SOAR into Mathematics—Number Theory
July 24–August 11, 2000
List of Topics (Tentative)

1. *Foundations of Number Theory*

   properties of the integers; divisibility; the Division Algorithm

2. *Greatest Common Divisors*

   greatest common divisors; coprimality; the Diophantine equation $ax + by = 1$; the Euclidean Algorithm; irrationality of $\sqrt{2}$; a geometric detour

3. *Prime Numbers*

   primes; the Fundamental Theorem of Arithmetic; Euclid and the infinitude of primes

4. *Modular Arithmetic*

   congruences; modular arithmetic; congruences and division; solving linear congruences

5. *The Multiplicative Group*

   special properties of arithmetic modulo primes; the Chinese remainder theorem

6. *The Multiplicative Group Modulo n*

   the Euler ϕ-function; Fermat's Little Theorem; multiplicative order; primitive roots; solving radical congruences

7. *Factoring Integers*

   trial division; shortcuts for small primes; Fermat's differences-of-squares method; primality tests; advanced algorithms

8. *Egyptian Fractions*

   the Rhind papyrus; algorithms for Egyptian fraction expansion; the splitting formula; largest and second-largest denominators; contemporary research

9. *Cryptography*

   Diffie–Hellman public key exchange; public-key cryptography; the RSA cryptosystem

10. *Survey of Additive Number Theory*

    sums of two squares; Lagrange's four-squares theorem; representation by three squares; Waring's problem; Twin Primes and Goldbach conjectures

Greg Martin and Emmanuel Knafo
Department of Mathematics
University of Toronto