Problem Solving Session

March 2022

1 Notation

1. $\mathbb{N} = \{1, 2, 3 \cdots\}$
2. $\mathbb{P}_n = \{p \in \mathbb{P} : p|n,\ n \in \mathbb{N}\}$
3. iff:= if and only if
4. Any problem in the problem section that is starred (*) is a standard theorem as well and therefore is highly recommended to be learnt.

2 Problem Solutions

Problem 2.1. Give an example of 20 consecutive numbers being composite.

Proof. The main idea for the problem is that composite numbers should be readily factorizable to test whether they are indeed composite.
Consider $\{21! + 2, 21! + 3, \cdots, 21! + 21\}$. □

Problem 2.2. Determine with proof whether following is an integer or not :

$$N = \sqrt{1976^{1977} + 1978^{1979}}.$$

Proof. Note that this should most likely not be an integer (Intuition). If N is an integer than there exists $x \in \mathbb{N}$ such that

$$x^2 = 1977^{1976} + 1981^{1979},$$

However $x^2 \equiv 0, 1 \pmod 4$, while $1977^{1976} + 1982^{1979} \equiv 2 \pmod 4$. □

Problem 2.3. Prove that for $m, n \in \mathbb{N}$

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn},$$

whenever $\gcd(m, n) = 1$.

Proof. By Euler's theorem,

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{n},$$
$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{m}.$$

Now either by CRT (Chinese Remainder Theorem) or by the following argument we have our proof. This implies that $1 + n\alpha = 1 + m\beta \iff n\alpha = m\beta$ for some $\alpha, \beta \in \mathbb{Z}$. Since $\gcd(n, m) = 1$, we have that $m|\alpha$, which implies that $\alpha = md$, where d is some integer. Hence $m^{\varphi(n)} + n^{\varphi(m)} = 1 + n\alpha = 1 + nmd$. □

Problem 2.4. Prove that

$$\sum_{d|n} \tau^3(d) = \left(\sum_{d|n} \tau(d)\right)^2.$$

Proof. Note that since τ is multiplicative so are are both the summation functions on the either side of the equality. Therefore all that remains is to check that the equality holds for prime powers.

If $n = p^a$ then

$$\sum_{d|n} \tau^3(d) = 1^3 + 2^3 + \cdots + (a+1)^3 = (1 + \cdots + a)^2 = \left(\sum_{d|n} \tau(d)\right)^2.$$

□

Problem 2.5. (Simon Marais 2021) Define the sequence of integers $a_1, a_2, \cdots$ by $a_1 = 1$ and

$$a_{n+1} = (n + 1 - \gcd(a_n, n)) \times a_n$$

for all integers ≥ 1. Prove that $\frac{a_{n+1}}{a_n} = n \iff n \in \mathbb{P}$ or $n = 1$.

Proof. One of the preliminary observation that one makes quite readily is that $a_j | a_n, \forall\ 1 \leq j < n$. In fact going along these lines a power full observation/conjecture that one can actually prove is that $p|a_n$ if and only if $p < n,\ p \in \mathbb{P}$. Note that this fact is enough to resolve the problem, try to see why.

Lemma: We proceed to prove the proposition $P(n)$ that $p|a_n$ iff $p \in \mathbb{P}$ such that $p < n$.

Proof. Clearly $P(1)$ holds trivially. We assume that $P(k)$ holds for some positive integer k.

Note that $1 \leq \gcd(a_n, n) \leq n$ implying that $a_n \leq a_{n+1} \leq na_n$ and combined with the induction hypothesis we arrive at the fact that $a_{n+1} = (n + 1 - \gcd(a_n, n))a_n$ is divisible by all primes less than n and is not divisible by any prime greater than or equal to n. It follows that $P(n + 1)$ holds.

$\square$

Note that if n is composite than $\gcd(a_n, n) = k > 1$ therefore $a_{n+1} < na_n$ while if n is prime than $a_{n+1} = na_n$ using the lemma.

$\square$

Problem 2.6. (Wilson's Theorem)* A natural number $n > 1$ is prime $\iff$

$$(n-1)! \equiv -1 \pmod{n}.$$

Hint: Consider the polynomial $g(x) = (x - 1)(x - 2) \cdots (x - (p - 1))$.

Proof. The result holds when $p = 2$ therefore we consider odd primes $p \geq 3$. Consider the polynomial $g(x) = (x - 1)(x - 2) \cdots (x - (p - 1))$ where the constant term (being $(p - 1)!$) is what we are interested in.

Note that $h(x) = x^{p-1} - 1$ has the same roots as $g(x)$ modulo p. So if we consider $f(x) = (g - h)(x)$ then we have $\deg f$ at most $p - 2$ having roots $1, 2, \cdots, p - 1$. But note that since $\mathbb{Z}/p$ is a field therefore a polynomial over the field has at most as many roots as its degree therefore f has at most $p - 2$ roots which contradicts what we had earlier except if $f \equiv 0$, so its constant term is $(p - 1)! + 1 \equiv 0 \pmod{p}$. $\square$

Problem 2.7. (Putnam A3 2014) Let $a_0 = 5/2$ and $a_k = a_{k-1}^2 - 2$ for $k \geq 1$. Compute

$$\prod_{k=0}^{\infty} \left(1 - \frac{1}{a_k}\right).$$

Proof. Since the recursion is non-linear. We try to find other ways to either find a explicit formulation or find facts that directly relate to the question.

Note that $a_0 = 2 + \frac{1}{2}$ this effectively give us the explicit form for our recurrence sequence, $a_1 = \left(2 + \frac{1}{2}\right)^2 - 2 = 2^2 + \frac{1}{2^2}$. Implying

$$a_k = 2^{2^k} + \frac{1}{2^{2^k}},$$

which is a clearly increasing unbounded sequence, $\lim_{n\to\infty} a_n \to \infty$.

Using $a_{k+1} + 1 = (a_k - 1)(a_k + 1)$, we have

$$\prod_{k=0}^{\infty} \left(1 - \frac{1}{a_k}\right) = \frac{2}{7} \frac{a_{n+1} + 1}{a_0 a_1 \cdots a_n},$$

Using the identity

$$\prod_{k=0}^{n}\left(1+x^{2^k}\right)=\frac{x^{2^{n+1}}-1}{x-1},\ x\in\mathbb{R},$$

we see that

$$a_0a_1\cdots a_n=\frac{2}{3}\frac{4^{2^{n+1}}-1}{2^{2^{n+1}}}.$$

Hence

$$\lim_{n\to\infty}\prod_{k=0}^{\infty}\left(1-\frac{1}{a_k}\right)=\frac{3}{7}$$

□

Problem 2.8. Let n be a positive integer. Prove that

$$\sum_{k\geq 1}\varphi(k)\left\lfloor\frac{n}{k}\right\rfloor=\frac{n(n+1)}{2}.$$

Proof. The key idea is to rewrite the floor as a sum involving divisors:

$$\sum_{k\geq 1}\varphi(k)\left\lfloor\frac{n}{k}\right\rfloor=\sum_{k\geq 1}\varphi(k)\sum_{\substack{m\leq n\\ k|m}}1=\sum_{k\geq 1}\sum_{\substack{m\leq n\\ k|m}}\varphi(k),$$

$$\sum_{k\geq 1}\sum_{\substack{k|m\\ m\leq n}}\varphi(k)=\sum_{m=1}^{n}\sum_{k|m}\varphi(k)=\sum_{m=1}^{n}m.$$

□