

MA10209 Algebra 1A

Sheet 5 Problems and Solutions v2: GCS

28-x-11

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

Hand in work to your tutor by 13:00, Monday Nov 7.

1. (a) Find $g = \gcd(75, 27)$ by means of a hand calculation.

Solution $75 = 2 \times 27 + 21$; $27 = 1 \times 21 + 6$; $21 = 3 \times 6 + 3$; $6 = 2 \times 3 + 0$. Therefore $\gcd(75, 27) = 3$.

- (b) Find integers λ_0 and μ_0 such that $75\lambda_0 + 27\mu_0 = g$.

Solution $3 = 1 \times 21 - 3 \times 6 = 1 \times 21 - 3 \times (27 - 21) = 4 \times 21 - 3 \times 27 = 4 \times (75 - 2 \times 27) - 3 \times 27 = 4 \times 75 - 11 \times 27$. (Notice that it is easy to verify that this statement is correct). Therefore we may choose $\lambda_0 = 4$ and $\mu_0 = -11$.

- (c) Find all pairs of integers λ, μ such that $75\lambda + 27\mu = g$.

Solution Integers λ, μ satisfy $75\lambda + 27\mu = g$ if, and only if, $75(\lambda_0 - \lambda) + 27(\mu_0 - \mu) = 0$ and this happens if, and only if, $25(\lambda_0 - \lambda) + 9(\mu_0 - \mu) = 0$. 25 and 9 are coprime, so $\lambda_0 - \lambda = 9k$ for some $k \in \mathbb{Z}$, and then it follows that $\mu_0 - \mu = -25k$. Conversely, provided the integer k satisfies these conditions, then $75(\lambda_0 - \lambda) + 27(\mu_0 - \mu) = 0$. Therefore the legitimate values of (λ, μ) are the elements of the set $\{(4 - 9k, -11 + 25k) \mid k \in \mathbb{Z}\}$.

2. (a) Find $g = \gcd(8633, 13439)$ by means of a hand calculation.

Solution $13439 = 1 \times 8633 + 4806$; $8633 = 1 \times 4806 + 3827$; $4806 = 1 \times 3827 + 979$; $3827 = 3 \times 979 + 890$; $979 = 1 \times 890 + 89$; $890 = 10 \times 89 + 0$. Therefore $\gcd(8633, 13439) = 89$.

- (b) Find integers λ_0 and μ_0 such that $8633\lambda_0 + 13439\mu_0 = g$.

Solution $89 = 979 - 890 = 979 - (3827 - 3 \times 979) = 4 \times 979 - 3827 = 4 \times (4806 - 3827) - 3827 = 4 \times 4806 - 5 \times 3827 = 4 \times 4806 - 5 \times (8633 - 4806) = 9 \times 4806 - 5 \times 8633 = 9 \times (13439 - 8633) - 5 \times 8633 = 9 \times 13439 - 14 \times 8633$. This may be directly verified. Thus we may choose $\lambda_0 = -14$ and $\mu_0 = 9$.

- (c) Find all pairs of integers λ, μ such that $8633\lambda + 13439\mu = g$.

Solution Integers λ, μ satisfy $8633\lambda + 13439\mu = 89$ if, and only if, $8633(\lambda_0 - \lambda) + 13439(\mu_0 - \mu) = 0$ and this happens if, and only if, $97(\lambda_0 - \lambda) + 151(\mu_0 - \mu) = 0$ (dividing through by 89) Now 97 and 151 are coprime, so $\lambda_0 - \lambda = 151k$ for some $k \in \mathbb{Z}$, and then it follows that $\mu_0 - \mu = -97k$. Conversely, provided the integer k satisfies these conditions, then $97(\lambda_0 - \lambda) + 151(\mu_0 - \mu) = 0$. Therefore the legitimate values of (λ, μ) are the elements of the set $\{(-14 - 151k, 9 + 97k) \mid k \in \mathbb{Z}\}$.

- (d) Show that there are positive integers a, b in the range $1 \leq a, b \leq 15$ such that a/b and $8633/13439$ differ by less than $1/2000$.

Solution $9 \times 13439 - 14 \times 8633 = 89$ so $9/14 - 8633/13439 = 89/(13439 \times 14) = 1/(151 \times 14) = 1/2114 < 1/2000$.

3. The integers m and n are not both 0 and $g = \gcd(m, n)$. Suppose that integers λ, μ are such that $\lambda m + \mu n = g$. Prove that there are integers u, v such that $\lambda u + \mu v = 1$.

