

Some Notes about the things I encountered

Simon Pohmann

June 13, 2022

Notation

If E is an Elliptic Curve defined over a finite field of characteristic p , we write $E^{(p)}$ for the curve defined by the equations of E after replacing all coefficients by their p -th power. Similarly, for an isogeny $\phi : E \rightarrow E'$, write $\phi^{(p)} : E^{(p)} \rightarrow E'^{(p)}$ for the isogeny defined by the polynomials of ϕ after replacing all coefficients by their p -th power. Furthermore, for a point $P = (x : y : z) \in \mathbb{P}^2$ write $P^{(p)} := (x^p : y^p : z^p)$. Finally, for a set of points or endomorphisms S write $S^{(p)} := \{s^{(p)} \mid s \in S\}$. Note that

$$\begin{aligned} \cdot^{(p)} : \mathbf{Ell} &\rightarrow \mathbf{Ell}, & E &\mapsto E^{(p)} \\ \mathrm{Hom}_{\mathbf{Ell}}(E, E') &\ni \phi \rightarrow \phi^{(p)} \end{aligned}$$

is a covariant endofunctor on the category \mathbf{Ell} of Elliptic Curves defined over $\bar{\mathbb{F}}_p$ and their isogenies.

Sometimes, we abuse terminology and speak of Elliptic Curves when we mean isomorphism classes of Elliptic Curves.

Many examples will be over \mathbb{F}_{101^2} . Let $p = 101$ and $q = p^2$. We usually use the generator $\alpha \in \mathbb{F}_q$ with minimal polynomial $x^2 + 97x + 2$.

1 Example - The cases I, II and III

1.1 Case I

Finding examples of case I is trivial - just take a curve E with $j(E) \in \mathbb{F}_p$. Then clearly $E^{(p)} = E$ and so also $E_0^{(p)} = E_0$ (since $\cdot^{(p)}$ maps the path $E \rightarrow E_0$ to $E = E^{(p)} \rightarrow E_0^{(p)}$).

Furthermore, it is easy to see that there are a lot of curve E such that the associated E_0 is defined over \mathbb{F}_p (and we are again in case I).

1.2 Case II

Here I was not quite sure if it even occurs. As it turns out, it does. Consider E with $j(E) = 17\alpha + 45$. Then $[\mathcal{O}_K : \mathbb{Z}[\pi]] = 2^3$ so E lies on the crater of the 3-isogeny graph. However there is a 3-isogeny $E \rightarrow E^{(p)}$ since $j(E^{(p)}) = j(E)^p = 84\alpha + 12$. In fact, in

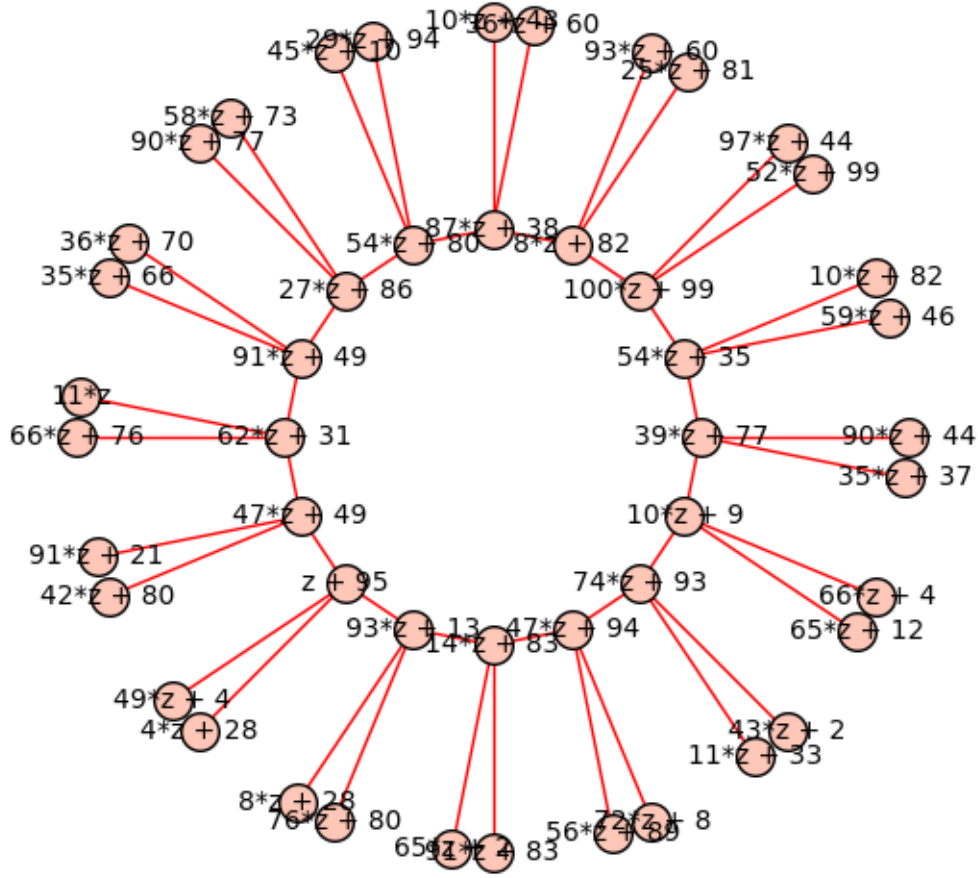


Figure 1: A 3-isogeny vulcano over $\mathbb{F}_{101^2} = \mathbb{F}_{101}[\alpha]$ that satisfies case II (in the plot have $z = \alpha$). Note that e.g. $(39\alpha + 77)^{101} = 62\alpha + 31$.

this case, the crater consists only of E and $E^{(p)}$. For a more interesting example, see Figure 1.

Further, when we consider the path $E = E_0 \rightarrow \dots \rightarrow E_n = E^{(p)}$ on the crater, there are more or less two possibilities for the $\cdot^{(p)}$ conjugate path¹.

- It could be that the conjugate of $E_i \rightarrow E_{i+1}$ is the dual of $E_{n-i-1} \rightarrow E_{n-i}$, hence we just go the path $E \rightarrow \dots \rightarrow E^{(p)}$ backwards.
- It could be that the conjugate of $E_i \rightarrow E_{i+1}$ is $E_{n+i} \rightarrow E_{n+i+1}$, where

$$E_0, \dots, E_n, E_{n+1}, \dots, E_{n+m} = E_0$$

is the cycle along the whole crater.

¹Remember that $\cdot^{(p)}$ is functorial, hence we can also apply to isogenies $E_i \rightarrow E_{i+1}$

However, as we will see, the first case is impossible.

Note that we have

Proposition 1.1. *Let $[\mathfrak{b}] \in \text{Cl}(\mathcal{O})$ where $\mathcal{O} = \text{End}(E)$ for an ordinary Elliptic Curve E/\mathbb{F}_{p^2} such that $[\mathfrak{b}].E = E^{(p)}$. Then $[\mathfrak{b}]^2 = [(1)]$.*

Proof. I think there is some mistake with my definition of the class group action, see also the next paragraph. With the current (probably wrong) definition, the following works. Otherwise, I suppose that anyway we have $[\mathfrak{b}] = [(p, \pi)]$ and then the claim follows by Lemma 2.5.

We recall the definition of the class group action in the case $[\mathfrak{b}].E^{(p)}$. For an ideal $\mathfrak{b}' \leq \text{End}(E^{(p)})$, have by definition

$$[\mathfrak{b}'].E^{(p)} = E^{(p)}/E^{(p)}[\mathfrak{b}'] = E^{(p)} / \bigcap_{\beta \in \mathfrak{b}'} \ker(\beta)$$

However, \mathfrak{b} is an ideal in $\text{End}(E)$, which is only isomorphic to $\text{End}(E^{(p)})$. Since $\text{End}^0(E)$ is a quadratic imaginary number field, it has one nontrivial field automorphism, and thus the isomorphism $\text{End}(E) \cong \text{End}(E^{(p)})$ is not unique. But there is a unique canonical isomorphism, i.e. an isomorphism that is induced by an (equivalently any) isogeny $\phi : E \rightarrow E^{(p)}$ as

$$\Phi_* : \text{End}(E) \rightarrow \text{End}(E^{(p)}), \quad \alpha \mapsto \frac{1}{\deg(\phi)} \phi \circ \alpha \circ \hat{\phi}$$

This is the isomorphism we use, i.e. we say

$$E^{(p)}[\mathfrak{b}] = E^{(p)}[\Phi_*(\mathfrak{b})] \quad \text{and} \quad [\mathfrak{b}].E^{(p)} = [\Phi_*(\mathfrak{b})].E^{(p)} = E^{(p)}/E^{(p)}[\mathfrak{b}]$$

Now let $\phi : E \rightarrow E/E[\mathfrak{b}] = E^{(p)}$ be a separable isogeny with kernel $E[\mathfrak{b}]$ (by choosing the representative \mathfrak{b} of $[\mathfrak{b}] \in \text{Cl}(\mathcal{O})$ correspondingly, we can assume that). We have

$$\ker(\phi^{(p)}) = E[\mathfrak{b}]^{(p)} = \bigcap_{\beta \in \mathfrak{b}} \ker(\beta)^{(p)} = \bigcap_{\beta \in \mathfrak{b}} \ker(\beta^{(p)}) = \bigcap_{\beta \in \mathfrak{b}^{(p)}} \ker(\beta)$$

Now note that the Frobenius isogeny $\pi : E \rightarrow E^{(p)}$, $P \mapsto P^{(p)}$ induces the canonical isomorphism $\text{End}(E) \rightarrow \text{End}(E^{(p)})$ and so the image of \mathfrak{b} under that isomorphism is $\mathfrak{b}' = \mathfrak{b}^{(p)} \leq \text{End}(E^{(p)})$. Thus

$$\bigcap_{\beta \in \mathfrak{b}^{(p)}} \ker(\beta) = \bigcap_{\beta \in \mathfrak{b}'} \ker(\beta) = E^{(p)}[\mathfrak{b}'] = E^{(p)}[\mathfrak{b}]$$

