Math 209-16 Homework 1

Due Date: Sep 15, 2022

P1.(1 pt) Prove that $n^2 - n$ is divisible by 2 for every integer n; that $n^3 - n$ is divisible by 6; that $n^5 - n$ is divisible by 30.

Proof. Since $n^2 - n = (n-1)n$, and either $n-1$ or n is even, $2 \mid (n^2 - n)$. Similarly, $n^3 - n = (n-1)n(n+1)$, thus, we have $2 \mid (n^3 - n)$ and $3 \mid (n^3 - n)$, which imply that $6 \mid (n^3 - n)$ because $(2, 3) = 1$. Finally, $n^5 - n = (n-1)n(n+1)(n^2+1)$, we have shown that $6 \mid (n^5 - n)$ so it suffices to show that $5 \mid (n^5 - n)$. This can be done by considering $n = 5k + i$ for $i = 0, 1, 2, 3, 4$. $\square$

P2.(2 pts) Let $n \geqslant 2$ and k be any positive integers. Prove that $(n-1)^2 \mid (n^k - 1)$ if and only if $(n-1) \mid k$.

Proof. $n^k - 1 = ((n-1)+1)^k - 1 = \sum_{i=0}^{k} \binom{k}{i} (n-1)^i - 1 = \sum_{i=1}^{k} \binom{k}{i} (n-1)^i$, since $(n-1)^2 \mid \binom{k}{i}(n-1)^i$ for $i \geqslant 2$, we see that $(n-1)^2 \mid (n^k - 1)$ if and only if $(n-1)^2 \mid \binom{k}{1}(n-1)$, i.e., $(n-1) \mid k$. $\square$

P3.(2 pts) Evaluate (ab, p^4) and $(a+b, p^4)$ given that $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime.

Solution. Since $(a, p^2) = p$ and $(b, p^3 = p^2)$, we can write $a = a_1 p$ and $b = b_1 p^2$ for some $a_1, b_1 \in \mathbb{Z}$ with $(a_1, p) = (b_1, p) = 1$. Then we have

$$(ab, p^4) = (a_1 b_1 p^3, p^4) = p^3 (a_1 b_1, p) = p^3$$
$$(a+b, p^4) = (a_1 p + b_1 p^2, p^4) = p(a_1 + b_1 p, p^3) = p$$

The last equality in the second row follows because $p \nmid (a_1 + b_1 p)$. $\square$

P4.(2 pts) For any positive integer $n > 1$, prove that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.

Proof. Let 2^k be the largest power of 2 less than or equal to n. Then 2^k cannot divide $i \in \{1, ..., n\}$ except for $i = 2^k$. If not, suppose $i = 2^k i_1$ with $i_1 \geqslant 3$, then $2^{k+1} \leqslant i \leqslant n$, which is a contradiction! Then we have

$$2^{k-1}(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}) = 2^{k-1} \sum_{i \in \{2^m \mid m=1,...,k\}} \frac{1}{i} + 2^{k-1} \sum_{i \in \{2,...,n\} \setminus \{2^m \mid m=1,...,k\}} \frac{1}{i}$$

The first term is $2^{k-2} + \cdots + 1 + \frac{1}{2}$, and the second term is $\frac{2^{k-1}}{3} + \frac{2^{k-1}}{5} + \frac{2^{k-2}}{3} + \cdots$ whose denominator is odd after simplification. Therefore, the sum of them is not an integer, namely, $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer. $\square$

P5.(3 pts) Prove that if $m > n$ then $a^{2^n} + 1$ is a divisor of $a^{2^m} - 1$. Show that if a, m, n are positive with $m \neq n$, then

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{if } a \text{ is even,} \\ 2, & \text{if } a \text{ is odd.} \end{cases}$$

Proof. Notice that

$$\begin{aligned} a^{2^m} - 1 = (a^{2^{n+1}})^{2^{m-n-1}} - 1 &= (a^{2^{n+1}} - 1)((a^{2^{n+1}})^{2^{m-n-1}-1} + \cdots + 1) \\ &= (a^{2^n} + 1)(a^{2^n} - 1)((a^{2^{n+1}})^{2^{m-n-1}-1} + \cdots + 1) \end{aligned}$$

so $a^{2^n} + 1$ is a divisor of $a^{2^m} - 1$ if $m > n$. For the second part, we may assume $m > n$, then $(a^{2^m} + 1, a^{2^n} + 1) = (a^{2^m} - 1 + 2, a^{2^n} + 1) = (2, a^{2^n} + 1)$. If a is even, then $a^{2^n} + 1$ is odd $\Longrightarrow (2, a^{2^n} + 1) = 1$, otherwise, $(2, a^{2^n} + 1) = 2$, which completes the proof. $\square$

P6.(2 pts) Use the result in Problem 5 to show that there are infinitely many primes.
Proof. Suppose that there are only finitely many primes. Consider the sequence $\{2^{2^n} + 1\}_{n=1}^{\infty}$, they are coprime to each other, which is impossible. $\square$

P7.(3 pts) Show that if $(a, b) = 1$ and p is an odd prime, then $(a + b, \frac{a^p + b^p}{a+b}) = 1$ or p.
Proof. Let $(a + b, \frac{a^p+b^p}{a+b}) = d$, then $d \mid (a + b) \iff a \equiv -b \pmod{d}$, moreover, $d \mid \frac{a^p+b^p}{a+b} = (a^{p-1} - a^{p-2}b + \cdots + b^{p-1})$ since p is an odd prime, or equivalently,

$$a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \equiv 0 \pmod{d}$$

Therefore, $a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \equiv a^{p-1} + a^{p-1} + \cdots + a^{p-1} \equiv pa^{p-1} \equiv 0 \pmod{d}$. If $d \mid a$, then $d \mid ((a + b) - a) = b \Longrightarrow d \mid (a, b) = 1 \Longrightarrow d = 1$. If $d \nmid a$, then $d = p$. $\square$

P8.(2 pts) Prove that $n^2 - 81n + 1681$ is a prime for $n = 1, 2, 3, ..., 80$, but not for $n = 81$.
Proof. By direct verification.

P9.(3 pts) Prove that no polynomial $f(x)$ of degree > 1 with integral coefficients can represent a prime for every positive integer x.
Proof. It's equivalent to proving this for every nonnegative integer x because we can set $g(x - 1) = f(x)$. Assume that $f(x) = a_n x^n + \cdots + a_0$ with $a_i \in \mathbb{Z}$ can represent a prime for every nonnegative integer x. Then $a_n > 0$ and $a_0 = f(0)$ is a prime, however, $f(ma_0) = a_n(ma_0)^n + \cdots + a_0 = a_0(a_n m^n a_0^{n-1} + \cdots + 1)$ is not a prime for sufficiently large m, which contradicts the assumption. $\square$