MA10209 Algebra 1A

Sheet 4 Problems and Solutions v1: GCS

24-x-11

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

Hand in work to your tutor by 13:00, Monday Oct 31.

1. Suppose that p is a prime number and that $p > 3$. Prove that there is a natural number m such that $p = 6m + 1$ or $p = 6m - 1$.
   Solution Each natural number is of the form $6m - 1, 6m, 6m + 1$, $6m + 2$, $6m + 3$ or $6m + 4$. Prime numbers $p > 3$ cannot be even, so they cannot be of the form $6m, 6m + 2$ or $6m + 4$. They cannot be divisible by 3, so they cannot be of the form $6m + 3$. The only remaining possibilities are the ones specified.

2. Prove that there infinitely many prime numbers of the form $4n + 3$, where n is a natural number. *Hint: modify Euclid's argument (given in lectures) that there are infinitely many prime numbers.*
   Solution We copy but modify Euclid's proof of the existence of infinitely many prime numbers that we mentioned in lectures. Suppose, for contradiction, that there are only finitely many prime numbers p_i $(1 \leq i \leq k)$ of the form $4n + 3$. Let N be the product of these primes. Therefore N is of the form $4m + 1$ or $4m + 3$. In the first case, look at a prime factor q of $N + 2$ which happens to be of the form $4q + 3$ (the numbers of the form $4m + 1$ are closed under multiplication, so there must be one). Now q divides N and $N + 2$ and so divides 2 which is absurd. Next suppose that N is of the form $4m + 3$. Now $N + 4$ is of similar form, and just as before it must have a prime factor q of the form $4t + 3$. Now q divides both N and $N + 4$ and so it divides 4. This is also absurd.

3. There are n glasses, and each glass contains the same amount of water. The glasses are big enough so that each one could hold all the water. It is allowed to pour from any glass to any second glass exactly as much water as the second glass held before the pouring began. For what values of n is it possible to collect all the water in one glass? *Experimenting with small values of n should give you some useful ideas.*
   Solution: Let there be 1 unit of water in each glass at the outset. Let glass i contain $a_i(t)$ units of water at time t. So $a_1(0) = a_2(0) = \ldots = a_n(0) = 1$. Time moves in unit steps. Let h_t be the g.c.d. of $a_1(t), a_2(t), \ldots, a_n(t)$. A pouring takes place after time t and before time $t + 1$ until we are stuck. It turns out that h_{t+1} must be either h_t or $2h_t$.

   Here is the algebra. Suppose that $x_1, \ldots, x_n$ are non-negative integers with $x_1 > x_2 \geq 0$ and their gcd is g. Let $y_1 = x_1 - x_2, y_2 = 2x_2$ and $y_i = x_i$ for all other i. Let $h = \gcd(y_1, y_2, \ldots, y_n)$. Clearly $g \mid h$. Also

   $$h \mid \gcd(2x_1 - 2x_2, 2x_2, 2x_3, \ldots, 2x_n)$$

$$= 2\gcd(x_1 - x_2, x_2, x_3, \ldots, x_n)$$
$$= 2\gcd(x_1, x_2, x_3, \ldots, x_n) = 2g.$$

Now $g \mid h \mid 2g$ so $h = g$ or $h = 2g$.

Therefore if all the water can eventually be put into one glass, then n must be a power of 2.

Conversely, if $n = 2^m$ is a power of 2, then all the water can be placed in one glass by the following procedure. Label the glasses with the binary strings from m zeros to m ones. The first round of pourings consist of emptying the contents of each glass labelled with a string ending in a 1 into the glass with the same label except the final digit is 0. Discard the odd labelled glasses, relabel the remaining glasses by erasing the final zero, and repeat the process until all the water is in one glass.

4. Let n be a natural number. Show that the sum of the largest odd divisors of $n+1$, $n+2$, …, $2n$ is a perfect square.
Solution The sum of the consecutive odd integers
$$1 + 3 + \cdots + (2m - 1)$$
is m^2 by induction on m. If N is a positive integer, then $N = 2^a b$ for unique non-negative integers a and b. We call b the *odd part* of N. The odd parts of the numbers $n+1$, $n+2$, …, $2n$ must be different since if natural numbers u and v have the same odd part, then one must divide the other. These odd parts are therefore the odd numbers from 1 to $2n-1$, and as we observed earlier, it is easy to show that this is n^2.

5. Suppose that you have ten distinct two-digit numbers. Is it necessarily true that one may choose two disjoint non-empty subsets so that their elements have the same sum? *Hint:* $10 \times 99 = 990 < 1024 = 2^{10}$.
Solution Select any 10 numbers in the given range. Their sum is less than 990. Consider all possible subsets of the set of 10 numbers. There are $2^{10} = 1024$ such sets, and all their sums are less than 990. By the Dirichlet (pigeon-hole) principle, two of the sums (that of the different sets A and B) must co-incide. If A and B are disjoint, we are done. Otherwise remove from both A and B all their common elements, and the resulting sets will do the job. You are guaraneeed not to end up with an empty set as one of your pair for several reasons, one of which is that the sum of the elements of a non-empty set of numbers is not 0.

