

$$20x \equiv 48 \pmod{55}$$

$$4x \equiv 5 \pmod{11}$$

$$x \equiv 1 \pmod{11}$$

$$20x \equiv 48 \pmod{11}$$

$$55 \equiv 1 \pmod{11}$$

$$\gcd(4, 11) = 1$$

$$\gcd(4, 11) = 1$$

$$2. 16 \text{ numbers } + 78519211 \equiv 15811151423$$

yes to gods, probably
some digit errors

$$3. 5 \mid a^5 - a \quad \forall a \in \mathbb{Z}$$

$5 \mid 1305$ } ~~equivalent~~ equivalent congruence

$$a^5 \equiv a \pmod{5}$$

$$a^5 \equiv a \pmod{13}$$

$$a^5 \equiv a \pmod{5}$$

equivalent simultaneous congruence

$$\phi(5) = 5 - 1 = 4$$

True by Fermat's theorem $\forall a$
as 13 is prime

By defn. prime $\gcd(5, a) = 1$

$$a^4 \equiv 1 \pmod{5}$$

$$a^4 \equiv 1 \pmod{5} \quad \checkmark$$

By Fermat's theorem again

$$5 \mid a$$

Trivially holds

$$0^5 \equiv 0 \pmod{5}$$

$$0 \equiv 0 \pmod{5}$$

Because all components of the ^{equiv} congruence hold, they must be divisible.

$$4. 19(49!) - 6! \\ 701 \downarrow$$

$$19 \cdot (701-2)! \equiv 6! \pmod{701}$$

$$19 \cdot (701-2)! \equiv 30 \cdot 24 \equiv 720 \equiv 19 \pmod{701}$$

$$\gcd(19, 701) = 1$$

$$(701-2)! \equiv 1 \pmod{701}$$

$$\times 701$$

$$(701-1)! \equiv -1 \pmod{701}$$

True via Wilson's Theorem

$$5. -2^{125} \pmod{77}$$

$$77 = 7 \cdot 11$$

~~Handwritten scribbles and text, possibly "Handwritten scribbles and text"~~

$$\begin{array}{r} 11 \cdot 3 \cdot 2 \cdot 1 = 126 \\ 126 \cdot 3 = 378 \\ 378 \cdot 2 = 756 \\ 756 \cdot 1 = 756 \end{array}$$

$$64 \cdot 701$$

$$-64 \cdot 701$$

$$\begin{array}{r} -44 \\ +700 \\ \hline 2560 \\ 28000 \\ \hline 30800 \end{array}$$

$$\begin{array}{r} 126 \\ 126 \cdot 3 = 378 \\ 378 \cdot 2 = 756 \\ 756 \cdot 1 = 756 \end{array}$$

$$\begin{array}{r} 53 \\ 701 \cdot 53 = 37153 \\ 37153 \cdot 3 = 111459 \\ 111459 \cdot 2 = 222918 \\ 222918 \cdot 1 = 222918 \end{array}$$

$$\begin{array}{r} 64 \cdot 701 \\ 64 \cdot 701 = 44864 \\ 44864 \cdot 3 = 134592 \\ 134592 \cdot 2 = 269184 \\ 269184 \cdot 1 = 269184 \end{array}$$

$$\begin{array}{r} 701 \\ 701 \cdot 3 = 2103 \\ 2103 \cdot 2 = 4206 \\ 4206 \cdot 1 = 4206 \end{array}$$

$$30 \cdot 24 \quad \frac{30}{24} = \frac{5}{4}$$

c. $\sum_{d|n} \mu(d) \tau(d) = (-1)^r$ for some r ?

~~is~~ $\mu(d) \tau(d)$ is multiplicative because both μ and τ are multiplicative. thus

$$f(mn) = \mu(mn) \tau(mn) = \mu(m) \mu(n) \tau(m) \tau(n) = f(m) f(n)$$

Because of this, the $\sum_{d|n} f(d)$ is multiplicative.

Thus wlog we can choose to operate only on primes

~~the~~ prime powers are dominated by the $\mu(n)$ function
 thus we don't need to worry of that case

for prime p

$$\sum_{d|p} \mu(d) \tau(d) = \mu(1) \tau(1) + \mu(p) \tau(p) = (-1)(2) + 1 \cdot 1 = 1$$

Because function is multiplicative, it will always return 1 thing ($\equiv 0 \pmod{2}$)

~~$$\sum_{d|pq} \mu(d) \tau(d) = \mu(1) \tau(1) + \mu(p) \tau(p) + \mu(q) \tau(q) + \mu(pq) \tau(pq)$$~~

