MA10209 Algebra 1A

Sheet 6 Solutions : GCS

5-xi-2018

Hand in work to your tutor at the time specified by your tutor. The latest possible hand in time will be 17:15, Monday Nov 12th.

1. How many integers in the range $0 \le i \le 2014$ are coprime to 2015?
   Solution Note that $2015 = 5*403 = 5*13*31$ and these factors are (co)prime. $\varphi(2015) = \varphi(5)\varphi(13)\varphi(31) = 4 \cdot 12 \cdot 30 = 1440$ since φ is multiplicative with respect to coprime arguments.

2. Suppose that m is an odd natural number. Prove that there is a natural number n such that m divides $2^n - 1$.
   Solution Let $n = \varphi(m)$ and the Euler-Fermat theorem applies.

3. Find all integers x such that $x \equiv 3 \bmod 7$ and $x \equiv 4 \bmod 9$.
   Solution You can spot a simultaneous solution, but we will work one out by unwrapping Euclid's algorithm. $9 = 1 \cdot 7 + 2; 7 = 3 \cdot 2 + 1$ and $2 = 2 \cdot 1 + 0$. Therefore $1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (9 - 7) = 4 \cdot 7 - 3 \cdot 9$. Therefore $28 = 1 + 3 \cdot 9 = 4 \cdot 7$ so $28 \equiv 1 \bmod 9$ and $28 \equiv 0 \bmod 7$. Also $-27 = -3 \cdot 9 \equiv 0 \bmod 9$ and $-27 \equiv 1 \bmod 7$. Therefore $3(-27) + 4(28) = 31$ satisfies $31 \equiv 3 \bmod 7$ and $31 \equiv 4 \bmod 9$. The set of all integers satisfying the two congruences simultaneously is $\{31 + 63k \mid k \in \mathbb{Z}\}$.

4. Find all integers y such that 9 divides $2y + 1$ and 11 divides $3y + 6$.
   Solution The condition $2y \equiv -1 \bmod 9$ is equivalent to $y \equiv 4 \bmod 9$ (the second congruence follows from the first by multiplying through by 5; the first follows from the second by multiplying through by 2). Also the condition $3y \equiv -6 \bmod 11$ is equivalent to $y \equiv 9 \bmod 11$ (for similar reasons; we can deduce each congruence from the other). We could simply spot a solution (say 31), but here is a way to calculate one: $11 = 1 \cdot 9 + 2$; $9 = 4 \cdot 2 + 1$; $2 = 2 \cdot 1 + 0$. Therefore $1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11$. Now $45 \equiv 1 \bmod 11$ and $45 \equiv 0 \bmod 9$. Also $-44 \equiv 0 \bmod 11$ and $-44 \equiv 1 \bmod 9$. Therefore $4 \cdot (-44) + 9 \cdot 45 = 229$ solves all congruences and the original divisibility conditions. The set of all solutions is $\{229 + 99k | k \in \mathbb{Z}\} = \{31 + 99k | k \in \mathbb{Z}\}$.

5. Find the smallest positive integer z such that $z \equiv 10 \bmod 11$, $z \equiv 12 \bmod 13$, $z \equiv 17 \bmod 18$. *Hint: this is much easier than it looks.*

Solution The integer -1 is a similtaneous solution to all three congruences. By the Chinese Remainder Theorem, the set of all possible solutions is $\{-1 + 2574k \mid k \in \mathbb{Z}\}$ so the smallest positive solution is 2573.

6. Suppose that $p > 3$ is a prime number. Prove that $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$ is a multiple of p.
Solution Let $n = 2^{p-2} + 3^{p-2} + 6^{p-2}$ so, using Fermat's Little Theorem, $6n \equiv 3 + 2 + 1 \equiv 6 \bmod p$. Note that we have chosen $p > 3$ so FLT applies. Now 6 and p are coprime so 6 has a multiplicative inverse in $\mathbb{Z}_p$, so there is an integer x (in fact there are lots) such that $6x \equiv 1 \bmod p$. Multiply by x so $6xn \equiv 6x \bmod p$ and therefore $n \equiv 1 \bmod p$. *Note that 2^{p-2} is the multiplicative inverse of 2 modulo p, by Fermat's Little Theorem. Similar observations apply to 3^{p-2} and 6^{p-2}, so if we are brave enough to allow fraction notation, we are being asked to show that $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \equiv 1 \bmod p$, which is hardly a surprise.*

7. Show that there are 1000 consecutive positive integers, each of which is divisible by at least 1000 different prime numbers.
Solution There are infinitely many prime numbers (thank you Euclid). Therefore we can form 1000 pairwise disjoint sets A_i $(1 \leq i \leq 1000)$, each of which consists of 1000 different prime numbers. Let n_i be the product of the elements of A_i, so the 1000 natural numbers n_i are pairwise coprime. Now consider 1000 congruences $x \equiv -i \bmod n_i$ for $i = 1, \ldots, 1000$. The conditions for CRT apply so there is an integer m (a value for x) which simultaneously satisfies all these congruences. From CRT we can shoose m to be positive. Now for each i, n_i divides $m + i$, which therefore has at least 1000 different prime divisors. The numbers $m + i$ for $i = 1, 2, \ldots, 1000$ are the required consecutive positive integers. There are a host of related results one can prove in similar fashion. For example, that there are a million consecutive positive integers, each of which has a square divisor larger than 1.

