- 1. Find the highest common factor of 12345 and 54321.
- 2. Find integers x and y with 76x + 45y = 1. Do there exist integers x and y with 3381x + 2646y = 21?
- 3. Prove that if a is coprime to b and also to c then it is coprime to bc. Give two proofs: one based on Euclid's algorithm / Bezout's theorem and one based on prime factorisation.
- 4. Show that a positive integer n is a multiple of 9 if and only if the sum of its digits is a multiple of 9.
- 5. The Fibonacci numbers F_1, F_2, F_3, \ldots are defined by: $F_1 = F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all n > 2 (so eg. $F_3 = 2$, $F_4 = 3$, $F_5 = 5$). Is F_{2020} even or odd? Is it a multiple of 3?
- 6. Solve (ie. find all solutions of) the equations
- (i) $7x \equiv 77 (40)$
- (ii) $12y \equiv 30 \ (54)$
- (iii) $3z \equiv 2$ (17) and $4z \equiv 3$ (19).
- 7. An RSA encryption scheme (n, e) has modulus n = 187 and coding exponent e = 7. By prime-factorising n, find a suitable decoding exponent d. Check your answer (without electronic assistance) by encoding the number 35 and then decoding the result.
- 8. Explain (without electronic assistance) why 23 cannot divide $10^{881} 1$.
- 9. Let p be a prime of the form 3k + 2. Show that, in \mathbb{Z}_p , the only solution to $x^3 = 1$ is x = 1. Deduce, or prove directly, that every element of \mathbb{Z}_p has a cube root.
- 10. By considering numbers of the form $(2p_1p_2...p_k)^2 + 1$, prove that there are infinitely many primes of the form 4n + 1.
- 11. What is the 5th-last digit of $5^{5^{5^5}}$?
- 12. Is there a positive integer n for which $n^7 77$ is a Fibonacci number?
- 13. Let a and b be distinct positive integers, with a < b. Prove that every block of b consecutive positive integers contains two distinct numbers whose product is a multiple of ab. If a, b and c are distinct positive integers, with a < b < c, must every block of c consecutive positive integers contains three distinct numbers whose product is a multiple of abc?
- $^{+}14$. Let n and k be positive integers. Suppose that n is a kth power (mod p) for all primes p. Must n be a kth power?