NUMBER THEORY PROBLEMS FOR THE UBC-SFU COMPETITION

PROF. DRAGOS GHIOCA

Problem 1. (7 points.) Show that there is no integer n larger than 1 with the property that n divides

$$625^{n-1} - 125^{n-1} + 25^{n-1} - 5^{n-1} + 1.$$

Solution. Assume there exists some integer $n > 1$ dividing $625^{n-1} - 125^{n-1} + 25^{n-1} - 5^{n-1} + 1$.

Noting that the above number is odd, we also get that n must be odd and so, $n-1 > 1$. We let α be the exponent of 5 in $n-1$; we have that α is a non-negative integer.

Since

$$625^{n-1} - 125^{n-1} + 25^{n-1} - 5^{n-1} + 1 = \frac{5^{5(n-1)} + 1}{5^{n-1} + 1}$$

we get that n must divide $5^{5(n-1)} + 1$ and furthermore, because

$$5^{5(n-1)} + 1 = \frac{5^{10(n-1)} - 1}{5^{5(n-1)} - 1},$$

we get that n must divide $5^{10(n-1)} - 1$.

Let p be a prime number dividing $n-1$; then

$$p \mid 5^{10(n-1)} - 1$$

which shows that the order $\mathrm{ord}_p(5)$ of 5 modulo p must divide $10(n-1)$. We prove next that $\mathrm{ord}_p(5)$ doesn't divide $2(n-1)$, which is equivalent with showing that p doesn't divide

$$5^{2(n-1)} - 1.$$

Indeed, if p were to divide

$$5^{2(n-1)} - 1 = \left(5^{n-1} - 1\right) \cdot \left(5^{n-1} + 1\right),$$

then this means that either

$$p \mid 5^{n-1} - 1 \text{ or } p \mid 5^{n-1} + 1.$$

Hence,

$$5^{n-1} \equiv \pm 1 \pmod{p},$$

which would contradict the fact that

$$p \mid 5^{4(n-1)} - 5^{3(n-1)} + 5^{2(n-1)} - 5^{n-1} + 1;$$

note that p cannot divide 5 because p is not 5 since 5 doesn't divide

$$5^{4(n-1)} - 5^{3(n-1)} + 5^{2(n-1)} - 5^{n-1} + 1.$$

So, indeed p doesn't divide $5^{2(n-1)} - 1$, which means that

$$\mathrm{ord}_p(5) \mid 10(n-1) \text{ but } \mathrm{ord}_p(5) \nmid 2(n-1).$$

Hence, noting that 5^α divides $n-1$, we get that

$$5^{\alpha+1} \mid \mathrm{ord}_p(5).$$

Always - using Fermat's Little Theorem - we have that

$$\mathrm{ord}_p(5) \mid p-1$$

because $p \mid 5^{p-1}-1$ (note again that $p \neq 5$); so, we conclude that

$$5^{\alpha+1} \mid p-1.$$

Since the above divisibility holds for each prime p dividing n, we conclude that actually

$$5^{\alpha+1} \mid n-1,$$

thus contradicting the definition of α. (For the last step, note that

$$p \equiv 1 \pmod{5^{\alpha+1}}$$

for each prime p dividing n and so,

$$n \equiv 1 \pmod{5^{\alpha+1}}$$

since n is a product of primes satisfying the above congruence equation.)

Problem 2. (7 points.) Let $f \in \mathbb{Z}[x]$ be a polynomial of degree 2022 with integer coefficients. Show that there exist infinitely many positive integers n with the property that

$$\sqrt[5]{f(n)} \text{ is not an integer.}$$

Solution. We argue by contradiction and therefore assume that $f(n)$ is the fifth power of an integer for each $n > N$ (for some positive integer N). Then replacing $f(x)$ by $f(x+N)$, we may (and do) assume that $\sqrt[5]{f(n)} \in \mathbb{Z}$ for each positive integer n.

We write $f(x)$ as a product of irreducible polynomials with integer coefficients, i.e.,

$$f(x) = A \cdot \prod_{i=1}^{r} f_i(x)^{e_i},$$

where A is a nonzero integer, the e_i's are positive integers, while the f_i's are (non-constant, distinct) irreducible polynomials with integer coefficients. Since the degree of $f(x)$ is 2022, which is not divisible by 5, then there must exist some $i_0 \in \{1, \dots, r\}$ such that e_{i_0} is not a multiple of 5.

The next claim is valid for any non-constant polynomial with integer coefficients.

