inkMaths

ANSWER BOOK

Modular arithmetic and Fermat's little theorem

Further Pure 2 · Year FM

6 questions · 21 marks

NAVY EDITION

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. [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. 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 $x \equiv$ 6 (mod 13). 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. [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. Any integer claimed to be a cube must pass that test. [3]

SECTION C · Stretch

C1 First reduce the base: $15 \equiv 2 \pmod{13}$, so the problem is 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. Reducing base and exponent kept every number below 512. [4]