SOLUTIONS TO HOMEWORK 5

1. (a) If $x^2 - x \equiv 0 \pmod{p^k}$, then $p^k | x(x-1)$. But $(x, x-1) = (x, -1) = 1$, so the latter implies that $p^k | x$ or $p^k | (x-1)$, whence $x \equiv 0 \pmod{p^k}$ or $x \equiv 1 \pmod{p^k}$. Plainly, both of these residue classes yield a solution, so we find that the congruence $f(x) \equiv 0 \pmod{p^k}$ has precisely two solutions for each k.

(b) Let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. Then $N(m)$ is a multiplicative function of m satisfying $N(p^k) = 2$ for each prime power p^k. Thus, writing r for the number of different prime numbers dividing m,we obtain

$$N(m) = \prod_{p^k \| m} N(p^k) = \prod_{p | m} 2 = 2^r.$$

2. (a) The Euclidean Algorithm supplies integers r and s with $r(p-1) + sn = (n, p-1) = 1$, so that $(x^n)^s (x^{p-1})^r = x^{ns + r(p-1)} \equiv x \pmod{p}$. If $x^n \equiv a \pmod{p}$, then as a consequence of Fermat's Little Theorem, one obtains $x \equiv a^s \pmod{p}$, and so we conclude that the congruence has precisely one solution.

(b) Suppose that $(n, p-1) = d$, and that $x^n \equiv 1 \pmod{p}$. By the Euclidean algorithm, there exist integers u and v with $nu + (p-1)v = (n, p-1) = d$. Then by Fermat's Little Theorem, one has $x^d \equiv (x^n)^u (x^{p-1})^v \equiv 1 \pmod{p}$. We saw in class that when $d | (p-1)$, the congruence $y^d \equiv 1 \pmod{p}$ has precisely d solutions modulo p, and so it follows that there are precisely d solutions for x.

3. (a) Write $f(x) = x^4 + x + 1$. 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,

$$x_1 \equiv x_0 - f(x_0) f'(x_0)^{-1} \equiv 1 - (-1) \cdot 3 \equiv 4 \pmod 9$$

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

$$x_2 \equiv x_1 - f(x_1) f'(x_1)^{-1} \equiv 4 - (-1) \cdot 261 \equiv 265 \equiv -5 \pmod{27}$$

solves $f(x_2) \equiv 0 \pmod{27}$. So $x = -5$ solves the congruence in question.

(b) One has $x^2 + 6x + 31 \equiv 0 \pmod{121}$ only if $(x+3)^2 + 22 \equiv 0 \pmod{11}$, whence $x + 3 \equiv 0 \pmod{11}$. But then $(x+3)^2 \equiv 0 \pmod{121}$, so that the congruence in question is soluble only when $22 \equiv 0 \pmod{121}$, giving a contradiction. Then the congruence is not soluble.

4. (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 $a^{h/2} \equiv -1 \pmod{p^k}$.

5. 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.