So by the uniqueness of the image curve for an isogeny with fixed kernel yields that $E = \text{im}(\phi^{(p)}) = [\mathfrak{b}].E^{(p)}$. Thus $[\mathfrak{b}]^2.E = [\mathfrak{b}].E^{(p)} = E$ and since the class group action is free, we see that $[\mathfrak{b}]^2 = [(1)]$. \square

From this we get the

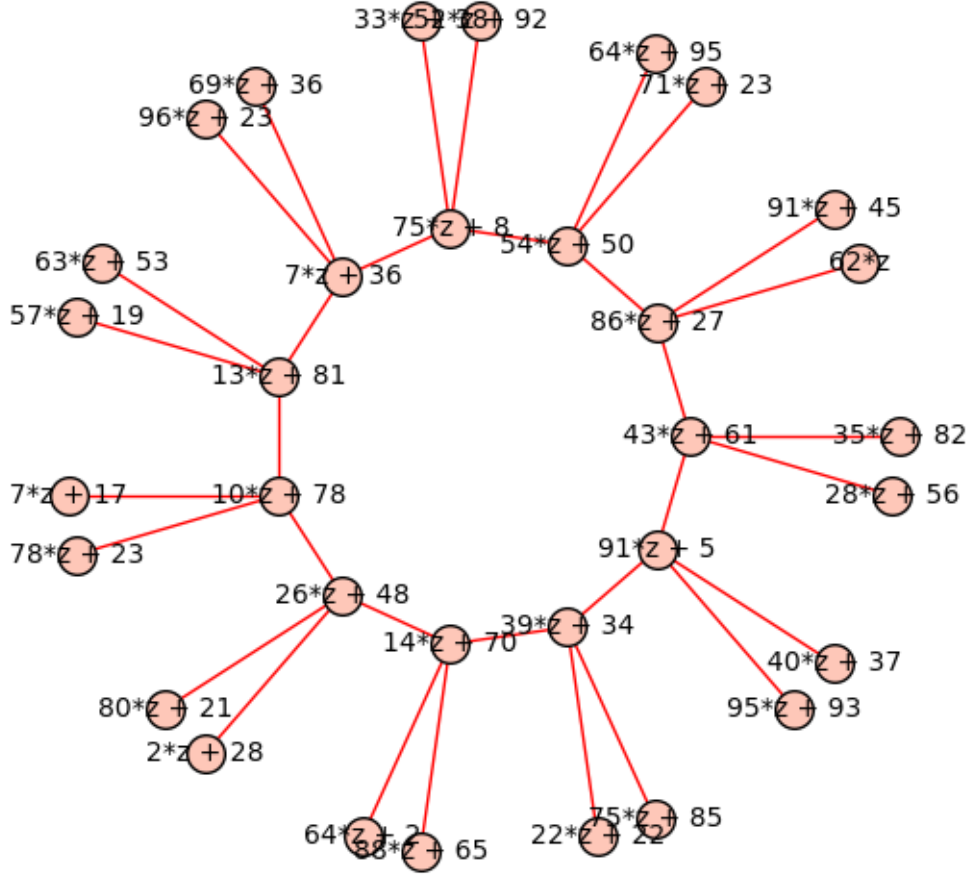


Figure 2: A 3-isogeny volcano over $\mathbb{F}_{101^2} = \mathbb{F}_{101}[\alpha]$ that satisfies case III (in the plot have $z = \alpha$).

Corollary 1.2. *Assume that $E = E_0 \rightarrow E_1 \rightarrow \dots \rightarrow E_n = E$ is the cycle once around the crater (and $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$). If $E^{(p)} = E_i$ then n is even and $i = n/2$, i.e. $E^{(p)}$ is on the other side of the crater².*

Proof. If l does not split in \mathcal{O}_K , then the crater has at most two elements and this is trivial. So assume $(l) = l_1 l_2$. It is known that then the action of $[l_1]$ resp. $[l_2]$ corresponds to walking around the crater in one direction resp. the other. So wlog $[l_1].E_i = E_{i+1}$.

Now assume that $E^{(p)} = E_i$, so $[b].E = E_i = [l_1]^i.E$. Since the action is free, it follows that $[b] = [l_1]^i$. By the previous theorem, we have now $[l_1]^{2i} = [b]^2 = [(1)]$ and so $[l_1]^{2i}.E = E_{2i} = E$. Thus $i = n/2$ and the claim follows. \square

In particular, the path between E and $E^{(p)}$ is likely to have length $\omega(\log(p))$, since the crater is usually large. This is displayed e.g. Figure 1.

1.3 Case III

We give the example displayed in Figure 3. Consider E with $j(E) = 64\alpha + 5$. Then $j(E^{(p)}) = j(E)^p = 37\alpha + 59$. However, we have that E lies on the crater, together with curve of j -invariants

$$88\alpha + 70, 54\alpha + 52, 95\alpha + 11$$

Hence there is no 3-isogeny path from E to $E^{(p)}$. Note that $[\mathcal{O}_K : \mathbb{Z}[\pi]] = 2^2 \cdot 3^2$ but $[\mathcal{O}_K : \text{End}(E)] = 2^2$, which shows that E lies on the crater.

Now we want to have a closer look onto the class group action in this case. Have $d(\text{End}(E)) = -320$, so $K = \mathbb{Q}(\sqrt{-5})$ and $d(\mathcal{O}_K) = -5$. Hence, we have $\text{End}(E) \cong \mathbb{Z}[4\sqrt{-5}]$ and $\mathcal{O}_K \cong \mathbb{Z}[\sqrt{-5}]$.

Sage tells us that $h(\mathcal{O}_K) = 2$ and $h(\text{End}(E)) = 8$. With this, we can already see that

$$64\alpha + 5, 88\alpha + 70, 54\alpha + 52, 95\alpha + 11$$

and

$$(64\alpha + 5)^p, (88\alpha + 70)^p, (54\alpha + 52)^p, (95\alpha + 11)^p$$

is the set of j -invariants of all Elliptic Curves with endomorphism ring $\cong \text{End}(E)$. On this set, $\text{Cl}(\mathbb{Z}[4\sqrt{-5}])$ then acts freely and transitively. Now it would be of course interesting to find out how $\text{Cl}(\mathbb{Z}[4\sqrt{-5}])$ really looks like.

2 Properties of the endomorphism ring vs the cases

Proposition 2.1. *Let E be an ordinary Elliptic Curve defined over a finite field of characteristic p .*

- $\text{End}(E)$ has an element of norm p iff $j(E) \in \mathbb{F}_p$.
- $\text{End}(E)$ has a nontrivial element (i.e. $\neq \epsilon p$ for a unit ϵ) of norm p^2 iff $j(E) \in \mathbb{F}_{p^2}$.

²Note that this does not hold if $E, E^{(p)}$ are not in the same crater, see Figure 2.

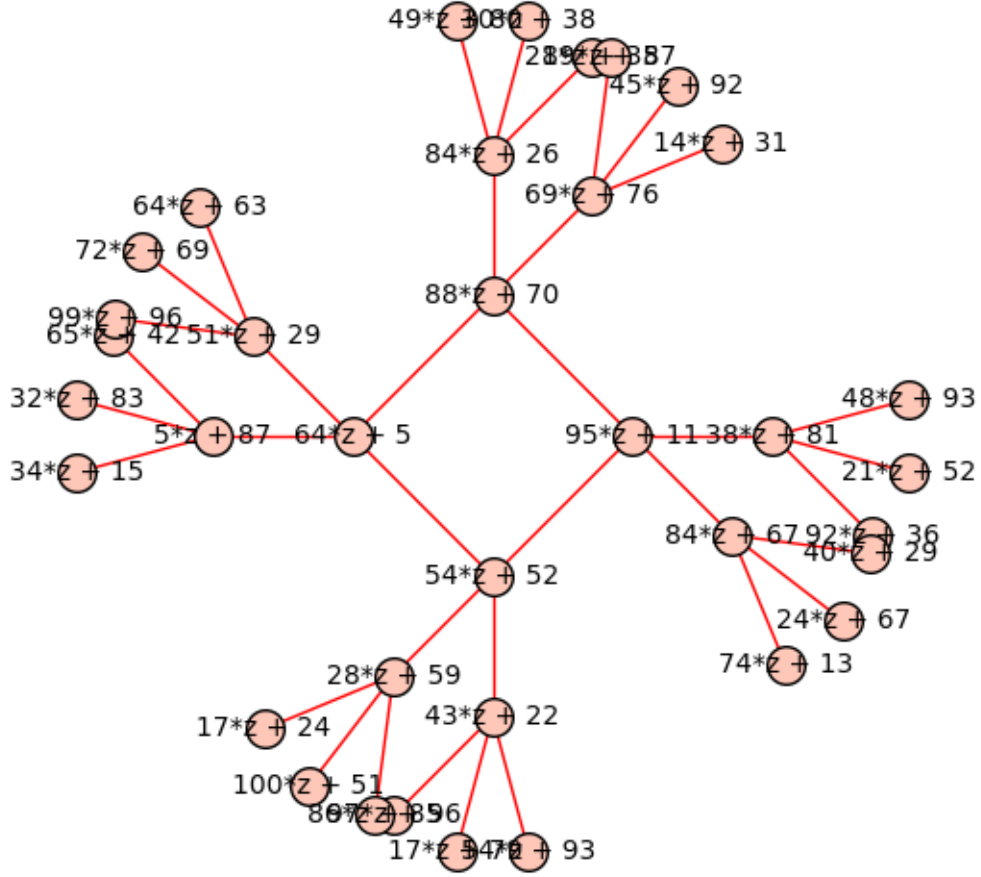


Figure 3: A 3-isogeny volcano over $\mathbb{F}_{101^2} = \mathbb{F}_{101}[\alpha]$ that satisfies case III (in the plot have $z = \alpha$).

Proof. The directions \Leftarrow is clear, as the norm of the q -th power Frobenius endomorphism is q .