~~$$= (-1)(2) + (-1)(2) + (-1)(2) + 1 \cdot 4 = -2$$~~

~~$$= 3 \cdot 2 + 1 \cdot 4 + (-2) \cdot 3 + 1$$~~

$$f_0 f(n) = \sum_{d|n} \sigma(d) \quad \forall n \geq 1$$

$$f(2^{100} \cdot 77) = ?$$

$$f(2^{100} \cdot 77) = \left(\left(\frac{2^{101} - 1}{2^{100} - 1} \right) \left(\frac{2^{100} - 1}{2^{99} - 1} \right) \cdots \left(\frac{2^2 - 1}{2 - 1} \right) \left(\frac{77^2 - 1}{77 - 1} \right) \right)^2$$

$$f(n) = \left(\frac{2^{101} - 1}{2^{100} - 1} \right) \left(\frac{77^2 - 1}{76} \right) = \left(\prod_{i=1}^{100} \left(\frac{2^{i+1} - 1}{2^i - 1} \right) \right)^2 \left(\frac{77^2 - 1}{76} \right)^2$$

∴ order of 2 mod 23

at most or factor of it

$$\phi(23) = 23 - 1 = 22$$

22

$$22 = 2 \cdot 11$$

$$22 = 2 \cdot 11$$

$$2^2 = 4 \times (2^{11} = 2048)$$

the order of 2 mod 23

$$2^{11} \equiv 1 \pmod{23}$$

$$23 \overline{) 2048} \rightarrow$$

$$\begin{array}{r} 89 \\ 23 \overline{) 2048} \\ \underline{184} \\ 208 \\ \underline{204} \\ 4 \end{array}$$

∴ $2^n - 1$ pseudoprime? $n | \phi(2^n - 1)$

for $n > 1$, $2^n - 1 \equiv 3 \pmod{4}$

~~2^n - 1 is not a pseudoprime~~

~~23~~

$$\phi(23) = 22 \leq 22$$

$$23 \overline{) 92}$$

44 - 5

$$\begin{array}{r} 4 \\ 23 \overline{) 92} \\ \underline{92} \\ 0 \end{array}$$

$$\begin{array}{r} 23 \\ 23 \overline{) 44} \\ \underline{46} \\ -2 \\ 23 \overline{) 69} \\ \underline{69} \\ 0 \\ 23 \overline{) 92} \\ \underline{92} \\ 0 \\ 23 \overline{) 115} \\ \underline{115} \\ 0 \\ 23 \overline{) 138} \\ \underline{138} \\ 0 \\ 23 \overline{) 161} \\ \underline{161} \\ 0 \\ 23 \overline{) 184} \\ \underline{184} \\ 0 \\ 23 \overline{) 207} \\ \underline{207} \\ 0 \\ 230 \\ 253 \\ 276 \end{array}$$

$$8 \times 254$$

-18

1, 2, 4, 8, 16, 1, 18

$$254$$

$$48 \times 912$$

$$1024$$

$$2048$$

$$\begin{array}{r} 8 \\ 16 \overline{) 128} \\ \underline{128} \\ 0 \end{array}$$

$$11. S = \{3, 2 \cdot 3, \dots, (\frac{4001-1}{2}) \cdot 3\}$$

$$n = |\text{filter}(S, \text{keeping elements } > \frac{4001}{3})|$$

$$(3/4001) = (-1)^n \neq 1$$

$$4001 \bmod 12 = 5$$

$$\begin{array}{r} 333 \overline{) 4001} \\ \underline{399} \\ 1 \\ \underline{12} \\ 9 \\ \underline{84} \\ 5 \end{array}$$

$$\begin{array}{r} 12 \\ 24 \\ 36 \\ 48 \end{array}$$

$$12. (p-1/p) = -1, \forall p \equiv 3 \pmod{4}$$

restated using Euler's criterion:

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

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

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

$$\text{need: } (p-1)/2 \equiv 1 \pmod{2}$$

$$\begin{aligned} 13. (23/31) &= -(31/23) = -(8/23) = \\ &= -(2/23)(2/23)(2/23) = \\ &= -1 \cdot 1 \cdot 1 = 1 \end{aligned}$$

$$\begin{aligned} 14. (300/43) &= (-1/43) \\ &= (-1)^{\frac{43-1}{2}} = -1 \neq 1 \end{aligned}$$

$$23 \nmid 4^3$$

$$23 \bmod 4 = 3$$

$$23 \bmod 8 = -1 = 7$$

$$3^0$$

$$\frac{42}{2} = 21$$

$$7 \cdot 43 = 301$$

$$28$$

$$4 \cdot 4 = 21$$

$$115 = 10$$

$$31 \bmod 4 = 3$$

$$\begin{array}{r} 21 \\ 31 \\ \underline{-23} \\ 8 \end{array}$$

$$8 \nmid 23$$

$$300 = 5 \cdot 2 \cdot 3^2$$

$$\begin{array}{r} 435 \overline{) 300} \\ \underline{258} \\ 42 \end{array}$$

$$\begin{array}{r} 143 \\ \underline{-84} \\ 59 \\ \underline{-29} \\ 30 \end{array}$$