P U M ∴ C

Individual Finals A Solutions

1. Let $p > 3$ be a prime and $k \geq 0$ an integer. Find the multiplicity of $X - 1$ in the factorization of

$$f(X) = X^{3p^k-1} + X^{3p^k-2} + \cdots + X + 1$$

modulo p; in other words, find the unique non-negative integer r such that $(X-1)^r$ divides $f(X)$ modulo p, but $(X-1)^{r+1}$ does not divide $f(X)$ modulo p.

Proposed by Michael Cheng and Steven Wang

Solution: First note

$$f(X) = \frac{X^{3p^k} - 1}{X - 1}.$$

The key trick is to make the substitution $X = Y + 1$, so we are instead looking for the multiplicity of Y in

$$f(Y) = \frac{(Y+1)^{3p^k} - 1}{Y}.$$

Now

$$(Y+1)^{3p^k} = \sum_{\ell=0}^{3p^k} \binom{3p^k}{\ell} Y^\ell,$$

and we claim the coefficient $\binom{3p^k}{\ell}$ is divisible by p unless $p^k \mid \ell$.

We use the notation

$$v_p(n) = \{k \in \mathbb{Z}_{\geq 0} : p^k \mid n \text{ and } p^{k+1} \nmid n\}.$$

It is well-known that

$$v_p(n!) = \sum_{r=0}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor.$$

Therefore

$$v_p\left(\binom{3p^k}{\ell}\right) = v_p\left(\frac{(3p^k)!}{\ell!(3p^k-\ell)!}\right) = \sum_{r=0}^{\infty} \underbrace{\left(\left\lfloor \frac{3p^k}{p^r} \right\rfloor - \left\lfloor \frac{\ell}{p^r} \right\rfloor - \left\lfloor \frac{3p^k-\ell}{p^r} \right\rfloor\right)}_{S_r}.$$

We have three cases depending on r:

- $r > k$: then all three floor functions are 0 (here we used the assumption that $p > 3$), so $S_r = 0$.
- $r \leq k$: then $p^r \mid 3p^k$, so $S_r \geq 0$. More careful analysis shows that $S_r = 0$ iff $p^r \mid \ell$.

Therefore, $v_p\left(\binom{3p^k}{\ell}\right) = 0$ iff $p^k \mid \ell$. Thus, modulo p, we have

$$\begin{aligned} f(Y) &= \frac{(Y+1)^{3p^k} - 1}{Y} \\ &= \frac{1}{Y}\left[\sum_{\ell=0}^{3p^k} \binom{3p^k}{\ell} Y^\ell - 1\right] \\ &\equiv \frac{1}{Y}\left(Y^{3p^k} + AY^{2p^k} + AY^{p^k}\right) \qquad A = \binom{3p^k}{2p^k} = \binom{3p^k}{p^k} \\ &= Y^{3p^k-1} + AY^{2p^k-1} + AY^{p^k-1}, \end{aligned}$$

and $p \nmid A$, so the answer is $\boxed{p^k - 1}$.

Remark. The $X = Y + 1$ trick can be used to prove the cyclotomic polynomial $\Phi_{p^k}(X) = X^{p-1} + \cdots + X + 1$ is irreducible over $\mathbb{Z}$. In fact, one can check that $\Phi_{p^k}(Y + 1)$ satisfies the Eisenstein criterion.

2. On an infinite triangular lattice, there is a single atom at a lattice point. We allow for four operations as illustrated in Figure 1. In words, one could take an existing atom, split it into three atoms, and place them at adjacent lattice points in one of the two displayed fashions (a "split"). One could also reverse the process, i.e. taking three existing atoms in the displayed configurations, and merge them into a single atom at the center (a "merge").

Figure 1: See Individual Finals Problems document for diagram.

Assume that, after finitely many operations, there is again only a single atom remaining on the lattice. Show that this is possible if and only if the final atom is contained in the sublattice implied by Figure 2.

Figure 2: See Individual Finals Problems document for diagram.