For the direction \Rightarrow , assume there is an element $\alpha \in \text{End}(E)$ with $N(\alpha) = p$. If α is inseparable (as isogeny), then we have that it factors through the p -th power Frobenius endomorphism π , and thus $\alpha = \lambda \circ \pi$ for an isomorphism $\lambda : E^{(p)} \rightarrow E$. Thus $j(E^{(p)}) = j(E)$.

On the other hand, if α is separable, it must have kernel of size p , so $\ker(\alpha) = E[p]$ since $\#E[p] = p$ (E is ordinary). Thus $\ker(\alpha) \subseteq \ker([p])$ and we see that $[p]$ factors through α as $[p] = \psi \circ \alpha$. Now have that $\deg(\psi) = p = p^2/\deg(\alpha)$ and clearly ψ is inseparable. The claim follows as above.

For the second point, assume $\alpha \in \text{End}(E)$ has norm $N(\alpha) = p^2$ and $\alpha \neq \pm p$. If α is purely inseparable, we are done. If α is separable, its kernel must be $E[p^2]$ and so it factors through $[p^2]$. Since $[p^2]$ has inseparability degree p^2 , we see that $[p^2] = \pi^2 \circ \alpha$ where π is the p -th power Frobenius morphism. Since α is an endomorphism of E , find $\pi^2 : E \rightarrow E$, thus $j(E) \in \mathbb{F}_{p^2}$.

Finally, if α has inseparability degree p , then its kernel must be $E[p]$ and so $\alpha = \beta \circ \pi$ where $\beta : E^{(p)} \rightarrow E$ is separable with kernel $E^{(p)}[p]$. However, by the uniqueness of the separable isogeny with kernel $E^{(p)}[p]$, we know that (up to isomorphism) also $[p]$ is $\beta \circ \pi$. This now implies that $\alpha = \epsilon p$ for some unit ϵ . \square

Proposition 2.2. *Let $D < 0$. Then the curves E with $\text{End}(E) = \mathbb{Z}[\sqrt{D}]$ have $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ if and only if*

$$a^2 - b^2 D = p$$

has no solution $a, b \in \mathbb{Z}$ and

$$a^2 - b^2 D = p$$

has a nontrivial solution $a, b \in \mathbb{Z}$.

Let E/\mathbb{F}_{p^2} be an ordinary Elliptic Curve and write $\mathcal{O} := \text{End}(E)$, $\mathcal{K} := \text{End}(E) \otimes \mathbb{Q}$. Let π be the $q = p^2$ -th power Frobenius endomorphism and let t be its trace. Assume $p \neq 2$.

Lemma 2.3. *Have $(p) = (p, \pi)(p, \pi - t)$ in $\mathbb{Z}[\pi]$, \mathcal{O} resp. $\mathcal{O}_{\mathcal{K}}$.*

Proof. Have

$$(p, \pi)(p, \pi - t) = (p^2, p\pi, p\pi - pt, \pi^2 - t\pi) = (p^2, pt, p\pi, -p^2) = (up^2 + vtp, \dots) = (p)$$

where $up + vt = 1$ (note that $t \perp p$ since E is ordinary). \square

Lemma 2.4. *(p, π) is principal (in \mathcal{O}) if and only if E/\mathbb{F}_p .*

Proof. If (p, π) is principal, then its generator is an element of norm p , so E/\mathbb{F}_p . On the other hand, if E/\mathbb{F}_p , then the p -th power Frobenius endomorphism π_p satisfies $p = \pi_p(t_p - \pi_p)$, $\pi = \pi_p^2$ and $\pi_p = u(\pi + p) + v\pi_p p$, where t_p is its trace and $ut + vp = 1$. \square

There must be some problem in my definition of the class group action, as it can happen that $[(p, \pi)]$ is not $[(1)]$, but $E[(p, \pi)]$ is clearly trivial, so³ $(p, \pi).E = E/E[(p, \pi)] = E$. However, this contradicts the freeness of the class group action.

Lemma 2.5. *Assume $j \neq 0, 1728$. $[(p, \pi)]$ has order ≤ 2 in $\text{Cl}(\mathcal{O})$ resp. $\text{Cl}(\mathcal{O}_K)$.*

Proof. Since E/\mathbb{F}_{p^2} , we know that there is a nontrivial element α of norm p^2 . Now have in \mathcal{O}_K that $(\alpha)|(p)^2$ and with $p = (p, \pi)(p, \pi - t)$ have thus $(\alpha) = (p)$ or $(\alpha) = (p, \pi)^2$ or $(\alpha) = (p, \pi - t)^2$. However, by assumption we only have units ± 1 in \mathcal{O}_K resp. \mathcal{O} , so the first case is impossible, as it implies $\alpha = \pm p$.

Note that $[(p, \pi)] = [(p, \pi - t)^{-1}]$, so wlog assume $(\alpha) = (p, \pi)^2$. It follows that $(p, \pi)^2$ is principal, so $[(p, \pi)]^2 = [(1)]$. \square

3 Ideals in \mathcal{O} resp. \mathcal{O}_K

Consider an ordinary Elliptic Curve E/\mathbb{F}_q , $\mathcal{O} := \text{End}(E)$, $K := \mathcal{O} \otimes \mathbb{Q}$ and \mathcal{O}_K the ring of integers in K . Assume that $j(E) \in \mathbb{F}_q$ is not contained in any proper subfield of \mathbb{F}_q and let π be the q -th power Frobenius endomorphism. Let t be its trace.

Proposition 3.1. $p \nmid d(\mathcal{O})$

Proof. Have that

$$d(\mathbb{Z}[\pi]) = t^2 - 4q \perp p$$

since $t \perp p$ as E is ordinary. The claim follows since $d(\mathcal{O}) \mid d(\mathcal{O})[\mathcal{O} : \mathbb{Z}[\pi]]^2 = d(\mathbb{Z}[\pi])$. \square

Proposition 3.2. *Let $\mathfrak{a} \leq \mathcal{O}$. Then $\mathfrak{a} \cap \mathbb{Z} = (a)$ with $a \mid [\mathcal{O} : \mathfrak{a}] \mid a^2$. Note that if $\mathfrak{a} = \mathfrak{p}$ is prime, then trivially a must be prime.*

Proof. Clearly $[\mathcal{O} : \mathfrak{a}] \in \mathfrak{a}$ as $1 \in \mathcal{O}/\mathfrak{a}$ has order dividing $\#(\mathcal{O}/\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, so $a \mid [\mathcal{O} : \mathfrak{a}]$. On the other hand, have $[\mathcal{O} : \mathfrak{a}] \mid [\mathcal{O} : a\mathcal{O}] = a^2$. \square

Lemma 3.3. *Let $\mathfrak{p} \leq \mathcal{O}_K$ be a prime with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then \mathfrak{p} has a set of generators in \mathcal{O} .*

Proof. Suppose \mathfrak{p} is a prime over p , and let $\mathcal{O} = \mathbb{Z}[\phi]$. If $\text{MiPo}(\phi) = f(X)g(X) \pmod{p}$ splits, then have

$$p\mathcal{O}_K = (p, f(\phi))(p, g(\phi))$$

and so the prime ideals over p are $(p, f(\phi))$ and $(p, g(\phi))$. If $\text{MiPo}(\phi) \pmod{p}$ is irreducible, then have that $p\mathcal{O}_K$ is prime and thus the only prime ideal over p . Hence, all prime ideals over p (including \mathfrak{p}) have a set of generators in \mathcal{O} . \square

Corollary 3.4. *Let $\mathfrak{a} \leq \mathcal{O}_K$ be an ideal with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then \mathfrak{a} has a set of generators in \mathcal{O} .*

³We know that (p, π) is invertible, as $\frac{1}{p}(p, \pi)(p, \pi - t) = (1)$.

Proposition 3.5. *Let $\mathfrak{p} \leq \mathcal{O}$ be a prime and $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_K$. Then $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}'}$.*

Proof. We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[f\alpha]$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Thus $f \notin \mathfrak{p}$ and so $f \in \mathcal{O}_{\mathfrak{p}}^*$. Therefore $\mathcal{O}_K \subseteq \mathcal{O}_{\mathfrak{p}}$ and thus $(\mathcal{O}_K)_{\mathfrak{p}'} \subseteq \mathcal{O}_{\mathfrak{p}}$. \square

Proposition 3.6. *Let $\mathfrak{I}(\mathcal{O})$ resp. $\mathfrak{I}(\mathcal{O}_K)$ denote the set of invertible ideals of norm $\perp [\mathcal{O}_K : \mathcal{O}]$. Then*

$$\mathfrak{I}(\mathcal{O}) \rightarrow \mathfrak{I}(\mathcal{O}_K), \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$$

is a monoid isomorphism with inverse

$$\mathfrak{I}(\mathcal{O}_K) \rightarrow \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

Proof. Clearly, this is a well-defined monoid homomorphism. Hence, we have to show that it is bijective.

By Corollary 3.4, we know that any $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$ has generators in \mathcal{O} , thus $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. This shows that $\mathfrak{a} \cap \mathcal{O}$ is a preimage of \mathfrak{a} , and so the map is surjective.

Assume now $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$ with $\mathfrak{a}\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K$ and $\mathfrak{N}(\mathfrak{a}), \mathfrak{N}(\mathfrak{b}) \perp [\mathcal{O}_K : \mathcal{O}]$. We show that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ for all primes $\mathfrak{p} \leq \mathcal{O}$. Note that if $\mathfrak{N}(\mathfrak{p}) \not\perp [\mathcal{O}_K : \mathcal{O}]$, this holds trivially, as $\mathfrak{a}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$. Otherwise, note that

$$\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}} = \mathfrak{a}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}\mathcal{O}_K(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}(\mathcal{O}_K)_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$$

as $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}}$. This shows that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ at all primes, so $\mathfrak{a} = \mathfrak{b}$ and our map is injective. Furthermore, since $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$, we see that it has the inverse

$$\mathfrak{I}(\mathcal{O}_K) \rightarrow \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

which must then be well-defined. \square

Example 3.7. Let $K = \mathbb{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ which is a PID. Let further $\mathcal{O} = \mathbb{Z}[2\sqrt{-3}]$, so $f = [\mathcal{O}_K : \mathcal{O}] = 4$.

