UBC Math Circle 2022 Problem Set 1

1. Prove that the Diophantine equation

$$x^3 + y^3 + z^3 + x^2y + y^2z + z^2x + xyz = 0$$

has no solutions in nonzero integers. (Hint: Consider the parity of the left hand side in various cases.)

Solution: (Joanna Weng)

Using the hint, we find that the given equation has integer solutions (x, y, z) only when x, y, z are all even. This is because in all other cases the left hand side is odd while the right hand side is even.

So for some $a, b, c \in \mathbb{Z}$,

$$x = 2a, \quad y = 2b, \quad z = 2c.$$

Substituting, we see that

$$8(a^3 + b^3 + c^3 + a^2b + b^2c + c^2a) = 0,$$

which implies that (a, b, c) is also a solution to the given equation. But then a, b, c must all be even. This leads to an infinite descent (assuming x, y, z are not all zero); hence, the given equation cannot have solutions in nonzero integers.

2. Let k be a positive integer. The sequence $(a_n)_n$ is defined by $a_1 = 1$, and for $n \geq 2$, a_n is the nth positive integer greater than a_{n-1} that is congruent to n modulo k. Find a_n in closed form.

Solution: (Young Lin)

Since $a_{n-1} \equiv n - 1 \bmod k$, it follows that

$$a_n = a_{n-1} + 1 + (n-1)k$$

by definition of a_n. Then solving

$$\begin{aligned} a_n &= a_{n-1} + 1 + (n-1)k, \\ a_1 &= 1 \end{aligned}$$

we obtain a_n in closed form:

$$a_n = n + \frac{n(n-1)k}{2}.$$

Solutions edited by Josh Gomes and Victor Wang.

3. (a) Show that there exist infinitely many integers x, y and z such that

$$x^2 + y^2 = 2z^3 + 8.$$

(b) Show that there exist infinitely many integers a, b, c such that

$$a^2 + b^2 = c^2 + 3.$$

Solution: (Yuqi Xiao)

(a) By letting $z = t^2$ we observe that

$$2z^3 + 8 = 2t^6 + 8 = (t^3 + 2)^2 + (t^3 - 2)^2.$$

Hence,

$$x = t^3 + 2, \quad y = t^3 - 2, \quad z = t^2 \quad (t \in \mathbb{Z})$$

generates infinitely many solutions.

(b) First, we let $c = 3k + 1$ and observe that

$$c^2 + 3 = 9k^2 + 6k + 4 = (3k - 2)^2 + 18k.$$

Then letting $k = 18\ell^2$, we see that

$$a = 54\ell^2 - 2, \quad b = 18\ell, \quad c = 54\ell^2 + 1 \quad (\ell \in \mathbb{Z})$$

generates infinitely many solutions.

4. A subset S of $\mathbb{N}$ is called *highly composite* if for every $n \geq 2$ and every choice of distinct elements $a_1, a_2, \ldots, a_n \in S$, the sum $\sum_{i=1}^{n} a_i$ is composite. For example, the set $\{3, 5, 7\}$ is highly composite since $3 + 5$, $3 + 7$, $5 + 7$ and $3 + 5 + 7$ are all composite.

(a) Prove or disprove: There exists an infinite highly composite set S containing only prime numbers.

(b) Can the set P of all primes be partitioned into infinite highly composite subsets?

Solution: (Oakley Edens)