Proposed by Michael Cheng and Steven Wang

Solution: First we show that the sublattice is the only possible loci for the final atom. Consider the following numbering/weighting of the lattice:

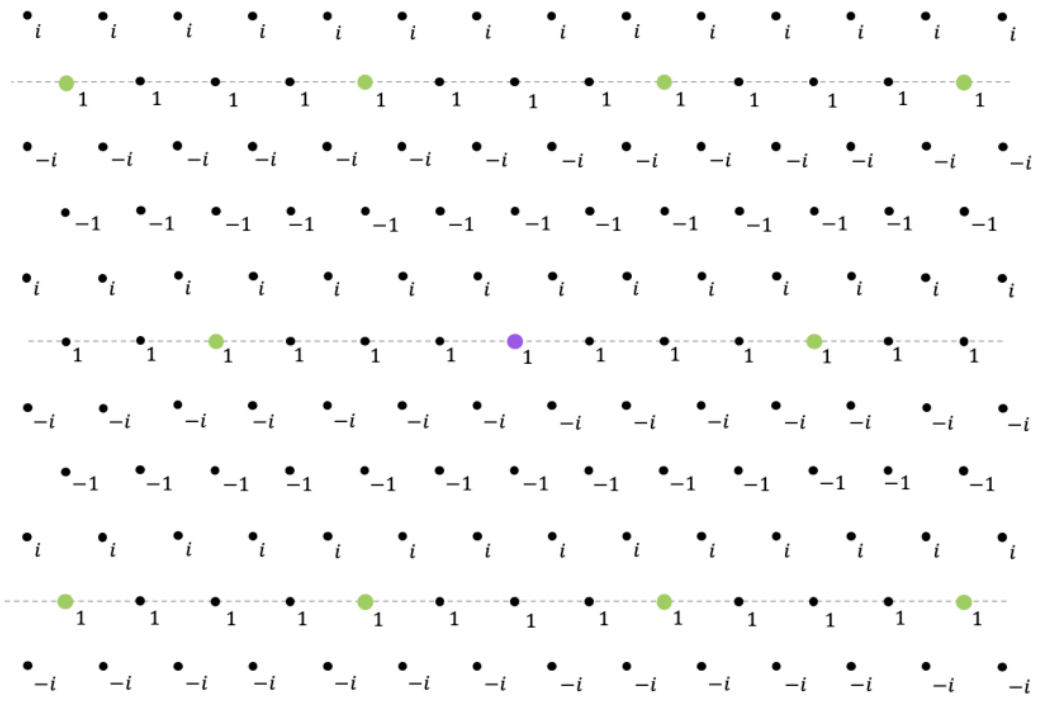

Figure 3: Weighting of lattice

It is easy to check that any of the operations does not change the total weight of the atoms. Therefore the final atom must appear on a lattice point with weight 1. Similarly one can rotate this picture by 60° or 120°, and one can conclude that only points of the given sublattice are possible final positions of the atom.

Remark. It might be of interest how one can come up with the weighting above. In fact, to obtain an invariant one needs the "local ratios" of the weights to be translational invariant (i.e. at each lattice point, the ratio of its weight to the six nearby ones is the same everywhere). Thus the entire weighting is defined by two numbers as exampled below:

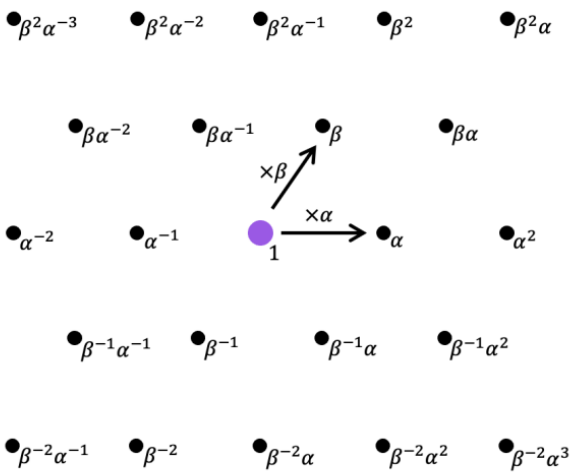

Figure 4: Labelling with indeterminants

We then want

$$\alpha + \beta\alpha^{-1} + \beta^{-1} = \beta + \alpha^{-1} + \beta^{-1}\alpha = 1.$$

There are six pairs of solutions, but they all give Figure 3 under rotational and reflectional symmetry.

