LP-307: Quantum Consensus Protocol

Eisenstein Series and Amplitude Amplification for Distributed Agreement

Zach Kelling

Lux Industries

Original: May 2023 | Revised: March 2026

Abstract

We introduce the Quantum Consensus Protocol (QCP), an approach to distributed agreement that leverages quantum computation and the analytic structure of Eisenstein series. The protocol encodes lattice summations as quantum superpositions, performs series evaluation via state interference, and adjusts computational difficulty through Grover-style amplitude amplification. We derive convergence bounds for truncated Eisenstein series in the quantum setting and analyze the resulting consensus properties.

This paper records a 2023 research direction. Section 7 maps QCP's ideas to the production Quasar consensus protocol (LP-020), distinguishing what was adopted from what remained theoretical.

Contents

1 Introduction

1.1 Background

Classical consensus protocols—PBFT, Tendermint, HotStuff, Avalanche—operate entirely within the computational model of classical Turing machines. Their security guarantees (BFT tolerance of $f < n/3$, liveness under partial synchrony) are well understood. However, as quantum computing hardware approaches fault-tolerant scale, two questions arise:

1. Can quantum computational primitives *improve* consensus performance (latency, throughput, or fault tolerance)?
2. Can a consensus protocol be designed such that its difficulty adjustment is itself a quantum computation, enabling the network to exploit quantum resources when available?

The Quantum Consensus Protocol addresses both questions by using Eisenstein series—objects from analytic number theory with natural lattice structure—as the computational kernel of the consensus mechanism.

1.2 Goals

- A consensus protocol whose verification is classically efficient but whose optimal *proposal* computation benefits from quantum speedup.
- Difficulty adjustment via amplitude amplification (Grover's algorithm [1]), providing quadratic speedup for parameter search.
- Convergence guarantees derived from the analytic properties of Eisenstein series.

2 Eisenstein Series and Quantum Computation

2.1 Overview of Eisenstein Series

Eisenstein series are fundamental objects in the theory of modular forms. For a complex variable z in the upper half-plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ and an even integer weight $k \geq 4$, the Eisenstein series is:

$$G_k(z) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\neq(0,0)}} \frac{1}{(cz+d)^k} \tag{1}$$

The sum ranges over the integer lattice $\mathbb{Z}^2$ excluding the origin. The series converges absolutely for $\mathrm{Re}(k) > 2$ and transforms as a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$:

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k\, G_k(z), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

In the context of this work, we consider Eisenstein series associated to cusps of the Hilbert–Blumenthal modular group, which provide additional structure for multi-dimensional lattice summations.

2.2 Quantum Representation of Complex Numbers

To evaluate Eisenstein series on a quantum computer, we must encode complex arithmetic in the qubit model. Let $z = a + bi$ where $a, b \in \mathbb{R}$. We use a fixed-point representation with p bits of precision for each component:

Definition 2.1 (Quantum Complex Register)**.** *A quantum complex number on $2p$ qubits is a state $|z\rangle = |a_1 a_2 \ldots a_p\rangle \otimes |b_1 b_2 \ldots b_p\rangle$ where $a_i, b_i \in \{0,1\}$ encode the fixed-point binary representations of $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$.*

Arithmetic operations (addition, multiplication, reciprocal) on quantum complex registers require $O(p \log p)$ gates via quantum Fourier transform techniques [2]. The key operation for Eisenstein evaluation is the computation of $(cz + d)^{-k}$, which decomposes into:

1. Multiply: $w \leftarrow cz + d$ $\quad (O(p \log p)$ gates)
2. Power: w^k via repeated squaring $\quad (O(k \cdot p \log p)$ gates)
3. Invert: w^{-k} via Newton iteration $\quad (O(p^2)$ gates)

2.3 Quantum State Construction

Each term (c, d) in the Eisenstein series is represented by a computational basis state $|c, d\rangle$ with c, d encoded as signed integers on ℓ qubits each. We prepare the uniform superposition over a truncated lattice $\Lambda_N = \{(c, d) \in \mathbb{Z}^2 : |c|, |d| \leq N, (c, d) \neq (0, 0)\}$:

$$|\Psi_0\rangle = \frac{1}{\sqrt{|\Lambda_N|}} \sum_{(c,d)\in\Lambda_N} |c, d\rangle \otimes |0\rangle \tag{2}$$

where $|\Lambda_N| = (2N+1)^2 - 1$. This superposition is prepared in $O(\ell)$ Hadamard gates followed by a single ancilla-controlled rejection of the $(0, 0)$ state.

