problem}}{=} -1$$

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

every

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

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

2

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

Scanned with CamScanner

$$\left(\frac{-7000}{757}\right) = \left(\frac{-1}{757}\right)\left(\frac{2^3}{757}\right)\left(\frac{5^3}{757}\right)\left(\frac{7}{757}\right) = 1\cdot(-1)\cdot(-1)\cdot 1 = 1$$

$$\left(\frac{-1}{757}\right) = (-1)^{\frac{757-1}{2}} = (-1)^{\frac{756}{2}} = 1$$ even

$$\left(\frac{2^3}{757}\right) = \left(\frac{2^2}{757}\right)\left(\frac{2}{757}\right) = (-1)^{\frac{757^2-1}{8}} = -1$$ even $= 71631 = \text{odd}$

$$\left(\frac{5^3}{757}\right) = \left(\frac{5^2}{757}\right)\left(\frac{5}{757}\right) = \left(\frac{5}{757}\right) = -1$$

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

$$\left(\frac{757}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

3

Scanned with CamScanner

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

odd

$$\left(\frac{757}{7}\right) = \left(\frac{757 \bmod 7}{7}\right) = \left(\frac{1}{7}\right) = 1 \quad \text{so}$$

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

4

Scanned with CamScanner

1) Next Problem is VERY IMPORTANT, REMEMBER IT! (5)

- -2 is quadratic residue iff $\boxed{p \equiv 1, 3 \mod 8}$

($\Leftarrow$) Take $p \equiv 1, 3 \mod 8$ we need to compute $\left(\frac{-2}{p}\right) = 1$

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

$p = 8k+1 \vee \frac{p-1}{2} = \frac{8k+1-1}{2} = 4k = \text{even}$

$p = 8k+3 \vee \frac{p-1}{2} = \frac{8k+3-1}{2} = 4k+1 = \text{odd}$

$\vee \frac{p^2-1}{8} = \frac{(8k+1)^2-1}{8} = \frac{64k^2+16k+1-1}{8} = 8k^2+2k = \text{even}$

$\vee \frac{p^2-1}{8} = \frac{(8k+3)^2-1}{8} = 8k^2+2k+1 = \text{odd}$

$$= (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = \begin{cases} \text{even} + \text{even} & p \equiv 1 \mod 8 \\ \text{odd} + \text{odd} & p \equiv 3 \mod 8 \end{cases} = \begin{cases} 1 \\ 1 \end{cases}$$

$= 1$ ∎

Scanned with CamScanner

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

6

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

$$2 \mid \frac{p-1}{2} + \frac{p^2-1}{8} \Longrightarrow p \equiv 1, 3 \pmod 8$$

- $p = 8k+5$

$\frac{p-1}{2} = 4k+2 = \text{even}$

$+ \frac{p^2-1}{8} = \frac{(8k+5)^2-1}{8} = 8k^2 + 10k + 3 = \text{odd}$

$\boxed{\text{odd}}$

$p \equiv \cancel{0}$

$p \equiv 1$ ✓

$p \equiv \cancel{2}$

$p \equiv 3$ ✓

$p \equiv \cancel{4}$

— $p \equiv 5$ ✓

$p \equiv \cancel{6}$

— $p \equiv 7$ ✓

?

$p = 8k+7$

$\frac{p-1}{2} = 4k+3$ — odd

$\frac{p^2-1}{8} = \frac{(8k+7)^2-1}{8} =$

$= 8k^2 + 14k + 6$

$\parallel$

even

Scanned with CamScanner

- 2 is quadratic residue mod p iff $p \equiv \pm 1 \pmod 8$

ALL OF YOU PLEASE DO THIS

7

($\Leftarrow$) $p = \pm 1 \bmod 8$ then $p = 8k+1$ $\quad 8k-1$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} (-1)^{\frac{(8k+1)^2-1}{8}} = 1 & p = 8k+1 \\ (-1)^{\frac{(8k-1)^2-1}{8}} = 1 & p = 8k-1 \end{cases} = \underline{1}.$$

($\Rightarrow$) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$, so $2 \mid \frac{p^2-1}{8}$ we need $p = \pm 1 \bmod 8$

we can exclude $p \equiv 3, 5 \bmod 8$.

