Chapter 6: Number Theory for Factoring

This section is already in the book plan, but it has not been written fully yet. The book owner can press Generate section to write this part with the language model connected to TheoryTrace.

Section plan:

Introduces divisibility, modular arithmetic, greatest common divisors, Euclid's algorithm, congruences, modular inverses, Euler's theorem, Fermat's little theorem, and multiplicative order. These tools prepare the reader to understand how factoring reduces to period finding.

References

References will be added when this section is generated.

Document information

Chapter 6: Number Theory for Factoring

Project	Shor's Algorithm from First Principles
Document	Document 1.10
Author	mujirin
Verifier	Not verified
Downloaded	July 04, 2026 19:17 KST
Status	Working
Document link	https://www.theorytrace.com/projects/shors-algorithm-from-first-principles/documents/-chapter-6-number-theory-for-factoring/