MATH 312 ASSIGNMENT 6 SOLUTIONS

27/11/12

(1) Modulo 10 : $\{1, 3, 7, 9\}$

Modulo 17 : $\{1, 2, 3, 4, \ldots, 15, 16\}$

---

(2) $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4.$

Euler's Thm

Since $\gcd(7, 10) = 1$, $7^{\phi(10)} \equiv 7^4 \equiv 1 \pmod{10}$.

So $7^{999999} = 7^{999996} \cdot 7^3 = (7^4)^{249999} \cdot 7^3$

$$\equiv 1^{249999} \cdot 343 \pmod{10}$$

$$\equiv 3 \pmod{10}.$$

---

(3) $\phi(16) = \phi(2^4) = 2^3 = 8$

Euler's Thm

Since $\gcd(3, 16) = 1$, $3^{\phi(16)} \equiv 3^8 \equiv 1 \pmod{16}$

So $3 \cdot 3^7 \equiv 1 \pmod{16}$.

$$3x \equiv 5 \pmod{16}$$

$$(3^7 \cdot 3)x \equiv 3^7 \cdot 5 \pmod{16}$$

Thus, $x \equiv 3^4 \cdot 3^3 \cdot 5 \pmod{16}$

$\equiv 1 \cdot 3^3 \cdot 5 \pmod{16}$ since $3^4 = 81 \equiv 1 \pmod{16}$

$\equiv 135 \pmod{16}$

$\equiv 7 \pmod{16}$

④ First, notice that $\phi(2^k) = 2^{k-1} \neq 6$ for $k \in \mathbb{N}$.

So if $n \in \mathbb{N}$ s.t. $\phi(n) = 6$, n must be divisible by some odd prime. Thus, we can write the prime power factorisation of n as

$$n = 2^k \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{where } k \in \mathbb{Z}^{\geq 0}$$

$\alpha_i \in \mathbb{N}$

p_i are distinct odd primes.

Now notice that if $p_i \geq 11$, then $\phi(p_i) \geq 10 \nmid 6$.
Also, if $p_i = 5$, $\phi(p_i) = 5 - 1 = 4 \nmid 6$.
Furthermore, for $\alpha_i \in \mathbb{N}$, $\phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)$

$$= p_i^{\alpha_i - 1} \cdot \phi(p_i)$$

which cannot divide 6 for $p_i = 5$ or $p_i \geq 11$.

Thus, the only odd primes that can be in the prime power factorisation of n are 3 & 7.

So we can write $n = 2^k \cdot 3^a \cdot 7^b$, $k, a, b \in \mathbb{Z}^{\geq 0}$

To yield $\phi(n) = 6$, you can check that $b = 0, 1$. If $b = 1$, then $a = 0$ and $k = 0$ or 1.
If $b = 0$, then $a = 2$ and $k = 0$ or 1.

Thus, $n = 7, 9, 14$ or 18.

(5) $n = 101 \Rightarrow \phi(n) = 101 - 1 = 100.$

$\{$ For p prime, $p < 101$, $\phi(p) = p - 1 < 100.\}$

$\{$ For c composite, $c < 101$, $\phi(c) < 100$ because not all positive numbers less than c are coprime with $c \}$.

---

(6) $$f(p^k) = \frac{\phi(p^k)}{p^k} = \frac{p^{k-1}(p-1)}{p^k} = \frac{p-1}{p} = \frac{\phi(p)}{p} = f(p).$$

---

(7) For p prime and $a \in \mathbb{N}$, we know that

$$\sigma(p^a) = p^a + p^{a-1} + \cdots + p^2 + p + 1.$$

When $k = 1$, we need $n = 1$ as $n \geq 2$ has more than 1 positive divisor already. So $k = 1$ only has 1 solution.

When $k \geq 2$, $n \geq 2$, so we can write the prime power factorisation for n as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$ where $\alpha_i \in \mathbb{N}$, $r \in \mathbb{N}$ and p_i are distinct primes.

So $$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}) \quad \{\text{since } \sigma \text{ is multiplicative}\}$$

$$= \prod_{i=1}^{r} (p_i^{\alpha_i} + p_i^{\alpha_i - 1} + \cdots + p_i + 1)$$

We see that $p_i > k \Rightarrow \sigma(n) > k$. So there are only finitely many possible p_i that can occur in the factorisation of n. Also, for each i, α_i is bounded. [For example, we cannot have $p_i^{\alpha_i} > k$] Since there are finitely many possibilities for p_i & $\alpha_i \Rightarrow$ finitely many possibilities for n

⑧ <u>Lemma</u>. For $a, b \in \mathbb{N}$ s.t. $a \mid b$,

$$(2^a - 1) \mid (2^b - 1)$$

$$46189 = 11 \cdot 13 \cdot 17 \cdot 19$$

So, for example, since $11 \mid 46189$,
by the Lemma, $(2^{11} - 1) \mid (2^{46189} - 1)$. ■ {End of solution}

<u>Proof of Lemma</u>.

If you have trouble seeing why the first step is true, think of it as $(2^a - 1) \equiv 0 \pmod{2^a - 1}$

$$2^a \equiv 1 \pmod{2^a - 1}$$

Since $\frac{b}{a} \in \mathbb{N}$, we also have

$$(2^a)^{\frac{b}{a}} \equiv 1^{\frac{b}{a}} \equiv 1 \pmod{2^a - 1}.$$

i.e. $2^b \equiv 1 \pmod{2^a - 1}$

Thus $(2^a - 1) \mid (2^b - 1)$.

(9) $\phi(\phi(19)) = \phi(18) = 6$

So there are 6 incongruent primitive roots of 19.

We note that 2 is a primitive root mod 19:

$$2^{18} \equiv 1 \pmod{19} \text{ by FLT.}$$

but $2^9 \equiv 512 \equiv -1 \not\equiv 1 \pmod{19}$

$2^6 \equiv 64 \equiv 7 \not\equiv 1 \pmod{19}$

(I'm checking 2^d for $d \mid 18$ to double-check that 18 is indeed the smallest positive power s.t. $2^{18} \equiv 1 \pmod{19}$. Thus 2^i, for $i = 1, 2, \ldots, 18$ generates the reduced residue system mod 19).

The reduced residue system mod $\underline{\underline{18}}$ is

$\{1, 5, 7, 11, 13, 17\}$.

So the incongruent primitive roots mod $\underline{\underline{19}}$ are

$$2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$$

or, simplified:

2, 3, 10, 13, 14 and 15.

(10) The polynomial has <u>no</u> roots mod 11.

Because all the powers of x are even, we only need to do "half" the work.

[For e.g. if $x \equiv 3$ is a solution, then

$$x \equiv -3 \equiv 8 \pmod{11} \text{ is also}].$$

x	$x^4+x^2+1 \pmod{11}$
0	1
1	3
2	10
3	3
4	9
5	2

And we conclude there are <u>no</u> solutions to

$$x^4+x^2+1 \equiv 0 \pmod{11}$$

■ {End of answer}

---

x	$x^4+x^2+1 \pmod{11}$
6	2
7	9
8	3
9	10
10	3