Proposition 3.8. *Let $\mathfrak{a} \leq R$ be a radical ideal in a commutative unital ring R . If $\alpha \in \mathfrak{p}$ for all primes $\mathfrak{p} \supseteq \mathfrak{a}$ then $\alpha \in \mathfrak{a}$.*

Proof. We have that $\mathfrak{a}_{\alpha} \neq (1)$ otherwise $\alpha^n \in \mathfrak{a}$, so $\alpha \in \mathfrak{a}$. Thus $\mathfrak{a}_{\alpha} \subseteq \mathfrak{m}$ for a maximal ideal $\mathfrak{m} \leq R_{\alpha}$. A preimage under $R \rightarrow R_{\alpha}$ is now a prime \mathfrak{p} with $\mathfrak{a} \subseteq \mathfrak{p}$ and $\alpha \notin \mathfrak{p}$. \square

Corollary 3.9. *If $q \perp d(\mathcal{O})$ is an integer and $q \mid \alpha$ in \mathcal{O}_K , then also $q \mid \alpha$ in \mathcal{O} .*

Proof. It suffices to prove this for primes q . Since $q \nmid d(\mathcal{O})$, we know that (q) is unramified, hence radical. Now observe that $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}}$ for primes \mathfrak{p} over q and so $\alpha \in \mathfrak{p}$ for all primes \mathfrak{p} over q . The previous proposition now shows that $\alpha \in (q)$. \square

4 Norm equations

Lemma 4.1. *Let $D < 0$ and \mathcal{O} be the imaginary quadratic order of discriminant D . Then $1, \alpha$ with $\alpha = \frac{D+\sqrt{D}}{2}$ is a \mathbb{Z} -basis of \mathcal{O} and*

$$N(a + b\alpha) = \left(a + \frac{D}{2}b\right)^2 - \frac{D}{4}b^2$$

Proof.

$$\begin{aligned} N(\alpha) &= a^2 + ab\frac{D+\sqrt{D}}{2} + ab\frac{D-\sqrt{D}}{2} + \frac{D^2-D}{4}b^2 = a^2 + Dab + \frac{D^2-D}{4}b^2 \\ &= \left(a + \frac{D}{2}b\right)^2 - \frac{D}{4}b^2 \end{aligned}$$

□

Corollary 4.2. *Let l be a prime and $D < 0$. Let \mathcal{O} be the quadratic imaginary order of discriminant D . If there exists a nontrivial element $\alpha \in \mathcal{O}$ of norm l^e (i.e. $\alpha \notin \mathbb{Z}$), then*

$$e \geq \log_l(-D) - \log_l(4)$$

Corollary 4.3. *Let $E/\bar{\mathbb{F}}_p$ be an ordinary Elliptic Curve such that $\text{End}(E)$ has discriminant D . Suppose that $j(E_0) \notin \mathbb{F}_p$. Then the shortest l -isogeny path between E and $E^{(p)}$ has length at least*

$$\frac{1}{2} \log_l(-D) - \log_l(2)$$

Proof. First, define E_0 to be the corresponding curve on the crater of the l -isogeny volcano. Let $v \in \mathfrak{N}$ be maximal with $l^v \mid [\text{End}(E_0) : \text{End}(E)]$, so $\text{End}(E_0)$ has discriminant D/l^v . Now we know that $E_0^{(p)}$ is at the opposite side of the crater, and the size of the crater is the order of $[\mathfrak{l}_1]$ in $\text{Cl}(\text{End}(E_0))$ where $l = \mathfrak{l}_1 \mathfrak{l}_2$. If e is this order, then we know that there must be a nontrivial element of order l^e in $\text{End}(E_0)$, so

$$e \geq \log_l(-D/l^v) - \log_l(4)$$

Thus, the distance of E_0 and $E_0^{(p)}$ is at least

$$\frac{1}{2}e \geq \frac{1}{2} \log_l(-D/l^v) - \frac{1}{2} \log_l(4) = \frac{1}{2} \log_l(-D) - \frac{1}{2}v - \log_l(2)$$

However, the shortest path from E to E_0 has length v , and similarly for the shortest path from $E^{(p)}$ to $E_0^{(p)}$. Thus we find that the length of the shortest path from E to $E^{(p)}$ is at least

$$\frac{1}{2} \log_l(-D) - \frac{1}{2}v - \log_l(2) + 2v \geq \frac{1}{2} \log_l(-D) - \log_l(2)$$

□

$j(E)$	$h(\text{End}(E))$	$[\mathcal{O}_K : \text{End}(E)]$	$d(\text{End}(E))$	$[\text{End}(E) : \mathbb{Z}[\pi]]$
α	36	3	-36315	1
$4\alpha + 99$	64	1	-40020	1
$61\alpha + 16$	2	1	-24	28
$48\alpha + 73$	64	?	-37440	?
$12\alpha + 79$	12	?	-2548	?
$91\alpha + 34$	24	?	-16468	?
$95\alpha + 20$	64	?	-40548	?
$97\alpha + 12$	48	?	-35475	?
$97\alpha + 8$	48	?	-35620	?
$93\alpha + 8$	24	?	-23643	?
$77\alpha + 16$	16	?	-2340	?
$21\alpha + 48$	30	?	-35179	?
$31\alpha + 59$	48	?	-29355	?
$82\alpha + 39$	24	?	-18603	?
$64\alpha + 38$	36	?	-40075	?
$92\alpha + 74$	32	?	-30195	?
$38\alpha + 18$	16	?	-2340	?
$69\alpha + 25$	40	?	-31588	?
$99\alpha + 64$	32	?	-30195	?
$56\alpha + 4$	32	?	-30195	?
$26\alpha + 90$	12	?	-2548	?
$93\alpha + 49$	48	?	-36708	?
$17\alpha + 16$	32	?	-13908	?
$84\alpha + 67$	4	?	-180	?
$100\alpha + 34$	56	?	-40788	?
$30\alpha + 2$	16	?	-2244	?
$21\alpha + 41$	2	?	-52	?
$24\alpha + 59$	24	?	-26643	?
$67\alpha + 94$	64	?	-37204	?
$88\alpha + 99$	2	?	-88	?
$47\alpha + 26$	48	?	-24420	?
$12\alpha + 7$	16	?	-2520	?
$55\alpha + 77$	24	?	-17395	?
$95\alpha + 92$	8	?	-987	?
$68\alpha + 12$	12	?	-756	?
$82\alpha + 66$	28	?	-4532	?
$91\alpha + 38$	16	?	-6948	?
$99\alpha + 20$	24	?	-18603	?
$52\alpha + 77$	80	?	-40404	?

Table 1: Table of class numbers of $\text{End}(E)$ for Elliptic Curves $E/\mathbb{F}_{101^2} = \mathbb{F}_{101}[\alpha]$. Note that the j -values are not uniformly chosen, in particular, j -values that lead to a conductor $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ with “big” prime power divisors have been ignored, as the current implementation of computing the endomorphism ring would take ages for them.

5 Example - j-invariant $61\alpha + 16$

Let E be an Elliptic Curve defined over \mathbb{F}_{101^2} with j-invariant $61\alpha + 16$. Then the q -th power Frobenius π has minimal polynomial

$$X^2 - 190X + 10201$$

Furthermore, we find that $\text{End}(E) = \mathcal{O}_{\mathcal{K}}$ for $\mathcal{K} = \mathbb{Q}(\sqrt{-6})$. So

$$\pi = \frac{190 + 28\sqrt{-6}}{2} = 95 + 14\sqrt{-6}$$

or

$$\sqrt{-6} = \frac{\pi - 95}{14}$$

Note that $\pi - 95$ has norm $2^3 \cdot 3 \cdot 7^2$. The class group of \mathcal{O} has order 2, and a generator is e.g. the coset of $(2, \sqrt{-6})$. Hence, to find $E[(2, \sqrt{-6})]$ we need to find

$$\ker\left(\frac{\pi - 95}{14}\right) \cap E[2] = 14 \ker(\pi - 95) \cap E[2] = 14(\ker(\pi - 95) \cap E[28])$$

Now choose a $\mathbb{Z}/4\mathbb{Z}$ -basis P_1, P_2 of $E[4]$ and a $\mathbb{Z}/7\mathbb{Z}$ -basis Q_1, Q_2 of $E[7]$. Have that w.r.t. these basis, π is given by the matrices

$$\begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$$

Since $95 \equiv 3 \pmod{4}$ and $95 \equiv 4 \pmod{7}$, we see that $\ker(\pi - 95) \cap E[28]$ projects to

$$\langle P_1, 2P_2 \rangle \subseteq E[4] \quad \text{and} \quad E[7] \subseteq E[7]$$

and thus is $E[14] + \langle P_1 \rangle$. This implies that $E[(2, \sqrt{-6})] = \langle 2P_1 \rangle$. Note that we picked

$$P_1 = ((59+7\alpha), (48+75\alpha)+(73+3\alpha)t), \quad P_2 = ((7+17\alpha)+100t, (71+72\alpha)+(31+88\alpha)t)$$

before, where t has minimal polynomial $(24 + 51\alpha) + (94 + 84\alpha)T + T^2$

To find the whole kernel, pick a $\mathbb{Z}/8\mathbb{Z}$ -basis P_1, P_2 of $E[8]$, a $\mathbb{Z}/3\mathbb{Z}$ -basis Q_1, Q_2 of $E[3]$ and a $\mathbb{Z}/49\mathbb{Z}$ -basis R_1, R_2 of $E[49]$. Find then that modulo 8, 3 resp. 49, π is given by the matrix

$$\begin{pmatrix} 3 & 6 \\ 4 & 3 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \quad \text{resp.} \quad \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

6 Example - The ordinary endomorphism ring

The information in this section is all known material - I just wanted to understand properly how one can compute the endomorphism ring, and what problems occur.