(a) Let S be a finite highly composite subset of $\mathbb{N}$ containing only primes; such a set exists as the set $\{2\}$, for instance, satisfies this condition. To show that we can (recursively) construct an infinite highly composite set containing only primes, it is enough to show that we can find a prime $p \notin S$ such that $S \cup \{p\}$ is highly composite. The remaining details can be filled in by the reader. Let $r_1, \ldots, r_{2^n-1}$ be the distinct nonempty sums of elements in S, and let $q_1, \ldots, q_{2^n-1}$ be distinct primes such that $\gcd(r_i, q_i) = 1$. Consider the system of linear congruences: $x + r_i \equiv 0 \pmod{q_i}$. Since q_i and q_j are coprime for all $i \neq j$, by the Chinese Remainder Theorem, this system is equivalent to a single congruence $x + R \equiv 0 \pmod{Q}$ where $Q = \prod_{i=1}^{2^n-1} q_i$. Suppose $\gcd(R, Q) \neq 1$. Then there exists some $q_i \in Q$ with $q_i | R$. But then $R \equiv r_i \equiv 0 \pmod{q_i}$, which contradicts the choice of q_i. Thus $\gcd(R, Q) = 1$. Dirichlet's theorem on arithmetic progressions implies that $Qm - R$ is prime for infinitely many m. Let p be the smallest prime in this arithmetic progression such that $p + r_i \neq q_i$ for all i, and $p \notin S$. Then since $p + r_i$ is divisible by q_i yet $p + r_i \neq q_i$ for all $1 \leq i \leq 2^n - 1$, it follows that the set $S \cup \{p\}$ is highly composite as desired.

(b) We show that we can partition the set P of all primes into infinite highly composite subsets. To do this, we perform the following infinite procedure that takes as input an arbitrary prime p, and returns as output a desired partition.

procedure (p: prime)

Let $S_1^{(1)} := \{p\}$.

Let $\ell := 1$.

for $k = 1, 2, 3 \ldots$

Let m be the largest prime in $\bigcup_{i=1}^{\ell} S_i^{(k)}$.

Let $n_i := |S_i^{(k)}|$ for $1 \leq i \leq \ell$. (It is clear that $n_1 \geq n_2 \geq \cdots \geq n_\ell$.)

Let $r[i, 1], \ldots, r[i, 2^{n_i} - 1]$ be the distinct nonempty sums of elements in $S_i^{(k)}$ for $1 \leq i \leq \ell$ so that $r[i, 1]$ is the smallest among these sums.

Step 0: Choose $q[1], \ldots, q[2^{n_1} - 1]$ distinct primes such that $\gcd(r[i, j], q[j]) = 1$ for $1 \leq i \leq \ell$ and $1 \leq j \leq 2^{n_i} - 1$, and $r[u, 1] \not\equiv r[v, 1] \pmod{q[1]}$ for $u \neq v$. Let a_i be the smallest prime solution to the system of congruences $x + r[i, j] \equiv 0 \pmod{q[j]}$ that additionally satisfies $a_i \notin \bigcup_{i=1}^{\ell} S_i^{(k)}$ and $a_i + r[i, j] \neq q[j]$ for $1 \leq i \leq \ell$ and $1 \leq j \leq 2^{n_i} - 1$.

Step 1: Define sets $S_i^{(k+1)} := S_i^{(k)} \cup \{a_i\}$ for $1 \leq i \leq \ell$.

Step 2: Define sets $S_{\ell+i}^{(k+1)} := \{p_i\}$ where p_i is the i-th smallest prime such that $p_i \notin \bigcup_{i=1}^{\ell} S_i^{(k)}$ and $p_i < m$. If there are no new sets defined this way, define $S_{\ell+1}^{(k+1)} := \{p'\}$ where p' is the smallest prime larger than m.

Let $\ell :=$ the total number of sets $S_i^{(k+1)}$ defined in Step 1 and Step 2. (This number increases with each iteration.)

end for

return $\{\sup_k S_i^{(k)} \mid i \in \mathbb{N}\}$

end procedure

Now we prove that the output of this procedure is indeed a desired partition.

Define $S_i := \sup_k S_i^{(k)}$ for each $i \in \mathbb{N}$. From what was proved in (a), each S_i is an infinite highly composite subset of P. Thus it remains only to show that the sets S_i partition P.

