MATH3320 HW10 (Solution)
Outline of methods and proofs with remarks

(1) \( x^2 \equiv 1 \pmod{561} \) if and only if \( x \equiv 1 \) or \( -1 \pmod{3} \), \( \pmod{11} \) and \( \pmod{17} \) respectively. Therefore, the Chinese Remainder Theorem tells us that there are exactly 8 solutions modulo 561, which are 1, 188, 307, 67, 254, 373, 494, 560 \( \pmod{561} \). (cross reference: HW8, p.64, Q39)

(2) Textbook problems:
p.122, Q1 Fermat’s Theorem says that \( x^{13} \equiv x \pmod{13} \) and \( x^5 \equiv x \pmod{5} \) for all \( x \) (Note: including the case \( x \equiv 0 \)). Therefore one can keep using these formulae to reduce the given polynomial \( f(x) \) to a small-enough-degree polynomial \( g(x) \). (If the question asks you to find all the solutions of \( f(x) \), you can do that by trial-and-error since the degree of \( g(x) \) is small.)

For (a), \( f(x) \equiv x^5 + 3x - 4 \pmod{13} \). For (b), \( f(x) \equiv 4x^4 + 4x^3 + 4x^2 + 4x + 1 \pmod{5} \).

- Alternatively use long division by \( x^p - x \) as in the class notes.

Q12 Let \( f(x) = x^{71} - 1 \). Modulo 7, \( f(x) \equiv 0 \) has a unique solution \( x \equiv 1 \). \( f'(1) \equiv 71 \not\equiv 0 \) and therefore there is exactly one root modulo 7\(^j\) for any \( j \geq 1 \). Modulo 11, \( f(x) \equiv 0 \) has a unique solution \( x \equiv 1 \). Also \( f'(1) \equiv 71 \not\equiv 0 \) and therefore there is exactly one root modulo 11\(^k\) for any \( k \geq 1 \). Therefore, for all positive choices of \( j \) and \( k \), the Chinese Remainder Theorem guarantees that \( f(x) \equiv 0 \pmod{7^j \cdot 11^k} \) has a unique solution.

Q16 Let \( f(x) \equiv x^{35} + \cdots + x + 1 \). The trick is: \( x(x-1)f(x) \equiv x^{37} - x \equiv x(x-1)(x-2)\cdots(x-36) \pmod{37} \). Second equality follows from Fermat’s Theorem and polynomial factorization. Therefore, \( f(x) \equiv 0 \pmod{37} \) has solutions \( x \equiv 2, 3, \cdots, 36 \pmod{37} \) and hence there are 35 solutions.

(3) \( 1 + \sqrt{2} \) is a generator.