# SOLUTIONS TO HOMEWORK 5

**1.** (a) Write $f(x) = x^4 + x + 4$. Then $f(1) \equiv 0 \pmod 3$, and $f'(x) = 4x^3 + 1$, so that $3^0 \| f'(1)$. Put $x_0 = 1$. Then by applying the Hensel iteration,

$$x_1 \equiv x_0 - f(x_0)f'(x_0)^{-1} \equiv 1 - (-1) \cdot 6 \equiv -2 \pmod 9$$

solves $f(x_1) \equiv 0 \pmod{3^2}$, and

$$x_2 \equiv x_1 - f(x_1)f'(x_1)^{-1} \equiv -2 - (-1) \cdot 18 \equiv 16 \pmod{27}$$

solves $f(x_2) \equiv 0 \pmod{27}$. So $x = 16$ solves the congruence in question.

(b) One has $x^2+4x+18 \equiv 0 \pmod{49}$ only if $(x+2)^2+14 \equiv 0 \pmod 7$, whence $x+2 \equiv 0 \pmod 7$. But then $(x+2)^2 \equiv 0 \pmod{49}$, so that the congruence in question is soluble only when $14 \equiv 0 \pmod{49}$, giving a contradiction. Then the congruence is not soluble.

**2.** (a) Suppose that $a$ belongs to $h$ modulo $p$, and that $h = 2n$ is even. Then since $a^{2n} \equiv 1 \pmod p$, one has $a^n \equiv \pm 1 \pmod p$. But $a$ belongs to $2n$ modulo $p$, so that necessarily $a^n \not\equiv 1 \pmod p$. Thus we have $a^{h/2} \equiv -1 \pmod p$.

(b) If $a^{2n} \equiv 1 \pmod{p^k}$ $(k \geqslant 2)$, then $(a^n + 1)(a^n - 1) \equiv 0 \pmod{p^k}$. But since $(a^n - 1, a^n + 1) = (a^n - 1, 2) = 1$ or $2$, the latter congruence implies that when $p \neq 2$, one has $p^k | (a^n + 1)$ or $p^k | (a^n - 1)$. The second case contradicts the fact that $a$ has order $h$, and thus we deduce that $a^{h/2} \equiv -1 \pmod{p^k}$.

**3.** On combining Fermat's Little Theorem with Lagrange's Theorem, we find that the congruence $x^p \equiv x \pmod p$ has precisely $p$ solutions, namely $0, 1, \ldots, p-1$ modulo $p$. Put $f(x) = x^p - x$. Then $f'(x) = px^{p-1} - 1$ is coprime to $p$ for these congruence classes, and so it follows from Hensel's lemma that for each $j$ with $j \geqslant 1$, and for each $r$ with $0 \leqslant r \leqslant p - 1$, there is a unique integer $x$ satisfying $x^p \equiv x \pmod{p^j}$ and $x \equiv r \pmod p$. Thus, for every natural number $j$, the congruence $x^p \equiv x \pmod{p^j}$ has precisely $p$ solutions.