UBC MATH CIRCLE 2024 PROBLEM SET 4 SOLUTIONS

Problem 1. *For a positive integer n, define $S_n = 1! + 2! + \ldots + n!$. Prove that there exists an integer n such that S_n has a prime divisor greater than 10^{2024}.*

Proof. Assume for contradiction that S_n has no prime divisors larger than $N = 10^{2024}$ for an $n \in \mathbb{N}$. We write $\nu_p(m)$ for the highest power of p dividing n. We first prove the following claim.

Claim: If $\nu_p(m) < \nu_p(n)$ then $\nu_p(m+n) = \nu_p(m)$.

From the congruence $m + n \equiv m \mod p^{\nu_p(n)}$ together with the fact that $p^{\nu_p(m)} \mid p^{\nu_p(n)}$ we immediately conclude that $\nu_p(m+n) = \nu_p(m)$.

Returning to the proof, let $\mathcal{P}$ be the set of prime divisors $p \mid S_n$ for some $n \in \mathbb{N}$. Note that $\mathcal{P} \subset \{1, \ldots, N\}$ is finite, hence the Chinese remainder theorem implies that we may choose an $n \in \mathbb{N}$ such that $n \equiv -2 \mod p$ for all $p \in \mathcal{P}$. Suppose that $\nu_p(S_n) > \nu_p((n+1)!)$ for some $p \in \mathcal{P}$. Then by the earlier claim, $\nu_p(S_{n+1}) = \nu_p((n+1)!) < \nu_p((n+2)!)$ since $p \mid n+2$. We will show by induction that

$$\nu_p(S_m) < \nu_p((m+1)!) \text{ for } m \geq n+1 \tag{1}$$

Indeed, since $\nu_p(S_{n+1}) < \nu_p((n+2)!)$, we conclude by the claim that

$$\nu_p(S_{n+2}) = \nu_p(S_{n+1}) < \nu_p((n+2)!) \leq \nu_p((n+3)!)$$

Replacing $n+1$ by $n+2$ in (1) and inducting proves (1).

Hence taking a possibly larger solution to the congruences $n \equiv -2 \mod p$ for all $p \in \mathcal{P}$, we may assume that $\nu_p(S_n) \leq \nu_p((n+1)!)$ for all $p \in \mathcal{P}$. Since $p \mid n+2$ for all $p \in \mathcal{P}$, we have $p \nmid n+1$ for all $p \in \mathcal{P}$ and $\nu_p(S_n) \leq \nu_p((n+1)!) = \nu_p(n!)$ for all $p \in \mathcal{P}$. But since every divisor of S_n must lie in $\mathcal{P}$, this implies that $S_n \leq n!$ which is obviously false. □

Remark. Note that this proof didn't use anywhere that $N = 10^{2024}$. In particular, we conclude by the same argument that the set of prime divisors of $\{S_n : n \in \mathbb{N}\}$ is infinite.

Problem 2. *Prove or Disprove: The only polynomials $f \in \mathbb{Q}[x]$ which induce a bijection $\mathbb{Q} \to \mathbb{Q}$ are linear.*

Proof. We show that this is true. Obviously every linear polynomial gives a bijection $\mathbb{Q} \to \mathbb{Q}$ so we need only show the converse. Suppose that $f \in \mathbb{Q}[x]$ is a polynomial which gives a bijection $\mathbb{Q} \to \mathbb{Q}$. By dividing by the leading term of f, we may assume that f is monic (i.e. has leading term 1). Now, let p be a prime not dividing the numerator or denominator of any the coefficients of f. We claim that there is no $z \in \mathbb{Q}$ with $f(z) = 1/p$. Write $z = p^s m$ for $m \in \mathbb{Q}$ and $s \in \mathbb{Z}$ such that p is coprime to the numerator and denominator of m. Let $f(x) = x^d + a_1 x^{d-1} + \ldots + a_d$. Then

$$f(z) = p^{sd} m^d + a_1 p^{s(d-1)} m^{d-1} + \ldots + a_d = p^{sd}\left(m^d + a_1 p^{-s} m^{d-1} + \ldots + a_d p^{-sd}\right)$$

If $s \geq 0$ then none of the denominators of any of the terms in the first expression above are divisible by p and it follows that $f(z) \neq 1/p$. Hence we may assume that $s < 0$. In

Date: February 25, 2024.

