

Tutorial 4

1. Solve the following system of simultaneous congruences.

$$\begin{aligned} 3x &\equiv 1 \pmod{7} \\ 2x &\equiv 10 \pmod{16} \\ 5x &\equiv 1 \pmod{18} \end{aligned}$$

Solution.

The congruence $3x \equiv 1 \pmod{7}$ is equivalent to $3x \equiv -6 \pmod{7}$, or $x \equiv -2 \pmod{7}$. So $x = 7k - 2$ for some $k \in \mathbb{Z}$. In the second congruence above we should first divide everything by 2, to convert it to $x \equiv 5 \pmod{8}$. This gives $7k - 2 \equiv 5 \pmod{8}$, and after moving the 2 to the right we find that 7 cancels nicely, giving $k \equiv 1 \pmod{8}$, or $k = 1 + 8l$ for some $l \in \mathbb{Z}$. Thus $x = 7k - 2 = 7(1 + 8l) - 2 = 5 + 56l$ for some l . Putting this in the last congruence gives $5(5 + 56l) \equiv 1 \pmod{18}$, or $5(5 + 2l) \equiv 1 \pmod{18}$. This rearranges to $10l \equiv -24 \pmod{18}$, or (dividing everything by 2) $5l \equiv -12 \pmod{9}$. Or $-4l \equiv -12 \pmod{9}$. Cancelling 4 (OK since $\gcd(4, 9) = 1$) gives $l \equiv 3 \pmod{9}$. Thus $l = 3 + 9m$ for some $m \in \mathbb{Z}$, and $x = 5 + 56(3 + 9m) = 173 + 504m$ for some $m \in \mathbb{Z}$. So the solution is $x \equiv 173 \pmod{504}$.

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

Solution.

By Fermat's Little Theorem, $2^4 \equiv 1 \pmod{5}$, and hence $2^{4k} \equiv 1^k \equiv 1 \pmod{5}$ for all k . So $2^{2008} \equiv 1 \pmod{5}$, and, multiplying through by 2, it follows that $2^{2009} \equiv 2 \pmod{5}$. Similarly, $2^6 \equiv 1 \pmod{7}$ (by Fermat) gives $2^{2004} \equiv 1 \pmod{7}$, and $2^{2009} \equiv 2^5 \equiv 4 \pmod{7}$. Similarly again, $2^{10} \equiv 1 \pmod{11}$, whence $2^{2000} \equiv 1 \pmod{11}$, and $2^{2009} \equiv 2^9 \equiv 512 \equiv 6 \pmod{11}$. So our task is to solve $N \equiv 2 \pmod{5}$, $N \equiv 4 \pmod{7}$ and $N \equiv 6 \pmod{11}$ simultaneously.

The first condition gives $N = 5k + 2$ for some k , and substituting this in the second condition gives $5k + 2 \equiv 4 \pmod{7}$. So $-2k \equiv 2 \pmod{7}$, and $k \equiv -1 \pmod{7}$. So $k = 7h + 6$ for some h , giving $N = 35h + 32$. Thus we need $35h + 32 \equiv 6 \pmod{11}$, or $2h \equiv -26 \equiv -4 \pmod{11}$. So $h \equiv -2 \equiv 9 \pmod{11}$. Thus $h = 11\ell + 9$ for some ℓ , and $N = 35(11\ell + 9) + 32 \equiv 347 \pmod{385}$.

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

Solution.

For the shortest proof, see the the pdf file for Lecture 13. The proofs written below are not much longer, and perhaps are also worth reading.

Let $d = \gcd(a, m)$. By the definition, this means that

- 1) $d|a$ and $d|m$,
- 2) for all c , if $c|a$ and $c|m$ then $c|d$.

We also have the useful fact that there exist integers r and s with $ra + sm = d$.

To prove that kd is the gcd of ka and km it suffices to prove that kd satisfies the analogues of 1) and 2) for ka and km . That is, we want to show that

- 3) $kd|ka$ and $kd|km$,
- 4) for all c , if $c|ka$ and $c|km$ then $c|kd$.

