1. [illegible] 48 (mod 99) [illegible] 11

[illegible] (mod 11) [illegible]

[illegible]

[illegible] (mod 11)

2. [illegible] + [illegible] ≡ [illegible]

yes [illegible] gcd, probably

[illegible]

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

$65 = 13 \cdot 5$ ~~[illegible]~~ equivalent congruence

$a^{13} \equiv a \pmod{65}$ equivalent simultaneous congruence

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

True by Fermat's theorem as 13 is prime

$5 \nmid a$ $\quad 5 \mid a$ Trivially holds

By defn. prime $\gcd(5, a) = 1$ $\quad 0^{13} \equiv 0 \pmod{5}$

$0 \equiv 0 \pmod{5}$

$a^{12} \equiv 1 \pmod{5}$

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

By Fermat's theorem again

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

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

$701 |$

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

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

$\gcd(19, 701) = 1$

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

$\times 700$

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

True via Wilson's Theorem

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

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

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

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

$22 = 2 \cdot 11$

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

22

$22 = 2 \cdot 11$

$\phi(23) = 22$

≤ 22

the order of 2 mod 23

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

$23 \overline{)2048}$

184

208

207

1

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

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? $4 \mid \phi(2^n-1)$

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

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

#elements in $S \geq \frac{4001}{3}$

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

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

4001 mod 12 = 5

12
24
36
48

333 1/5
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:

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

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

need:

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

prime

QR both p,q ≡ 3 (mod 4)

31 mod 23 = 8

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

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

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

$23\overline{)4}^{3}$

23 mod 4 = 3

23 mod 8 = -1 = 7

7

28

4 · 4 = 21

4 · 5 = 10

31 mod 4 = 3

31/23

31
-23
8

$8\overline{)23}$

14. $(300/43) = (-1/43)$

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

30

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

7 · 43 = 301

300 = 5 · 2 · 3 · 2 · 2

300/43

4
$43\overline{)300}$
258
42

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