Now we return to the other direction of the proof. By rotational symmetry, it suffices to construct a sequence of moves that move the original atom 4 units to the right. The construction can be fun whilst mildly infuriating. One possible sequence is as follows (the original at purple, and the target at green):

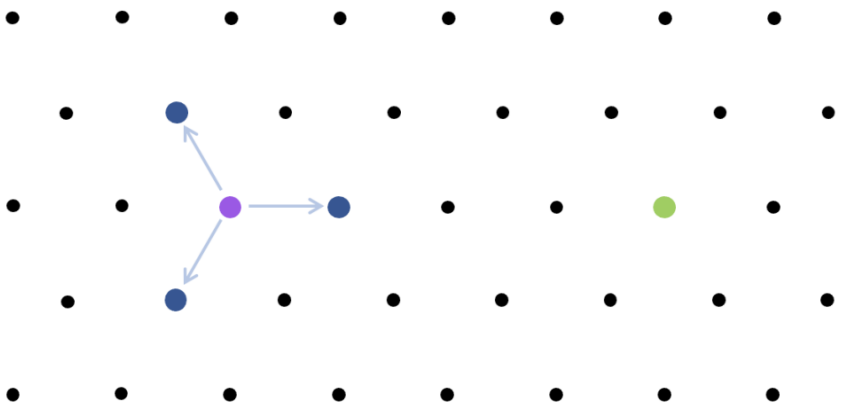

Figure 5: Step 1: apply the blue split.

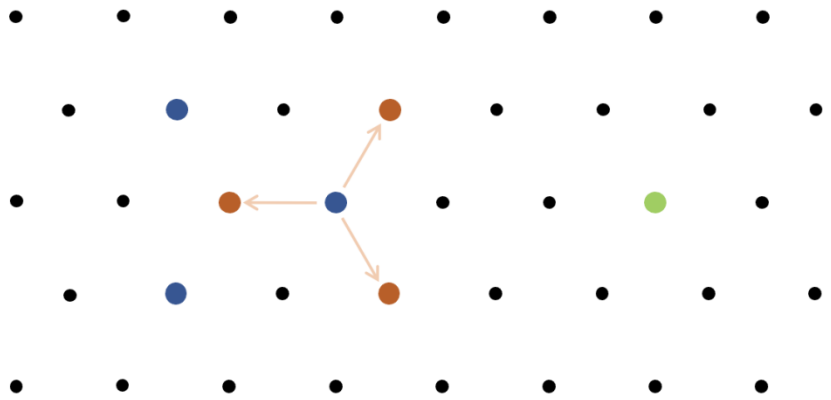

Figure 6: Step 2: apply the orange split.

At this stage, we observe a maneuver that we call the "propagation lemma:"

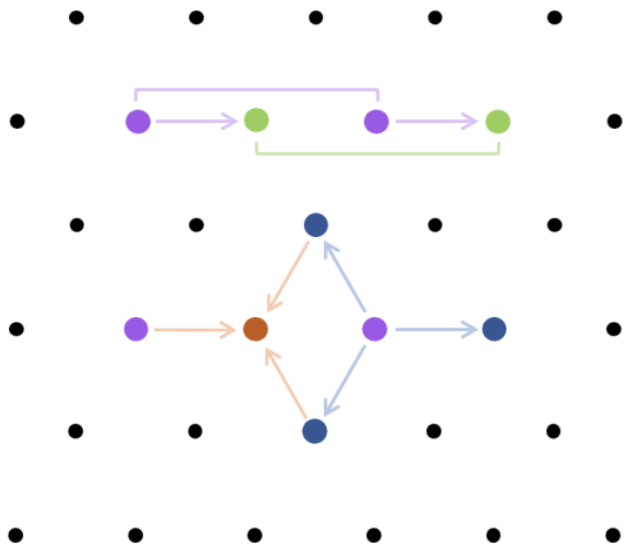

Figure 7: The "propagation lemma". Apply the blue split and then the orange merge to move the purple pair to the right by one unit.