if $p = 8k+3 \Rightarrow \frac{p^2-1}{8} = \frac{(8k+3)^2-1}{8} = \text{odd}$

$p = 8k+5 \Rightarrow \frac{p^2-1}{8} = \frac{(8k+5)^2-1}{8} = \text{odd}$

Scanned with CamScanner

- -3 is q. residue mod $p \iff p \equiv 1 \pmod 6$

8

$(\Leftarrow)$ $p = 6k+1$

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

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

$$\left(\frac{p}{3}\right) = \left(\frac{6k+1}{3}\right) = \left(\frac{6k+1 \bmod 3}{3}\right) = \left(\frac{1}{3}\right) = 1, \text{ so}$$

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

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{p-1} = (-1)^{6k} = \underline{1}.$$

Scanned with CamScanner

$(\Rightarrow)$?

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

$$p \equiv 1 \text{ or } \cancel{-1} \pmod 6$$

$\cancel{6k}$ $6k+1$ $\cancel{6k+2}$ $\cancel{6k+3}$ $\cancel{6k+4}$ $6k+5$

9

So suppose $p \equiv -1 \pmod 6$.

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right).$$ and by reciprocity

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

$$\left(\frac{p}{3}\right) = \left(\frac{6k-1}{3}\right) = \left(\frac{-1}{3}\right) = -1, \text{ so } \left(\frac{3}{p}\right)\cancel{(-1)} = (-1)^{\frac{p-1}{2}}(-1)$$

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

Scanned with CamScanner

• 3 is quadratic residue iff $p \equiv \pm 1 \mod 12$

($\Leftarrow$) $p \equiv 12k \pm 1$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = \begin{cases} (-1)^{\frac{12k+1-1}{2}} = 1 & \text{if } p = 12k+1 \\ (-1)^{\frac{12k+1-1}{2}} = -1 & \text{if } p = 12k-1 \end{cases}$$

$$\left(\frac{p}{3}\right) = \frac{12k \pm 1}{3} = \left(\frac{\pm 1}{3}\right) = \begin{cases} 1 & \text{if } p = 12k+1 \\ -1 & \text{if } p = 12k-1 \end{cases}$$

10

• if $p = 12k+1$ then

$$\left(\frac{3}{p}\right)\cdot\underbrace{\left(\frac{p}{3}\right)}_{=1} = 1 \Rightarrow \left(\frac{3}{p}\right) = 1.$$

if $p = 12k-1$ then

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

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

Scanned with CamScanner

$(\Longrightarrow)$ $\left(\frac{3}{p}\right) = 1 \Longrightarrow p \equiv \pm 1 \mod 12$

$\cancel{0}$ mod 12

$\cancel{1}$ ✓

$\cancel{2}$

$\cancel{3}$

$\cancel{4}$

5 ✓ $\rightsquigarrow$ impossible

$\cancel{6}$

7 ✓ $\rightsquigarrow$ impossible

$\cancel{8}$

$\cancel{9}$

$\cancel{10}$

$11 \equiv -1$.

11

Tale $p = 12k+5$

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

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

$$\Downarrow$$

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

Tale $p \equiv 7 \mod 12 \Longrightarrow p = 12k+7$

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

$$\left(\frac{p}{3}\right) = \left(\frac{12k+7}{3}\right) = \left(\frac{1}{3}\right) = 1$$

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

Scanned with CamScanner

59 p - prime Always $p>2$.

(12)

$\exists x : p \mid x^2 - x + 3$ iff $\exists y : p \mid y^2 - y + 25$.

HINT: $p \mid x^2 - x + 3 \iff p \mid 4x^2 - 4x + 12 = \underline{(2x-1)^2 + 11}$

$p \mid y^2 - y + 25 \iff p \mid 4(y^2 - y + 25) = \underline{(2y-1)^2 + 99}$

Now $p \mid (2x-1)^2 + 11 \iff -11 \equiv (2x-1)^2 \pmod{p} \iff$

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

$p \mid (2y-1)^2 + 99 \iff -99 \equiv (2y-1)^2 \bmod p \iff$

$$\left(\frac{-99}{9}\right) = 1$$

so what we need:

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

Scanned with CamScanner

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

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

Problem 55

$6 \mid p+1$, $p \mid a+b+c$, $p \mid a^4+b^4+c^4$ $\Rightarrow p \mid a,\ p \mid b,\ p \mid c$

