Revision

Q. $(2022)^{2021} \pmod 7 = ?$

$$2022 \equiv 6 \mod 7$$
$$\equiv -1 \mod 7$$
$$(-1)^{2021} \equiv (2022)^{2021} \pmod 7$$
$$-1 \equiv 6$$

$$(7K+6)^{2021} = 7\alpha + 6^{2021}$$
$$(7K'-1)^{2021} = 7\beta + (-1)^{2021}$$

Q. $7^{-1} \pmod{12} = ?$

i : 0 1 2 3 4 5 6 $\boxed{7}$ . . 11

$7i$:

$$7 \cdot 7 \equiv 49 \equiv 1 \pmod{12}$$
$$7^{-1} \equiv 7$$

$$\boxed{\varphi(n)} = \sum_{\substack{(d,n)=1 \\ d<n}} 1$$

$n = 12$

d: 1, 2, 3 4 5 6 7 8 9 10 11

Find

a) $\sum_{d<n} d = ? = S$

Find

a) $\sum_{\substack{d<n \\ (d,n)}} d = ? = S$

$$\left.\begin{aligned} S &= \sum_{i=1}^{\varphi(n)} d_i \\ S &= \sum_{i=1}^{\varphi(n)} d_{\varphi(n)-i+1} \end{aligned}\right\} \Rightarrow 2S = \sum_{i=1}^{\varphi(n)} n = n\varphi(n)$$

$d_i + d_{\varphi(n)-i+1} = n$

$S = \dfrac{n\varphi(n)}{2}$

$\boxed{\text{Ex} \qquad \text{b)} \quad \sum_{\substack{d<2n \\ (d,n)=1}} d}$

$0, 1, 2, \ldots, n-1$

n

$\{ \qquad \}$

$\{0, 1, 2, 3, 4, 5\}$ $\quad n = 6$

$\{0, 7, 14, 21, 28, 35\}$?

$0, 1, 2, 3, 4, 5$

$S \longrightarrow aS + b \qquad (a,n) = 1$

$a = 7, \ b = 0$

- $a^3 + (a+1)^3 + \cdots + (a+6)^3 = b^4 + (b+1)^4$ (RMO 2017)

Find (a,b) $\quad$ $(\cancel{1,2})$

A)

$\{a, a+1, \ldots, a+6\}$ — complete residue system mod $\underset{?}{7}$ ✓

$S = \{0, 1, 2, \ldots, 6\}$

$LHS \equiv 0^3 + 1^3 + \ldots + 6^3 \pmod 7$

$\equiv \left(\frac{6(7)}{2}\right)^2 \equiv 0 \pmod 7$

$7 \mid RHS$

$7 \nmid RHS$

x	0	1	2	3	4	5	6
x^4	0	1	2	4	4	2	1

$\{0, 1, 2, 4\}$

$5^4 \equiv (-2)^4 \bmod 7$

$\equiv 2^4$

$3^4 \equiv 2 \pmod 7$

$a^3 \equiv 3^3 \pmod 7$

$a+1 \equiv 4$

$a+2 \equiv 5$

6

0

1

$a+6 \equiv 2$

$m \qquad a^{\varphi(m)} \equiv 1 \pmod{m} \qquad (a, m) = 1$

$p \qquad a^{p-1} \equiv 1 \pmod{p} \qquad p \nmid a$

Thm: p – prime $\quad \exists\, x \in \{0, 1, \ldots, p-1\}$

(proof will be given later) $\{1, x, x^2, \ldots\ldots, x^{p-2}\}$

$x^{p-1} \equiv 1 \pmod{p}$

Quadratic Residues

a is Q.R. mod m $\qquad a \equiv x^2 \pmod{m}$

7	✓	✓	✓	✗	✓	✗	✗
i	0	1	2	3	4	5	6
i^2	0	1	4	2	2	4	1

$\{0, 1, 2, 4\}$

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

2 is QR "

($N = pq$ is x Q.R? $\longrightarrow$ open problem

Ex: Goldwasser Micali Encryption)

Legendre Symbol

(p - prime)

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is Q.R}, a \neq 0 \\ -1, & a \text{ is not} \\ 0, & p \mid a \end{cases}$$

$$0^2 \equiv 0 \pmod p \quad \checkmark$$

Q. no. of Q.R $\pmod p$?

<u>p - odd prime</u> $\{1, \ldots, p-1\}$

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

$A_i = \{i, p-i\} \quad 1 \leq i \leq \frac{p-1}{2}$

$A_i \longrightarrow i^2 \pmod p$ (one - one map)

$\underline{i^2 \equiv j^2} \Rightarrow (i-j)(i+j) \equiv 0$

$p \mid$ " "

$\underline{i-j \equiv 0}$ or $\underline{i+j \not\equiv 0}$

$(1, \ldots, p-1)$

$2 \leq i+j \leq p-1$

A_i: $\boxed{\left(\frac{p-1}{2}\right)}$

$$\left.\begin{array}{l} A_1 = \{1, 6\} \longrightarrow 1 \\ A_2 = \{2, 5\} \longrightarrow 4 \\ A_3 = \{3, 4\} \longrightarrow 2 \end{array}\right\}$$