8. Suppose that $m, n \in \mathbb{N}$. Consider the map $\pi_{mn} : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ defined by $[x]_{mn} \mapsto ([x]_m, [x]_n)$ for each $x \in \mathbb{Z}$, where $[x]_k$ denotes the equivalence class of x under the relation $\sim_k$. Determine $|\mathrm{Im}\ \pi_{mn}|$. *Note that if m and n are coprime, then the Chinese Remainder Theorem applies and the map π is surjective. In that case, the size of the image is mn. This question involves an investigation of how the CRT fails when m and n are not coprime.*
Solution Experiments with small m and n should indicate that π_{mn} is a "gcd (m, n) to 1" function. That is, to say, given any $\alpha \in \mathbb{Z}_{mn}$, the set $\{\beta \mid \beta \in \mathbb{Z}_{mn}, \pi_{mn}(\alpha) = \pi_{mn}(\beta)\}$ always has exactly $g = \gcd(m, n)$ elements. If this is true, $|\mathrm{Im}\ \pi_{mn}| = mn/g = \mathrm{lcm}(m, n)$.

So, to establish this attractive result, for each $\beta \in \mathbb{Z}_{mn}$ we seek to count the set $S_\beta = \{\alpha \mid \alpha \in \mathbb{Z}_{mn}, \pi_{mn}(\alpha) = \pi_{mn}(\beta)\}$. Note that it is easy to count $S_{[0]}$, because this is the number of common multiples t of m and n in the range

$0 \le t < mn$. This is the number multiples of $l = \text{lcm}(m, n)$ in this range. Now $lg = mn$, so the number multiples of l in the range is g, as required.

Now to count S_β where β is arbitrary. When $\gamma \in \mathbb{Z}_{mn}$ we have $\gamma \in S_\beta$ iff $\gamma - \beta \in S_{[0]}$, so each S_β has the same size as $S_{[0]}$ and the proof is complete.

Note that if m and n are not coprime, this shows that for some integers a and b, there will not be an integer x such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. However, if there is a simultaneous solution, there is an integer c such that the solution set is the set of integers x such that $x \equiv c \bmod \text{lcm}(m, n)$.

9. Let d be a positive integer. A d-arithmetic set is defined to be a set of the form $\{a+md \mid m = 0, 1, 2, \ldots\}$ for some positive integer a. Suppose that $N > 1$ is a positive integer and that we have a p-arithmetic set S_p for each prime number $p \le N$. Show that there are $2N + 1$ consecutive positive integers, all except two of which are in the union S of our sets S_p. *Hint: CRT & Eratosthenes*

   Solution If each set has $a = 0$, then we are looking at the sieve of Eratosthenes: every integer in the range 0 to N (inclusive) except 1 is divisible by a prime number which is at most N. If you were to run the sieve of Eratosthenes in both directions, you would obtain $2N + 1$ consecutive integers, all except -1 and 1 having a prime divisor which is at most N.

   Now we have to mimic this situation in the set up we have been given. Let a_p denote the smallest element of S_p. In fact any element would do. Now by the Chinese Remainder Theorem we can find an integer a such that $a \equiv a_p \bmod p$ for each p. Moreover we can choose such a to be as large as we wish. We choose a to be so large that it bigger than a_p+N for each of our prime numbers $p \le N$. Now viewing a as the analogue of 0 in the sieve of Eratosthenes (run both positively and negatively), we are done.

10. (Challenge!) A mathematical tree (i.e. a vertical unit interval) grows at each point of an infinite plane with integral co-ordinates except for the origin $(0, 0)$ where an observer, of height 1, stands. Many trees are visible, including those at $(1, 0), (7, 8)$ and $(45, -7)$. Other trees are invisible, because the view of them from the origin is obstructed by other trees. For example, the view of the tree at $(-14, 91)$ is obstructed by the tree at $(-2, 13)$.

    Show that it is possible for a *Tunguska Event* of diameter 10^{10} to happen, yet be unknown to the observer. In other words, show that there is a circle in the plane of diameter 10^{10} which has only invisible trees in its interior.

    Solution We use the result of Problem 7 of Sheet 4. For any positive integer n, there are n pairwise coprime natural numbers a_i, and n pairwise coprime natural numbers b_i, with no a_i coprime with any b_j. We solve the simultaneous congruences $x \equiv -i \bmod a_i$ using the CRT. Note that we may choose the integer x to be positive. Similarly we find a positive integer y such that $y \equiv -i \bmod b_i$ for every i in the range 1 to n.

For $1 \leq i, j \leq n$, the trees planted at $(x+i, y+j)$ are all invisible from the origin, because $x+i$ and $y+j$ are both divisible by $\gcd(a_i, b_j)$. Moreover, each of these invisible trees is actually obstructed by a tree outside the square region of trees that we have chosen, since if the view of a tree is obstructed by other trees in the square, the view of the obstructing tree nearest the origin must be obstructed by a tree outside the square, and that will obstruct all the trees on that line of sight.

Choosing n sufficiently large, the footprint of a Tunguska air burst of arbitrary diameter can sit inside a square of invisible trees, the flattening of which will not be perceived by an observer at the origin.