

# MA10209 Algebra 1A

Sheet 6 Problems and Solutions v3: GCS

18-xi-11

The course website is <http://people.bath.ac.uk/masgcs/diary.html>

*Hand in work to your tutor by 13:00, Monday Nov 14.*

1. Find all integers  $x$  such that  $x \equiv 3 \pmod{7}$  and  $x \equiv 4 \pmod{9}$ .

**Solution** Notice that  $(-5)7 + (4)9 = 1$ , so  $-35 \equiv 0 \pmod{7}$  and  $-35 \equiv 1 \pmod{9}$ . Also  $36 \equiv 1 \pmod{7}$  and  $36 \equiv 0 \pmod{9}$ . Therefore  $3 \times 36 + 4(-35) \equiv 3 \pmod{7}$  and  $3 \times 36 + 4(-35) \equiv 4 \pmod{9}$ . Thus we have found a simultaneous solution  $-32$  to the congruences. By the CRT (7 and 9 are coprime), the set of simultaneous solutions is  $\{-32 + 63k \mid k \in \mathbb{Z}\} = \{31 + 63k \mid k \in \mathbb{Z}\}$ .

2. Find all integers  $y$  such that 9 divides  $2y + 1$  and 11 divides  $3y + 6$ .

**Solution** 9 divides  $2y + 1$  is equivalent to  $2y \equiv -1 \pmod{9}$ . Multiplying by 5 we obtain  $y \equiv 4 \pmod{9}$ . The original congruence can be recovered by multiplying by 2, so the congruence  $y \equiv 4 \pmod{9}$  has exactly the same solutions as the congruence  $2y \equiv -1 \pmod{9}$ .

Next we give the other congruence similar treatment. 11 divides  $3y + 6$  is equivalent to  $3y \equiv -6 \pmod{11}$ . Multiplying by 4 we obtain  $y \equiv 9 \pmod{11}$ . The original congruence can be recovered by multiplying by 3, so the congruence  $y \equiv 9 \pmod{11}$  has exactly the same solutions as the congruence  $3y \equiv -6 \pmod{11}$ .

We are now required to solve  $y \equiv 4 \pmod{9}$  and  $y \equiv 9 \pmod{11}$  simultaneously. Using Euclid's algorithm unpicked, or a happy observation, we see that  $1 = (5)9 + (-4)11$  so  $45 \equiv 0 \pmod{9}$  and  $45 \equiv 1 \pmod{11}$ . Similarly  $-44 \equiv 1 \pmod{9}$  and  $-44 \equiv 0 \pmod{11}$ . We obtain the particular solution  $4(-44) + 9(45) = 229$ . By the CRT (9 and 11 are coprime), the set of simultaneous solutions is  $\{229 + 99k \mid k \in \mathbb{Z}\} = \{31 + 99k \mid k \in \mathbb{Z}\}$ .

3. Find all integers  $z$  such that  $z \equiv 10 \pmod{11}$ ,  $z \equiv 12 \pmod{13}$ ,  $z \equiv 17 \pmod{18}$ . *Hint: this is much easier than it looks. There is a very short method.*

**Solution** Observe that  $-1$  is a simultaneous solution to all three congruences. The Chinese Remainder Theorem applies, since the moduli are pairwise coprime. Notice that the product of the moduli is 2574 so the solution set is  $\{-1 + 2574k \mid k \in \mathbb{Z}\}$ .

4. Show that there are 1000 consecutive positive integers, each of which is divisible by at least 1000 different prime numbers.

**Solution** Let  $n_1$  be the product of the first 1000 prime numbers (in ascending order of size),  $n_2$

be the product of the next 1000 prime numbers, and so on. Consider the simultaneous congruences  $x \equiv 0 \pmod{n_1}$ ,  $x \equiv -1 \pmod{n_2}$ ,  $x \equiv -2 \pmod{n_3}$ , and for each  $i = 1, \dots, 1000$ ,  $x \equiv 1 - i \pmod{n_i}$ . Since the moduli are coprime, the Chinese Remainder Theorem applies. Let  $n$  be the product of all  $n_i$ . Let  $m$  be a simultaneous solution to this set of congruences (which exists by the CRT) then the solution set for the simultaneous congruences is  $\{m + kn \mid k \in \mathbb{Z}\}$ . This set contains a positive integer  $u$ . Now  $n_i$  divides  $u + i - 1$  for each  $i$ , so this run of consecutive positive integers has the required property.