2.4 Quantum Summation via State Interference

The core of the algorithm applies a unitary U_z that computes the term value in an ancilla register:

$$U_z \, |c, d\rangle \, |0\rangle = |c, d\rangle \, |(cz + d)^{-k}\rangle$$

The Eisenstein sum is then encoded in the amplitude of a target state. Define the projection operator P_{sum} that extracts the sum of ancilla values. By linearity of quantum mechanics:

$$U_z \, |\Psi_0\rangle = \frac{1}{\sqrt{|\Lambda_N|}} \sum_{(c,d)\in\Lambda_N} |c, d\rangle \, |(cz + d)^{-k}\rangle \tag{3}$$

The sum $\tilde{G}_k^{(N)}(z) = \sum_{(c,d)\in\Lambda_N} (cz + d)^{-k}$ is not directly observable as an amplitude (amplitudes are normalized), but it can be estimated via quantum phase estimation on a controlled-U_z circuit. The estimation requires $O(\sqrt{|\Lambda_N|}/\epsilon)$ queries for additive error ϵ, a quadratic improvement over classical summation.

3 Convergence Bounds for Truncated Eisenstein Series

3.1 Classical Truncation Error

The tail of the Eisenstein series satisfies a standard bound:

Theorem 3.1 (Truncation Bound)**.** *For $k \geq 4$ and $z \in \mathcal{H}$ with $\operatorname{Im}(z) \geq \delta > 0$:*

$$\left| G_k(z) - \tilde{G}_k^{(N)}(z) \right| \leq C_k \cdot \delta^{-k} \cdot N^{2-k}$$

where $C_k = 4\zeta(k-1)$ and ζ is the Riemann zeta function.

Proof sketch. For fixed $c \neq 0$, the standard lattice-point counting bound gives $\sum_{d\in\mathbb{Z}} |cz+d|^{-k} = O\big(|c \operatorname{Im}(z)|^{1-k}\big)$ (see Zagier [3], Section 1.5). Summing over $|c| > N$ and applying the integral comparison $\sum_{|c|>N} |c|^{1-k} = O(N^{2-k})$ yields the claimed $O(\delta^{-k} N^{2-k})$ bound, with constant factor $C_k = 4\zeta(k-1)$ from the inner $|c|$ summation. Full derivation in [3], Theorem 4.2. □

3.2 Quantum Estimation Error

Combining the truncation bound with quantum phase estimation error ϵ_{QPE}, the total error for the quantum evaluation of $G_k(z)$ is:

$$\left| G_k(z) - \hat{G}_k^{(N)}(z) \right| \leq C_k \delta^{-k} N^{2-k} + \epsilon_{\text{QPE}} \tag{4}$$

To achieve total error ϵ, set $N = \Theta((\epsilon \delta^k)^{1/(k-2)})$ and $\epsilon_{\text{QPE}} = \epsilon/2$. The quantum circuit depth is $O(N^2 \cdot k \cdot p \log p / \epsilon)$.

4 Difficulty Adjustment via Amplitude Amplification

4.1 The Difficulty Search Problem

In the consensus protocol, each proposer must find a truncation parameter N^* and evaluation point z^* such that the computed Eisenstein value $\tilde{G}_k^{(N^*)}(z^*)$ satisfies a difficulty target τ:

$$\left| \tilde{G}_k^{(N^*)}(z^*) - \tau \right| < \Delta$$

where Δ is the difficulty window. Classically, searching over M candidate pairs (N, z) requires $O(M)$ evaluations.

4.2 Grover-Accelerated Search

Amplitude amplification (Grover's algorithm [1]) provides a quadratic speedup. Define the oracle $O_\tau : |N, z\rangle |b\rangle \to |N, z\rangle |b \oplus f(N, z)\rangle$ where $f(N, z) = 1$ iff $|\tilde{G}_k^{(N)}(z) - \tau| < \Delta$.

Proposition 4.1 (Difficulty Search Complexity)**.** *Given M candidate parameter pairs with t satisfying solutions, the quantum difficulty search finds a valid (N^*, z^*) in $O(\sqrt{M/t})$ oracle queries, each requiring one Eisenstein evaluation circuit.*

The protocol dynamically adjusts the difficulty window Δ based on block production rate, analogous to Bitcoin's difficulty retargeting but with the search itself benefiting from quantum speedup.

4.3 Classical Verification

A critical property: while *finding* a valid (N^*, z^*) benefits from quantum speedup, *verifying* a proposed solution requires only a single classical Eisenstein evaluation. This asymmetry ensures that quantum-equipped proposers gain an advantage in block production without preventing classical nodes from validating the chain.

5 Consensus Protocol Design

5.1 Protocol Overview

The Quantum Consensus Protocol operates in rounds. Each round:

1. The network publishes a difficulty target τ_r and window Δ_r derived from the previous w rounds.
2. Each proposer searches for (N^*, z^*) satisfying the difficulty condition.
3. The first valid proposal is broadcast with a proof $(N^*, z^*, \tilde{G}_k^{(N^*)}(z^*))$.
4. Validators verify the proof classically and vote.
5. After $\geq 2n/3 + 1$ votes, the round finalizes.

5.2 Security Properties

- **Safety**: Follows from the BFT voting threshold. No two conflicting proposals can both receive $> 2n/3$ votes.
- **Liveness**: Guaranteed as long as $> 2n/3$ validators are honest and at least one proposer can evaluate the Eisenstein oracle (classically or quantum).
- **Quantum advantage**: Proposers with quantum hardware find valid parameters in $O(\sqrt{M/t})$ vs $O(M/t)$ time, but cannot forge proofs or bypass the voting threshold.

