MAT315 HOMEWORK 3 Rui Qiu #999292509

1.

(a). Solution:

① if $m \neq 2^n$ for any natural n.
then m has a prime factor $p \geq 2$.
Let $m = pk$, $k \in \mathbb{Z}$
Since $p > 3$ is odd
and $(p-1) \mid \phi(m) \Rightarrow \phi(m)$ is even. number.

② if $m = 2^n$ for some natural n.
then $\phi(m) = 2^n - 2^{n-1} = 2^{n-1}$ which is also an even

(b). Solution:

Write

$$\phi(m) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$
$$= p_1^{k_1}(p_1-1) \cdots p_r^{k_r}(p_r-1)$$

Set none of $p_i = 2$, so $p_i \equiv 1 \bmod 4$ or $3 \bmod 4$ for all i.
where i is an integer in $[1, r]$

① if $p_i \equiv 1 \bmod 4$
then $p_i^k - p_i^{k-1} \equiv 0 \bmod 4$ (divisible by 4)

② if $p_i \equiv 3 \bmod 4$
then $p_i^k - p_i^{k-1} \equiv 2 \bmod 4$

Why? $3^1 \equiv 3 \bmod 4$, $3^2 \equiv 1 \bmod 4$, $3^3 \equiv 3 \bmod 4$, ...
$3 - 1 \equiv 2 \bmod 4$
$1 - 3 \equiv -2 \equiv 2 \bmod 4$

So if there are 2 p_is congruent to $3 \bmod 4$, then $\phi(m)$ is divisible by 4.

③ if $p_i \equiv 2 \bmod 4 \Rightarrow$ i.e. $p_i = 2$
then for k_i in $p_i^{k_i}$, k_i needs to satisfy $k_i \geq 3$.

2. Solution:

$x \equiv 3 \bmod 7$
$x \equiv 5 \bmod 9$

$x = 7y + 3 \equiv 5 \bmod 9$
$7y \equiv 2 \bmod 9$

$7y - 9z = 2$ for some integer z
write $7u - 9v = \gcd(7,9) = 1$
so by Euclid's Algorithm:
$u = 4, v = 3$
hence $y_1 = 8, z_1 = 6$

hence $x = 8 \times 7 + 3 = 59$.

3. Solution:

$\phi(n) = 160$
divide 160 to 2 parts.
$\phi(n) = 1\times160, 2\times80, 4\times40, \boxed{5\times32}, 8\times20, 10\times16,$
But note that no $\phi(x) = 5$ exists for all x.
List some values.

	$\phi(n)=1$	$\phi(n)=2$	$\phi(n)=4$	$\phi(n)=8$	$\phi(n)=10$
n	2	3	5	15	11
		4	8	16	22
		6	10	20	
			12	24	
				30	

	$\phi(n)=?$	$\phi(n)=20$		$\phi(n)=40$	$\phi(n)=80$	$\phi(n)=160$
n	17	25		41	164	205
	32	33		55	165	⋮
	34	44		75	176	
	40	50		82	⋮	
	60			88		
				100		
				110		
				⋮		

So $\phi(11\times17)=\phi(187)=10\times16=160$

$\phi(11\times32)=\phi(352)=160$

$\phi(11\times40)=\phi(440)=160$

~~$\phi(25\times15)=\phi(375)=160$~~ $\phi(205)=160$

~~$\phi(50\times20)=\phi(1000)=160$~~ $\phi(3\times164)=\phi(492)=160$

Can still find ~~some of the numbers that~~ 7 more numbers.

which are 328, 374, 400, 410, 492, 528, 600, 660.

4. Solution:

$10^4=2^4\times5^4$

(2) $2^{1000}\equiv0 \mod 2^4$

$2^{500}\equiv1 \mod 5^4$ by Euler's formula ($5^4-5^3=500$)

Then $2^{1000}\equiv1 \mod 5^4$

Write. $x=0+2^4y$

$x=1+5^4z$

$x=2^{1000}=16y\equiv1 \mod 625$

$16y-625z=1$

$625=16\times39+1$

So $y=-39,\ z=1$

therefore $x=-39\times16\equiv-624 \mod 10^4$

$\equiv9376 \mod 10^4$.

ie. $2^{1000}\equiv9376 \mod 10^4$.