Now 3) is immediate from 1): for example, $d|a$ means that $a = de$ for some $e \in \mathbb{Z}$, and this gives $ka = (kd)e$, whence $kd|ka$. Similarly, $kd|km$.

To prove 4), choose r and s such that $d = ra + sm$. This gives $kd = r(ka) + s(km)$. Now suppose that $c|ka$ and $c|km$. Then c divides $r(ka)$ and also divides $s(km)$. Hence c divides $r(ka) + s(km) = kd$. So we have shown that if $c|ka$ and $c|km$ then $c|kd$; that is, 4) is satisfied. Since 3) and 4) are both satisfied it follows that kd is the gcd of ka and km , as required.

One can also prove the result by considering the method that we use to calculate gcd's, namely, the Euclidean Algorithm. If you were to use the Euclidean Algorithm to find $\gcd(a, m)$ then you would put $a_0 = a$ and $a_1 = m$, and then, starting at $i = 1$, you would divide a_i into a_{i-1} and find the remainder. This remainder is defined to be a_{i+1} . Then you increase i by 1 and repeat the process. The crucial relationships are, therefore, that

$$a_{i-1} = q_i a_i + a_{i+1} \text{ and } 0 \leq a_{i+1} < a_i.$$

for some quotient q_i (uniquely determined by the condition $0 \leq a_{i+1} < a_i$). The algorithm stops when you find that $a_j = 0$ for some j , and then a_{j-1} – the last nonzero term in the sequence – is the gcd.

Applying the same process to find $\gcd(ka, km)$ you would start with $b_0 = ka$ and $b_1 = km$, and then, starting at $i = 1$, divide b_i into b_{i-1} and let the remainder be b_{i+1} , increment i and repeat. So you obtain

$$b_{i-1} = q'_i b_i + b_{i+1}, \quad 0 \leq b_{i+1} < b_i.$$

The last nonzero term in the sequence (b_i) will be $\gcd(ka, km)$.

However, since $b_0 = ka_0$ and $b_1 = ka_1$ we have both

$$ka_0 = q'_1(ka_1) + b_2, \quad 0 \leq b_2 < ka_1$$

and

$$ka_0 = q_1(ka_1) + ka_2, \quad 0 \leq ka_2 < ka_1$$

the second of these coming from $a_0 = q_1 a_1 + a$ and $0 \leq a_2 < a_1$, multiplied through by k . Since the quotient and remainder in the Division Algorithm are unique, we must have $q'_1 = q_1$ and $b_2 = ka_2$. Now b_3 is the remainder when b_1 (which equals ka_1) is divided by b_2 (which equals ka_2). By the same reasoning we have just used, the remainder will be k times the remainder on dividing a_1 by a_2 . That is, $b_3 = ka_3$. And so it will continue. In particular, $b_j = 0$ if and only if $a_j = 0$, and the last nonzero term in the sequence (b_i) is $b_{j-1} = ka_{j-1}$. That is, $\gcd(ka, km) = k \gcd(a, m)$, as required.

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 $\phi(m) = pq - (p - 1) - (q - 1) - 1 = (p - 1)(q - 1)$.

Solution.

If $\gcd(a, m) = p$ then $a = pa'$ for some a' . This gives

$$p = \gcd(a, m) = \gcd(pa', pq) = p \gcd(a', q)$$

by Question 3; so $\gcd(a', q) = 1$. Conversely, if $\gcd(s, q) = 1$ then $\gcd(ps, pq) = p$. And $0 \leq s < q$ if and only if $0 \leq ps < pq$. So there is a one to one correspondence between the residues $a \pmod{pq}$ with $\gcd(a, m) = p$ and the residues $s \pmod{q}$ with $\gcd(s, q) = 1$. There are $\phi(q) = q - 1$ residues mod q that are coprime to q . So $N_p = q - 1$. By the same proof with p and q swapped, $N_q = p - 1$.

The only residue $a \pmod{m}$ with $\gcd(a, m) = m$ is $m = 0$ – this is the only residue that is divisible by m . So $N_m = 1$.

