MA10209 Algebra 1A

Sheet 5 Problems: GCS

29-x-18

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 5th. The course diary is `http://people.bath.ac.uk/masgcs/`.

1. (a) Find $g = \gcd(75, 27)$ by means of a hand calculation.
   (b) Find integers λ_0 and μ_0 such that $75\lambda_0 + 27\mu_0 = g$.
   (c) Find all pairs of integers λ, μ such that $75\lambda + 27\mu = g$.

2. (a) Find $g = \gcd(8633, 13439)$ by means of a hand calculation.
   (b) Find integers λ_0 and μ_0 such that $8633\lambda_0 + 13439\mu_0 = g$.
   (c) Find all pairs of integers λ, μ such that $8633\lambda + 13439\mu = g$.
   (d) Show that there are positive integers a, b in the range $1 \le a, b \le 15$ such that a/b and $8633/13439$ differ by less than $1/2000$.

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 $\lambda u + \mu v = 1$.

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

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) $\mathbb{Z}_4$;
   (b) $\mathbb{Z}_5$;
   (c) $\mathbb{Z}_6$;
   (d) $\mathbb{Z}_7$

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

(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.*

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.

   (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 $\frac{a_1 c_1}{b_1 d_1} = \frac{a_2 c_2}{b_2 d_2}$.

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

   (d) Why is part (b) vital to ensure that these definitions in part (c) makes sense?

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

   (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.*

9. Suppose that p is a prime number.

   (a) In $\mathbb{Z}_p$, show that $[x]^2 = [y]^2$ if, and only if, $[x] = \pm[y]$.

   (b) In $\mathbb{Z}_p$, show that more than half the equivalence classes are squares.

   (c) Prove that, in $\mathbb{Z}_p$, every equivalence class is the sum of two squares.

10. (Challenge!) Find all positive integers a and b for which there are three consecutive positive integers at which the polynomial $P(X) = \frac{X^5+a}{b}$ evaluates to an integer.