math115A hw4

Jonas Chen

October 10, 1000

Problem 1

> Use Fermat's Little Theorem to verify that 17 divides $11^{104} + 1$

Solution

$11^{104} = \left(11^2\right)^{52} \equiv 2^{52} = \left(2^{16}\right)^3 \cdot 2^4 \equiv 1 \cdot 16 = 16 \pmod{17}$
Then $11^{104} + 1 \equiv 16 + 1 \equiv 0 \pmod{17}$ as desired. $\square$

Problem 2

> Show that for any integer $n \geq 0, 13 \mid \left(11^{12n+6} + 1\right)$

Solution

$11^{12n+6} = \left(11^{12}\right)^{n} \cdot 11^{6} \equiv 1 \cdot \left(11^{2}\right)^{3} \equiv 4^{3} = 4^{2} \cdot 4^{1} = 3 \cdot 4 = 12 (\operatorname{mod} 13)$ (first equiv by Fermat's little theorem)

Then $11^{12n+6} + 1 \equiv 12 + 1 \equiv 0 (\operatorname{mod} 13)$ as desired. $\square$

Problem 3

> Let a be any integer. Show that a and a^5 have the same last digit.

Solution

Note by Euler's theorem that $a \cdot a^4 \equiv a (\operatorname{mod} 10)$ since $\phi(10) = 4$. This implies $a^5 \equiv a (\operatorname{mod} 10)$ which means that a^5 and a will have the same remainder after dividing by 10, and therefore will have the same last digit.

$\square$

Theorem: **Fermat's little**

> $a^p \equiv a (\bmod p)$ where p is prime
> $a^{p-1} \equiv 1 (\bmod p)$ if and only if $p \nmid a$

Problem 4

> Use Fermat's Little Theorem to show that, if p is an odd prime, then
> (i) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 (\bmod p)$
> (ii) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 0 (\bmod p)$

Solution

(i) Since $p \nmid 1, \ldots, p-1$ this equation mod p by Fermat's little theorem is congruent to $\underbrace{1 + \ldots + 1}_{\text{p-1 times}} = p - 1$

Also, note that $-1 \equiv p - 1 (\bmod p)$ and the claim follows.

(ii) By Fermat's little theorem this equation equals $1 + 2 + 3 + \ldots + (p-1) = \frac{p(p-1)}{2} \equiv 0 (\bmod p)$. (Since p is odd, $p - 1$ is even and divisible by 2)

Problem 5

> Prove each of the following assertions: (i) If n is an odd integer, then $\phi(2n) = \phi(n)$ (ii) If n is an even integer, then $\phi(2n) = 2\phi(n)$ (iii) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$ (iv) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$ (v) $\phi(n) = \frac{n}{2}$ if and only if $n = 2^k$ for some $k \geq 1$. [Hint: Write $n = 2^k N$, where N is odd, and use the condition $\phi(n) = \frac{n}{2}$ to show that $N = 1$]

Solution

(i) 2 and n are coprime therefore $\phi(2n) = \phi(2)\phi(n) = \phi(n)$

(ii) Let k, m be positive integers ≥ 0. Recall that an odd integer times an even integer is even. We can try to take advantage of the fact that ϕ is multiplicative and that $\phi(p^q) = p^{q-1}(p-1) = p^q - p^{q-1}(\dagger)$

Let n be even and m be odd. Then we can try to express n in terms of m. Let $n = 2^k m$ to take advantage of the above. Then $\phi(2n) = \phi\left(2 \cdot 2^k m\right) = \phi\left(2^{k+1}\right)\phi(m) = 2^k \phi(m)$

And $2\phi(n) = 2\phi\left(2^k m\right) = 2\phi\left(2^k\right)\phi(m) = 2\left(2^{k-1}\right)\phi(m) = 2^k \phi(m) \therefore \phi(2n) = 2\phi(n)$ for even n

(iii) $(\Rightarrow)$ Suppose that $\phi(3n) = 3\phi(n)$ and for contradiction assume that $3 \nmid n$. Then 3 and n are corpime therefore $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$. This means that $3 \mid n$

$(\Leftarrow)$ Suppose that $3 \mid n$ Similar to part (ii) we can first note that $n = 3^k m$ where $\left(3^k, m\right) = 1$ and $\phi(3n) = \phi\left(3 \cdot 3^k m\right) = \phi\left(3^{k+1} m\right) = \phi\left(3^{k+1}\right)\phi(m) = \left(3^{k+1} - 3^k\right)\phi(m) = 3\left(3^k - 3^{k-1}\right)\phi(m) = 3\phi\left(3^k\right)\phi(m) = 3\phi\left(3^k m\right) = 3\phi(n)$

(iv) $(\Leftarrow)$ Suppose that $3 \nmid n$ then $(3, n) = 1$ (3 and n are coprime) $\therefore \phi(3n) = \phi(3)\phi(n) = 2\phi(n)$

$(\Rightarrow)$ Suppose that $\phi(3n) = 2\phi(n) \neq 3\phi(n)$. In part (iii) we showed that $3 \mid n \Rightarrow \phi(3n) = 3\phi(n)$. Then the claim follows if we take the contraposition of the previous statement.

