Assignment 5

Speaker: Wisely

Question 1

- Suppose $F(x)$ is a polynomial such that all the coefficients are integers

  Also $F(0) = F(1) = 1$

- Show that F does not have any integral root.

  That is, no integer z such that $F(z) = 0$

Solution :

Since $F(0) = F(1) = 1$,

$$F(x) = xQ(x)+1$$

and $$F(x) = (x-1)Q'(x)+1$$

When z is even,

$$F(z) = zQ(z)+1 \neq \text{even}$$

When x is odd,

$$F(z) = (z-1)Q'(z)+1 \neq \text{even}$$

Thus, no integer z can be a root

Question 2

- Show that if n is an odd number, then

$$
\begin{array}{ll}
 & 1 \times 3 \times 5 \times \ldots \times (2n-1) \\
+ & 2 \times 4 \times 6 \times \ldots \times (2n)
\end{array}
$$

is a multiple of $2n + 1$

Solution :

$$1 \times 3 \times 5 \times \ldots \times (2n-1) + 2 \times 4 \times 6 \times \ldots \times (2n)$$

$$\equiv_{2n+1} 1 \times 3 \times 5 \times \ldots \times (2n-1) + (-(2n-1)) \times (-(2n-3)) \times \ldots \times (-3) \times (-1)$$

$$\equiv_{2n+1} 0 \quad (\because n \text{ is odd.})$$

Thus, $1 \times 3 \times 5 \times \ldots \times (2n-1) + 2 \times 4 \times 6 \times \ldots \times (2n)$ is a multiple of $2n+1$

Question 3

- Let p be a prime

- Show that if there exists n such that

$$n^2 \equiv -1 \pmod{p},$$

then $p \not\equiv 3 \pmod{4}$

Proof:

Assume there exists n such that

$$n^2 \equiv -1 \pmod{p}$$

If $p \equiv 3 \pmod{4}$, $(n^2)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

But, by the Fermat's Little Theorem,

$$n^{p-1} \equiv 1 \pmod{p}$$

Thus, $p \not\equiv 3 \pmod{4}$.

Question 4

- Let p be a prime
- Let a and b be two integers coprime to p
- Show that

$$ax \equiv b \pmod{p}$$

if and only if

$$x \equiv a^{p-2}b \pmod{p}$$

Proof :

[$\Rightarrow$]

Since $(a, p) = 1$, if we multiply a^{p-2} to both sides of $ax \equiv b$, we have :

$$a^{p-2}\, ax \equiv x \equiv a^{p-2}\, b \pmod{p}$$

[$\Leftarrow$]

Suppose $x \equiv a^{p-2}b \pmod{p}$. Then we have :

$$ax \equiv a^{p-1}b \equiv b \pmod{p}$$

Question 5

- Prove that if

$$n^j \equiv 1 \pmod m \quad \text{and} \quad n^k \equiv 1 \pmod m,$$

then $\quad n^{\gcd(j,k)} \equiv 1 \pmod m$

Proof :

Assume $aj - bk = \gcd(j, k)$

Then we have :

$$n^{bk} n^{\gcd(j,k)} = n^{aj} \equiv 1 \pmod{m}$$

Since $n^{bk} \equiv 1 \pmod{m}$, $n^{\gcd(j,k)} \equiv 1 \pmod{m}$

Question 6

- Prove that $\varphi(n^m) = n^{m-1}\varphi(m)$
- Proof :

Assume $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$

$$\varphi(n^m) = n^m \times (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_k})$$

$$= n^{m-1} \times [n \times (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_k})]$$

$$= n^{m-1}\varphi(n)$$

Question 7

- Compute $\varphi(999)$

- Solution :

$$999 = 3 \times 3 \times 37$$

$$999(1 - \frac{1}{3})(1 - \frac{1}{37}) = 648$$

Question 8

- *n* is a perfect number if the sum of all the proper divisors of *n* is exactly *n*

- Example:

$$6 = 1 + 2 + 3 = 6$$

$$28 = 1 + 2 + 4 + 7 + 14 = 28$$

Question 8

Theorem 1 (By Euler).

An even number n is a perfect number if and only if

$$n = 2^m(2^{m+1} - 1) \text{ and } 2^{m+1} - 1 \text{ is prime}$$

- Show that Theorem 1 is correct

Proof :

(🡐)

Since $n = 2^m(2^{m+1} - 1)$ and $2^{m+1} - 1$ is prime,

all the divisors of n are

$$1,\ 2,\ 2^2,\ 2^3,\ \quad \ldots \quad,\ 2^{m-1},\ 2^m,$$

$$(2^{m+1} - 1),\ 2\,(2^{m+1} - 1),\ \quad \ldots \quad,\ 2^m(2^{m+1} - 1)$$

Thus, the sum of these divisors is exactly

$$(2^{m+1} - 1) + (2^{m+1} - 1)\,(2^{m+1} - 1) = 2n$$

Proof : ($\Rightarrow$)

Suppose n is an even number, so that we can express n as $2^m Q$ for some odd integer Q

Let $\sigma(Q)$ = the sum of all divisors of Q

Let $d_1, d_2, .., d_k$ be all the divisors of Q

Then the divisors of n are :

$$1, 2, 2^2, 2^3, \ldots, 2^m,$$

$$d_1, 2d_1, 2^2 d_1, \ldots, 2^m d_1,$$

$$\ldots.$$

$$d_k, 2d_k, 2^2 d_k, \ldots, 2^m d_k$$

Proof (cont) :

The sum of all the divisors of n is :

$(2^{m+1} – 1)[1+d_1+d_2+\ldots+ d_k] = (2^{m+1} – 1)\ \sigma(Q)$

Thus, for n to be perfect, we need :

$$2n = 2^{m+1}Q = (2^{m+1}–1)\,\sigma(Q)\ .$$

Since $(2^{m+1}, 2^{m+1} – 1) = 1$,

Q would be a multiple of $2^{m+1} –1$

Suppose Q= $(2^{m+1} – 1)q$

➔ $\sigma(Q) \geqq Q + q$ (by the definition of $\sigma(Q)$).

Proof (cont) :

Then, $2^{m+1}q = \sigma(Q) \geqq Q+q = 2^{m+1}q$

Equivalently,

$$\sigma(Q) = Q+q$$

➔ Q must be a prime (by definition of $\sigma(Q)$)

➔ q must be 1

Thus, $n = 2^m(2^{m+1}-1)$ and $(2^{m+1}-1)$ is a prime

Question 9

- Show that for all $n > 1$,

$$2^n \not\equiv 1 \pmod{n}$$

Proof :

Let $n=pQ$, where p = smallest prime divisor of n

Suppose on the contrary that $2^n \equiv 1 \pmod{n}$

Then $2^n \equiv 1 \pmod{p}$

Also $2^{p-1} \equiv 1 \pmod{p}$

By Question 5, we have

$$2^{\gcd(p-1,n)} \equiv 1 \pmod{p}$$

However, by the choice of p, n has no divisor less than p ➔ $\gcd(p-1, n) = 1$

Thus, $2 \equiv 1 \pmod{p}$ and a contradiction occurs