Assignment 2

Numbers Made Dumber — Abhishek Shree
Project #13 — Roll: 200028

1. Given the polynomial

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

with integer coefficients $a_1, a_2, ..., a_n$ and given also that there exist four distinct integers a, b, c, d such that $f(a) = f(b) = f(c) = f(d) = 5$ show that there is no integer k such that $f(k) = 8$.

Sol. According to the problem $f(x) - 5$ has 4 distinct roots a, b, c, d

$$\therefore f(x) - 5 = g(x)(x-a)(x-b)(x-c)(x-d)$$

Let there be an $x = k \in \mathbb{Z}$ such that $f(x) = 8$. Then,

$$g(k)(k-a)(k-b)(k-c)(k-d) = 3$$

But as 3 has only 3 factors 1, -1, 3 all the five terms i.e. $g(k)$, $(k-a)$, $(k-b)$, $(k-c)$, $(k-d)$ cannot be distinct simultaneouly.

$\therefore f(x)$ can never be equal to 8 for any integral value of x.

---

2. Show that the cube roots of three distinct prime numbers cannot be three terms (not necessarily consecutive) of an arithmetic progression.

Sol. We can prove this by contradiction,

Let the three primes be a, b and c and common difference be d. Then,

$$\sqrt[3]{b} - \sqrt[3]{a} = \alpha d \tag{1}$$

$$\sqrt[3]{c} - \sqrt[3]{b} = \beta d \tag{2}$$

Dividing (1) by (2), we get

$$\frac{\sqrt[3]{b} - \sqrt[3]{a}}{\sqrt[3]{c} - \sqrt[3]{b}} = \frac{\alpha}{\beta}$$

$$\implies \alpha\sqrt[3]{c} + \beta\sqrt[3]{a} = (\alpha+\beta)\sqrt[3]{b} \tag{3}$$

Cubing equation (3) we get the <u>RHS as a rational number</u> and <u>LHS as an irrational number</u>, hence a contradiction arrises.

3. For which prime p is p^2+2 also prime?

Sol. Here, p cannot be 2 as p^2+2 will be even, and there are no even primes grater than 2.
Next $p=3$. Let p be some number not divisible by 3.
If $p = 3k+1 \implies p^2+2 = 9k^2+6k+1+2 = 3(3k^2+2k+1)$
If $p = 3k+2 \implies p^2+2 = 9k^2+12k+4+2 = 3(3k^2+4k+2)$
We get that p^2+2 is always divisible by 3 for any p not being a multiple of 3.
$\therefore p$ is a prime and a multiple of 3 i.e. $\boxed{p=3}$ and $p^2+2=11$ which is a prime too.

---

4. Show that if $p>1$ and p divides $(p-1)!+1$, then p is prime.

Sol. We can prove this by contradiction. Let's say p is not a prime but it divides $(p-1)!+1$.
As p is not a prime, p will have a factor $1<x<p$.
x will also divide $(p-1)!+1$, also x obviously divides $(p-1)!$ as $x \leq (p-1)$, hence our assumption implies that x divides 1. Thus a contradiction arrises here.
Hence, p cannot be composite if it divides $(p-1)!+1$, therefore p is a prime.

---

5. Show that $F_0F_1...F_{n-1} = F_n - 2$ for all $n \geq 1$, where F_i is the i-th fermat number.

Sol. Given:

$$F_0F_1...F_{n-1} = F_n - 2$$

$$\therefore F_0F_1...F_{n-1}F_n = (F_n-2)F_n$$

Now, $F_n = 2^{2^n}+1$

$$\begin{aligned}\therefore (F_n-2)F_n &= (2^{2^n}-1)(2^{2^n}+1)\\ &= 2^{2^{n+1}}+1\\ &= F_{n+1}-2\end{aligned}$$

$$\therefore \boxed{F_0F_1...F_{n-1}F_n = F_{n+1}-2}$$

Hence, by replacing n by n-1 we get $F_0F_1...F_{n-1} = F_n - 2$

---

6. Evaluate the Mersenne number M_{17}, and determine whether it is prime.

Sol. $M_{17} = 2^{17} - 1 = 131071$

If p is an odd prime, then any prime divisor of M_p ***is of the form*** $2kp+1$***.*** [1]

Numbers of such form ≤ 362 ($\approx \sqrt{131071}$) are 35, 79, 103, 137, 171, 205, 239, 273, 307, 341.

Now 35, 171, 205, 273, 341 are not primes, so we don't have to check for those numbers.

Finally 131071 is not divisible by 79, 103, 137, 239, 307.

$\therefore$ We can conclude that $M_{17} = 131071$ is a prime number.

---

7. Are the following statements true or false, where a and b are positive integers and p is prime? In each case, give a proof or counterexample.

(1) If $\gcd(a, p^2) = p$ then $\gcd(a^2, p^2) = p^2$

(2) If $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p^2$ then $\gcd(ab, p^4) = p^3$

(3) If $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p$ then $\gcd(ab, p^4) = p^2$

(4) If $\gcd(a, p^2) = p$ then $\gcd(a+p, p^2) = p$

Sol.

(1) $\gcd(a, p^2) = p \implies p|a \implies p^2|a^2$

$\therefore \gcd(a^2, p^2) = p^2$ is $\boxed{\text{TRUE}}$

(2) Let $a = 2$, $p = 2$ and $b = 8$ then $\gcd(2, 4) = 2 = \gcd(a, p^2) = p$,

$\gcd(8, 4) = 4 = \gcd(b, p^2) = p^2$

But, $\gcd(ab, p^4) = \gcd(16, 16) = 16 \neq p^3$.

Hence the statement is $\boxed{\text{FALSE}}$

(3) We can say that $a = \alpha p$ and $b = \beta p$ such that α and β are coprime to p.

$\therefore ab = p^2(\alpha\beta)$ such that $p \nmid \alpha\beta$. Hence, the statement is $\boxed{\text{TRUE}}$

(4) If $a = \alpha p$ then $a + p = (\alpha+1)p$

Now $\gcd((\alpha+1)p, p^2) = p^2$ if $(\alpha+1)p = p^2$ or $\alpha = p - 1 \implies a = p^2 - p$

Hence the statement is $\boxed{\text{FALSE}}$