Consider the finite field

$$\mathbb{F}_q = \mathbb{F}_{37^2} = \mathbb{F}_{37} + \alpha\mathbb{F}_{37}$$

where $\alpha^2 + 33\alpha + 2 = 0$. Further, consider the Elliptic Curve E/\mathbb{F}_q with j -invariant 3α , given by

$$E : y^2 = x^3 + (15\alpha + 17)x + (5\alpha + 3)$$

Then we find that the q -th power Frobenius endomorphism π satisfies the minimal equation

$$\pi^2 + 47\pi + 1369$$

and in particular, its trace is -47 . Hence, the number field $\mathcal{K} := \mathcal{O} \otimes \mathbb{Q}$ where $\mathcal{O} = \text{End}(E)$ contains $\sqrt{47^2 - 4 \cdot 1369} = \sqrt{-3^3 \cdot 11^2}$. We observe that $\mathcal{K} = \mathbb{Q}(\sqrt{-3})$ and has discriminant -3 . Furthermore the ring of integers is $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$.

Knowing the number field, we want to find the endomorphism ring. First, observe that the Frobenius order $\mathbb{Z}[\pi]$ has conductor 33. Now consider the endomorphism

$$\phi := 2\pi + 47$$

The advantage is that we can evaluate ϕ on points of E , but evaluating $\pi + 47/2$ is not so easy. Clearly $[\mathbb{Z}[\pi] : \mathbb{Z}[\phi]] = 2$ and so $\mathbb{Z}[\phi]$ has conductor 66.

Torsion points

In order to find whether $\phi/n \in \mathcal{O}$, we factor $66 = 2 \cdot 3 \cdot 11$ and compute the corresponding torsion groups. This turns out to be quite difficult.

Assume $\mathbb{F}_{37^{12}} = \mathbb{F}_{37}[\beta]$ with

$$\text{MiPo}_{\mathbb{F}_{37}}(\beta) = x^{12} + 4x^7 + 31x^6 + 10x^5 + 23x^4 + 18x^2 + 33x + 2$$

Then $E[2]$ is generated by

$$\begin{aligned} P_1 &= (11\beta^{11} + 19\beta^{10} + \beta^9 + 27\beta^8 + 8\beta^7 + 16\beta^6 + 17\beta^5 + 32\beta^4 + 12\beta^3 + 14\beta^2 + 24\beta + 32 : 0 : 1) \\ Q_1 &= (15\beta^{11} + 7\beta^{10} + 33\beta^9 + 11\beta^8 + 6\beta^7 + 12\beta^6 + 26\beta^5 + 7\beta^4 + 33\beta^3 + 25\beta^2 + 8\beta + 19 : 0 : 1) \end{aligned}$$

Further $E[3]$ is generated by

$$\begin{aligned} P_2 &= (19\beta^{11} + 34\beta^{10} + 3\beta^9 + 29\beta^8 + 7\beta^7 + 3\beta^6 + 18\beta^5 + 21\beta^4 + 23\beta^3 + 30\beta^2 + 23\beta + 25 \\ &\quad : 6\beta^{11} + 25\beta^{10} + 4\beta^9 + 13\beta^8 + 10\beta^7 + 23\beta^6 + 20\beta^5 + 30\beta^4 + 24\beta^3 + 6\beta^2 + 17\beta + 5 : 1) \\ Q_2 &= (31\beta^{11} + 24\beta^{10} + 35\beta^9 + 32\beta^8 + 2\beta^7 + 10\beta^6 + 23\beta^5 + 35\beta^4 + 22\beta^3 + 13\beta^2 + 12\beta + 12 \\ &\quad : 18\beta^{11} + 2\beta^{10} + 32\beta^9 + 26\beta^8 + 17\beta^7 + 5\beta^6 + 19\beta^5 + 31\beta^4 + 31\beta^3 + \beta^2 + 22\beta + 1 : 1) \end{aligned}$$

For $E[11]$ we must even go to the extension degree 110. So assume $\mathbb{F}_{37^{220}} = \mathbb{F}_{37}[\gamma]$. Then $E[11]$ is generated by P_3 and Q_3 . For the values of $\text{MiPo}_{\mathbb{F}_{37}}(\gamma)$ and P_3, Q_3 see Section 7.

Now we can compute $\phi(P_1), \phi(Q_1), \phi(P_2), \phi(Q_2), \phi(P_3), \phi(Q_3)$ and see that none of them is zero. Since $\deg(\phi) = [\mathcal{O} : \mathbb{Z}[\phi]] \mid [\mathcal{O}_K : \mathbb{Z}[\phi]] = 2 \cdot 3 \cdot 11$, we see that the kernel of ϕ is trivial. Thus no ϕ/n is contained in \mathcal{O} . Therefore we see that

$$\mathcal{O} \cap \mathbb{Z}[\sqrt{D}] = \mathbb{Z}[\phi]$$

The inclusion \supseteq is clear, and for the other direction, note that $\mathcal{O} \cap \mathbb{Z}[\sqrt{D}] = \mathbb{Z} + t\sqrt{D}\mathbb{Z}$ and $\mathbb{Z}[\phi] = \mathbb{Z} + s\sqrt{D}\mathbb{Z}$. Since $\mathbb{Z}[\phi] \subseteq \mathcal{O} \cap \mathbb{Z}[\phi]$ find thus $t \mid s$. Now observe that by choice of ϕ , have $\phi^2 \in \mathbb{Z}$ and so $\phi = s\sqrt{D}$. However, $\phi/\frac{s}{t} = t\sqrt{D} \in \mathcal{O}$. By the above, it follows that $\frac{s}{t} = 1$, i.e. $s = t$.

The index $[\mathcal{O} : \mathbb{Z}[\phi]]$

From the consideration of the torsion points, we see that $\mathcal{O} \cap \mathbb{Z}[\sqrt{D}] = \mathbb{Z}[\phi]$. However, since $[\mathcal{O}_K : \mathbb{Z}[\sqrt{D}]] \leq 2$, we deduce that $[\mathcal{O} : \mathbb{Z}[\phi]] \leq 2$ and so

$$\mathcal{O} = \mathbb{Z}[\pi]$$

7 P_3 and Q_3

The minimal polynomial of γ is

$$\begin{aligned} & x^{220} + 31x^{219} + 13x^{218} + 21x^{217} + 23x^{216} + 9x^{215} \\ & + 2x^{214} + 35x^{212} + 10x^{211} + 29x^{210} + 25x^{209} + 20x^{208} \\ & + 17x^{207} + 30x^{206} + 5x^{205} + 15x^{204} + 11x^{203} + 10x^{202} \\ & + 11x^{201} + 32x^{200} + 5x^{199} + 28x^{198} + 7x^{197} + 13x^{196} \\ & + 10x^{195} + 32x^{194} + 17x^{193} + 19x^{192} + 36x^{191} \\ & + 17x^{190} + 31x^{189} + 14x^{188} + 6x^{187} + 30x^{186} + 8x^{185} \\ & + 22x^{184} + 2x^{183} + 9x^{182} + 11x^{181} + 6x^{180} + 23x^{179} \\ & + 14x^{178} + 36x^{177} + 16x^{176} + 34x^{175} + 14x^{174} \\ & + 33x^{173} + 14x^{172} + 7x^{171} + 36x^{170} + 18x^{169} + 27x^{168} \\ & + 5x^{167} + 31x^{166} + 6x^{165} + 15x^{164} + 14x^{163} + 17x^{162} \\ & + 7x^{161} + 16x^{160} + 6x^{159} + 29x^{158} + 11x^{157} + 8x^{156} \\ & + 15x^{155} + 20x^{154} + 17x^{153} + 7x^{152} + 8x^{151} + 6x^{150} \\ & + 12x^{149} + 36x^{148} + 7x^{147} + 3x^{146} + 25x^{145} + 13x^{144} \\ & + 6x^{143} + 17x^{142} + 22x^{141} + 9x^{140} + 18x^{139} + 36x^{138} \\ & + x^{137} + 6x^{136} + 36x^{135} + 33x^{134} + 32x^{133} + 35x^{132} \\ & + 33x^{131} + 7x^{130} + 3x^{129} + 7x^{128} + 20x^{127} + 31x^{126} \\ & + 26x^{125} + 6x^{124} + 9x^{123} + 10x^{122} + 25x^{121} + 33x^{120} \\ & + 33x^{119} + 30x^{118} + 34x^{117} + 22x^{116} + 8x^{115} + 10x^{114} \\ & + 36x^{113} + 26x^{112} + 8x^{111} + 33x^{110} + 30x^{109} + 11x^{108} \\ & + 14x^{107} + 22x^{106} + 26x^{105} + 11x^{104} + 35x^{103} \\ & + 34x^{102} + 33x^{101} + 27x^{100} + 14x^{99} + 31x^{98} + 24x^{97} \\ & + x^{96} + 6x^{95} + 36x^{93} + 32x^{92} + 18x^{91} + 36x^{90} + 3x^{89} \\ & + 22x^{88} + 36x^{87} + 6x^{86} + 20x^{85} + 25x^{84} + 8x^{82} \end{aligned}$$

$$\begin{aligned}
& + 34*x^{81} + 7*x^{80} + 25*x^{79} + 21*x^{78} + 17*x^{77} + 29*x^{76} \\
& + 5*x^{75} + 19*x^{74} + 19*x^{73} + 8*x^{72} + 8*x^{71} + 26*x^{70} \\
& + 7*x^{69} + 27*x^{68} + 10*x^{67} + 31*x^{66} + 4*x^{65} + 29*x^{64} \\
& + 36*x^{62} + 3*x^{61} + 27*x^{60} + 13*x^{59} + 23*x^{58} + 33*x^{57} \\
& + 14*x^{56} + 19*x^{55} + 12*x^{54} + 20*x^{53} + 32*x^{52} + 18*x^{51} \\
& + 20*x^{49} + 20*x^{48} + x^{47} + 17*x^{46} + 16*x^{45} + 4*x^{44} \\
& + 12*x^{43} + 7*x^{42} + 34*x^{41} + 9*x^{40} + 16*x^{39} + 10*x^{38} \\
& + 25*x^{37} + 10*x^{36} + 10*x^{35} + 28*x^{34} + 33*x^{33} + 22*x^{32} \\
& + 24*x^{31} + 33*x^{30} + 6*x^{29} + 8*x^{28} + 8*x^{27} + 16*x^{26} \\
& + 31*x^{25} + 7*x^{24} + 26*x^{23} + 36*x^{22} + 29*x^{21} + 36*x^{20} \\
& + 7*x^{19} + x^{18} + 26*x^{17} + 18*x^{16} + 23*x^{15} + 10*x^{14} \\
& + 4*x^{13} + x^{12} + 24*x^{11} + 25*x^{10} + 34*x^9 + 33*x^8 \\
& + 33*x^7 + 8*x^6 + 12*x^5 + x^4 + 15*x^3 + 27*x^2 + 9*x + 2
\end{aligned}$$

