MAT246 HW3 Rui Qiu 11/20 #999292509

(1). Claim:

Proof: For $p^{p-1} \bmod p-1 \equiv$ ~~$p \bmod p-1$~~ $(1)^{p-1} \bmod p-1 \equiv 1 \bmod p-1$

Then let $p^{p-1} = k(p-1)+1$ for some $k \in \mathbb{Z}$

Hence $a^{p^{p-1}} \equiv a^{k(p-1)+1} \equiv (a^{p-1})^k \cdot a^1 \bmod p$

3/5 ~~3/5~~

By Fermat's Little theorem: ← Hypothesis?

$a^{p-1} \equiv 1 \bmod p$

By the condition $a \nmid p$: Why do we have this?

$a' \bmod p \equiv a \bmod p$

Therefore $a^{p^{p-1}} \equiv (1)^k \cdot a' \bmod p \equiv a \bmod p$. ■

(2).

Solution: The values of b are shown below:

$1 \le a \le 10$	$1 \le b \le 10$	$a \cdot b$	$a \cdot b \bmod 11$
1	1	$1 = 0 \cdot 11 + 1$	1
2	6	$12 = 1 \cdot 11 + 1$	1
3	4	$12 = 1 \cdot 11 + 1$	1
4	3	$12 = 1 \cdot 11 + 1$	1
5	9	$45 = 4 \cdot 11 + 1$	1
6	2	$12 = 1 \cdot 11 + 1$	1
7	8	$56 = 5 \cdot 11 + 1$	1
8	7	$56 = 5 \cdot 11 + 1$	1
9	5	$45 = 4 \cdot 11 + 1$	1
10	10	$100 = 9 \cdot 11 + 1$	1

(3).

Solution: ~~$\therefore 2^{100} \bmod 3 \equiv (2^4)^{25} \bmod 3$~~

For $2^n \bmod 6$ we have:

$2 \bmod 6 \equiv 2$

$2^2 \bmod 6 \equiv 4$

$2^3 \bmod 6 \equiv 2$

$2^4 \bmod 6 \equiv 4$

...

so $2^{2k+1} \bmod 6 \equiv 2$

$2^{2k} \bmod 6 \equiv 4$

for any $k \in \mathbb{Z}^+$

Then $2^{100} \bmod 6 \equiv 4$

Therefore $3^{2^{100}} \equiv 3^{6k+4} \bmod 7$

$\equiv (3^6)^k \cdot 3^4 \bmod 7$ for some $k \in \mathbb{Z}^+$

By Fermat's Little Theorem (note that $3 \nmid 7$)

$3^6 \bmod 7 \equiv 1 \bmod 7$

Then $3^{2^{100}} \equiv (3^6)^k \cdot 3^4 \bmod 7$

$\equiv (1^k) \cdot 3^4 \bmod 7$

$\equiv 81 \bmod 7$

$\equiv 4 \bmod 7$

(4).

(a). Solution: For $3^n \bmod 4$:

$3^1 \bmod 4 \equiv 3$

$3^2 \bmod 4 \equiv 1$

$3^3 \bmod 4 \equiv 3$

$3^4 \bmod 4 \equiv 1$

...

So $3^{2k+1} \bmod 4 \equiv 3$

$3^{2k} \bmod 4 \equiv 1$ for $k \in \mathbb{Z}^+$.

Then $3^{100} \bmod 4 \equiv 1$

Therefore $2^{3^{100}} \equiv 2^{4k+1} \bmod 5$

$\equiv (2^4)^k \cdot 2 \bmod 5$ for some $k \in \mathbb{Z}^+$

By Fermat's Little Theorem

$2^4 \bmod 5 \equiv 1 \bmod 5$

Then $2^{3^{100}} \equiv (2^4)^k \cdot 2 \bmod 5$

$\equiv 1^k \cdot 2 \bmod 5$

$\equiv 2 \bmod 5$

(b). Solution: We want to find the last digit of $2^{3^{100}}$, i.e. we need to calculate $2^{3^{100}} \bmod 10$.

According to Q(3) and Q(4)(a), for some $k \in \mathbb{Z}^+$

$3^{100} \bmod 10 \equiv 3^{4k} \bmod 10 \equiv 1 \bmod 10$

$\equiv 1 \bmod 4$

Say $3^{100} = 4m + 1$ for some $m \in \mathbb{Z}^+$

Then $2^{3^{100}} \equiv 2^{4m+1} \bmod 10$

$\equiv (2^4)^m \cdot 2 \bmod 10$

$\equiv 6 \cdot 2 \bmod 10 \equiv 2 \bmod 10$.

Hence the last digit is 2.

