UBC Math Circle 2020 Problem Set 6

Problems will be ordered roughly in increasing difficulty

1. Let $n, k \in \mathbb{Z}^+$ with $n \geq 2$. Prove that $(n-1)^2 \mid (n^k - 1)$ iff $(n-1) \mid k$.

Solution: We factor $n^k - 1 = (n-1)(n^{k-1} + \cdots + 1$. Thus we have $(n-1)^2 \mid (n^k - 1)$ iff $(n-1) \mid \sum_{i=0}^{k-1} n^i$. However, as we already observed, $(n-1) \mid (n^i - 1)$ for every $i > 0$. Therefore $(n-1) \mid \sum_{i=0}^{k-1}(n^i - 1) = \left(\sum_{i=0}^{k-1} n^i\right) - k$. Hence $(n-1) \mid \sum_{i=1}^{k-1} n^i$ iff $(n-1) \mid k$.

2. Let f be a nonconstant polynomial with integer coefficients. Prove that there exists $n \in \mathbb{Z}^+$ such that $f(n)$ is composite.

Extension: prove that
$S := \{p$ prime such that there are infinitely many positive integers n satisfying $p \,|\, f(n)\}$ is infinite.

Solution: Because $f(x) = a_k x^k + \cdots + a_0$ is non-constant, it cannot be bounded, ie it takes on values outside $\{0, 1, -1\}$. This is because $f(x)$, $f(x) - 1$, and $f(x) + 1$ can only have finitely many roots. Pick $n \in \mathbb{Z}^+$ such that $f(n) \notin \{0, 1, -1\}$. If $f(n)$ is composite, we win, so suppose it is a prime, call it p. Then consider

$$f(n + mp) = a_k(n + mp)^k + \cdots + a_0 = a_k n^k + ... + a_0 + \sum_{i=0}^{k} a_i \sum_{j=0}^{i} \binom{i}{j} n^{i-1} n^j (mp)^{i-j}$$

The first bit is just $f(n) = p$, whereas the second bit is divisible by p because every term in the sum has a non-zero power of p. Therefore, $p \mid f(n + mp)$ for all m. Thus $|f(n + mp)| \geq p$, with equality at most finitely many times, coming from the fact that $f(x) + p$ and $f(x) - p$ has at most finitely many roots. Hence, we can find some m such that $f(n + mp)$ is properly divisible by p, a composite number.

Extension: Let $S' = \{p$ prime: there exists some positive integer n such that $p \,|\, f(n)\}$.

We claim $S = S'$. Clearly $S \subset S'$. Now consider any element $q \in S'$. Then, there exists some positive integer $\hat{n}$ such that $q \,|\, f(\hat{n})$. Then, we also have that $q \,|\, f(\hat{n} + kq)$ for any $k \in \mathbb{N}$, which implies $q \in S$. Hence, $S' \subset S$, and thus $S = S'$.

So it suffices to show that S' is infinite. Suppose not, that S' consisted of finitely many distinct primes p_1, p_2, ..., p_r. We can also treat the case $r = 0$ if we take the convention that the value of the empty product is equal to 1 in the rest of the proof.

Now $f(1) \neq 0$, since if $f(1) = 0$, then every prime would divide $f(1)$, contradicting S' finite. For each $1 \leq i \leq r$, define $e_i = \exp_{p_i}(f(1))$.

Let $M = \prod_{i=1}^{r} p_i^{e_i+1}$. Note for all $k \in \mathbb{N}$, we have $f(1) \equiv f(1+kM) \pmod{M}$. In particular, for each $1 \leq i \leq r$, $\exp_{p_i}(f(1+kM)) = e_i$.

Note $\prod_{i=1}^{r} p_i^{e_i} = |f(1)|$, as $|f(1)|$ has no prime factors outside of S'. Thus, for all $k \in \mathbb{N}$, $f(1) \mid f(1+kM)$, and $p_i \nmid \frac{f(1+kM)}{f(1)}$ for all $1 \leq i \leq r$.

Since f is nonconstant, there exists some $k_0 \in \mathbb{N}$ such that $f(1+k_0M) \notin \{\pm f(1)\}$. Then $\frac{f(1+k_0M)}{f(1)} \notin \{\pm 1\}$, and so there exists some prime p such that $p \mid \frac{f(1+k_0M)}{f(1)}$. Moreover, $p \neq p_i$ for any $1 \leq i \leq r$. But $p \mid f(1+k_0M)$ and so $p \in S'$, contradiction.

So $S' = S$ is infinite.

3. Show that there are infinitely many $n \in \mathbb{Z}^+$ such that $\lfloor n\sqrt{2} \rfloor$ is a power of 2.

Solution: In binary expansion, $\frac{1}{\sqrt{2}} = \sum_{i=1}^{\infty} d_i 2^{-i}$, where $d_i \in \{0,1\}$. Since $\frac{1}{\sqrt{2}}$ is irrational, The d_i's contain infinitely many 0 and infinitely many 1.

Consider $k \in \mathbb{N}$ such that $d_{k+1} = 1$. Let $x_k = \sum_{i=1}^{k} d_i 2^{-i}$. Then $\frac{1}{\sqrt{2}} - 2^{-k} < x_k < \frac{1}{\sqrt{2}} - 2^{-(k+1)}$. Let $n_k = 1 + 2^k x_k = 1 + \sum_{i=1}^{k} d_i 2^{k-i} \in \mathbb{Z}^+$.