P_3 is given by

$$\begin{aligned}
& (23*z^{220}^{219} + 5*z^{220}^{218} + 26*z^{220}^{217} + 27*z^{220}^{216} \\
& + 26*z^{220}^{215} + 12*z^{220}^{214} + 11*z^{220}^{213} + 10*z^{220}^{212} \\
& + 29*z^{220}^{211} + 9*z^{220}^{210} + 16*z^{220}^{209} + 24*z^{220}^{208} \\
& + 18*z^{220}^{207} + 11*z^{220}^{206} + 11*z^{220}^{205} + 6*z^{220}^{204} \\
& + 24*z^{220}^{203} + 3*z^{220}^{202} + 34*z^{220}^{201} + 18*z^{220}^{200} \\
& + 17*z^{220}^{199} + 9*z^{220}^{198} + 26*z^{220}^{197} + 2*z^{220}^{196} \\
& + 31*z^{220}^{195} + 7*z^{220}^{194} + 15*z^{220}^{193} + 11*z^{220}^{192} \\
& + 15*z^{220}^{191} + 28*z^{220}^{190} + 13*z^{220}^{189} + 6*z^{220}^{188} \\
& + 7*z^{220}^{187} + 28*z^{220}^{186} + 9*z^{220}^{185} + 9*z^{220}^{184} \\
& + 7*z^{220}^{183} + 27*z^{220}^{182} + 36*z^{220}^{181} + 35*z^{220}^{180} \\
& + 30*z^{220}^{179} + 32*z^{220}^{178} + 16*z^{220}^{177} + 15*z^{220}^{176} \\
& + 16*z^{220}^{175} + 9*z^{220}^{174} + 21*z^{220}^{173} + 6*z^{220}^{172} \\
& + 15*z^{220}^{171} + 3*z^{220}^{170} + 25*z^{220}^{169} + 23*z^{220}^{168} \\
& + z^{220}^{167} + 8*z^{220}^{166} + 34*z^{220}^{165} + 14*z^{220}^{164} \\
& + 12*z^{220}^{163} + 20*z^{220}^{162} + 4*z^{220}^{161} + 9*z^{220}^{160} \\
& + z^{220}^{159} + 25*z^{220}^{158} + 16*z^{220}^{157} + z^{220}^{156} \\
& + 21*z^{220}^{155} + 10*z^{220}^{154} + 7*z^{220}^{153} + 13*z^{220}^{152} \\
& + 32*z^{220}^{151} + 31*z^{220}^{150} + 17*z^{220}^{148} + 24*z^{220}^{147} \\
& + 26*z^{220}^{146} + 28*z^{220}^{145} + 27*z^{220}^{144} + 4*z^{220}^{143} \\
& + 5*z^{220}^{142} + 14*z^{220}^{141} + 26*z^{220}^{140} + 10*z^{220}^{139} \\
& + 14*z^{220}^{138} + 19*z^{220}^{137} + 20*z^{220}^{136} + 18*z^{220}^{135} \\
& + 16*z^{220}^{134} + 11*z^{220}^{133} + 23*z^{220}^{132} + 35*z^{220}^{131} \\
& + 22*z^{220}^{130} + 31*z^{220}^{129} + 34*z^{220}^{128} + 17*z^{220}^{127} \\
& + z^{220}^{126} + 15*z^{220}^{125} + 2*z^{220}^{124} + 22*z^{220}^{123} \\
& + 27*z^{220}^{122} + 6*z^{220}^{121} + 10*z^{220}^{120} + 7*z^{220}^{119} \\
& + 4*z^{220}^{118} + 26*z^{220}^{117} + z^{220}^{116} + 32*z^{220}^{115} \\
& + 29*z^{220}^{114} + 32*z^{220}^{113} + 18*z^{220}^{112} + 3*z^{220}^{111} \\
& + 28*z^{220}^{110} + 20*z^{220}^{109} + 17*z^{220}^{108} + 17*z^{220}^{107} \\
& + 32*z^{220}^{106} + 32*z^{220}^{105} + 26*z^{220}^{104} + 24*z^{220}^{103}
\end{aligned}$$

$$\begin{aligned}
& + 17*z^{220}_{102} + 8*z^{220}_{101} + 3*z^{220}_{100} + 2*z^{220}_{99} \\
& + 16*z^{220}_{98} + 29*z^{220}_{97} + 19*z^{220}_{96} + 27*z^{220}_{95} \\
& + 4*z^{220}_{94} + 29*z^{220}_{93} + 24*z^{220}_{92} + 19*z^{220}_{91} \\
& + 2*z^{220}_{90} + 2*z^{220}_{89} + 32*z^{220}_{88} + 23*z^{220}_{87} \\
& + 32*z^{220}_{86} + 15*z^{220}_{85} + 24*z^{220}_{84} + 36*z^{220}_{83} \\
& + 29*z^{220}_{82} + 18*z^{220}_{81} + 2*z^{220}_{80} + z^{220}_{79} \\
& + 33*z^{220}_{78} + 34*z^{220}_{77} + 4*z^{220}_{76} + 11*z^{220}_{75} \\
& + 21*z^{220}_{74} + 15*z^{220}_{73} + 10*z^{220}_{72} + 24*z^{220}_{71} \\
& + 22*z^{220}_{70} + 22*z^{220}_{69} + 31*z^{220}_{68} + 32*z^{220}_{67} \\
& + 28*z^{220}_{66} + z^{220}_{65} + 17*z^{220}_{64} + 13*z^{220}_{63} \\
& + 32*z^{220}_{62} + 20*z^{220}_{61} + 32*z^{220}_{60} + 21*z^{220}_{59} \\
& + 34*z^{220}_{58} + 11*z^{220}_{57} + 29*z^{220}_{56} + 12*z^{220}_{55} \\
& + 22*z^{220}_{54} + 11*z^{220}_{53} + 36*z^{220}_{52} + 35*z^{220}_{51} \\
& + 19*z^{220}_{50} + 35*z^{220}_{49} + 8*z^{220}_{48} + 16*z^{220}_{47} \\
& + 16*z^{220}_{46} + 27*z^{220}_{45} + 32*z^{220}_{44} + 12*z^{220}_{43} \\
& + 15*z^{220}_{42} + 6*z^{220}_{41} + 36*z^{220}_{40} + 27*z^{220}_{39} \\
& + 17*z^{220}_{38} + 20*z^{220}_{37} + 33*z^{220}_{36} + 34*z^{220}_{35} \\
& + 34*z^{220}_{34} + 3*z^{220}_{33} + 12*z^{220}_{32} + 12*z^{220}_{31} \\
& + 12*z^{220}_{30} + 5*z^{220}_{29} + 10*z^{220}_{28} + 13*z^{220}_{27} \\
& + 36*z^{220}_{26} + 16*z^{220}_{25} + 16*z^{220}_{24} + 15*z^{220}_{23} \\
& + 36*z^{220}_{22} + 18*z^{220}_{21} + 13*z^{220}_{20} + 26*z^{220}_{19} \\
& + 25*z^{220}_{18} + 21*z^{220}_{17} + 35*z^{220}_{16} + 3*z^{220}_{14} \\
& + 31*z^{220}_{13} + 8*z^{220}_{12} + 7*z^{220}_{11} + 10*z^{220}_{10} \\
& + 10*z^{220}_9 + 6*z^{220}_8 + 5*z^{220}_7 + 33*z^{220}_6 \\
& + 6*z^{220}_5 + 4*z^{220}_4 + 31*z^{220}_3 + 27*z^{220}_2 + 27*z^{220} + 14
\end{aligned}$$

$$\begin{aligned}
& : 8*z^{220}_{219} + 17*z^{220}_{218} + 27*z^{220}_{217} + 14*z^{220}_{216} \\
& + 6*z^{220}_{215} + 19*z^{220}_{214} + 18*z^{220}_{213} + 6*z^{220}_{212} \\
& + 30*z^{220}_{211} + 24*z^{220}_{210} + 33*z^{220}_{209} + 19*z^{220}_{208} \\
& + 27*z^{220}_{207} + 16*z^{220}_{206} + 24*z^{220}_{205} + 3*z^{220}_{204} \\
& + 4*z^{220}_{203} + 25*z^{220}_{202} + 29*z^{220}_{201} + 31*z^{220}_{200} \\
& + 23*z^{220}_{199} + 7*z^{220}_{198} + 28*z^{220}_{197} + 4*z^{220}_{196} \\
& + 26*z^{220}_{195} + 36*z^{220}_{194} + 18*z^{220}_{193} + 24*z^{220}_{192} \\
& + 29*z^{220}_{191} + 25*z^{220}_{190} + 23*z^{220}_{189} + 14*z^{220}_{188} \\
& + 33*z^{220}_{187} + 19*z^{220}_{186} + 14*z^{220}_{184} + 21*z^{220}_{183} \\
& + 10*z^{220}_{182} + 13*z^{220}_{181} + 21*z^{220}_{180} + 24*z^{220}_{179} \\
& + 33*z^{220}_{178} + 19*z^{220}_{177} + 7*z^{220}_{176} + 36*z^{220}_{175} \\
& + 30*z^{220}_{174} + 34*z^{220}_{173} + 27*z^{220}_{172} + 3*z^{220}_{171} \\
& + 34*z^{220}_{170} + 5*z^{220}_{169} + 36*z^{220}_{168} + 19*z^{220}_{167} \\
& + 27*z^{220}_{166} + 14*z^{220}_{165} + 10*z^{220}_{164} + 2*z^{220}_{163} \\
& + 31*z^{220}_{162} + 22*z^{220}_{161} + 7*z^{220}_{160} + 14*z^{220}_{159} \\
& + 5*z^{220}_{158} + 3*z^{220}_{157} + 22*z^{220}_{156} + 32*z^{220}_{155} \\
& + 21*z^{220}_{154} + 17*z^{220}_{153} + 34*z^{220}_{152} + 9*z^{220}_{151}
\end{aligned}$$