This allows us to simultaneously move a pair of atoms spaced 2 units apart along the line they are on. Using this 4 times on the result of Figure 6 we can obtain the following:

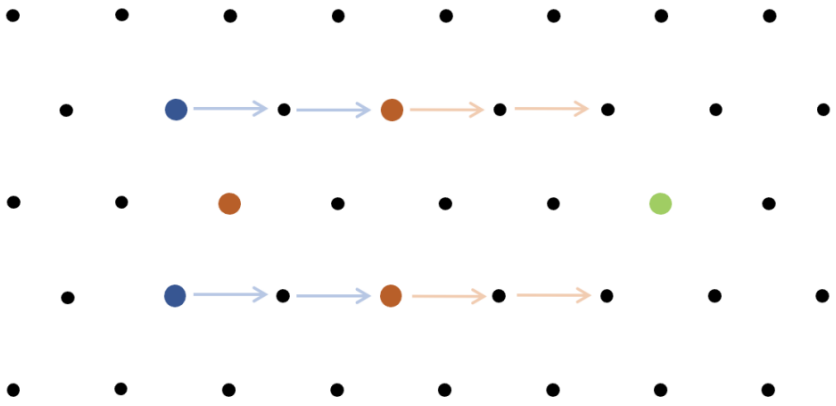

Figure 8: Step 3: apply the "propagation lemma" twice on the top row, and twice on the bottom row.

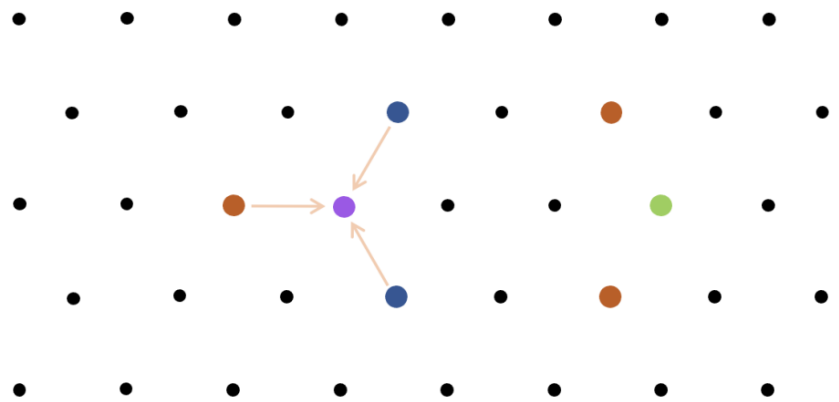

Figure 9: Step 4: apply the orange merge to get the purple atom.

Now we apply Steps 1-4 to the left-most atom (purple in Figure 9), treating it as the starting point:

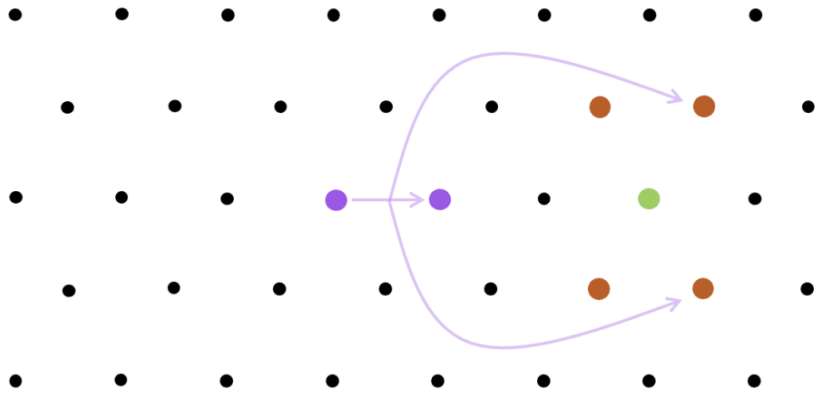

Figure 10: Step 5: repeat step 1-4 on the left-most atom, which replaces it with three new atoms on the right, indicated by the purple arrows.

Finally, we use two merges to achieve our goal!