(v) $(\Rightarrow)$ First note that n must be even since ϕ returns integers. Then we can write $n = 2^k N$ where N is odd. $\therefore \phi\left(2^k N\right) = 2^{k-1}\phi(N) = 2^{k-1} N$. And $N = \phi(N) \Rightarrow N = 1$. $\therefore \phi\left(2^k N\right) = 2^{k-1} = \frac{n}{2}$
$(\Leftarrow)$ Suppose that $n = 2^k$ then we showed in class that $\phi(n) = 2^{k-1} = \frac{n}{2}(\dagger)$

https://math.stackexchange.com/questions/2578183/is-this-proof-even-valid-is-it-true-that-all-odd-numbers-can-be-uniquely-expres

Note

The totient function $\phi(n)$ count the number of COPRIME integers to n where $n \in \mathbb{Z}^+$

Problem 6

> Use Euler's Theorem to establish the following:
> (i) For any integer a, $a^{37} \equiv a (\text{mod } 1729)$. [Hint: $1729 = 7 \times 13 \times 19$. First consider the case in which $(a, 1729) = 1$]
> (ii) For any odd integer a, $a^{33} \equiv a (\text{mod } 4080)$ [Hint: $4080 = 15 \times 16 \times 17$. First consider the case in which $(a, 4080) = 1$]

Solution

(i) Note that $7, 13, 19$ are coprime. Therefore if we show the following congruences hold:

$$a^{37} \equiv a (\text{mod } 7)$$
$$a^{37} \equiv a (\text{mod } 13)$$
$$a^{37} \equiv a (\text{mod } 19)$$

then it will follow that $a^{37} \equiv a (\text{mod } 7 \times 13 \times 19)$ by the lemma at the end of this document

Using euler's theorem we have

$$a^{\phi(7)} \equiv 1 (\text{mod } 7) \Rightarrow a^6 \equiv 1 (\text{mod } 7) \Rightarrow (a^6)^6 a \equiv a (\text{mod } 7)$$

$$a^{\phi(13)} \equiv 1 (\text{mod } 13) \Rightarrow a^{12} \equiv 1 (\text{mod } 13) \Rightarrow (a^{12})^3 a \equiv a (\text{mod } 13)$$

$$a^{\phi(19)} \equiv 1 (\text{mod } 19) \Rightarrow a^{18} \equiv 1 (\text{mod } 19) \Rightarrow (a^{18})^2 a \equiv a (\text{mod } 19)$$

□

(ii)

The proof is nearly identical to (i)

Note that $\phi(15) = 8 = \phi(16), \phi(17) = 16$

Then $(a^8)^4 a \equiv a (\text{mod } 16), (a^8)^4 a \equiv a (\text{mod } 15), (a^{16})^2 a \equiv a (\text{mod } 17)$ and the claim follows similarly. □

Problem 7

> (a) Use Fermat's Little Theorem to find the last digit of 3^{100}
> (b) Let a be any positive integer. Show that a and a^5 have the same last digit.

Solution

(a) note that $\phi(10) = 4$ therefore $3^{100} = \left(3^4\right)^{25} \equiv 1^{25} \equiv 1 (\operatorname{mod} 10)$
If we want to use Fermat's Little Theorem then we can note that $3^4 \equiv 1 (\operatorname{mod} 2), 3^4 \equiv 1 (\operatorname{mod} 5)$ then $3^4 \equiv 1 (\operatorname{mod} 10)$ by the lemma * at the end of this document

$\therefore \text{the last digit is } \; 1$

(b) proven more generally in problem 3

Problem 8

> (a) Find the remainder when $15!$ is divided by 17
> (b) Find the remainder when $2(26!)$ is divided by 29

Solution

(a) By Wilson's theorem we have that $16! \equiv -1 (\operatorname{mod} 17)$
Then $16! = 15! \cdot 16 \equiv 15!(-1) \equiv -1 \Rightarrow 15! \equiv 1 (\operatorname{mod} 17)$ and the remainder is 1

Note that $-a \equiv -b (\operatorname{mod} n)$ if and only if $a \equiv b (\operatorname{mod} n)$ (Intuitively, if we need to subtract/add k multiples of n from a to get b then we will need to add/subtract k multiples of n to $-a$ to get $-b$) (also we can apply modular arithmetic)

(b) Note that 29 is a prime. Therefore by Wilson's theorem, $28! \equiv -1 (\operatorname{mod} 29)$.

Then $28! = 28 \cdot 27 \cdot 26! \equiv -1 \cdot -2 \cdot 26! \equiv -1 \Rightarrow 2(26!) \equiv -1 \equiv 28 (\operatorname{mod} 29)$ so that the remainder (which must be positive) is 28

Problem 9

> Show that $18! \equiv -1 \pmod{437}$ [Hint: $437 = 19 \times 23$]

Solution

$18! \equiv -1 \pmod{19} (\dagger)$ and $22! \equiv -1 \pmod{23}$

Therefore $22! = 18!4! = 18!(1) \equiv -1 \pmod{23} \Rightarrow 18! \equiv -1 \pmod{23}$. Combining this result with $(\dagger)$ we have that $18! \equiv -1 (\operatorname{mod} 19 \times 23 = 437)$ (by lemma * below)

Lemma: *

> If $m \equiv a \pmod i \wedge m \equiv a \pmod j$ then $m \equiv a \pmod {i \times j}$ if $(i, j) = 1$

Proof:

Suppose the assumption then $m = k_1 i + a = k_2 j + a$ but (i,j) are coprime so in order for the equality to continue to hold we must have $k_1 = l_1 j$ and $k_2 = l_2 i$

Then $m = l_1 ij + a = l_2 ij + a$ and the claim holds.

□

Used by problems 9, 6 , 7