MAT246 HW4 Rui Qiu #999292309

(1). Claim

Proof: $\because \gcd(a,b)=1$ and $a|c$, $b|c$

~~$\therefore a=kc$, $b=jc$ for some integers k,j. $(k,j\neq 0)$~~

~~$\therefore ab=kcjc=c^2kj=c(ckj)$~~

~~$\therefore ab|c$.~~

4/5 $\therefore ak=bj=c$ for some non-zero integers k,j.

Algorithm

$ax+by=1$ for some ~~integers~~ non-zero integers x,y (by Euclidean)

$\therefore axbj+byak=c \Leftrightarrow ab(xj+yk)=c$

$\Leftrightarrow ab|c$

(2). Conclusion ■

Solution: $573=291\times 1+282$

~~282~~

$291=282\times 1+9$

$282=9\times 31+3$

$9=3\times 3$

So, $\gcd(291,573)=3$

$3=282-9\times 31$

$=(573-291)-(291-282)\times 31$

$=(573-291)-(291-(573-291)\times 3)$

$=573-291-2\times 31\times 291+31\times 573$

$=32\times 573-63\times 291$

$=32\times 573+(-63)\times 291$

Then such $x=-63$, $y=32$, satisfying

$291x+573y=\gcd(291,573)$.

8

(3).

Solution:

Since $\gcd(10, 21) = 1$

$\varphi(21) = (3-1)(7-1) = 12$

So $10^{\varphi(21)} \equiv 10^{12} \equiv 1 \bmod 21$ (By Euler Theorem)

We want to find $5^{101} \bmod 12$

Since $\gcd(5, 12) = 1$

$\varphi(12) = (2^2-2^1)(3-1) = 4$

So $5^{\varphi(12)} \equiv 5^2 \equiv 1 \bmod 12$ (By Euler Theorem)

Since $101 \equiv 1 \bmod 4$

Then $5^{101} \equiv (5^4)^{25} \cdot 5^1$

$\equiv 1^{25} \cdot 5^1$

$\equiv 5 \bmod 12$

So $5^{101} = 12k + 5$ for some integer k

Therefore $10^{5^{101}} \equiv 10^{12k+5} \equiv (10^{12k}) \cdot 10^5$

$\equiv 1 \cdot 10^5 \bmod 21$

$\equiv 10000 \bmod 21$

$\equiv 19 \bmod 21$

(since $10000 = 476 \times 21 + 19$)

(4). Claim: p_1, p_2, p_3 are distinct primes, then

$\varphi(p_1^{k_1} p_2^{k_2} p_3^{k_3}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})(p_3^{k_3} - p_3^{k_3-1})$ for some integers k_1, k_2, k_3.

Proof: ① First we need to calculate $\varphi(p_1^{k_1})$, ~~which means the difference between $p_1^{k_1}$ and all numbers divisible by $p_1^{k_1}$.~~

since p_1 is prime then all $1p_1, 2p_1, 3p_1, \cdots, p_1^{k_1}$ are ~~not divisible by~~ not relatively prime to $p_1^{k_1}$

The number of them is $\frac{p_1^{k_1}}{p_1} = p_1^{k_1-1}$

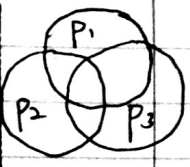
So $\varphi(p_1^{k_1}) = p_1^{k_1} - p_1^{k_1-1}$

Similarly we have

$$\varphi(p_2^{k_2}) = p_2^{k_2} - p_2^{k_2-1}$$

$$\varphi(p_3^{k_3}) = p_3^{k_3} - p_3^{k_3-1}$$

② Calculate $\varphi(p_1^{k_1} p_2^{k_2} p_3^{k_3})$



- Need to know how many numbers are not relatively prime to p_1 and $\leq p_1^{k_1} p_2^{k_2} p_3^{k_3}$

  $1p_1, 2p_1, \cdots, p_1^{k_1} p_2^{k_2} p_3^{k_3}$

  so there are $\frac{p_1^{k_1} p_2^{k_2} p_3^{k_3}}{p_1} = p_1^{k_1-1} p_2^{k_2} p_3^{k_3}$ such numbers.

- Similarly there are $p_1^{k_1} p_2^{k_2-1} p_3^{k_3}$ numbers which are not relatively prime to p_2 and $\leq p_1^{k_1} p_2^{k_2} p_3^{k_3}$.
- There are $p_1^{k_1} p_2^{k_2} p_3^{k_3-1}$ numbers which are not relatively prime to p_3 and $\leq p_1^{k_1} p_2^{k_2} p_3^{k_3}$.

- But note that we double-counted those numbers which are
  1). both divisible by p_1 and p_2
  2). both divisible by p_2 and p_3
  3). both divisible by p_3 and p_1

  And such types of numbers have those amounts respectively:

  1). $\frac{p_1^{k_1} p_2^{k_2} p_3^{k_3}}{p_1 p_2} = p_1^{k_1-1} p_2^{k_2-1} p_3^{k_3}$

  2). $\frac{p_1^{k_1} p_2^{k_2} p_3^{k_3}}{p_2 p_3} = p_1^{k_1} p_2^{k_2-1} p_3^{k_3-1}$

  3). $\frac{p_1^{k_1} p_2^{k_2} p_3^{k_3}}{p_3 p_1} = p_1^{k_1-1} p_2^{k_2} p_3^{k_3-1}$

- BUT notice again that triple-counted one type of number: those are divisible by p_1, p_2 and p_3.