Q. Is $-1 \equiv p-1$ a Q.R.?

-1 is Q.R :

$$\left.\begin{array}{l} i \equiv x^2 \\ -1 \equiv y^2 \end{array}\right\} \Longrightarrow \underset{(p-i)}{-i} \equiv x^2 y^2 \equiv (xy)^2$$

p = 5

i	1	2	3	4
i^2	1	4	4	1

p = 13

i	1	2	3	4	5	6	7	8	9	10	11	12
i^2	1	4	9	3	12	10	10	12	3	9	4	1

-1 is not QR:

p = 7 :

1	2	3	4	5	6
1	4	2	2	4	1

p = 3, 7, 11 -1 ✗	p = 5, 13 -1 ✓
$p \equiv 3 \pmod 4$	$p \equiv 1 \mod 4$

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

$(a, p) = 1$

$$\left(\frac{a}{p}\right) = \underbrace{a^{\left(\frac{p-1}{2}\right)}}_{x} \pmod p$$

$$\underbrace{a^{p-1}} \equiv 1 \pmod p$$

$$x^2 \equiv 1 \quad \Rightarrow \quad \underbrace{(x-1)}\underbrace{(x+1)} \equiv 0$$

$$x \equiv \pm 1$$

(Euler's Criterion) : $$\boxed{\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p}$$

Pf :

$$\{\underline{1, x, x^2}, \ldots, \underline{x^{p-2}}\}$$

even m : $\frac{p-1}{2}$

0 to $p-2$

QR ✓

odd m : non QR

$$a \equiv x^m$$

$$\Rightarrow \quad a^{\frac{p-1}{2}} \equiv x^{\frac{(p-1)m}{2}} \equiv \left(x^{\frac{m}{2}}\right)^{p-1} \equiv 1$$

$$m \text{ even} \Rightarrow a^{\frac{p-1}{2}} \equiv 1$$

$$\underline{x^{\left(\frac{p-1}{2}\right)(2r+1)}} \equiv \underbrace{\left(x^{p-1}\right)}_{1}\underbrace{\left(x^{\frac{p-1}{2}}\right)}_{\pm 1} \equiv -1$$

$$\underbrace{x^{\frac{p-1}{2}} \not\equiv 1} \qquad x^{\frac{p-1}{2}} \equiv -1$$

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

Q. 2 Q.R ? $\qquad$ p – prime

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

$$2 \cdot 4 \cdot \cdots\cdots (p-1) \equiv \boxed{2^{\left(\frac{p-1}{2}\right)}} \left(\frac{p-1}{2}\right)!$$

$$p = 19 \quad : \quad \boxed{\underbrace{2 \times 4 \times 6 \times 8}_{}}^{4} \times \boxed{\underbrace{10}_{-9} \times \underbrace{12}_{-7} \times \underbrace{14}_{-5} \times \underbrace{16}_{-3} \times \underbrace{18}_{-1}} \equiv 2^9\, 9!$$

$$(-1)^5 \cancel{9!} \equiv 2^9 \cancel{9!} \pmod{19}$$

$$p = 4k+1, \quad \text{LHS} = (\overbrace{2 \cdot \cdots\cdots 2k}^{k})(\overbrace{\underset{-(2k-1)}{2k+2} \cdots\cdots \underset{-1}{4k}}^{k})$$

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

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

$$p = 4k+3$$

$$(2 \cdot \cdots 2k)(\overbrace{2k+2 \cdots\cdots 4k+2}^{k+1})$$

$$2^{\frac{p-1}{2}} \equiv (-1)^{k+1}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1, 7 \pmod 8 \\ -1, & p \equiv 5, 3 \pmod 8 \end{cases}$$

Thm: (Guass Lemma)

u = no. of elements in $\{a, 2a, \ldots \left(\frac{p-1}{2}\right)a\}$ reduced to rem when divided by p which are $> p/2$

$$\left[\begin{array}{ll} a = 3 & \dfrac{3 \times 6 \times 9 \times 12 \times 15}{\underbrace{3 \times \underset{-5}{6} \times \underset{-2}{9} \times 1 \times 4}_{(-1)^2\, 5!}} \equiv 3^{\frac{11-1}{2}}\, 5! \\ p = 11 & \left(\frac{3}{11}\right) = 1 \end{array}\right]$$

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

Ex: p — odd prime

q — any number $(q, p) = 1$

$$q = p x_1 + r_1$$

$$2q = p x_2 + r_2$$

$$\vdots$$

$$\left(\frac{p-1}{2}\right) q = p\, x_{\left(\frac{p-1}{2}\right)} + r_{\left(\frac{p-1}{2}\right)}$$

Let $m = x_1 + x_2 + \cdots + x_{\left(\frac{p-1}{2}\right)}$

$m = f(u, p, q)$ Find f.

defined above