particular, all of the terms in the expression $m^d + a_1 p^{-s} m^{d-1} + \ldots + a_d p^{-sd}$ besides the first have numerators divisible by p. We can therefore write this as $m^d + \alpha/\beta$ where $\alpha, \beta \in \mathbb{Z}$ are coprime and $p \mid \alpha$. since the numerator and denominator of m are coprime to p, the resulting fraction $m^d + \alpha/\beta$ also has numerator and denominator coprime to p. Thus the exponent of p in the denominator of $f(z)$ is precisely p^{-sd}. In other words, $f(z) = 1/p$ implies that $-sd = 1$. This can only happen if $d = 1$. Hence f is linear. □

Remark. Note that we have in fact proved something stronger, the only polynomial maps $f : \mathbb{Q} \to \mathbb{Q}$ which are surjective are linear. We might also consider the problem of the existence of a two variable polynomial bijection $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$. Although this may seem easier, since the condition is evidently harder to satisfy, in fact this problem is still open. Note that there are now a lot of nonlinear surjective polynomials such as $x^2 + y$. It is also significantly harder to construct injective f. In the one variable case, a polynomial like $f(x) = x^3 + x$ works. However, in the two variable case, we need a polynomial $f(x, y)$ such that there is at most one solution to $f(x, y) = c$ over $\mathbb{Q}$ for any $c \in \mathbb{Q}$. Powerful results in arithmetic geometry suggest that any sufficiently general polynomial will work, but as of yet, no polynomial $f(x, y)$ has been shown to be injective. A weak form of the Bombieri-Lang conjecture would imply that there are no such bijections.

Problem 3. *A subset $S \subset \mathbb{Z}$ is called* square *if $a + b$ is a perfect square for any distinct $a, b \in S$. Two square subsets $S, T \subset \mathbb{Z}$ are called* equivalent *if there is a rational number $\alpha \in \mathbb{Q}$ such that $S = \alpha^2 T = \{\alpha^2 t : t \in T\}$. Prove that there are infinitely many inequivalent square subsets $S \subset \mathbb{Z}$ with $\#S = 4$.*

Remark. One can generalize this problem in a few ways, all of which very quickly lead to areas of active research. For example replacing squares by cubes still gives infinitely many inequivalent solutions, of which the first is $(-217792516, 255052220, 312611332, 350443516)$, degree 4 is unknown and degree 5 would be disproved by a generalization of Fermat's Last Theorem. One could also restrict to squares but ask that $\#S > 4$. In this case, it is known that there are infinitely many inequivalent square sets with $\#S = 5$, of which the first is $(7442, 28658, 148583, 177458, 763442)$. For $\#S = 6$ only one solution is known:

$$(339323777731946898, 1393697157060854002, 2146648434867118098,$$
$$8397374854916636127, 12982930844119795409 8, -3037047761557459 98)$$

Beyond this is unknown. In all of these cases, a very big conjecture in arithmetic geometry (the Bombieri Lang conjecture) implies that the size of such sets is bounded.

Proof. Let $S = \{x_1, x_2, x_3, x_4\} \subset \mathbb{Z}$ be square. We reduce the problem to the existence of infinitely many inequivalent $n \in \mathbb{Z}$ which can be written as the sum of two perfect squares in three different ways. Indeed, suppose that $n = a_1^2 + b_1^2 = a_2^2 + b_2^2 = a_3^2 + b_3^2$ and consider the system of linear equations

$$x_1 + x_2 = 4a_1^2$$
$$x_1 + x_3 = 4a_2^2$$
$$x_1 + x_4 = 4a_3^2$$
$$x_3 + x_4 = 4b_1^2$$

We claim that this can be solved over $\mathbb{Z}$ (if you know something about determinants, this is obvious since the matrix representing the system on the left has determinant 2). Indeed, subtracting the first equation from the second and third gives

$$\begin{aligned} x_1 + x_2 &= 4a_1^2 \\ -x_2 + x_3 &= 4a_2^2 - 4a_1^2 \\ -x_2 + x_4 &= 4a_3^2 - 4a_1^2 \\ x_3 + x_4 &= 4b_1^2 \end{aligned}$$

Subtracting the second equation from the third and adding the result to the final equation gives

$$\begin{aligned} x_1 + x_2 &= 4a_1^2 \\ -x_2 + x_3 &= 4a_2^2 - 4a_1^2 \\ -x_3 + x_4 &= 4a_3^2 - 4a_2^2 \\ 2x_4 &= 4b_1^2 + 4a_3^2 - 4a_2^2 \end{aligned}$$