The total number of residues is $m = pq$. For each residue a we must have $\gcd(a, m) = 1, p, q$ or pq , since these are the only positive integers that are divisors of m . So $pq = N_1 + N_p + N_q + N_m$, and this gives

$$N_1 = pq - (q - 1) - (p - 1) - 1 = pq - q - p + 1 = (p - 1)(q - 1).$$

But N_1 , the number of residues mod m that are coprime to m , is just $\phi(m)$, by the definition of $\phi(m)$. So $\phi(m) = (p - 1)(q - 1)$, as required.

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.

Solution.

If $\gcd(a, m) = pq$ then $a = pqa'$ for some a' . And $\gcd(pqa', m) = \gcd(pqa', pqr)$ equals $pq \gcd(a', r)$. So there is a one to one correspondence between the residues $a \pmod{m}$ with $\gcd(a, m) = pq$ and the residues $a' \pmod{r}$ with $\gcd(a', r) = 1$. Thus $N_{pq} = r - 1$. Similarly $N_{pr} = q - 1$ and $N_{qr} = p - 1$. If $\gcd(a, m) = p$ then $a = pa'$ for some a' . And $\gcd(pa', m) = \gcd(pa', pqr) = p \gcd(a', qr)$. So the residues $a \pmod{m}$ with $\gcd(a, m) = p$ are in one to one correspondence with the residues $a' \pmod{qr}$ with $\gcd(a', qr) = 1$. So by Question 4, $N_p = (q - 1)(r - 1)$. Similarly $N_q = (p - 1)(r - 1)$ and $N_r = (p - 1)(q - 1)$. And $N_m = 1$, as in Question 4. So now $\phi(pqr) = N_1$ equals

$$pqr - 1 - (p - 1) - (q - 1) - (r - 1) - (p - 1)(q - 1) - (p - 1)(r - 1) - (q - 1)(r - 1)$$

which is $(p - 1)(q - 1)(r - 1)$. (Expand $((p - 1) + 1)((q - 1) + 1)((r - 1) + 1)$.)

We can now use induction on k to prove that if $m = \prod_{i=1}^k p_i$, where the p_i are pairwise distinct primes, then $\phi(m) = \prod_{i=1}^k (p_i - 1)$. Let $K = \{1, 2, \dots, k\}$ (so that $m = \prod_{i \in K} p_i$), and for each $S \subseteq K$ let $d(S) = \prod_{i \in S} p_i$. Then the numbers $d(S)$, for the various subsets S , are all the divisors of m , and if we write S' for the complement of S in K then $m = d(S)d(S')$ in all cases. By Exercise 3, an integer a satisfies $\gcd(a, m) = d(S)$ if and only if $a = bd(S)$ for some integer b satisfying $\gcd(b, d(S')) = 1$; thus $N_{d(S)} = \phi(d(S'))$, and if $S' \neq \emptyset$ then the inductive hypothesis tells us that $\phi(d(S')) = \prod_{i \in S'} (p_i - 1)$. So

$$\begin{aligned} \phi(m) &= N_1 = m - \sum_{d|m, d \neq 1} N_d = m - \sum_{S \subseteq K, S \neq \emptyset} N_{d(S)} \\ &= m - \sum_{T \subsetneq K, T \neq \emptyset} \left(\prod_{i \in T} (p_i - 1) \right) = \prod_{i \in K} (p_i - 1) \end{aligned}$$

since expanding the product $m = \prod_{i \in K} ((p_i - 1) + 1)$ gives $m = \sum_{T \subseteq K} \left(\prod_{i \in T} (p_i - 1) \right)$.

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.

Solution.

- (i) $273 = 3 \times 91 = 3 \times 7 \times 13$. So $\phi(273) = 2 \times 6 \times 12 = 144$.
(ii) Let N be the residue of $4^{291} \pmod{273}$. Since $\phi(273) = 144$ by Part (i), the Euler-Fermat Theorem tells us that $4^{144} \equiv 1 \pmod{273}$. So $4^{288} \equiv 1^2 \equiv 1 \pmod{273}$, and $4^{291} \equiv 4^3 \pmod{273}$. So the residue N is $4^3 = 64$.

- *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 $s_r \equiv 4 \pmod{r}$.