SOLUTIONS TO HOMEWORK 4

1. (i) By inspection (or by observing that $(\frac{1}{2}(p-1)!)^2 \equiv -1 \pmod p$ when $p \equiv 1 \pmod 4$), one finds that $2^2 \equiv -1 \pmod 5$ and $4^2 \equiv -1 \pmod{17}$. It therefore follows that whenever $x \equiv 2 \pmod 5$ and $x \equiv 4 \pmod{17}$, then $x^2 \equiv -1 \pmod{85}$. But a solution of the congruence $17y_1 \equiv 1 \pmod 5$ is given by $y_1 = 3$, and a solution of the congruence $5y_2 \equiv 1 \pmod{17}$ is given by $y_2 = 7$. Then since $85 = 5 \cdot 17$, it follows from the Chinese Remainder Theorem that a solution of the desired type is

$$x = 17 \cdot 3 \cdot 2 + 5 \cdot 7 \cdot 4 = 242 \equiv -13 \pmod{85}.$$

(ii) The congruence $x^2 \equiv -1 \pmod 5$ has the 2 solutions $x \equiv \pm 2 \pmod 5$, and the congruence $x^2 \equiv -1 \pmod{17}$ has the 2 solutions $x \equiv \pm 4 \pmod{17}$. Then, by the Chinese Remainder Theorem, the congruence $x^2 \equiv -1 \pmod{85}$ has $2 \cdot 2 = 4$ solutions modulo 85.

2. (i) By Fermat's Little Theorem, for all integers a one has $a^p \equiv a \pmod p$, and hence $a^p - a + 1 \equiv 1 \pmod p$. Thus we see that $x^p - x + 1 \equiv 0 \pmod p$ has no integral solution.
(ii) If $(x, 40) = d$, then $d|(x^{16} - x)$. Consequently, if $x^{16} - x + 3 \equiv 0 \pmod{40}$, we see that $x^{16} - x + 3 \equiv 0 \pmod d$, and hence $d|3$. But $d|40$ and $(40, 3) = 1$, and so $d = 1$. Observe next that $\varphi(40) = \varphi(8)\varphi(5) = 4 \cdot 4 = 16$. Thus, when $(a, 40) = 1$, it follows from Euler's theorem that $a^{16} \equiv 1 \pmod{40}$. In such circumstances, it follows that $a^{16} - a + 3 \equiv 4 - a \pmod{40}$. Then if $(x, 40) = 1$, we have $x^{16} - x + 3 \equiv 0 \pmod{40}$ if and only if $x \equiv 4 \pmod{40}$, yet $(4, 40) \neq 1$, so we arrive at a contradiction. Hence, the equation $x^{16} - x + 3 \equiv 0 \pmod{40}$ has no solutions.

3. One has $561 = 3 \cdot 11 \cdot 17$. By Fermat's Little Theorem, whenever $(a, 561) = 1$, one has $a^2 \equiv 1 \pmod 3$ because $(a, 3) = 1$, and $a^{10} \equiv 1 \pmod{11}$ because $(a, 11) = 1$, and $a^{16} \equiv 1 \pmod{17}$ because $(a, 17) = 1$. Hence, for all integers a with $(a, 561) = 1$ one has

$$\begin{aligned} a^{560} &= (a^2)^{280} \equiv 1 \pmod 3, \\ a^{560} &= (a^{10})^{56} \equiv 1 \pmod{11}, \\ a^{560} &= (a^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Thus we conclude that $a^{560} \equiv 1 \pmod{561}$, since $561 = 3 \cdot 11 \cdot 13$.

4. (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

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

5. (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.