

Topic 12 · Sheet A: Questions

Greatest common divisors, the euclidean algorithm and Bézout's lemma

Suggested time

About 75 minutes

Total marks

74

Questions

12

Builds on

Topics 1 to 11

How to use this sheet. Work on your own paper. The questions start gently and get harder; questions 11 and 12 are exam style. Marks are a guide to how much working is expected, roughly one minute per mark. You need divisor sets, greatest common divisors, the slow and fast euclidean algorithms, division with remainder and the backwards euclidean algorithm plus Topics 1 to 11.

Notation. $D(n) = \{d \in \mathbb{N} \mid d \text{ divides } n\}$, and $\gcd(a, b) = \max(D(a) \cap D(b))$, with $\gcd(0, 0) = 0$. Present the slow algorithm as a table with columns n, A_n, B_n and the action (subtract or swap); the fast algorithm with columns n, A_n, B_n, q_n, r_n ; and the backwards algorithm with columns n, C_n, D_n , starting from $C_N = 0$ and $D_N = (-1)^N$. Bézout's lemma is in the form $ad - bc = \gcd(a, b)$.

1

4 marks

- (a) List $D(28)$. [1]
- (b) List $D(45)$. [1]
- (c) Find $D(28) \cap D(45)$. Are 28 and 45 relatively prime? [1]
- (d) Find $\gcd(0, 17)$ and $\gcd(0, 0)$. [1]

2

4 marks

Use prime factorisations to find each greatest common divisor.

- (a) $\gcd(360, 84)$ [2]
- (b) $\gcd(2^5 \cdot 3^2 \cdot 7, 2^3 \cdot 3^4 \cdot 5)$ [1]
- (c) $\gcd(17, 51)$ [1]

3

6 marks

Run the slow euclidean algorithm on $a = 30, b = 12$.

- (a) Give the full table of steps. [4]
- (b) How many subtractions and how many swaps did it use? [1]
- (c) What is $\gcd(30, 12)$? [1]

4

6 marks

Run the fast euclidean algorithm on $a = 252$, $b = 198$.

- (a) Give the full table of steps, and state $\gcd(252, 198)$. [4]
- (b) What is N ? [1]
- (c) How many subtractions would the slow algorithm use on the same input? [1]

5

6 marks

Use division with remainder to find q and r with $a = qb + r$ and $0 \leq r < b$.

- (a) $a = 100$, $b = 7$ [1]
- (b) $a = 1234$, $b = 56$ [1]
- (c) $a = 56$, $b = 1234$ [1]
- (d) $a = 999$, $b = 37$ [1]
- (e) Find a if division by $b = 13$ gives $q = 8$ and $r = 5$. [1]
- (f) Use $\gcd(a, b) = \gcd(b, r)$ and part (b) to find $\gcd(1234, 56)$. [1]

6

6 marks

- (a) Find $\gcd(91, 91)$, $\gcd(91, 0)$ and $\gcd(91, 1)$. [1]
- (b) Use $\gcd(a, b) = \gcd(a, b - a)$ to find $\gcd(144, 145)$. [1]
- (c) Find $\gcd(14, 16)$. [1]
- (d) Which of the pairs $(35, 64)$, $(91, 65)$, $(17, 85)$, $(27, 64)$ are relatively prime? [3]

7

6 marks

Let $a = 30$ and $b = 12$.

- (a) Run the fast algorithm, recording $q_0, \dots, q_{N-1}$ and N . [1]
- (b) Run the backwards euclidean algorithm, giving the table of C_n and D_n . [3]
- (c) Check that $aD_0 - bC_0 = \gcd(30, 12)$. [2]

8

6 marks

Let $a = 252$ and $b = 198$, as in question 4.

- (a) Run the backwards euclidean algorithm, giving the table of C_n and D_n . [4]
- (b) Check that $aD_0 - bC_0 = \gcd(252, 198)$. [1]
- (c) Write down integers x and y with $252x + 198y = 18$. [1]

9

6 marks

This question explores the speed of the fast algorithm.

- (a) Run the fast algorithm on $a = 13, b = 8$. What are the q_n , and what is N ? [3]
- (b) Without writing out every row, how many steps does it take on $a = 144, b = 89$? [1]
- (c) How many steps does it take on $a = 144, b = 12$? [1]
- (d) The fast algorithm takes at most $2 \log_2(a) + 1$ steps. What bound does this give for $a = 144$? [1]

10

6 marks

Let $a = 21$ and $b = 8$.

- (a) Run the fast and backwards algorithms to find integers c and d with $21d - 8c = 1$. [4]
- (b) Use your answer to find $[x]_8$ with $[21]_8 \times [x]_8 = [1]_8$. [1]
- (c) Use your answer to find $[y]_{21}$ with $[8]_{21} \times [y]_{21} = [1]_{21}$. [1]

11

9 marks

Exam style. Let $a = 1071$ and $b = 462$.

- (a) Run the fast euclidean algorithm and state $\gcd(1071, 462)$. [3]
- (b) Check your answer by factorising 1071 and 462 into primes. [2]
- (c) Run the backwards algorithm to find c and d with $1071d - 462c = \gcd(1071, 462)$, giving the table of C_n and D_n . [3]
- (d) Check your c and d . [1]

12

9 marks

Exam style. Let $a = 13$ and $b = 5$.

- (a) Run the slow algorithm. Count the subtractions and the swaps. [3]
- (b) Run the fast algorithm. Check that the sum of the q_n equals the number of subtractions, and that N equals the number of swaps. [2]
- (c) Find c and d with $13d - 5c = 1$, giving the table of C_n and D_n . [3]
- (d) Hence find $[x]_{13}$ with $[5]_{13} \times [x]_{13} = [1]_{13}$. [1]

End of questions. Worked answers and the mark scheme are in the matching answers PDF.