6. Suppose that we have a set S of 15 positive integers x in the range $1 < x \leq 2011$. Suppose also that each pair of elements of S is coprime. Prove that S contains a prime number.
Solution Suppose, for contradiction, that S contains no prime number. For each $s \in S$ let p_s denote the smallest prime divisor of s. Coprimality ensures that the primes p_s are distinct. The 15th smallest prime is 47. Thus there is $t \in S$ with $p_t \geq 47$. Now t is not prime and its smallest prime divisor is at least 47, so $t \geq 47^2 > 2011$. This is absurd.

7. Suppose that $m, n \in \mathbb{N}$. The *lowest common multiple* of m and n is the smallest positive integer into which they both divide. It is written $\operatorname{lcm}(m, n)$. Prove that
$$\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn.$$
Hint: what happens when m and n are powers of the same prime number?
Solution Let $p_1, p_2, \ldots, p_k$ be a complete list (without repetition) of the prime divisors of mn. Suppose that $m = \prod_{i=1}^{k} p_i^{a_i}$ and $n = \prod_{i=1}^{k} p_i^{b_i}$ where each a_i and b_i is a non-negative

integer. From the Fundamental Theorem of Arithmetic, we have $\gcd(m,n) = \prod_{i=1}^{k} p_i^{c_i}$ and $\mathrm{lcm}(m,n) = \prod_{i=1}^{k} p_i^{d_i}$ where for each i, $c_i = \min\{a_i, b_i\}$ and $d_i = \max\{a_i, b_i\}$. The result now follows from the observation that if $x, y \in \mathbb{R}$, then $x + y = \min\{x, y\} + \max\{x, y\}$.

8. (Interesting) Suppose that n is a positive integer. Show that $f(n) = 2^{2^n} + 2^{2^{n-1}} + 1$ has at least n different prime factors. *Hint: the polynomial $x^4 + x^2 + 1$ has a non-trivial factorization.*
Solution Observe that $f(1) = 7$ and so the result holds when $n = 1$. We now seek on induction argument, and we may assume that $n > 1$.

Observe the polynomial factorization

$$x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1).$$

Put $x = 2^{2^{n-2}}$ so

$$2^{2^n} + 2^{2^{n-1}} + 1 = (2^{2^{n-1}} - 2^{2^{n-2}} + 1)(2^{2^{n-1}} + 2^{2^{n-2}} + 1).$$

The factors in the right are coprime. This is because they are odd, and any common factor would have to divide their difference which is a power of 2. Choose a prime factor of $2^{2^{n-1}} - 2^{2^{n-2}} + 1$ (which therefore cannot be a prime factor of $2^{2^{n-1}} + 2^{2^{n-2}} + 1$) and finish by induction on n.

9. Let $F_0 = 0$ and $F_1 = 1$. Let $F_n = F_{n-1} + F_{n-2}$ for all integers $n > 1$. This is the *Fibonacci sequence*. Prove that $\gcd(F_n, F_{n-1}) = 1$ for all $n \in \mathbb{N}$.
Solution Suppose that m is a natural number and m divides F_n and F_{n-1} for some positive integer n. Then m divides $F_n - F_{n-1} = F_{n-2}$. Repeating this argument finitely many times (if you like, a finite reverse induction) we discover that m divides $F_1 - F_0 = 1$. Therefore $\gcd(F_m, F_{m-1}) = 1$.

10. (Harder) Using the Fibonacci sequence defined in Question 9, prove that

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

for all $m, n \in \mathbb{N}$.
Solution Not yet!

Here is the solution to Problem 10 on Sheet 2. *Prove that there exist two functions $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f \circ g$ is strictly decreasing and $g \circ f$ is strictly increasing.* This is problem 1, day 1 of the 4th Romanian Master of Mathematics Competition, 25–ii–2011, Bucharest. The authors were Andrzej Komisarski & Marcin Kuczma of Poland.
Solution Let

$$A = \bigcup_{k \in \mathbb{Z}} \left(\left[-2^{2k+1}, -2^{2k} \right) \cup \left(2^{2k}, 2^{2k+1} \right] \right);$$

$$B = \bigcup_{k \in \mathbb{Z}} \left(\left[-2^{2k}, -2^{2k-1} \right) \cup \left(2^{2k-1}, 2^{2k} \right] \right).$$

If $X \subseteq \mathbb{R}$, we introduce the notation $2X = \{2x \mid x \in X\}$ and $-X = \{-x \mid x \in X\}$. Notice that $A = 2B$, $B = 2A$, $A = -A$, $B = -B$, $A \cap B = \emptyset$, $A \cup B \cup \{0\}$. Since neither A nor B contains 0, we have a partition $\mathbb{R} = A \cup B \cup \{0\}$.

Define $f : \mathbb{R} \longrightarrow \mathbb{R}$ by $f(x) = x$ if $x \in A$, $f(x) = -x$ if $x \in B$ and $f(0) = 0$. Define $g : \mathbb{R} \longrightarrow \mathbb{R}$ by $g(x) = 2f(x)\ \forall x \in \mathbb{R}$. Therefore $f(g(x)) = f(2f(x)) = -2x$ and $g(f(x)) = 2f(f(x)) = 2x$ for all $x \in \mathbb{R}$.

There were 6 UK students competing. Full marks on a question scored 7/7. Two British students produced perfect solutions, and another three scored 6, 6 and 5, so had minor imperfections in essentially correct solutions, and one failed to score on this question. The UK tied for first place on this problem, with Italy and Russia. See

`http://rmms.lbi.ro/index.php?id=results_math`