(5). Solution:

$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \bmod 7$

$\equiv 4 \cdot 4 \cdot 5 \cdot 6 \cdot 5 \bmod 7$

~~$\equiv 16 \cdot 30 \bmod 7$~~

~~$\equiv 2 \cdot 2 \bmod 7$~~

~~$\equiv 4 \bmod 7$~~

$\equiv 16 \cdot 5 \cdot 30 \bmod 7$

$\equiv 2 \cdot 5 \cdot 2 \bmod 7$

$\equiv 6 \bmod 7$

(6). Solution:

Let $X = 1 + x + x^2 + \cdots + x^n$, both sides time $(1-x)$ then we have

$$(1-x)X = (1-x)(1+x+x^2+\cdots+x^n)$$
$$= 1 + x + x^2 + \cdots + x^n - x - x^2 - \cdots - x^n - x^{n+1}$$
$$= 1 - x^{n+1}$$

so $X = \frac{1-x^{n+1}}{1-x}$

Then $1 + 2 + 2^2 + \cdots + 2^{219} = \frac{1-2^{220}}{1-2} = 2^{220} - 1$

so $2^{220} - 1 \bmod 13 \equiv 2^4 - 1 \bmod 13 \equiv 15 \bmod 13 \equiv 2 \bmod 13$

(7). Proof: ~~Since $a \nmid bc$~~

Since $\gcd(a,b) = 1$

Then $a \nmid b$ → Always true?

As $bc = b \cdot c$, $a \mid bc$

By Fundamental Theorem of Arithmetic,

~~then $a \nmid b$~~ $a \mid c$. What?

■

If we don't assume $\gcd(a,b) = 1$, then the conclusion may not hold. Here's a counter-example: Give a, b, c explicitly.

Say $bc = (m \cdot n) \cdot (k \cdot l)$ where m, n, k, l are primes.

Then say $a = n \cdot k$, $a \nmid b$, $a \mid c$, $\gcd(a,b) = k \neq 1$

But ~~$a \nmid b$~~ $a \mid bc$.

Hence ~~it~~ it is not true while not assuming $\gcd(a,b) = 1$.

0/5

Problems on textbook:

#6. Proof: $\because 1^2 2^2 3^2 \cdots (p-1)^2 - 1 = (1\cdot 2\cdot 3\cdots(p-1))^2 - 1^2$

$= ((p-1)!+1)((p-1)!-1)$

$\because$ By Wilson's Theorem:

$p \mid (p-1)!+1$ for p is a prime.

$\therefore p \mid ((p-1)!+1)((p-1)!-1)$

$\therefore p \mid 1^2 \cdot 2^2 \cdot 3^2 \cdots (p-1)^2 - 1$ ■

#8.

(a). Solution: By Fermat's Little Theorem that $a^{10k} \equiv 1 \bmod 11$ for any $a, k \in \mathbb{Z}^+$ (*)

Let $a = 9! \times 16 + 4311$. then $a^{3603} \equiv a^{3600} \cdot a^3 \equiv x \bmod 11$ (x is the solution)

Then $(a^{10})^{36} \cdot a^3 \equiv 1 \times a^3 \equiv x \bmod 11$

Since $a \equiv 9! \times 16 + 4311 \equiv 1 \times 5 + 10 \bmod 11 \equiv 4 \bmod 11$

Therefore $x \equiv a^3 \equiv 4^3 \bmod 11 \equiv 64 \bmod 11 \equiv 9 \bmod 11$

So the remainder is 9.

(b). Solution: Since $42! \equiv 1\cdot 2 \cdots 29 \cdot 30 \cdots 42 \bmod 29 \equiv 0 \bmod 29$

$7^{28} \equiv 1 \bmod 29$ (by Wilson's Theorem)

$66 \equiv 8 \bmod 29$

Then $(42)! + 7^{28} + 66 \bmod 29 \equiv 1+8 \bmod 29 \equiv 9 \bmod 29$.

So the remainder is 9.

#13. Proof: According to Wilson's Theorem.

$(p-1)! + 1 \equiv 0 \pmod p$

Good.

Since $(2(p-3)!+1) - ((p-1)!+1) = (p-3)!(2-(p-2)(p-1))$

$= (p-3)!\, p(-p+3)$

$= p(3-p)(p-3)!$

So $p \mid 2(p-3)!+1$

Then $2(p-3)! + 1 \equiv 0 \pmod p$

Therefore $2(p-3)! \equiv -1 \pmod p$ for all primes > 3. ■

MAT246 HW3 Rui Qiu #999292509

#16.

Proof: Suppose k has other prime divisors other than 2, which should be odd of course. Say $k=ab$ and b is odd. What about $b=1$?

So

$$\begin{aligned} 2^k+1 &\equiv 2^{ab}+1 \bmod 2^a+1 \\ &\equiv (2^a)^b+1 \bmod 2^a+1 \\ &\equiv (2^a+1-1)^b+1 \bmod 2^a+1 \\ &\equiv (-1)^b+1 \bmod 2^a+1 \\ &\equiv -1+1 \bmod 2^a+1 \\ &\equiv 0 \bmod 2^a+1 \end{aligned}$$

i.e. 2^k+1 is divisible by 2^a+1

And this contradicts the definition of prime number and the condition of 2^k+1 is a prime.

Thus the assumption is false.

Therefore k has no other prime divisors other than 2. ∎

3

3/5