5. (a) Suppose that  $u, v, d$  are integers, with  $u$  and  $d$  coprime. Show that if  $d$  divides  $uv$ , then  $d$  divides  $v$ .

**Solution** You can obtain this result via the Fundamental Theorem of Arithmetic. However, there is a quick way. Since  $u, d$  are coprime, then there are integers  $\lambda, \mu$  such that  $1 = \lambda d + \mu u$ . Multiply by  $v$  so  $v = \lambda d + \mu uv$ . Now  $d$  divides the right-hand side, so  $d \mid v$ .

- (b) Suppose that  $m$  is an odd natural number. Prove that there is a natural number  $n$  such that  $m$  divides  $2^n - 1$ .

**Solution** Work in  $\mathbb{Z}_m$ . Consider the powers of  $[2]$ :  $[1], [2], [2]^2, [2]^3, \dots$ . There are infinitely many terms of this sequence, but  $\mathbb{Z}_m$  is finite, so two terms must be equal. There are  $i, j$  with  $0 \leq i < j$  such that  $[2]^i = [2]^j$ . Therefore  $[2^j - 2^i] = [0]$  so  $m$  divides  $2^i(2^{j-i} - 1)$ . Since  $m$  is odd,  $m$  is coprime to  $2^i$  and part (a) applies, so  $m$  divides  $2^{j-i} - 1$ .

6. Suppose that  $m, n \in \mathbb{N}$ . Consider the map  $\pi_{mn} : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$  defined by  $[x]_{mn} \mapsto ([x]_m, [x]_n)$  for each  $x \in \mathbb{Z}$ , and  $[x]_k$  denotes the equivalence class of  $x$  under the relation  $\sim_k$ . Determine  $|\text{Im } \pi_{mn}|$ .

**Solution** Suppose that  $\pi_{mn}([x_0]) \in \text{Im } \pi_{mn}$ . The fibre of  $\pi_{mn}([x_0])$  is the set of equivalence classes  $[y] \in \mathbb{Z}_{mn}$  such that  $\pi_{mn}([y]) = ([x_0]_m, [x_0]_n)$ , and this is the set of equivalence classes  $[y]$  such that  $[y - x_0]$  is in the fibre of  $([0]_m, [0]_n)$ . The integers  $y$  in question are those such that  $y = x_0 + kl$  where  $k$  is an integer and  $l$  is the lcm of  $m$  and  $n$ . The number of different equivalence classes  $[y]$  as  $k$  varies is determined by counting the number of integers of the form  $x_0 + kl$  in a consecutive run of  $mn$  integers. Look at the consecutive run  $x_0 + 1, x_0 + 2, \dots, x_0 + mn$  we see that there are  $mn/l$  equivalence classes in each non-empty fibre. Therefore  $\pi_{mn}$  is a “ $mn/l$  to 1” function. The domain of  $\pi_{mn}$  has size  $mn$ , so the image has size  $mn/(mn/l) = l = \text{lcm}(m, n)$ .

Notice how this generalizes the case when  $m$  and  $n$  are coprime. In that case the CRT tells us that  $\pi_{mn}$  is a bijection, and so an onto map. Our calculation uses  $l = mn$ , so the fibres of  $\pi_{mn}$  have size 1 and the image has size  $mn$  as expected.

7. Let  $G$  be a group with ‘multiplication’  $*$  and identity element 1.

- (a) Suppose that  $x, y, z \in G$  and  $x * y = x * z$ . Prove that  $y = z$ .

