Teoría de números

Sugerencia de programa 2012

Números primos (Dos semanas)

1. División entera, algoritmo de Euclides, factorización única
2. Infinitud de los números primos

Congruencias (Dos semanas)

1. Ecuaciones lineales
2. Teoremas de Fermat y de Euler
3. Teorema chino de los restos
4. Cálculo de inversos y potencias, raíces primitivas

Criptografía de clave pública (Dos semanas)

1. Intercambio de clave Diffie-Hellman, criptosistema RSA
2. Ataques al RSA y factorización

Reciprocidad cuadrática (Tres semanas)

1. Residuos cuadráticos, criterio de Euler,
2. Demostración de la ley
3. Sumas de Gauss, otra demostración
4. Cálculo de raíces módulo p

Fracciones continuas (Dos semanas)

1. Fracciones continuas finitas, convergencia de fracciones continuas infinitas
2. Irracionales cuadráticos y fracciones continuas periódicas
3. Reconocimiento de racionales

Formas cuadráticas (Dos semanas)

1. Sumas de dos cuadrados, algunos teoremas de Fermat
2. Representación de números por formas cuadráticas
3. Clases de formas cuadráticas, reducción
4. Representación por discriminante y número de clases 1.

Curvas elípticas y criptografía (Dos semanas)

1. Definición, ley de grupo geométrica
2. Factorización usando curvas elípticas
3. Criptografía usando curvas elípticas, ElGamal, problema del logaritmo discreto

Bibliografía

[1] Stein, W. *Elementary Number Theory: Primes, Congruences, and Secrets.* Springer, Undergraduate texts in mathematics, 2009.