Then $1 + 2^k\left(\frac{1}{\sqrt{2}} - 2^{-k}\right) < n_k = 1 + 2^k x_k < 1 + 2^k\left(\frac{1}{\sqrt{2}} - 2^{-(k+1)}\right)$

$\Rightarrow 2^k < n_k\sqrt{2} < 2^k + 1$

$\Rightarrow \lfloor n_k \rfloor = 2^k$.

There are infinitely many k such that $d_{k+1} = 1$, so there are infinitely many such n_k.

4. Let $n \in \mathbb{N}$. Let F_k be the k-th Fibonacci number, defined by $F_k = F_{k-1} + F_{k-2}$, and $F_1 = 1 = F_2$. Show that there is some m such that F_m ends with n consecutive 9's (in base 10).

Solution: We observe that $F_{-1} = -1$. We will show that F_n is cyclic modulo k for any k, so there will indeed be a positive m such that $F_m \cong -1$ modulo k. In the case that $k = 10^n$, this means that F_m ends in n consecutive 9's.

We have $F_n = F_{n-1} + F_{n-2}$. There are at most k^2 possible pairs (F_{n-1}, F_{n-2}) modulo k, so after k^2 terms in the sequence, we must have a pair that repeats. Once we repeat one such pair, we repeat the pair (F_n, F_{n-1}) as well, and so on, so we repeat all F_n (modulo k), with a period of at most k^2.

5. Let p, q be primes such that $p = 2q + 1$. Show that some positive integer multiple of p has digit sum at most 3 (in base 10).

Solution: If $p = 5$, then $10 = 2 \cdot 5$ satisfies, since it has digit sum 1. Else, p and 10 are relatively prime.

By Fermat's little theorem, $10^{2q} \equiv 1 \bmod p$. Since p is prime, either $10^q \equiv -1 \bmod p$ or $10^q \equiv 1 \bmod p$. If it's the former case, $10^q + 1$ is a multiple of p with digit sum of 2.

If it's the latter case, we note $\text{ord}_p(10) = q$ (since the order must divide q prime, and it isn't 1 since $p \neq 3$). So 10^1, 10^2, ..., 10^q have distinct residues modulo p.

If there exist $1 \leq a, b \leq q$ such that $10^a \equiv -10^b \bmod p$, then $10^a + 10^b$ satisfies.

Otherwise, let S be the set of residues modulo p among 10^1, 10^2, ..., 10^q. Then for any nonzero residue x modulo p, $x \in S$ iff $-x \notin S$.

Now assume, by way of contradiction, that there do not exist $x, y, z \in S$ such that $x+y+z \equiv 0 \bmod p$. Then, $\forall x, y \in S$, we note that $x+y$ is a nonzero residue modulo p with $-(x+y) \notin S$, i.e. $x + y \in S$. So S is closed under addition (modulo p). But $10^q \equiv 1 \bmod p \in S$, which implies that every residue modulo p must be in S. This contradicts $|S| = q < p$.

So there must exist $x, y, z \in S$ such that $x+y+z \equiv 0 \bmod p$. This gives $1 \leq a, b, c \leq q$ such that $10^a + 10^b + 10^c \equiv 0 \bmod p$. This positive integer multiple of p has digit sum 3.

6. (Indonesia MO 2005) Let $p(n)$ be the product of the digits of n, in base 10. Find all n such that $11p(n) = n^2 - 2005$. Bonus: Find all n such that $4p(n) = n^2 - 2020$.

Solution: We first show that n must have exactly two digits. If n had one digit, then $11p(n) = 11n > 0$, and $n^2 \leq 9^2$, so $n^2 - 2020 < 0$. Thus n must have at least two digits. If n has at k digits, then $p(n) \leq 9^k$, but $n^2 \geq 10^{2k-2}$. Clearly n^2 grows faster, so it suffices to show that n cannot have three digits. We have $9^3 = 729 \geq 11p(n) = n^2 - 2005 \geq 100^2 - 2005 > 7000$. Hence n must have two digits if it is to exist. Write $n = 10a + b$, so $p(n) = ab$ and $n^2 + 100a^2 + 20ab + b^2$. Then we have $100a^2 + 9ab + b^2 = 2005$. Reducing mod 5, we get $b^2 \cong ab$ mod 5. Thus either $b = 5$ or $a \equiv b$ mod 5. We can also reduce mod 4 to get $ab + b^2 \cong 1$. Writing out the possible remainders for a and b, we get $a \cong 0$ mod 4. Thus our possible solutions are 44, 45, and 49. Checking all three gives us that 49 is the only one that works.

For the bonus, one applies the same technique to get that it has to be a two digit number satisfying $100a^2 + 16ab + b^2 = 2020$. Reducing mod 4 gives $b^2 \cong 0$, so b has to be even. Reducing mod 5 gives $ab + b^2 \cong 0$, so $b \cong 0$ or $a \cong -b$. We have that $\sqrt{2020} > 44$, so $n \geq 45$. Finally, we note that if $b = 0$, then $4p(n) = 0$, so we need $n^2 = 2020$, which is not possible because 2020 is not a perfect square. This lets us elimate the $b \cong 0 \pmod 5$ possibility. Hence we are looking for b even and $a \cong -b$

mod 5. Thus we have the following possibilities: $82, 64, 46, 96, 78$. We see that 64 is already too big, because $\frac{64^2-2020}{4} = 519 > 91 \geq p(n)$. Hence the only possible solution is 46, which works.