5.3 Economic Considerations

The protocol creates a natural market for quantum computing resources: validators who invest in quantum hardware produce blocks faster, earning proportionally more rewards. As quantum hardware commoditizes, the difficulty window narrows, maintaining target block times. This is analogous to the ASIC arms race in proof-of-work, but with the important difference that quantum advantage is bounded (quadratic, not exponential) and verification remains classical.

6 Implementation Considerations

6.1 Scalability

The quantum circuit for a single Eisenstein evaluation at precision p with truncation N requires $O(N^2 \cdot k \cdot p \log p)$ gates. For practical parameters ($k = 4$, $p = 32$, $N = 64$), this is approximately 10^7 gates—within reach of early fault-tolerant quantum computers but beyond current NISQ devices.

6.2 Security Against Quantum Adversaries

The protocol's BFT security does not depend on quantum hardness assumptions. Even an adversary with an arbitrarily powerful quantum computer cannot violate safety (which requires $> n/3$ corrupt validators) or forge Eisenstein evaluations (which are deterministic given the inputs). The quantum advantage is limited to the *speed* of finding valid proposals.

6.3 Classical Fallback

Every round can be completed by classical proposers, albeit more slowly. The protocol degrades gracefully: if no quantum proposer participates, block times increase by at most a factor of $\sqrt{M/t}$, and the difficulty adjustment compensates within w rounds.

7 2026 Status: Mapping QCP to Quasar

The Quantum Consensus Protocol was a 2023 research exploration. The production consensus protocol for Lux Network is Quasar (LP-020), which incorporates several QCP ideas while departing from others.

7.1 What Was Adopted

- **Lattice-based cryptographic foundation**: Quasar uses Pulsar lattice signatures alongside BLS-381, providing post-quantum security at the consensus layer. The lattice hardness assumptions (SVP, LWE) that underpin QCP's Eisenstein approach also underpin Pulsar.
- **Classical verification of quantum-hard problems**: Quasar maintains the asymmetry principle—consensus proofs are classically verifiable even though the underlying cryptographic assumptions are quantum-resistant.

- **Leaderless architecture**: QCP's model where any proposer can submit a valid proof influenced Quasar's leaderless design, where all validators participate symmetrically.
- **Difficulty as a protocol parameter**: The concept of network-adaptive difficulty evolved into Quasar's dynamic validator weighting based on stake and performance.

7.2 What Remained Theoretical

- **Eisenstein series as consensus kernel**: The specific use of modular forms for difficulty proofs was not adopted. Quasar uses BLS aggregate signatures and ML-DSA for consensus votes—simpler, well-audited, and no quantum hardware needed.
- **Quantum proposal advantage**: Quasar does not give quantum-equipped validators any advantage. All validators participate equally. The economic incentive model is stake-based, not computation-based.
- **Amplitude amplification for parameter search**: Without a computation-based proof requirement, Grover search has no role in Quasar.
- **Quantum circuit implementation**: No quantum hardware dependency exists in the production protocol. Quasar runs on classical hardware with post-quantum cryptographic primitives (ML-DSA-65, Pulsar, ML-KEM-768).

7.3 Assessment

QCP demonstrated that quantum computational structure (specifically, the analytic properties of Eisenstein series over lattices) could in principle be harnessed for consensus. The convergence bounds (Theorem 3.1) and the difficulty search framework remain mathematically sound. However, the practical path to post-quantum consensus turned out to be simpler: use post-quantum *signatures* on a classical consensus protocol, rather than building a consensus protocol that requires quantum *computation*.

Quasar achieves the same security goals—BFT safety, sub-second finality, post-quantum resistance—without requiring quantum hardware, which is the correct engineering tradeoff for a production network in 2026.

8 Conclusion

The Quantum Consensus Protocol establishes that Eisenstein series provide a mathematically rich structure for consensus proof construction, with provable convergence bounds and natural difficulty adjustment via amplitude amplification. The asymmetry between quantum-accelerated proposal and classical verification is a desirable property for any computation-based consensus mechanism.

The production Lux Network adopted QCP's philosophical commitments— lattice-based security, leaderless architecture, classical verifiability—while choosing a more conservative implementation path in Quasar. The Eisenstein approach remains a valid research direction for future consensus protocols that can assume ubiquitous quantum hardware.

References

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," *STOC*, pp. 212–219, 1996.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Ed., Cambridge University Press, 2010.

[3] D. Zagier, "Elliptic Modular Forms and Their Applications," in *The 1-2-3 of Modular Forms*, Springer, pp. 1–103, 2008.

[4] T. Miyake, *Modular Forms*, Springer-Verlag, 1989.

[5] Z. Kelling, "LP-020: Quasar—Hybrid BLS + Lattice Consensus for Post-Quantum Finality," Lux Industries, 2026.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[7] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemporary Mathematics*, vol. 305, pp. 53–74, 2002.