  How many? $\frac{p_1^{k_1} p_2^{k_2} p_3^{k_3}}{p_1 p_2 p_3} = p_1^{k_1-1} p_2^{k_2-1} p_3^{k_3-1}$

— divisible by single prime numbers

So the value of $\varphi(p_1^{k_1}p_2^{k_2}p_3^{k_3})$ should be the whole number + double counted numbers − triple counted numbers ("Inclusion-exclusion")

Thus $\varphi(p_1^{k_1}p_2^{k_2}p_3^{k_3}) = p_1^{k_1}p_2^{k_2}p_3^{k_3} - p_1^{k_1-1}p_2^{k_2}p_3^{k_3} - p_1^{k_1}p_2^{k_2-1}p_3^{k_3} - p_1^{k_1}p_2^{k_2}p_3^{k_3-1}$
$+p_1^{k_1-1}p_2^{k_2-1}p_3^{k_3} + p_1^{k_1-1}p_2^{k_2}p_3^{k_3-1} + p_1^{k_1}p_2^{k_2-1}p_3^{k_3-1} - p_1^{k_1-1}p_2^{k_2-1}p_3^{k_3-1}$

$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})(p_3^{k_3} - p_3^{k_3-1})$
$= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\varphi(p_3^{k_3})$

Textbook Problems (4, 5, 17, 21)

#4.

(a). Solution: $3x+4y=14$

$4 = 3\times 1 + 1$

$3 = 3\times 1$

So $1 = 4\times 1 + 3\times(-1)$

Therefore for $m \in \mathbb{Z}$

$3(-14-4m)+4(14+3m)=14.$

(b). Solution: Since the solutions should be natural.

then $\begin{cases} -14-4m \geq 0 \\ 14+3m \geq 0 \end{cases}$

$\Rightarrow -4\frac{2}{3} \leq m \leq -3\frac{1}{2}$

Note that $-14-4m$ and $14+3m$ need to be natural

therefore $m=-4$

So $x = -14 - 4\times(-4) = 2$

$y = 14 + 3\times(-4) = 2$

Thus $x=2, y=2$ is the only pair of such solutions.

MAT246 Rui Qiu 999292509

#5. Solution:

(a). $\varphi(12)=\varphi(2^2\cdot 3)=(2^2-2^1)(3^1-1)=4$

(b). $\varphi(26)=\varphi(2\cdot 13)=(2-1)(13-1)=12$

(c). $\varphi(21)=\varphi(3\cdot 7)=(3-1)(7-1)=12$

(d). $\varphi(36)=\varphi(2^2\cdot 3^2)=(2^2-2^1)(3^2-3^1)=2\times 6=12$

(e). $\varphi(97)=97-1=96$ (97 is a prime)

(f). $\varphi(73)=73-1=72$ (73 is a prime)

(g) $\varphi(101\cdot 37)=(101-1)(37-1)=3600$

(h) $\varphi(3^{100})=3^{100}-3^{100-1}=3^{100}-3^{99}$

#17. Proof: Claim

Since m and n are relatively prime

then $\gcd(m,n)=1$

Say $pm+qn=1$ for some integers p, q (by Bezout Identity)

Then $pm\equiv 1 \bmod n$

and $qn\equiv 1 \bmod m$

4/5 ~~Here we set an $x=bpm+aqn$ for some integers a, b~~

~~Then $x\equiv bpm+bqm+aqn$~~

~~$\equiv a\cdot 1+0$~~

Here we set an $x=aqn+bqm$ for some integers a.b.

Then $x\equiv aqn+bpm$

$\equiv a\cdot 1+0 \bmod m$ and $\equiv 0+b\cdot 1 \bmod n$

$\equiv a \bmod m$ $\equiv b \bmod n$.

Conclusion

#21.

Proof: Since $a^{\varphi(b)} \equiv 1 \bmod b$

$b^{\varphi(a)} \equiv 1 \bmod a$

a, b are coprime ~~positive~~ integers.

~~Then $a^{\varphi(b)} = bk+1$~~

~~$b^{\varphi(a)} = aj+1$ for some integers k, j.~~

~~So $a^{\varphi(b)} + b^{\varphi(a)} = bk+1+aj+1$~~

~~$= a^{\varphi(b)} + aj + 1$~~

Then $a^{\varphi(b)} + b^{\varphi(a)} \equiv 0 + 1 \bmod a \equiv 1 \bmod a$

$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 + 0 \bmod b \equiv 1 \bmod b$

Therefore $a^{\varphi(b)} + b^{\varphi(a)} \equiv aj + 1 = bk + 1$ for some integers j, k.

since ~~$a^{\varphi(b)} - b$~~ $a^{\varphi(b)} + b^{\varphi(a)} - 1 = aj = bk$

so $a \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$

$b \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$

Use the conclusion from Problem 1 in this problem set that $\gcd(a,b) = 1$ and $a \mid c$, $b \mid c \iff ab \mid c$.

$\because bk = aj = a^{\varphi(b)} + b^{\varphi(a)} - 1$

$bx + ay = 1$ for some integers x, y

$\therefore aybk + ajbx = a^{\varphi(b)} + b^{\varphi(a)} - 1$

$\therefore ab(yk + jx) = a^{\varphi(b)} + b^{\varphi(a)} - 1$

$\therefore ab \mid a^{\varphi(b)} + b^{\varphi(a)} - 1$

Hence ~~$ab + ab$~~ $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \bmod ab$.

■