Solution Let $u = m/g$ and $v = n/g$ so $u, v \in \mathbb{Z}$.

4. (a) Which natural numbers n have an odd number of natural number divisors?

Solution The squares are precisely the numbers with this property. If a positive integer is not a square, its positive divisors come in pairs d, d' where $dd' = n$ so there are an even number of them. In the case that

$n = k^2$ for $k \in \mathbb{N}$, then the pair k, k counts the divisor k twice when it should only be counted once, so n has an odd number of divisors. There is an alternative solution where you use the Fundamental Theorem of Arithmetic to express n as a product $\prod_i p_i^{a_i}$ of distinct prime numbers. Then n has $\prod_i (a_i + 1)$ positive divisors, and this number is odd if, and only if, each a_i is even, and by the FTA, this happens if, and only if, n is a perfect square.

(b) Which natural numbers m have a prime number of natural number divisors?

Solution 1 has 1 divisor. Suppose that $n > 1$ has prime factorization $n = \prod_i p_i^{a_i}$, then n has $\prod_i (a_i + 1)$ positive integer divisors. This expression is prime if, and only if, there is only one prime p_1 in the factorization, and $a_i = q - 1$ where q is prime. Thus the required numbers are those of the form q^{p-1} as p, q range over the prime numbers.

(c) Suppose that $k > 1$ is a natural number. Prove that there are infinitely many natural numbers n which each have exactly k natural number divisors.

Solution Suppose that p is a prime number, then p^{k-1} has exactly k positive divisors. This yields infinitely many examples since p can be any prime number.

5. Suppose that n is a natural number. Let \sim_n denote the equivalence relation on \mathbb{Z} defined by $a \sim_n b$ if, and only if, $n \mid (a - b)$. The equivalence classes of this relation form a finite set \mathbb{Z} / \sim_n . This notation is ponderous, so we introduce compact notation \mathbb{Z}_n for \mathbb{Z} / \sim_n . Write out the addition and multiplication tables for

(a) \mathbb{Z}_4 ;

Solution

$+$	[0]	[1]	[2]	[3]	and	\times	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]		[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[0]		[1]	[0]	[1]	[2]	[3]
[2]	[2]	[3]	[0]	[1]		[2]	[0]	[2]	[0]	[2]
[3]	[3]	[0]	[1]	[2]		[3]	[0]	[3]	[2]	[1]

(b) \mathbb{Z}_5 ;

Solution

$+$	[0]	[1]	[2]	[3]	[4]	and	\times	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]		[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[0]		[1]	[0]	[1]	[2]	[3]	[4]
[2]	[2]	[3]	[4]	[0]	[1]		[2]	[0]	[2]	[4]	[1]	[3]
[3]	[3]	[4]	[0]	[1]	[2]		[3]	[0]	[3]	[1]	[4]	[2]
[4]	[4]	[0]	[1]	[2]	[3]		[4]	[0]	[4]	[3]	[2]	[1]

(c) \mathbb{Z}_6 ;

Solution

$+$	[0]	[1]	[2]	[3]	[4]	[5]	and	\times	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]		[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[0]		[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[3]	[4]	[5]	[0]	[1]		[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[4]	[5]	[0]	[1]	[2]		[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[5]	[0]	[1]	[2]	[3]		[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[0]	[1]	[2]	[3]	[4]		[5]	[0]	[5]	[4]	[3]	[2]	[1]

(d) \mathbb{Z}_7 .

Solution

$+$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	and	\times	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]		[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]		[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]		[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]		[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]		[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]		[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]		[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

6. (a) What is the remainder when $2^{2^{100}}$ is divided by 7?

Solution In \mathbb{Z}_7 we have $[2^6] = [1]$. Now $2^{100} = 6k + r$ where k, r are integers and $0 \leq r \leq 5$. In \mathbb{Z}_6 we have $[2]^{2^m} = [4]$ for all positive integers m by induction, so $[2^{100}] = [4]$ and so $2^{100} = 6k + 4$ for some positive integer k . Now return to working in \mathbb{Z}_7 . We have $[2^{2^{100}}] = [2^{6k+4}] = [2^6]^k [2]^4 = [1]^k [2] = [2]$. Therefore $2^{2^{100}}$ leaves remainder 2 on division by 7.

(b) Show that no prime number p of the form $4m + 3$ is the sum of two squares. *There is a theorem of Fermat which states that all the other prime numbers can be written as the sum of two squares. This is not part of the course, but if you are interested search on: Proofs of Fermat's theorem on sums of two squares.*

Solution In \mathbb{Z}_4 , the squares are $[0]$ and $[1]$. The sum of two equivalence classes, each one of these two, cannot be $[3]$. Therefore integers of the form $4m + 3$ cannot be the sum of two squares.

