InkMaths

ANSWER BOOK

Modular arithmetic and Fermat's little theorem

Further Pure 2 · Year FM

7 questions · 27 marks

NAVY EDITION

inkphysics.co.uk/maths

SECTION A · Warm-up

A1 7 is prime and 3 is not a multiple of it, so Fermat gives $3^6 \equiv 1 \pmod 7$. Reducing the exponent: $100 = 16 \times 6 + 4$, so $3^{100} \equiv 3^4 = 81$. Finally $81 = 11 \times 7 + 4$, so the residue is **4**. M1 for using Fermat, M1 for reducing the exponent, A1 for the residue 4. [3]

A2 The last digit is the residue modulo 10. Powers of 7 give 7, 9, 3, 1 and then repeat, so $7^4 \equiv 1 \pmod{10}$. Since 2024 is a multiple of 4, $7^{2024} \equiv 1$ and the last digit is **1**. M1 for working modulo 10, A1 for the cycle of length 4, A1 for the last digit. Fermat does not apply directly here, because 10 is not prime, but the cycle is still there. [3]

SECTION B · Standard

B1 Since 5 and 13 are coprime, 5 has an inverse. Trying multiples: $5 \times 8 = 40 = 3 \times 13 + 1$, so the inverse is 8. Multiplying both sides gives $x \equiv 32 \pmod{13}$, and $32 = 2 \times 13 + 6$, so $x \equiv \mathbf{6} \pmod{13}$. M1 for seeking the inverse of 5, A1 for the inverse 8, M1 for multiplying through, A1 for the residue 6. Checking: $5 \times 6 = 30 = 2 \times 13 + 4$. [4]

B2 Since $10 \equiv -1 \pmod{11}$, powers of 10 alternate between 1 and -1, so a number is congruent to its alternating digit sum taken from the right. For 8294 that is $4 - 9 + 2 - 8 = -11$, a multiple of 11, so **8294** is divisible (it is 11×754). For 8291 it is $1 - 9 + 2 - 8 = -14$, which is not, so **8291** is not. B1 for $10 \equiv -1 \pmod{11}$, M1 for the alternating digit sum, A1 for 8294, A1 for 8291. [4]

B3 Every integer is congruent to one of 0, ±1, ±2, ±3, ±4 modulo 9, and cubing those gives 0, ±1, ±8, ±27, ±64. Reducing: $\pm 8 \equiv \mp 1$, $\pm 27 \equiv 0$ and $\pm 64 \equiv \pm 1$. So the only residues that occur are **0,** 1 and 8, that is 0 and ±1. M1 for considering every residue mod 9, A1 for the reduced cubes, A1 for the conclusion. Any integer claimed to be a cube must pass that test. [3]

B4 First reduce the base: $15 \equiv 2 \pmod{13}$, so the problem becomes 2^{81}. Since 13 is prime and 2 is not a multiple of it, Fermat gives $2^{12} \equiv 1$, so the exponent may be reduced modulo 12.
$81 = 6 \times 12 + 9$, leaving $2^9 = 512$. Finally $512 = 39 \times 13 + 5$, so the remainder is **5**. M1 for reducing the base, M1 for reducing the exponent by Fermat, A1 for $2^9 = 512$, A1 for the remainder 5. Reducing the base and the exponent separately kept every number below 512; reducing the exponent modulo 13 rather than 12 is the standard error. [4]

SECTION C · Stretch

C1 [6]

$42 = 2 \times 3 \times 7$, three distinct primes. Show that each divides $n^7 - n$, and since they are pairwise coprime their product must divide it too. That last sentence is a mark on its own; without it the three parts prove nothing together.

Mod 7. Fermat's little theorem gives $n^7 \equiv n \pmod 7$ directly, so 7 divides $n^7 - n$. Use the $n^p \equiv n$ form, not $n^{p-1} \equiv 1$, which needs n not to be a multiple of 7. The first form holds for every n, including the multiples.

Mod 3. Fermat gives $n^3 \equiv n \pmod 3$. Then $n^7 = (n^3)^2 n \equiv n^2 \cdot n = n^3 \equiv n$, so 3 divides $n^7 - n$.

Mod 2. Fermat gives $n^2 \equiv n \pmod 2$. Then $n^7 = (n^2)^3 n \equiv n^3 \cdot n = n^4 \equiv n$, so 2 divides $n^7 - n$. Checking n even and n odd separately does the same job in one line.

Each of 2, 3 and 7 divides $n^7 - n$, and they share no factor, so **42** divides $n^7 - n$ for every integer n.

B1 for $42 = 2 \times 3 \times 7$ with the coprime argument, B1 for the mod 7 case, M1 for reducing n^7 modulo 3, A1 for 3 dividing $n^7 - n$, M1 for reducing n^7 modulo 2, A1 for 2 dividing $n^7 - n$.

The choice of 7 is not an accident. The same argument shows p divides $n^p - n$ for any prime p, and 42 is the product of every prime q for which $q - 1$ divides 6.