**Solution** By the definition of a group, there is  $x' \in G$  such that  $x' * x = x * x' = 1$ . Now  $x' * (x * y) = x' * (x * z)$  so  $(x' * x) * y = (x' * x) * z$  thanks to the associative law. Now  $x' * x = 1$  so  $1 * y = 1 * z$  but 1 is a two-sided identity element so  $y = z$ . Therefore in a group  $G$ , you can ‘cancel’ on the left.

- (b) Suppose that  $x, y, z \in G$  and  $y * x = z * x$ . Prove that  $y = z$ .

**Solution** By the definition of a group, there is  $x' \in G$  such that  $x' * x = x * x' = 1$ . Now

$(y*x)*x' = (z*x)*x'$  so  $y*(x*x') = z*(x*x')$  thanks to the associative law. Now  $x*x' = 1$  so  $y*1 = z*1$  but 1 is a two-sided identity element so  $y = z$ . Therefore in a group  $G$ , you can ‘cancel’ on the right.

- (c) Suppose that  $e \in G$  and  $e*x = x$  for some  $x \in G$ . Prove that  $e = 1$ , so that  $e*y = y = y*e$  for every  $y \in G$ .

**Solution** We have  $e*x = x = 1*x$ . Now use part (b) to deduce that  $e = 1$ , so  $e*y = 1*y = y$  for each  $y \in G$ . *Informally, if an element  $e$  behaves just a little bit like 1, then it is 1.*

- (d) Suppose that  $G$  is a finite group and that  $x \in G$ . Prove that there is  $k \in \mathbb{N}$  such that  $x^k = 1$ .

**Solution** Consider the sequence  $x^1, x^2 = (x*x), x^3 = x*x^2, \dots$ . Since  $G$  is finite, the terms of this sequence cannot all be different, so there are natural numbers  $i < j$  such that  $1*x^i = x^i = x^j = x^{j-i}*x^i$ . Now apply part (b) to cancel the factor of  $x^i$  on the right (i.e. multiply by its inverse). Therefore  $x^{j-i} = 1$ .

8. Suppose that  $m \in \mathbb{N}$ .

- (a) Let  $i$  be an integer in the range  $1 \leq i \leq m$ . Prove that  $[i]$  has a multiplicative inverse in  $\mathbb{Z}_m$  if, and only if,  $i$  and  $m$  are coprime.

**Solution** If  $[i]$  has a multiplicative inverse  $[j] \in \mathbb{Z}_m$ , then  $[ij] = [1]$  so there is an integer  $t$  such that  $1 = ij + tm$  and therefore  $i$  and  $m$  are coprime. Conversely, if  $i$  and  $m$  are coprime, then there are integers  $j$  and  $t$  such that  $1 = ij + tm$ . Now work in  $\mathbb{Z}_m$ . We have  $[ij + tm] = [1]$  and so  $[ij] + [0] = [1]$  and therefore  $[i][j] = [1]$  and so  $[i]$  has a multiplicative inverse.

- (b) For each  $n \in \mathbb{N}$ , let  $\varphi(n)$  denote the number of integers  $i$  in the range  $1 \leq i \leq n$  which are coprime to  $n$ . Calculate  $\varphi(n)$  for  $1 \leq n \leq 12$ .

**Solution**  $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \varphi(9) = 6, \varphi(10) = 4, \varphi(11) = 10$  and  $\varphi(12) = 4$ .

- (c) Suppose that  $m, n$  are coprime natural numbers. By considering the natural map  $\pi_{mn} : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$  defined in Problem 6 (or otherwise), prove that  $\varphi(mn) = \varphi(m)\varphi(n)$ .

**Solution** By part (a),  $\varphi(n)$  is the number of elements of  $\mathbb{Z}_n$  which have multiplicative inverses. Recall that the map  $\pi_{mn}$  (bijective by CRT) ‘preserves structure’. The multiplicative identity of  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  is  $([1]_m, [1]_n)$  and  $([r]_m, [s]_n) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$  will have a multiplicative inverse  $([r']_m, [s']_n)$  if, and only if, both  $[r]_m$  has a multiplicative inverse  $[r']_m \in \mathbb{Z}_m$  and  $[s]_n$  has a multiplicative inverse in  $[s']_n \in \mathbb{Z}_n$ . The bijection  $\pi_{mn}$  carries multiplicatively invertible elements to multiplicatively invertible elements, so  $\varphi(mn) = \varphi(m)\varphi(n)$ .

