

COSC413 Tutorials on Number Theoretic Algorithms

(1) Prove that $\equiv \pmod{m}$ is an equivalence relation.

(2) Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

$$(a) a \pm c \equiv b \pm d \pmod{m} \quad (b) a \cdot c \equiv b \cdot d \pmod{m}$$

(3) Make the addition and multiplication table for Z_7 .

(4) Make the multiplication table for Z_{15}^* .

(5) List up all primitive roots of 7, 10 and 13.

(6) Let H be a subgroup of G . Prove that congruence modulo is an equivalence relation.

(7) Prove that $|H| = |Ha|$.

(8) Check Fermat's theorem for a such that $\gcd(a, m) = 1$ for $m=9$ and several a 's.

(9) For primes p and q , prove $\varphi(pq) = (p-1)(q-1)$.

(10) Solve the recurrence equation (difference equation)

$$y(0) = 0, y(1) = 4,$$

$$y(n+2) = 4y(n+1) - y(n) \quad (n \geq 0)$$

Check the result for $y(3)$ by the recurrence and expanding the solution.

(11) Trace the Euclidean algorithm to compute $7^{-1} \pmod{13}$.

(12) Prove that if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, and $\gcd(m, n) = 1$, $a \equiv b \pmod{mn}$. You can assume all are positive integers.

(13) Prove that if $a \equiv b \pmod{m}$,

$$a \text{ is a quadratic residue mod } m \Leftrightarrow b \text{ is a quadratic residue mod } m.$$

(14) Prove that if c is a solution for $x^2 \equiv a \pmod{m}$, d such that $d \equiv c \pmod{m}$ is also a solution.

(15) Check Solovay and Strassen's algorithm for $n = 9$ with all a such that $\gcd(a, n) = 1$ and $0 < a < n$.

(16) Draw the data flow graph for FFT with $n = 16$.

(17) Do some computational experiments on the Chinese Remaindering Theorem with $m_1=7$, $m_2=11$ and $m_3=13$.