(c) Prove that there are infinitely many natural numbers which are not the sum of three squares. *Lagrange proved that every positive integer is the sum of four squares.*

Solution In \mathbb{Z}_8 , the squares are $[0]$, $[1]$ and $[4]$. The sum of three equivalence classes, each one these three, cannot be $[7]$. Therefore numbers of the form $8m + 7$ cannot be sums of three squares.

7. Let $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Define a relation \sim on S via $(u_1, v_1) \sim (u_2, v_2)$ if, and only if, $u_1 v_2 = u_2 v_1$.

(a) Prove that \sim is an equivalence relation.

Solution Suppose that $(u, v) \in S$. Then $uv = uv$ so $(u, v) \sim (u, v)$ and we have reflexivity. Next suppose that $(u, v), (w, x) \in S$ and $(u, v) \sim (w, x)$. Therefore $ux = wv$, so $wv = ux$ and thus $(w, x) \sim (u, v)$. Symmetry is established. Finally suppose that $(u, v), (w, x), (y, z) \in S$ and that $(u, v) \sim (w, x)$ and $(w, x) \sim (y, z)$. Therefore $ux = wv$ and $wz = yx$. Now multiplying we have $uxwz = wvyx$. If $w \neq 0$, we divide by the non-zero integer xw to obtain $uz = vy$ and thus $(u, v) \sim (y, z)$. On the other hand, if $w = 0$, then $u = y = 0$ so $(u, v) \sim (y, z)$. Transitivity is established and we have an equivalence relation.

(b) Pretend the rational numbers do not exist, and create them anew by putting $\mathbb{Q} = S / \sim$. Introduce the notation $\frac{a}{b}$ for $[(a, b)]$, the equivalence class of (a, b) . Suppose that $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$, prove that $\frac{a_1 d_1 + b_1 c_1}{b_1 d_1} = \frac{a_2 d_2 + b_2 c_2}{b_2 d_2}$ and $\frac{a_1 c_1}{b_1 d_1} = \frac{a_2 c_2}{b_2 d_2}$.

Solution We have $a_1 b_2 = a_2 b_1$ and $c_1 d_2 = c_2 d_1$. The first (addition) condition will hold provided that we can show that $(a_1 d_1 + b_1 c_1) b_2 d_2 = (a_2 d_2 + b_2 c_2) b_1 d_1$ i.e. $a_1 b_2 d_1 d_2 + b_1 b_2 c_1 d_2 = a_2 b_1 d_1 d_2 + b_1 b_2 c_2 d_1$ and this follows from our first two equations. As for the second formula, we need to show that $a_1 b_2 c_1 d_2 = a_2 b_1 c_2 d_1$ and again this follows immediately from our first two equations.

(c) Show how to define addition and multiplication on \mathbb{Q} .

Solution Define addition $+$ in \mathbb{Q} via $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Define multiplication \times on \mathbb{Q} via $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$.

(d) Why is part (b) vital to ensure that this definition makes sense?

Solution Until we check (b) holds (say for addition), then there is the concern that the definition of addition given in (c) is nonsense, because each given equivalence class has many names. For example $\frac{2}{4} = \frac{3}{6}$. Once you know that (b) holds, it does not matter which name for each equivalence class you use in the recipe for addition in (c). A similar remark applies to multiplication.

8. (a) Suppose that $x \in \mathbb{Z}$ is a square. Which are the possible equivalence classes $[x]$ in \mathbb{Z}_7 ?

Solution These are $[0]^2 = [0]$, $[1]^2 = [6]^2 = [1]$, $[2]^2 = [5]^2 = 4$, $[3]^2 = [4]^2 = [2]$.

- (b) Suppose that C is a set of six consecutive positive integers. Is it possible that C can be partitioned into two subsets A and B so that the product of all the elements of A is the same as the product of all the elements of B ? If $S = \{s\}$ is a singleton subset of \mathbb{Z} , we define the product of all the elements of S to be s .

Solution Suppose, for contradiction, that such a partition exists. Clearly 7 cannot divide any of these 6 consecutive integers else the FTA will ensure that the two products are different. Work in \mathbb{Z}_7 . The product of the six consecutive integers will be in the equivalence class $[6!] = [6]$, but $[6]$ is not a square in \mathbb{Z}_7 by part (a). This is the required contradiction.