- (d) How many integers in the range  $1 \leq i \leq 990$  are coprime to 990?

**Solution** We have  $990 = 9 \times 110$  and 9 is coprime to 110. Also  $110 = 10 \times 11$  and 10 is coprime to 11. Therefore  $\varphi(990) = \varphi(9)\varphi(110) = \varphi(9)\varphi(10)\varphi(11) = 6 \times \varphi(2)\varphi(5) \times 10 = 6 \times 4 \times 10 = 240$ .

9. Let  $d$  be a positive integer. A  $d$ -arithmetic set is defined to be a set of the form  $\{a + md \mid m = 0, 1, 2, \dots\}$  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  $p \leq N$ . 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** Choose  $x_p \in S_p$  for each  $p$ . Solve  $x \equiv x_p \pmod{p}$  simultaneously using the Chinese remainder theorem. Since the solution set is an AP with non-zero common difference, we may

choose  $x$  arbitrarily large; sufficiently large that  $x - N$  is greater than the first term of each AP. Now  $x$  is in every one of our APs. The sieve of Eratosthenes is being applied, using  $x$  as ‘zero’. The integers  $z \geq x$  which are in  $S$  are precisely those which are such that  $z - x$  is a multiple of some prime  $p \leq N$ . Thus  $x, x + 2, x + 3, x + 4, \dots, x + N$  are all in the union. Since  $x$  has been chosen sufficiently large,  $x - 2, x - 3, \dots, x - N$  are also in  $S$ . We have our required  $2N + 1$  consecutive positive integers.

In order to finish, observe that  $x + 1$  and  $x - 1$  are not in  $S$ , since  $x$  is in each  $S_p$ , and primes are bigger than 1.

10. (Tutor pacifier) 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** Not yet, but here is a solution to Problem 10 of Sheet 4.

Using the Fibonacci sequence defined in Question 9, prove that

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}$$

for all  $m, n \in \mathbb{N}$ .

There are all sorts of identities relating Fibonacci numbers. This one is quite well known:

$$F_{m+n} = F_{m+1}F_n + F_mF_{n-1} \quad (*)$$

for all integers  $m, n \geq 0$ . We address the main result by induction on  $m + n$ . The result holds by inspection when  $m = n = 1$ , because

$$\gcd(F_1, F_1) = \gcd(1, 1) = 1 = F_1 = F_{\gcd(1,1)}.$$

Assume that  $m + n > 2$ . The result holds by inspection when  $m = n$ , and without loss of generality we may assume that  $m > n$ .

Replace  $m$  by  $m - n$  in  $(*)$  to obtain  $F_m = F_{m-n+1}F_n + F_{m-n}F_{n-1}$ . Recall that  $F_{n-1}$  is coprime to  $F_n$  (Sheet 4, Problem 9), so any integer which is a common divisor of  $F_m$  and  $F_n$  must divide  $F_{m-n}$  (we are invoking the result of Problem 5(a)). Conversely any integer which is a common divisor of  $F_n$  and  $F_{m-n}$  will divide  $F_m$ . Therefore the pairs  $(F_m, F_n)$  and  $(F_{m-n}, F_n)$  have the same common divisors, and hence the same gcds. Now by induction  $\gcd(F_{m-n}, F_n) = F_{\gcd(m-n,n)}$ . However, the pairs  $(m, n)$  and  $(m - n, n)$  have the same common divisors and hence the same gcds. Therefore

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}.$$

It remains to establish the equation  $(*)$ . This is an easy matter by induction on  $m$  while holding  $n$  fixed, using  $F_{m+n} = F_{(m-1)+n} + F_{(m-2)+n}$  for all  $m \geq 2$ .