§ Problem Statement

Find all primes $p \geq 5$ for which

$$\left\{2^{-1}, 3^{-1}, \ldots, \left(\frac{p-1}{2}\right)^{-1}\right\} = \left\{-2, -3, \ldots, -\frac{p-1}{2}\right\} \pmod{p}.$$

§ Solutions

The answer is $p \in \boxed{\{5, 7, 13\}}$, which can be checked to work.

Solution A

To show that no other p work, check $p = \{11, 17, 19\}$ manually and assume $p \geq 21$. Then

$$\left\{-10, -\frac{p-5}{2}\right\} \in \left\{-2, -3, \ldots, -\frac{p-1}{2}\right\},$$

but their reciprocals differ by

$$\frac{1}{10} - \frac{2}{p-5} = \frac{p-1}{2}$$

and thus cannot both lie in $\left\{-2, -3, \ldots, -\frac{p-1}{2}\right\}$.

Solution B

To show that no other p work, check $p = 11$ manually, and assume $p = 2^k n + 1 \geq 17$ for some odd n.

- If $n = 1$, then $p = 2^k + 1$. Since $\frac{p+1}{2}$ must be prime, both $2^{k-1} + 1$ and $2^k + 1$ are consecutive Fermat primes. Since $k - 1$ and k must be powers of 2, this forces $k = 2$, which gives $p = 5$.
- If $n = 3$, then $p = 3 \cdot 2^k + 1$. Since $\frac{2p+1}{3} = 2^{k+1} + 1$ must be prime, $k = 2^c - 1$. $c \in \{1, 2\}$ gives $p \in \{7, 13\}$. If $c \geq 3$, then

  $$5 \mid 3 \cdot 2^{2^c - 1} + 1 = p,$$

  contradiction.
- If $n \geq 5$, then

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

  shows that this case yields no solutions.

Solution C

No other p work; to see why, let $q > 2$ be the smallest prime not dividing $p - 1$.

Lemma 1. *$q^2 < \frac{p}{2}$ unless $p \in S = \{5, 7, 13, 19, 31, 37, 43, 61, 211\}$.*

Proof. Casework on q.

- $q = 3$ gives $p = 5$.

- $q = 5$ gives $p \in \{13, 19, 37, 43\}$.
- $q = 7$ gives $p \in \{31, 61\}$.
- $q = 11$ gives $p = 211$.

No larger q work because

$$13^2 < \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{2}$$

and $p_{n+1}^2 < \frac{p_1 p_2 \ldots p_n}{2}$ for $n \geq 5$ by induction using $p_{i+1} < 2p_i$, where p_i are the primes in increasing order. □

Now, $q' \mid (q'-1)p + 1$ for all primes $q' < q$ by minimality of q, but $q \mid kp + 1$ for some $0 < k < q - 1$, since $q \nmid p - 1$. Therefore, $q \operatorname{rad}(k+1) \mid kp + 1$, so

$$(q \operatorname{rad}(k+1)) \cdot \frac{kp+1}{q \operatorname{rad}(k+1)} \equiv 1 \pmod{p}.$$

If $p \notin S$, the first factor can be bounded as

$$q \operatorname{rad}(k+1) < q^2 < \frac{p}{2}$$

and the second factor as

$$\frac{kp+1}{q \operatorname{rad}(k+1)} < \frac{(k+1)p}{(k+1)2} = \frac{p}{2}.$$

Therefore, no $p \notin S$ satisfy the problem condition.

To finish the problem, it suffices to show no $p \in S \setminus \{5, 7, 13\}$ work. Indeed,

$$\begin{aligned} 4 \cdot 5 &\equiv 1 \pmod{19} \\ 4 \cdot 8 &\equiv 1 \pmod{31} \\ 5 \cdot 15 &\equiv 1 \pmod{37} \\ 4 \cdot 14 &\equiv 1 \pmod{43} \\ 8 \cdot 23 &\equiv 1 \pmod{61} \\ 4 \cdot 53 &\equiv 1 \pmod{211}, \end{aligned}$$

as desired.

§ Variants

Variant A. Find all primes p for which the the only solution to $p \mid ab-1$ with $1 \le a \le b \le \frac{p}{2}$ is $a = b = 1$.

Solution. The answer is $p \in \boxed{\{2, 3, 5, 7, 13\}}$. Aside from small p, this is equivalent to the original problem.

Variant B. Find all primes p for which the the only solution to $p \mid ab-1$ with $1 \le a \le b \le \frac{p}{3}$ is $a = b = 1$.

Solution. I am not sure how to solve this variant; neither of the solutions above generalize to handle this setting. In fact, I was unable to solve Variant A under the condition $1 \le a \le b \le (\frac{1}{2} - \varepsilon)p$ for *any* $\varepsilon > 0$.

§ Comments

I came up with this problem while I was in Ghana teaching students about modular arithmetic. To help the students visualize modular inverses, I drew a 12×12 grid and marked all squares whose coordinates were inverses modulo 13; the 6×6 square in the corner seemed *suspiciously* empty.

§ Metadata

This problem was selected as Problem 2 of the 2023 HMIC.

- Title: Modular Inverses Are Modular Negatives
- Author: Holden Mui
- Subject: number theory
- Description: find all primes p for which two sets are equal in $\mathbb{F}_p$
- Keywords: modular inverse, negative, prime, set
- Difficulty: TST 2/5
- Collaborators: Serena An, Kevin Cong, Ram Goel, Andrew Gu, Milan Haiman, Rey Li, James Lin, Yuka Machino, Isabella Quan, Michael Ren, Luke Robitaille, Carl Schildkraut, Eric Shen (Harvard '25), Colin Tang, Zi Song Yeoh, Isaac Zhu
- Date written: January 2022
- Submission history: 2023 TST, 2023 TSTST, 2023 HMIC
- Other credits: the authors of solution A are Brian Liu Luke Robitaille, and the author of Solution C is James Lin.