1. $20x \equiv 45 \pmod{55}$ $\qquad 55 = 5 \cdot 11$

$4x \equiv 8 \pmod{11}$ $\qquad$ gcd all terms 5

$\overline{4} \quad \overline{4}$ $\qquad \gcd(4, 11) = 1$

$x \equiv 2 \pmod{11}$

2. $1600000x + 98349211y = 93849732423$

yes b/c gcd's probably
from digit endings

3. $65 \mid a^{13} - a \quad \forall a \in \mathbb{Z}$

$65 = 13 \cdot 5$ ~~contra~~ equivalent congruence

$a^{13} \equiv a \pmod{65}$ $\qquad$ equivalent simultaneous congruences ~~cer~~

$a^{13} \equiv a \pmod{13}$ $\qquad a^{13} \equiv a \pmod{5}$ $\qquad \phi(5) = 5 - 1 = 4$

True by fermat's theorem as 13 is prime

$5 \nmid a$ $\qquad 5 \mid a$

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

$0^{13} \equiv 0 \pmod{5}$

$0 \equiv 0 \pmod{5}$

$a^{14} \equiv 1 \pmod{5}$

$a^{4} \equiv 1 \pmod{5}$ ✓

By fermats theorem again

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

$r \quad \sum \mu(d)\tau(d) = (-1)^r$ for some r ?

4. $19(699!) - 6!$ 701 prime

$701 \mid$

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

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

$\gcd(19, 701) = 1$

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

$\times 700$

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

True via Wilson's theorem

5. $-2^{125} \bmod 77$ $77 = 7 \cdot 11$

$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2760$

$30 \cdot 24$

$30 \times 24 = 720$

$701 - 638 = 63$

~~$\mu(d)\tau(d)$ is multiplicative~~

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

$\mu(d)\tau(d)$ is multiplicative because both $\mu(n)$ and $\tau(n)$ are multiplicative. thus

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

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

Thus wlog we can choose to operate only on primes

prime powers ≥ 2 are eliminated by the $\mu(n)$ function thus we don't need to worry of that case

for prime p

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

Because function is multiplicative, it will always return 1 thus ($r \equiv 0 \bmod 2$)

~~$\sum \mu(d)\tau(d) = \mu(p)\tau(p) + \mu(q)\tau(q) + \mu(pq)\tau(pq) + \mu(1)\tau(1)$~~

~~$= (-1)\cdot 2 + (-1)\cdot 2 + 1\cdot 3 + 1\cdot 1 \neq 1$~~ why?

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

7. $f(n) = \sum_{d|n} \sigma(d) \quad \forall n \geq 1 \qquad f(2^{100} \cdot 77) = ?$

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

$$\sigma(n) = \left(\frac{2^{101}-1}{2^{100}-1}\right)\left(\frac{77^2-1}{76}\right)$$

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

8. order of 2 mod 23

at most or factor of it

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

$22 = 2 \cdot 11$

$2^2 = 4$ X $\quad 2^{11} = 2048$

the order of 2 mod 23 is 11 as $2^{11} \equiv 1 \pmod{23}$

22

$22 = 2 \cdot 11$

$\phi(23) = 22$

≤ 22

$23 \overline{)2048}$ 89

184

208

207

1

1, 2, 4, 8, 16, 9, 18

1, 2, 4, 8, 16, 32, 64, 128, 256

256, 512, 1024, 2048

23, 46, 69, 92, 115, 138, 161, 184, 207, 230, 253, 276

9. $2^n - 1$ pseudoprimes? $4 | \phi(2^n - 1)$

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

11. $S = \{3, 2\cdot 3, \ldots, (\frac{4001-1}{2})\cdot 3\}$ $\qquad$ #elements in $S \geq \frac{4001}{3}$

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

12
24
36
42

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

$4001 \bmod 12 = 5$

33315
12)4001
36
40
36
41
36
5

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

restated using euler's criterion:

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

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

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

prime $\qquad$ QR both $p, q \equiv 3 \pmod 4$ $\qquad$ $31 \bmod 23 = 8$

$\rightarrow 28 \qquad 31 \bmod 4 = 3$

13. $(23/31) = -(31/23) = -(8/23) =$

$= -(2/23)(2/23)(2/23)$

$= -1 \cdot 1 \cdot 1 = 1$

$23\overline{)4}$ 3

$4 \cdot 4 = 24$
$4 \cdot 5 = 20$

$23 \bmod 4 = 3$

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

31
−23
8

$8\overline{)23}$

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

1	43
2	86
3	129
4	172
5	215
6	258
7	301

6. $(300/43) = (-1/43)$

$= (-1)^{(43-1)/2} = -1^{21} = -1$

30

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

$7 \cdot 43 = 301$

6
43)300
258
42