Hence $x_4 = 2b_1^2 + 2a_3^2 - 2a_2^2$ and we back substitute to solve for $x_1, x_2, x_3 \in \mathbb{Z}$. Obviously the sums $x_1 + x_2, x_1 + x_3, x_1 + x_4$ and $x_3 + x_4$ are squares. For the remaining two, note that

$$\begin{aligned} x_2 + x_4 &= (x_1 + x_2) + (x_3 + x_4) - (x_1 + x_3) = 4a_1^2 + 4b_1^2 - 4a_2^2 = 4b_2^2 \\ x_2 + x_3 &= (x_1 + x_2) + (x_3 + x_4) - (x_1 + x_4) = 4a_1^2 + 4b_1^2 - 4a_3^2 = 4b_3^2 \end{aligned}$$

by the choice of n. Note that $x_1, \ldots, x_4$ will be distinct as soon as the numbers $4a_1^2, 4a_2^2, 4a_3^2, 4b_1^2$ are distinct and that inequivalent sets of squares in the decomposition of n will naturally give rise to inequivalent sets $\{x_1, \ldots, x_4\}$.

To construct integers n which are the sum of two squares in three different ways, note first that $65 = 1^2 + 8^2 = 4^2 + 7^2$. Define $a_1 + b_1 i = (1 + mi)(1 + 8i) = (1 - 8m) + (m + 8)i$ and $a_2 + b_2 i = (1 + mi)(4 + 7i) = (4 - 7m) + (4m + 7)i$ and $a_3 + b_3 i = (1 + mi)(4 - 7i) = (4 + 7m) + (4m - 7)i$. We claim that $a_1^2 + b_1^2 = a_2^2 + b_2^2 = a_3^2 + b_3^2$. Indeed,

$$\begin{aligned} a_1^2 + b_1^2 &= (1 - 8m)^2 + (m + 8)^2 = 65(m^2 + 1) \\ a_2^2 + b_2^2 &= (4 - 7m)^2 + (4m + 7)^2 = 65(m^2 + 1) \\ a_3^2 + b_3^2 &= (4 + 7m)^2 + (4m - 7)^2 = 65(m^2 + 1) \end{aligned}$$

Now, we must show that $a_1^2, a_2^2, a_3^2, b_1^2$ are distinct for all but finitely many m. For this, we may show that the any two polynomials a_1, a_2, a_3, b_1 differ by a sign ± 1 at most once. Since none of the polynomials $1 - 8m, 4 - 7m, 4 + 7m, m + 8$ are a scalar multiple of each other, any equalities up to sign between any pair can happen at most twice (one for $+$ and one for $-$). Finally, to show that there are infinitely many m such that the sets $\{a_i, b_i\}$ are all inequivalent, let $p > 13$ be a prime and $k \in \mathbb{N}$ a positive integer. Choose m_k such that $1 - 8m_k \equiv p^k \mod p^{k+1}$ (which exists since $p \neq 2$). Let $S_k = \{a_1, a_2, a_3, b_1, b_2, b_3\}$ be the set resulting from the construction above applied to m_k. Then

$$\begin{aligned} p &\nmid 8(m_k+8) = 65-(1-8m_k) \\ p &\nmid 8(4-7m_k) = 25+7(1-8m_k) \\ p &\nmid 2(4m_k+7) = 15-(1-8m_k) \\ p &\nmid 8(4+7m_k) = 39-7(1-8m_k) \\ p &\nmid 2(4m_k-7) = -13-(1-8m_k) \end{aligned}$$

Since $p > 13$. In other words, for each $k \in \mathbb{N}$, the set S_k has a term congruent to p^k mod p^{k+1} and all other terms are not divisible by p. For different k, the sets above will be inequivalent since if multiplication by $\alpha \in \mathbb{Q}$ sends S_k to S_l, then p cannot divide either the numerator or denominator of α since both S_k, S_l have terms which are not divisible by p. But then multiplication by α does not change the highest power of p dividing an element of either S_k or S_l. Hence $k = l$. Since there are only finitely many k for which the terms S_k are not distinct, this gives infinitely many inequivalent numbers which are the sum of two squares in three different ways and hence infinitely many inequivalent square sets of size 4. $\square$