$$\begin{aligned}
& + 33*z^{220}_{150} + 32*z^{220}_{149} + 24*z^{220}_{148} + 16*z^{220}_{147} \\
& + 19*z^{220}_{146} + 6*z^{220}_{145} + 26*z^{220}_{144} + 24*z^{220}_{143} \\
& + 34*z^{220}_{141} + 25*z^{220}_{140} + 17*z^{220}_{139} + 25*z^{220}_{138} \\
& + 19*z^{220}_{137} + 36*z^{220}_{136} + 7*z^{220}_{134} + 32*z^{220}_{133} \\
& + 24*z^{220}_{132} + 6*z^{220}_{131} + 12*z^{220}_{130} + 30*z^{220}_{129} \\
& + 35*z^{220}_{128} + 13*z^{220}_{127} + 29*z^{220}_{126} + 2*z^{220}_{125} \\
& + 24*z^{220}_{124} + 36*z^{220}_{123} + 34*z^{220}_{122} + 2*z^{220}_{121} \\
& + 33*z^{220}_{120} + 10*z^{220}_{119} + 33*z^{220}_{118} + 2*z^{220}_{117} \\
& + 17*z^{220}_{116} + 33*z^{220}_{115} + 14*z^{220}_{114} + 22*z^{220}_{113} \\
& + 27*z^{220}_{112} + 20*z^{220}_{111} + 23*z^{220}_{110} + 34*z^{220}_{109} \\
& + 6*z^{220}_{108} + 33*z^{220}_{107} + 14*z^{220}_{106} + 28*z^{220}_{105} \\
& + 29*z^{220}_{104} + 36*z^{220}_{103} + 22*z^{220}_{102} + 35*z^{220}_{101} \\
& + 8*z^{220}_{100} + 10*z^{220}_{99} + 10*z^{220}_{98} + 16*z^{220}_{97} \\
& + 19*z^{220}_{96} + 17*z^{220}_{95} + 21*z^{220}_{94} + 13*z^{220}_{93} \\
& + 24*z^{220}_{92} + 36*z^{220}_{91} + 25*z^{220}_{90} + 25*z^{220}_{89} \\
& + 22*z^{220}_{88} + 27*z^{220}_{87} + 28*z^{220}_{86} + 11*z^{220}_{85} \\
& + 3*z^{220}_{84} + 14*z^{220}_{82} + 31*z^{220}_{81} + 7*z^{220}_{80} \\
& + 33*z^{220}_{79} + 33*z^{220}_{78} + 2*z^{220}_{77} + 15*z^{220}_{76} \\
& + 17*z^{220}_{75} + 32*z^{220}_{74} + 4*z^{220}_{73} + 18*z^{220}_{72} \\
& + 10*z^{220}_{71} + 34*z^{220}_{70} + 9*z^{220}_{69} + 3*z^{220}_{68} \\
& + 20*z^{220}_{67} + 33*z^{220}_{66} + 23*z^{220}_{65} + 5*z^{220}_{64} \\
& + 20*z^{220}_{63} + 36*z^{220}_{62} + 29*z^{220}_{61} + 2*z^{220}_{60} \\
& + 25*z^{220}_{59} + 14*z^{220}_{58} + 16*z^{220}_{57} + 31*z^{220}_{56} \\
& + 22*z^{220}_{55} + 31*z^{220}_{54} + 33*z^{220}_{53} + 19*z^{220}_{52} \\
& + 22*z^{220}_{51} + 23*z^{220}_{50} + 36*z^{220}_{49} + 11*z^{220}_{48} \\
& + 15*z^{220}_{47} + 15*z^{220}_{46} + 35*z^{220}_{45} + 7*z^{220}_{44} \\
& + 27*z^{220}_{43} + 28*z^{220}_{42} + 15*z^{220}_{41} + 31*z^{220}_{40} \\
& + 12*z^{220}_{39} + 19*z^{220}_{38} + 21*z^{220}_{37} + 18*z^{220}_{36} \\
& + 3*z^{220}_{35} + 36*z^{220}_{33} + z^{220}_{32} + 35*z^{220}_{31} \\
& + 21*z^{220}_{30} + 2*z^{220}_{29} + 13*z^{220}_{28} + 19*z^{220}_{27} \\
& + 6*z^{220}_{26} + 22*z^{220}_{24} + 26*z^{220}_{23} + 9*z^{220}_{22} \\
& + 7*z^{220}_{21} + 31*z^{220}_{20} + 31*z^{220}_{19} + 9*z^{220}_{18} \\
& + 23*z^{220}_{17} + 23*z^{220}_{16} + 6*z^{220}_{15} + 27*z^{220}_{14} \\
& + 36*z^{220}_{13} + 4*z^{220}_{12} + 26*z^{220}_{11} + 30*z^{220}_{10} \\
& + 9*z^{220}_9 + 8*z^{220}_8 + 15*z^{220}_7 + 26*z^{220}_6 \\
& + 17*z^{220}_5 + 29*z^{220}_4 + 24*z^{220}_3 + 8*z^{220}_2 \\
& + 29*z^{220}_1 : 1)
\end{aligned}$$

Q_3 is given by

$$\begin{aligned}
& (35*z^{220}_{219} + 22*z^{220}_{218} + 36*z^{220}_{216} + 24*z^{220}_{215} \\
& + 19*z^{220}_{214} + 32*z^{220}_{213} + 13*z^{220}_{212} + 19*z^{220}_{211} \\
& + 3*z^{220}_{210} + 36*z^{220}_{209} + 29*z^{220}_{208} + 35*z^{220}_{206} \\
& + 31*z^{220}_{205} + 32*z^{220}_{204} + 23*z^{220}_{203} + 21*z^{220}_{202} \\
& + 10*z^{220}_{201} + 32*z^{220}_{200} + 32*z^{220}_{199} + 21*z^{220}_{198}
\end{aligned}$$

$$\begin{aligned}
& + 16*z^{220}_{197} + 23*z^{220}_{196} + 32*z^{220}_{195} + 12*z^{220}_{194} \\
& + 9*z^{220}_{193} + 35*z^{220}_{192} + 8*z^{220}_{191} + 19*z^{220}_{190} \\
& + 33*z^{220}_{189} + 13*z^{220}_{188} + 11*z^{220}_{187} + 35*z^{220}_{186} \\
& + 25*z^{220}_{185} + 28*z^{220}_{184} + 5*z^{220}_{183} + 7*z^{220}_{182} \\
& + 24*z^{220}_{181} + 35*z^{220}_{180} + 33*z^{220}_{179} + 18*z^{220}_{178} \\
& + 5*z^{220}_{177} + 31*z^{220}_{176} + 18*z^{220}_{175} + 30*z^{220}_{174} \\
& + 27*z^{220}_{173} + 3*z^{220}_{172} + 8*z^{220}_{171} + 24*z^{220}_{170} \\
& + 14*z^{220}_{169} + 2*z^{220}_{168} + 16*z^{220}_{167} + 14*z^{220}_{166} \\
& + 18*z^{220}_{165} + 22*z^{220}_{164} + 32*z^{220}_{163} + 28*z^{220}_{162} \\
& + 7*z^{220}_{161} + 19*z^{220}_{160} + 3*z^{220}_{159} + 14*z^{220}_{158} \\
& + 27*z^{220}_{157} + 35*z^{220}_{156} + 8*z^{220}_{155} + 25*z^{220}_{154} \\
& + 11*z^{220}_{153} + 19*z^{220}_{152} + 21*z^{220}_{151} + 10*z^{220}_{150} \\
& + 2*z^{220}_{149} + 4*z^{220}_{148} + 4*z^{220}_{147} + 31*z^{220}_{146} \\
& + 26*z^{220}_{145} + 17*z^{220}_{143} + 14*z^{220}_{142} + 12*z^{220}_{141} \\
& + 17*z^{220}_{140} + 22*z^{220}_{139} + 30*z^{220}_{138} + 30*z^{220}_{137} \\
& + 15*z^{220}_{136} + 16*z^{220}_{135} + 25*z^{220}_{134} + 8*z^{220}_{133} \\
& + 28*z^{220}_{132} + 5*z^{220}_{131} + 14*z^{220}_{130} + 26*z^{220}_{129} \\
& + 13*z^{220}_{128} + 10*z^{220}_{127} + 13*z^{220}_{126} + 10*z^{220}_{125} \\
& + 17*z^{220}_{124} + 33*z^{220}_{123} + 9*z^{220}_{122} + 9*z^{220}_{121} \\
& + 10*z^{220}_{120} + 12*z^{220}_{119} + 4*z^{220}_{118} + 6*z^{220}_{117} \\
& + 33*z^{220}_{116} + 21*z^{220}_{115} + 14*z^{220}_{114} + 33*z^{220}_{113} \\
& + 11*z^{220}_{112} + 4*z^{220}_{111} + 3*z^{220}_{110} + 3*z^{220}_{109} \\
& + 3*z^{220}_{108} + 3*z^{220}_{107} + 27*z^{220}_{106} + 8*z^{220}_{105} \\
& + 25*z^{220}_{104} + 10*z^{220}_{103} + 24*z^{220}_{102} + 2*z^{220}_{101} \\
& + 12*z^{220}_{100} + 35*z^{220}_{99} + 30*z^{220}_{98} + 14*z^{220}_{97} \\
& + 8*z^{220}_{96} + 16*z^{220}_{95} + 24*z^{220}_{94} + 23*z^{220}_{93} \\
& + 34*z^{220}_{91} + 3*z^{220}_{90} + 13*z^{220}_{89} + 10*z^{220}_{88} \\
& + 20*z^{220}_{87} + 14*z^{220}_{86} + 9*z^{220}_{85} + 36*z^{220}_{84} \\
& + 33*z^{220}_{83} + 12*z^{220}_{82} + 20*z^{220}_{81} + 5*z^{220}_{80} \\
& + 27*z^{220}_{79} + 27*z^{220}_{78} + 9*z^{220}_{77} + 23*z^{220}_{76} \\
& + 4*z^{220}_{75} + 26*z^{220}_{74} + 8*z^{220}_{73} + 11*z^{220}_{72} \\
& + 25*z^{220}_{71} + 35*z^{220}_{70} + 19*z^{220}_{69} + 36*z^{220}_{68} \\
& + 35*z^{220}_{67} + 24*z^{220}_{66} + 8*z^{220}_{65} + 32*z^{220}_{64} \\
& + 10*z^{220}_{63} + 3*z^{220}_{62} + 18*z^{220}_{61} + 35*z^{220}_{60} \\
& + 17*z^{220}_{59} + 30*z^{220}_{58} + 2*z^{220}_{57} + 25*z^{220}_{56} \\
& + 7*z^{220}_{55} + 20*z^{220}_{54} + 27*z^{220}_{53} + z^{220}_{52} \\
& + 10*z^{220}_{51} + 2*z^{220}_{50} + 18*z^{220}_{49} + 30*z^{220}_{48} \\
& + 32*z^{220}_{47} + 20*z^{220}_{46} + 4*z^{220}_{45} + 16*z^{220}_{43} \\
& + 16*z^{220}_{42} + 11*z^{220}_{41} + 8*z^{220}_{40} + 12*z^{220}_{39} \\
& + 15*z^{220}_{38} + 25*z^{220}_{37} + 33*z^{220}_{36} + 4*z^{220}_{35} \\
& + 11*z^{220}_{34} + 6*z^{220}_{33} + 7*z^{220}_{32} + 32*z^{220}_{31} \\
& + 19*z^{220}_{30} + 19*z^{220}_{29} + 16*z^{220}_{28} + 10*z^{220}_{27} \\
& + 7*z^{220}_{26} + 10*z^{220}_{25} + 33*z^{220}_{24} + 25*z^{220}_{23}
\end{aligned}$$

