

Tutorial 4

1. Solve the following system of simultaneous congruences.

$$3x \equiv 1 \pmod{7}$$

$$2x \equiv 10 \pmod{16}$$

$$5x \equiv 1 \pmod{18}$$

2. Find the residue of 2^{2009} modulo 385.

3. Let a, k, m be integers. Prove that $\gcd(ka, km) = k \gcd(a, m)$.

4. Let $m = pq$, where p and q are distinct primes, and let $S = \{0, 1, \dots, m-1\}$. For each divisor d of m let N_d be the number of $a \in S$ such that $\gcd(a, m) = d$.

(i) Use Question 3 to show that $N_p = q - 1$ and $N_q = p - 1$,

(ii) What is the value of N_m ?

(iii) Use the results of (i) and (ii) to show that the value of $\phi(m)$ is given by $\phi(m) = pq - (p - 1) - (q - 1) - 1 = (p - 1)(q - 1)$.

5. Let $m = pqr$, where p, q and r are distinct primes, let $S = \{0, 1, \dots, m-1\}$, and for each divisor d of m let N_d be the number of $a \in S$ such that $\gcd(a, m) = d$. Use Questions 3 and 4 to find $N_p, N_q, N_r, N_{pq}, N_{pr}$ and N_{qr} , and write down also the value of N_m . Hence find the number of elements of the set $\{d \in S \mid \gcd(a, m) \in \{p, q, r, pq, pr, qr, pqr\}\}$, and use your answer to show that $\phi(m) = (p - 1)(q - 1)(r - 1)$. MATH2988: Generalize this method to find $\phi(m)$ whenever m is a product of distinct primes.

6. (i) Use Question 5 to find $\phi(273)$.

(ii) Use the Euler-Fermat Theorem and Part (i) to find the remainder when 4^{291} is divided by 273.

- *7. Define s_i via the recurrence $s_i = 4s_{i-1} - s_{i-2}$, subject to the initial values $s_0 = 2$ and $s_1 = 4$. Find a closed formula for s_i . (It has the form $s_i = \lambda a^i + \mu b^i$, where a^i and b^i satisfy the same recurrence as s_i .) Then show that the integers r_i appearing in the Lucas-Lehmer test (see Q6 of Computer Tutorial 5) are related to the s_i via $r_i \equiv s_{2^i}$. Show also that if r is prime then $s_r \equiv 4 \pmod{r}$.