Observe that, at the kth iteration, Step 1 adjoins a prime to each $S_i^{(k)}$ that is distinct from those that belong to any $S_i^{(k)}$. Thus for each prime $p \in P$, there is an eventual Step 1 where a prime larger than p is adjoined to a constructed set. Following this, Step 2 produces a set containing p if p had not already belonged to some previously constructed set. Thus $\bigcup_{i=1}^{\infty} S_i = P$.

Next, at the kth iteration: It is clear that Step 2 cannot produce a set $\{p\}$ if $p \in S_i^{(k)}$ for some i. Similarly, Step 1 cannot adjoin a prime p to a set $S_i^{(k)}$ if p is in any of the sets $S_i^{(k)}$. Thus if $S_i^{(k)} \cap S_j^{(k)} \neq \emptyset$ for some $i \neq j$, then $a_i = a_j$ at some iteration $k' < k$. But by construction, the smallest primes $p_i \in S_i^{(k')}$ and $p_j \in S_j^{(k')}$ do not coincide, whence $a_i \equiv -p_i = -r[i,1] \not\equiv -r[j,1] = -p_j \equiv a_j \pmod{q[1]}$ at iteration k'. This is a contradiction. So $S_i \cap S_j = \emptyset$ for all $i \neq j$. Thus the sets S_i partition P into infinite highly composite subsets.

5. Given a positive integer $k \geq 2$, set $a_1 = 1$ and, for every integer $n \geq 2$, let a_n be the smallest solution of equation
$$x = 1 + \sum_{i=1}^{n-1} \left\lfloor \sqrt[k]{\frac{x}{a_i}} \right\rfloor$$
that exceeds a_{n-1}. Prove that all primes are among the terms of the sequence $a_1, a_2, \ldots$

Solution: (Arvin Sahami)

Consider a positive integer $k \geq 2$. Let S be the set of all kth power free natural numbers, i.e., the set of all $n \in \mathbb{N}$ such that there is no prime p where $p^k | n$.

For every $n \in \mathbb{N}$ we define its *kth power free part* as the smallest divisor d of n such that $\frac{n}{d}$ is a perfect kth power. It is not hard to see that the kth power free part of any natural number is unique.

Let $s_1, s_2, \ldots$ be the members of S listed in increasing order.

We show by induction that $a_i = s_i$ for all $i \in \mathbb{N}$.

The base case when $i = 1$ is clear.

Assume that this claim holds for $i = 1, \ldots, n$.

Let $m_i := \left\lfloor \sqrt[k]{\dfrac{x}{s_i}} \right\rfloor$ where $i = 1, \ldots, n$.

Observe that m_i is the largest integer such that $m_i^k \cdot s_i \leq x$.

So m_i is the number of positive integers less than or equal to x that have s_i as their kth power free part. Then the sum $\sum_{i=1}^{n} m_i$ can be interpreted as the total number of positive integers less than or equal to x with one of $s_1, \ldots, s_n$ as their kth power free part. Since $\sum_{i=1}^{n} m_i + 1$ is an integer, we need only consider integer values for x.

Now a natural number $z < s_{n+1}$ has a kth power free part among $s_1, s_2, \ldots, s_n$; if $z = s_{n+1}$ then its kth power free part is s_{n+1}. And so, when $x = s_{n+1}$, the sum $\sum_{i=1}^{n} m_i$ is exactly $x - 1$.

Hence,

$$\sum_{i=1}^{n} \left\lfloor \sqrt[k]{\frac{s_{n+1}}{s_i}} \right\rfloor + 1 = s_{n+1}.$$

But if $s_n < x < s_{n+1}$, then by the same reasoning, the sum $\sum_{i=1}^{n} m_i$ is exactly x. Therefore, s_{n+1} is the smallest solution of

$$\sum_{i=1}^{n} \left\lfloor \sqrt[k]{\frac{x}{s_i}} \right\rfloor + 1 = x$$

that is larger than $a_n = s_n$.

So the sequence $a_1, a_2, \ldots$ is precisely the sequence $s_1, s_2, \ldots$ Since all primes are of course kth power free, it follows that they are among $a_1, a_2, \ldots$