9. Let n be a natural number. Prove that there are natural numbers a_1, a_2, \dots, a_n and natural numbers b_1, \dots, b_n such that the following conditions are satisfied.

- (a) If $i \neq j$, then a_i and a_j are coprime.
 (b) If $i \neq j$, then b_i and b_j are coprime.
 (c) The numbers a_i and b_j are not coprime for all i and for all j .

Solution Choose n^2 different prime numbers and write them in an n by n square. There is an infinite supply of prime numbers, thanks to Euclid, so this can be done. Let a_i denote the product of the numbers in the i -th row, and let b_j denote the product of the numbers in the j -th column. That does it.

If you would like to be a touch more formal, for $i = 1 \dots n$ and $j = 1 \dots n$ let p_{ij} be a different prime number. Let $a_i = \prod_{j=1}^n p_{ij}$ and $b_j = \prod_{i=1}^n p_{ij}$. Then for each i and for each j , $\gcd(a_i, b_j) = p_{ij} \neq 1$.

10. (Tutor Pacifier) Let S be a finite set of positive integers which has the following property: if x is an element of S , then so too are all positive divisors of x . A non-empty subset T of S is *good* if whenever $x, y \in T$ and $x < y$, the ratio y/x is a power of a prime number. A non-empty subset T of S is *bad* if whenever $x, y \in T$ and $x < y$, the ratio y/x is not a power of a prime number. A single element set is considered both good and bad (by definition, or by vacuous reasoning, as you please). Let k be the largest possible size of a good subset of S . Prove that k is also the smallest number of pairwise-disjoint bad subsets whose union is S .

Solution Not yet, but here is the solution to Problem 10 of Sheet 3. This was to Prove the *Schröder-Bernstein Theorem unaided* (no books, internet etc). The theorem states that if A, B are sets, and there are injective maps $f : A \rightarrow B$ and $g : B \rightarrow A$, then there is a bijective map $h : A \rightarrow B$. *By replacing B with an appropriate copy of itself if necessary, you can assume that $A \cap B = \emptyset$. This trick may well simplify writing up the proof.*

Proof We may assume wlog that $A \cap B = \emptyset$. Suppose that $x \in A \setminus \text{Im } g$, then we say that x is an *A-stopper*. Any element of A obtained from an *A-stopper* by finitely many applications of the map $g \circ f$ is also an *A-stopper*. Suppose that $y \in B \setminus \text{Im } f$. We say that $g(y)$ is a *B-stopper*. Any element of A obtained from $g(y)$ by finitely many applications of the map $g \circ f$ is also called a *B-stopper*.

If $a \in A$, then by looking at successive (unique where defined) preimages of a under g , then f , then g , then f etc, so see that the *A-stoppers* and the *B-stoppers* form disjoint subsets of A . The elements which are neither *A-stoppers* nor *B-stoppers* we call *non-stoppers*.

If $y \in B$, we say that y is an *A-stopper*, *B-stopper* or *non-stopper* as $g(y)$ is an *A-stopper*, *B-stopper* or *non-stopper*. Notice the ‘meaning’ of this language. Given any element of A or B , you can look for a pre-image of this element under f or g as appropriate, and if you succeed, iterate (do it again and again). Either you can do this indefinitely, or you get stuck (you stop) in A or in B .

We now define a map $\theta : A \rightarrow B$ which will be the required bijection. Suppose that $a \in A$. If a is a *B-stopper*, we define $\theta(a)$ to be the unique element of B such that $g(\theta(a)) = a$. Otherwise a is an *A-stopper* or a *non-stopper*. In that case we define $\theta(a)$ to be $f(a)$.

Notice that θ maps *A-stoppers* to *A-stoppers*, *B-stoppers* to *B-stoppers* and *non-stoppers* to *non-stoppers*.

Injectivity: suppose that $\theta(a_1) = \theta(a_2)$ is an *A-stopper* or a *non-stopper*, then $f(a_1) = f(a_2)$ so $a_1 = a_2$ by injectivity of f . If $\theta(a_1) = \theta(a_2)$ is a *B-stopper*, then $a_1 = g(\theta(a_1)) = g(\theta(a_2)) = a_2$. Therefore θ is injective.

Now suppose that $b \in B$ is an *A-stopper* or a *non-stopper*, so there is $a \in A$ such that $b = f(a) = \theta(a)$. on the other hand, suppose that $b \in B$ is a *B-stopper*. Therefore $\theta(g(b)) = b$. Therefore θ is surjective, and hence a bijection.