inkMaths

ANSWER BOOK

# The Euclidean algorithm and Bezout's identity

Further Pure 2 · Year FM

7 questions · 28 marks

NAVY EDITION


inkphysics.co.uk/maths/ · youtube.com/@InkPhysics

## SECTION A · Warm-up

**A1** $1001 = 2 \times 357 + 287$; $357 = 1 \times 287 + 70$; $287 = 4 \times 70 + 7$; $70 = 10 \times 7 + 0$. The last non-zero remainder is **7**. M1 for the repeated division, A1 for a correct chain of divisions, A1 for 7. No factorisation of either number was needed. [3]

**A2** The highest common factor is the last non-zero remainder, **7**. Work back up the divisions, one line at a time. [3]
From the third line, $7 = 287 - 4 \times 70$.
Substituting $70 = 357 - 287$: $7 = 287 - 4(357 - 287) = 5 \times 287 - 4 \times 357$.
Substituting $287 = 1001 - 2 \times 357$: $7 = 5(1001 - 2 \times 357) - 4 \times 357 = \mathbf{5} \times 1001 - 14 \times 357$.
So $x = 5$ and $y = -14$. Check: $5005 - 4998 = 7$. M1 for working back through the divisions, A1 for a correct intermediate line, A1 for $x = 5$ and $y = -14$. Keep 287 and 70 as symbols until the end; multiplying them out early loses the structure and the method mark with it.

## SECTION B · Standard

**B1** $2024 = 2 \times 748 + 528$; $748 = 1 \times 528 + 220$; $528 = 2 \times 220 + 88$; $220 = 2 \times 88 + 44$; $88 = 2 \times 44 + 0$, so the factor is **44**. Unwinding: $44 = 220 - 2 \times 88 = 5 \times 220 - 2 \times 528 = 5 \times 748 - 7 \times 528 = \mathbf{19} \times 748 - 7 \times 2024$. Check: $14212 - 14168 = 44$. M1 for the divisions, A1 for 44, M1 for the back substitution, A1 for the Bezout form. [4]

**B2** $391 = 1 \times 299 + 92$; $299 = 3 \times 92 + 23$; $92 = 4 \times 23 + 0$, so the highest common factor is **23** and the numbers are not coprime. M1 for the algorithm, A1 for 23, B1 for the statement that they share a factor. (Indeed $391 = 17 \times 23$ and $299 = 13 \times 23$, though the algorithm found the factor without looking for it.) [3]

**B3** $26 = 2 \times 11 + 4$; $11 = 2 \times 4 + 3$; $4 = 1 \times 3 + 1$, so the numbers are coprime. Unwinding: $1 = 4 - 3 = 3 \times 4 - 11 = 3 \times 26 - 7 \times 11$. Reducing modulo 26 gives $-7 \times 11 \equiv 1$, so the inverse is $-7 \equiv \mathbf{19}$. M1 for the algorithm, A1 for the Bezout identity, M1 for reducing modulo 26, A1 for 19. Checking: $11 \times 19 = 209 = 8 \times 26 + 1$. [4]

**B4** The highest common factor of 12 and 45 is 3, which divides 6, so solutions exist. Had it not divided 6 there would be none. [4]
Euclid gives $45 = 3 \times 12 + 9$ and $12 = 1 \times 9 + 3$, so $3 = 12 - 9 = 12 - (45 - 3 \times 12) = 4 \times 12 - 45$.
Doubling: $6 = 8 \times 12 - 2 \times 45$, giving the particular solution $x = 8$, $y = -2$.
Adding $45/3 = 15$ to x and subtracting $12/3 = 4$ from y leaves the left-hand side unchanged, so the general solution is **x** $= 8 + 15t$, $y = -2 - 4t$ for integer t. B1 for checking that 3 divides 6, M1 for a particular solution, A1 for $x = 8$ and $y = -2$, A1 for the general form. Dividing by the highest common factor before forming those steps is essential; using 45 and 12 themselves gives only some of the solutions.

## SECTION C · Stretch

**C1** **The** algorithm. [7]

$84 = 1 \times 55 + 29$

$55 = 1 \times 29 + 26$

$29 = 1 \times 26 + 3$

$26 = 8 \times 3 + 2$

$3 = 1 \times 2 + 1$

$2 = 2 \times 1 + 0$

The last non-zero remainder is **1**, so the two numbers are **coprime**.
**Back** substitution. Take the lines in reverse, replacing one remainder at a time and never multiplying out:

$1 = 3 - 2$

$= 3 - (26 - 8 \times 3) = 9 \times 3 - 26$

$= 9(29 - 26) - 26 = 9 \times 29 - 10 \times 26$

$= 9 \times 29 - 10(55 - 29) = 19 \times 29 - 10 \times 55$

$= 19(84 - 55) - 10 \times 55 = \mathbf{19} \times 84 - 29 \times 55$.

So x = **19** and y = **−29**. Check: $1596 - 1595 = 1$.
**The** inverse. Reducing modulo 84 kills the 84 term, leaving $-29 \times 55 \equiv 1$, so the inverse of 55 is $-29 \equiv$ **55** (mod 84). Check: $55^2 = 3025 = 36 \times 84 + 1$, so 55 is its own inverse.
**General** solution. Adding 55 to x and subtracting 84 from y changes nothing, since $84 \times 55 - 55 \times 84 = 0$. So **x** $= 19 + 55t$, $y = -29 - 84t$ for integer t.
M1 A1 for the algorithm, A1 for the coprimality statement, M1 A1 for the back substitution, B1 for the inverse, A1 for the general solution.
Six divisions is long for a pair this size. That is what consecutive Fibonacci-like numbers do to the algorithm, and it is exactly when a slip in one quotient quietly wrecks every line below it. Check the identity at the end.