(3) $3^8 \mod 2^4\equiv1 \mod 2^4$

$3^{500} \mod 5^4\equiv1 \mod 5^4$

so $3^{1000}\equiv1 \mod 5^4$

ie. the last 4 digits are '0001'.

(4) $4^{1000}=(2^2)^{1000}=(2^{1000})^2\equiv9376^2 \mod 10^4\equiv9376 \mod 10^4$.

(5) $5^8 \mod 2^4\equiv1 \mod 2^4 \Rightarrow 5^{1000} \mod 2^4\equiv1 \mod 2^4$

$5^{1000} \mod 5^4\equiv0 \mod 5^4$

Similarly, use Chinese Remainder Theorem and Euclid's Algorithm:

$16y+1=625z \Rightarrow y=39,\ z=1$

so $5^{1000} \mod 10^4\equiv625 \mod 10^4 \Rightarrow$ 4 digits are "0625"

⑥ $6^{1000} \equiv 2^{1000} \cdot 3^{1000} \equiv 9376 \cdot 1 \equiv 9376 \bmod 10^4$.

⑦ ~~$7^8 \bmod 10^4$~~

$7^8 \bmod 2^4 \equiv 1 \bmod 2^4$

$7^{500} \bmod 5^4 \equiv 1 \bmod 5^4$

so $7^{1000} \bmod 10^4 \equiv 1 \bmod 10^4$

⑧ $8^{1000} \equiv (4^{1000})^2 \equiv (9376)^2 \bmod 10^4$

$\equiv 9376 \bmod 10^4$

⑨ $9^{1000} \equiv (3^{1000})^2 \bmod 10^4 \equiv 1 \bmod 10^4$

⑩ $10^{1000} \equiv 0 \bmod 10^4$.

5.

(a). Solution:

Suppose already have a finite list of primes that are congment to 5 mod 6.

Suppose we have

$5, p_1, p_2, \cdots, p_r$.

Let $A = p_1 p_2 \cdots p_r + 5 \equiv 5 \bmod 6$

Know $A = q_1 q_2 \cdots q_s$ for some primes.

① Claim that at least one of q_i's is congruent to 5 mod 6.

if not, $q_1, \cdots, q_s$ would all be 1 mod 6.

(why not 2 mod 6, 3 mod 6, 4 mod 6? NOT PRIME)

so the product $A \equiv 1 \bmod 6$. but $A \equiv 5 \bmod 6$.

So we say $q_j \equiv 5 \bmod 6$

② Claim that for q_j, q_j ∉ the original list.

Because $q_j \mid A$, but none of $5, p_1, \cdots, p_r$ divides A.

Hence the list of primes congruent to 5 mod 6 is infinite.

(b). Counter example:

$19\times5+4=95+4=99=3\times3\times11$ it's not prime.

~~but $3\equiv3 \bmod 5$~~

~~$11\equiv1 \bmod 5$~~

~~neither is $4 \bmod 5$~~

<The problem is that it's possible to get $A\equiv4 \bmod 5$ without any prime factor that is also congruent to 4 mod 5.

6. Solution:

(1). $5!=1\times2\times3\times4\times5 \Rightarrow 2^3 \mid 5!$

$10!=1\times\cdots\times10 \Rightarrow 2^1\cdot2^2\cdot2^3\cdot2^1\cdot2^1=2^8 \Rightarrow 2^8 \mid 10!$

$100! \Rightarrow$ 50 2^1

25 2^2

12 2^3

6 2^4

3 2^5

1 2^6

$50+25+12+6+3+1=97$

$2^{97} \mid 100!$

(2). $p^k \mid n!$

$k=[\frac{n}{p}]+[\frac{n}{p^2}]+\cdots+[\frac{n}{p^t}]$. $t=[\log_p n]$

(3). $p^m \mid n! \Rightarrow m<\frac{n}{p-1}$

Proof: $m\le[\frac{n}{p}]+\cdots+[\frac{n}{p^t}]\le\frac{(p^{t-1}+\cdots+p^0)n}{p^t}=\frac{n\frac{1-p^t}{1-p}}{p^t}=\frac{(1-p^t)n}{(1-p)p^t}<\frac{n}{p-1}$.

b/c $\frac{p^t-1}{(p-1)p^t}<\frac{1}{p-1}$