$$\begin{aligned}
& + 21*z^{220^22} + 35*z^{220^21} + 15*z^{220^20} + z^{220^19} \\
& + 19*z^{220^18} + 16*z^{220^17} + 10*z^{220^16} + 18*z^{220^15} \\
& + 17*z^{220^14} + 2*z^{220^13} + 35*z^{220^12} + 30*z^{220^11} \\
& + 17*z^{220^10} + 30*z^{220^9} + 26*z^{220^8} + 9*z^{220^7} \\
& + 34*z^{220^6} + 4*z^{220^5} + 12*z^{220^4} + 16*z^{220^3} \\
& + 27*z^{220^2} + 12*z^{220} + 36 \\
& : 21*z^{220^219} + 24*z^{220^218} \\
& + 33*z^{220^217} + 31*z^{220^216} + 29*z^{220^215} + 16*z^{220^214} \\
& + 26*z^{220^213} + 7*z^{220^212} + 15*z^{220^211} + 9*z^{220^210} \\
& + 19*z^{220^209} + 18*z^{220^208} + 16*z^{220^207} + 23*z^{220^206} \\
& + 27*z^{220^205} + 16*z^{220^204} + 5*z^{220^203} + 10*z^{220^202} \\
& + 2*z^{220^201} + 19*z^{220^200} + 19*z^{220^199} + 8*z^{220^198} \\
& + 30*z^{220^197} + 9*z^{220^196} + 27*z^{220^195} + 7*z^{220^194} \\
& + 20*z^{220^193} + 8*z^{220^192} + 29*z^{220^191} + 10*z^{220^190} \\
& + 32*z^{220^189} + 9*z^{220^188} + 4*z^{220^187} + 31*z^{220^186} \\
& + 8*z^{220^185} + 4*z^{220^184} + 8*z^{220^183} + 11*z^{220^182} \\
& + 13*z^{220^181} + 5*z^{220^180} + 29*z^{220^179} + 13*z^{220^178} \\
& + 20*z^{220^177} + 9*z^{220^176} + 3*z^{220^175} + 32*z^{220^174} \\
& + 3*z^{220^173} + 25*z^{220^172} + 33*z^{220^171} + 36*z^{220^170} \\
& + 11*z^{220^169} + 22*z^{220^168} + 18*z^{220^167} + 7*z^{220^166} \\
& + 4*z^{220^165} + 9*z^{220^164} + 33*z^{220^163} + 33*z^{220^162} \\
& + 18*z^{220^161} + 3*z^{220^160} + 35*z^{220^159} + 31*z^{220^158} \\
& + 20*z^{220^157} + 28*z^{220^155} + 33*z^{220^154} + 30*z^{220^153} \\
& + 28*z^{220^152} + 18*z^{220^151} + z^{220^150} + 34*z^{220^149} \\
& + 16*z^{220^148} + 23*z^{220^147} + 30*z^{220^146} + 3*z^{220^144} \\
& + 28*z^{220^143} + 8*z^{220^142} + 35*z^{220^140} + 11*z^{220^139} \\
& + 16*z^{220^138} + 20*z^{220^137} + 31*z^{220^136} + 11*z^{220^135} \\
& + 24*z^{220^134} + 29*z^{220^133} + 29*z^{220^132} + 8*z^{220^131} \\
& + 25*z^{220^130} + 11*z^{220^129} + 35*z^{220^128} + 36*z^{220^127} \\
& + 33*z^{220^126} + 18*z^{220^125} + 8*z^{220^124} + 9*z^{220^123} \\
& + 31*z^{220^122} + 29*z^{220^121} + 7*z^{220^120} + 4*z^{220^119} \\
& + 3*z^{220^118} + 13*z^{220^117} + 35*z^{220^116} + 17*z^{220^115} \\
& + 6*z^{220^114} + 3*z^{220^113} + 13*z^{220^112} + 5*z^{220^111} \\
& + 31*z^{220^110} + 32*z^{220^109} + 17*z^{220^108} + 28*z^{220^107} \\
& + 21*z^{220^106} + 14*z^{220^105} + 25*z^{220^104} + 17*z^{220^103} \\
& + 33*z^{220^102} + 19*z^{220^101} + 4*z^{220^100} + 2*z^{220^99} \\
& + 7*z^{220^98} + 34*z^{220^97} + 15*z^{220^96} + 7*z^{220^95} \\
& + 34*z^{220^94} + 22*z^{220^93} + 22*z^{220^92} + 11*z^{220^91} \\
& + 33*z^{220^90} + 32*z^{220^89} + 19*z^{220^88} + 21*z^{220^87} \\
& + 23*z^{220^86} + 34*z^{220^85} + 35*z^{220^84} + 23*z^{220^83} \\
& + 27*z^{220^82} + 25*z^{220^81} + 26*z^{220^80} + 2*z^{220^79} \\
& + 33*z^{220^78} + 32*z^{220^77} + 8*z^{220^76} + 32*z^{220^75}
\end{aligned}$$

$$\begin{aligned}
& + 15*z^{220^74} + 17*z^{220^73} + 31*z^{220^72} + 7*z^{220^71} \\
& + 8*z^{220^70} + 8*z^{220^69} + 22*z^{220^68} + 7*z^{220^67} \\
& + 14*z^{220^66} + 15*z^{220^65} + 26*z^{220^64} + 26*z^{220^63} \\
& + 35*z^{220^62} + 19*z^{220^61} + 18*z^{220^60} + 22*z^{220^59} \\
& + 25*z^{220^57} + 4*z^{220^56} + 5*z^{220^55} + 4*z^{220^54} \\
& + 20*z^{220^53} + 32*z^{220^52} + 17*z^{220^51} + 14*z^{220^50} \\
& + 31*z^{220^49} + 9*z^{220^48} + 30*z^{220^47} + 20*z^{220^46} \\
& + 7*z^{220^45} + 16*z^{220^43} + 23*z^{220^42} + 12*z^{220^41} \\
& + 21*z^{220^40} + 14*z^{220^39} + 8*z^{220^38} + 14*z^{220^37} \\
& + 35*z^{220^36} + 14*z^{220^35} + 22*z^{220^34} + 8*z^{220^33} \\
& + z^{220^32} + 24*z^{220^31} + 21*z^{220^30} + 33*z^{220^29} \\
& + 21*z^{220^28} + 22*z^{220^26} + 33*z^{220^25} + 13*z^{220^24} \\
& + 13*z^{220^23} + 5*z^{220^22} + 35*z^{220^21} + 3*z^{220^20} \\
& + 31*z^{220^19} + 13*z^{220^18} + 33*z^{220^17} + 30*z^{220^16} \\
& + 16*z^{220^15} + 30*z^{220^14} + 16*z^{220^13} + 11*z^{220^12} \\
& + 35*z^{220^11} + 22*z^{220^10} + 11*z^{220^9} + 8*z^{220^8} \\
& + z^{220^7} + 25*z^{220^6} + 8*z^{220^5} + 27*z^{220^4} + z^{220^3} \\
& + 29*z^{220^2} + 34*z^{220} + 29 : 1)
\end{aligned}$$