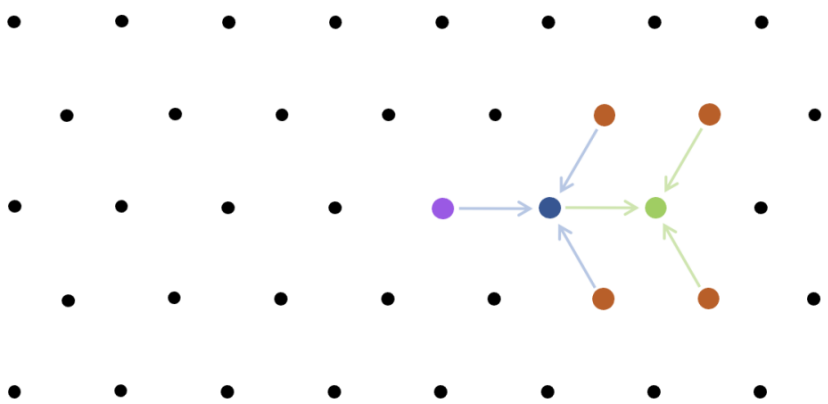

Figure 11: Step 6: apply the blue merge and then the green merge to get the desired green atom. No other atom is left on the lattice and we are done.

3. Let $f(X)$ be a monic irreducible polynomial over $\mathbb{Z}$; therefore, by Gauss's Lemma, f is also irreducible over $\mathbb{Q}$ (you may assume this). Moreover, assume $f(X) \mid f(X^2+n)$ where n is an integer such that $n \notin \{-1, 0, 1\}$. Show that $n^2 \nmid f(0)$.

   Proposed by Michael Cheng and Steven Wang

   Solution: Let $g(X) = X^2 + p$, so $f(X) \mid f(g(X))$. Note that if x is a (complex) root of $f(X)$, then so is $g(x)$. Therefore $g^2(x), g^3(x), \cdots$ are all roots of f, where $g^k(x) = g(\cdots g(x))$ with g is applied k times. However, f has finitely many roots, so there must be some root x_0 of f and some $k \geq 1$ such that $g^k(x_0) = x_0$. This means that x_0 is a root of the polynomial

$$h(X) = g^k(X) - X.$$

   Irreducibility of f implies that $f \mid h$ (this is a standard fact; we assume this for now and supply an elementary proof later), and thus $f(0) \mid h(0)$. However, it is easy to see that

$$h(0) = n + (n + \cdots)^2,$$

   so $n^2 \nmid h(0)$ and $n^2 \nmid f(0)$.

   Now we prove the claim that we assumed in the proof above:

   > **Claim.** *Let $\alpha \in \mathbb{C}$ be an algebraic number (i.e. α is the root of some rational polynomial). Then there is some unique irreducible monic polynomial $f(X) \in \mathbb{Q}[X]$ with $f(\alpha) = 0$; moreover, for any polynomial $h(X) \in \mathbb{Q}[X]$ with $h(\alpha) = 0$, we have $f(X) \mid h(X)$ in $\mathbb{Q}[X]$.*
   >
   > *Proof.* Let $f(X)$ be a monic polynomial having α as a root with minimal degree. We claim that f satisfies the desired properties.
   >
   > Assume for contradiction that f is not irreducible, so $f(X) = g(X)h(X)$ with $g, h \in \mathbb{Q}[X]$ and non-constant; moreover we may assume that g and h are both monic. Then α is a root of one of them, which contradicts the minimality of f.
   >
   > Now assume that $h \in \mathbb{Q}[X]$ with $h(\alpha) = 0$. By the Euclidean algorithm (a.k.a. long division of polynomials), we can write
   >
$$h(X) = f(X)q(X) + r(X),$$
   >
   > with $q, r \in \mathbb{Q}[X]$ and $\deg r < \deg f$. Now plugging in $X = \alpha$ gives $r(\alpha) = 0$, which contradicts the minimality of f unless $r \equiv 0$, so $f \mid h$.
   >
   > The uniqueness of f thus follows. If g is another monic polynomial with the same properties, then $f \mid g$ and $g \mid f$, so $f(X) = cg(X)$ for some constant c, but $c = 1$ since both are monic. □

   In our case, f is the unique irreducible polynomial with x_0 as a root, thus $f \mid h$ in $\mathbb{Q}[X]$; that is $h(X) = f(X)g(X)$ for some $g(X) \in \mathbb{Q}[X]$. However, since $f \in \mathbb{Z}[X]$ and monic by assumption, and $h \in \mathbb{Z}[X]$ obviously, we actually have $g(X) \in \mathbb{Z}[X]$ (this follows from the Euclidean algorithm).