Claim 0.1. *Let $g \in \mathbb{Z}[x]$ be a non-constant polynomial. Then there exist infinitely many primes p with the property that for some $n \in \mathbb{N}$, we have that $p \mid g(n)$.*

Proof of Claim 0.1. We write

$$g(x) = \sum_{k=0}^{m} c_k x^k,$$

where $m = \deg(g)$ (so, $c_m \neq 0$). Assuming the conclusion doesn't hold, then there exist finitely many primes

$$p_1, \dots, p_\ell$$

with the property that each $g(n)$ (for $n \in \mathbb{N}$) is divisible only by primes p_i from the above list. If $c_0 = 0$, then simply

$$p \mid g(p)$$

for each prime p and so, the above list of primes can never be exhaustive. So, we assume from now on that $c_0 \neq 0$. Then we let

$$n_1 = Nc_0^2 \cdot \prod_{i=1}^{\ell} p_i$$

for some positive integer N. Then - for any $N \in \mathbb{N}$ - we have that

$$g(n_1) = c_0 \cdot m_1$$

for some integer m_1 satisfying

$$m_1 \equiv 1 \pmod{\prod_{i=1}^{\ell} p_i}.$$

Since we cannot have that $g(n_1) = c_0$ for infinitely many integers n_1 as above (because g is not a constant polynomial), we conclude that there exist (even infinitely many $N \in \mathbb{N}$ such that for the corresponding) integers n_1, we have

$$g(n_1) = c_0 \cdot m_1 \text{ where } m_1 \neq 1 \text{ and } m_1 \equiv 1 \pmod{\prod_{i=1}^{\ell} p_i}.$$

Thus $g(n_1)$ must be divisible by some other prime p not from the above list of the p_i's. This completes the proof of Claim 0.1. □

Now, returning to our problem, since the polynomials f_i are distinct, then they are coprime and so, for each $j \neq i_0$, there exist some polynomials P_j and Q_j along with some nonzero integer constants B_j such that

$$P_j(x) \cdot f_{i_0}(x) + Q_j(x) \cdot f_j(x) = B_j. \tag{1}$$

(This is just the Euclidean algorithm for polynomials.)

Similarly, because f_{i_0} is an irreducible non-constant polynomial, then there exist some polynomials $P_{i_0}(x)$ and $Q_{i_0}(x)$ along with a nonzero integer B_{i_0} such that

$$P_{i_0}(x) \cdot f_{i_0}(x) + Q_{i_0}(x) \cdot f'_{i_0}(x) = B_{i_0}, \tag{2}$$

where f'_{i_0} is simply the derivative of the polynomial f_{i_0}. (Here we use the fact that the polynomial $f_{i_0}(x)$ cannot be divisible by another polynomial - non-constant and with integer coefficients - of smaller degree; thus f_{i_0} would have to be coprime with any other nonzero polynomial of smaller degree than $\deg(f_{i_0})$.)

Let p be a prime number satisfying the following conditions:

(i) there exists $n \in \mathbb{N}$ such that $p \mid f_{i_0}(n)$;
(ii) $p > |A|$; and
(iii) $p > \max_{i=1}^{r} |B_i|$.

The existence of such a prime is guaranteed by Claim 0.1 applied to f_{i_0}.

Then for any $n \in \mathbb{N}$, if $p \mid f_{i_0}(n)$, then condition (iii) above applied to each B_j for $j \neq i_0$ (see equation (1)) yields the fact that $p \nmid f_j(n)$ for each $j \neq i_0$.

Now, we immediately compute that

$$f(n + p) \equiv f(n) + pf'(n) \pmod{p^2}; \tag{3}$$

in particular, we get that if $p \mid f(n)$ then also $p \mid f(n + p)$.

Condition (iii) above applied to B_{i_0} (see equation (2)) yields that if $p \mid f(n)$ then $p \nmid f'(n)$. So, using this information in equation (3) yields that we cannot have that both $f(n)$ and $f(n+p)$ are divisible by p^5.

Therefore, we obtained the existence of some prime p which doesn't divide A (see condition (ii) above) and moreover for some positive integer n_0, we have that

(1) $p \mid f_{i_0}(n_0)$ but $p^5 \nmid f_{i_0}(n_0)$;
(2) $p \nmid f_j(n_0)$ for each $j \neq i_0$.

Combining conditions (1)-(2) with the fact that $p \nmid A$ and with the fact that e_{i_0} is not divisible by 5, we get that the exponent of p in $f(n_0)$ is not divisible by 5, thus contradicting the fact that $\sqrt[5]{f(n_0)} \in \mathbb{Z}$.

This concludes our proof.