$p \equiv -1 \bmod 6$ $\rightsquigarrow$ Problem 53 $\rightsquigarrow$ $\left(\frac{3}{p}\right)$ is important

$p \equiv -1 \bmod 12$

$\Downarrow$

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

$p \equiv -1 \bmod 6$

$\Downarrow$ Seen dot

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

Scanned with CamScanner

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

$$a+b+c \equiv 0 \pmod{p}$$

$$\Downarrow$$

$$c \equiv -(a+b) \pmod{p} \text{ so}$$

$$a^4+b^4+c^4 \equiv \underbrace{a^4+b^4+(a+b)^4}_{\text{Key point}} \pmod{p}$$

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

Scanned with CamScanner

$6 \mid p+1 \rightsquigarrow p \equiv -1 \pmod 6 \overset{(5)}{\rightsquigarrow} \left(\frac{-3}{p}\right) = -1$.

(15)

$6 \mid a^4+b^4+c^4$

$6 \mid a+b+c \rightsquigarrow c = -(a+b) \pmod p$, so

$$a^4+b^4+c^4 \equiv a^4+b^4+(a+b)^4 = 2(a^2+ab+b^2)^2 \bmod p, \text{ so}$$

(NICE IDENTITY)

$p \mid 2(a^2+ab+b^2)^2$, but $p>2$, so $p \mid a^2+ab+b^2$.

$$a^2+ab+b^2 \equiv 0 \pmod p \quad | \cdot 4 \qquad (b^{-1})^2$$

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

$$(2a+b)^2+3b^2 \equiv 0 \pmod p \Rightarrow -3 \cdot b^2 \equiv (2a+b)^2 \bmod p.$$

Now suppose $(b,p)=1$, $-3 \equiv \left(\frac{2a+b}{b}\right)^2 := (2a+b)^2 \cdot (b^{-1})^2 \bmod p$.

$(b \cdot b^{-1} \equiv 1 \bmod p)$ $\left(\frac{-3}{p}\right) = 1$. ↯, so $p \mid b$.

Scanned with CamScanner

$$-3b^2 \equiv (2a+b)^2 \quad (b^{-1})^2$$

$$-3 \cdot \underbrace{b^2 (b^{-1})^2}_{\substack{(b \cdot b^{-1})^2 \\ \| \\ 1}} \equiv \left((2a+b) \cdot b^{-1}\right)^2 \text{ mod } p$$

16

$$\| $$

$$-3 \equiv \left((2a+b) \cdot b^{-1}\right)^2 \text{ mod } p \Rightarrow \left(\frac{-3}{p}\right) = 1.$$

Inverse modulo p : $(a,p) = 1 \rightsquigarrow \exists\, b$ s.t

$$\boxed{ab \equiv 1 \text{ mod } p}$$

$$a := b^{-1}.$$

$\{1, \dots, p-1\} = \mathbb{Z}_p$

$\downarrow$

<u>is field</u>.

Scanned with CamScanner

<u>Prove</u> 2^n+1 has no prime divisor of the form $8k-1$

Suppose some $p \mid 2^n+1$ and has form $8k-1$

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

17

- n is even, $n=2k$, then

$$(2^k)^2 = 2^{2k} \equiv -1 \pmod p \rightsquigarrow \left(\frac{-1}{p}\right) = 1 \rightsquigarrow (-1)^{\frac{p-1}{2}} = 1 \text{ but}$$

$$\frac{p-1}{2} = \frac{8k-1-1}{2} = \frac{8k-2}{2} = 4k-1 \text{ — odd so}$$

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

↯

- n is odd, $n=2k+1$, then

$$2^n \equiv -1 \pmod p, \text{ so } 2^{2k+1} \equiv -1 \pmod p \;\Big|\; \cdot 2 \Rightarrow$$

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

but 53 1st dol $\Rightarrow \left(\frac{-2}{p}\right) = 1$ iff $\boxed{p \equiv 1,3 \bmod 8}$

↯

Scanned with CamScanner

if n is even :

$$2^{2k}+1 = (2^k)^2 + 1^2 \text{ is divisible by } p = 8k-1$$

$$p = 8k-1 \equiv 3 \pmod 4 \text{ so}$$

$\lightning$

18

Scanned with CamScanner