

NUMBER THEORY TRACK, PROBLEM SET 4

The Chinese Remainder Theorem

Recall the statement of the *Chinese Remainder Theorem*: let m_1, m_2, \dots, m_r denote r nonzero integers which are relatively prime in pairs (i.e. $(m_i, m_j) = 1$ if $i \neq j$) and let a_1, a_2, \dots, a_r denote any r integers. Then the r congruences $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_r \pmod{m_r}$ have a common solution. Also, if x_0 is one such solution, then an integer x is a common solution if and only if $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

- (1) Find all integers that simultaneously satisfy: $x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 5 \pmod{2}$.
- (2) Find all integers that give the remainders 1, 2, and 3 when divided by 3, 4, and 5 respectively.
- (3) Let m_1, m_2, \dots, m_r be relatively prime in pairs. Assuming that each of the congruences $b_i x \equiv a_i \pmod{m_i}$ has a solution, prove that these r congruences have a simultaneous solution.

The Euler ϕ -function

Recall that the Euler function $\phi(n)$ is defined to be the number of integers between 1 and n (inclusive) which are relatively prime to n .

- (4) As we will see, $\phi(p^k) = p^{k-1}(p-1)$ for p a prime. Given this, prove that $\frac{\phi(n)}{n}$ is the product $\prod(1 - \frac{1}{p})$, where the product is taken over all primes p dividing n .
- (5) Evaluate $\phi(n)$ for $n = 1, 2, \dots, 12$.
- (6) Find the number of positive integers ≤ 3600 which are relatively prime to 3600. Find the number of positive integers ≤ 7200 which are relatively prime to 3600.
- (7) Find all solutions x of the equation $\phi(x) = 24$.
- (8) Prove that the equation $\phi(x) = 14$ has no solution x .
- (9) Find the smallest positive integer n so that $\phi(x) = n$ has: no solution; exactly two solutions; exactly three solutions; exactly four solutions. (It is conjectured that there is no integer n such that $\phi(x) = n$ has exactly one solution, but this is an unsolved problem.)
- (10) Show that $\phi(nm) = n\phi(m)$ if every prime that divides n also divides m .
- (11) If $\phi(m) = \phi(mn)$ and $n > 1$, prove that $n = 2$ and m is odd.
- (12) Characterize the set of positive integers n satisfying $\phi(2n) = \phi(n)$. Characterize the set of positive integers n satisfying $\phi(2n) > \phi(n)$.
- (13) Show that

$$n = \sum_{d|n} \phi(d).$$

Here, the sum is to be taken over all positive divisors d of n . (Hint: calculate how many integers x between 1 and n have $(x, n) = d$.)

A couple of miscellaneous questions

- (14) Exhibit a complete residue system module 7 composed entirely of 0 and of powers of 3.
- (15) Show that $7|(3^{2n+1} + 2^{n+2})$ for all n .