Homework 4

Section 1.5:

For Ex 5 see pg 299.

4. (i) Consider the given polynomial over $\mathbb{Z}_2$. If $[x]_2 = [0]_2$, then $[0]_2^4 + [0]_2^2 + [1]_2 = [1]_2 \neq [0]_2$; while for $[x]_2 = [1]_2$, $[1]_2^4 + [1]_2^2 + [1]_2 = [1]_2 \neq [0]_2$. Thus $x^4 + x^2 + 1$ has no roots over $\mathbb{Z}_2$, and thus has also no integer roots.

Over $\mathbb{Z}_3$, $x^4 + x^2 + 1 = x^4 + 4x + 4 = (x^2+2)^2 = (x^2-1)^2 = (x+1)^2(x-1)^2$. Thus $[1]_3$, and $[2]_3$ are both roots for this polynomial over $\mathbb{Z}_3$.

(ii) If $[x]_3 = [0]_3$, we see that $7[0]_3^3 - 6[0]_3^2 + 2[0]_3 - [1]_3 = -[1]_3 \neq [0]_3$; while when $[x]_3 = [1]_3$, we get $7[1]_3^3 - 6[1]_3^2 + 2[1]_3 - [1]_3 = [2]_3 \neq [0]_3$, or when $[x]_3 = [2]_3$, we get $7[2]_3^3 - 6[2]_3^2 + 2[2]_3 - [1]_3 = [2]_3 \neq [0]_3$. As above it follows that the given polynomial has no integer solutions.

Section 1.6:

For Ex. 1, 2, 5, 6 see pg 299.

3. We need to show that $a^5 \equiv a \mod 10$ for all positive numbers a. We could use induction to do so, but in this section we prefer to apply Euler's Theorem. Let us first notice that if a is not a multiple of 5 then, by Fermat's theorem or by Euler's Theorem, we have $a^4 \equiv 1 \mod 5$ since $\varphi(5) = 4$. Thus $a^5 \equiv a \mod 5$. On the other hand if a is a multiple of 5, then $a^5 \equiv a \mod 5$ is certainly true. Therefore for any positive number a, we always have $a^5 \equiv a \mod 5$. A similar reasoning provides $a^5 \equiv a \mod 2$. Since the least common multiple of 2 and 5 is 10, we may combine these two congruences to get $a^5 \equiv a \mod 10$.

7. Let m be a number of among $2, 3, 5, 7, 13$. If m divides n, this implies that m

divides $n^{13} - n$. Thus we may assume that m and n are relatively prime. Observe that $\varphi(2) = 1, \varphi(3) = 2, \varphi(5) = 4, \varphi(7) = 6, \varphi(13) = 12$. By Euler's Theorem, we have $n^{\varphi(m)} \equiv 1 \mod m$ but since $\varphi(m)$ divides 12, we deduce that $n^{12} \equiv 1 \mod m$. Thus $n^{13} \equiv n \mod m$.

8. Suppose that p is prime, $p|n$ but $p^2 \not| n$. Then we can write $n = pm$ with $(p, m) = 1$. By Euler's Theorem, $p^{\varphi(m)} \equiv 1 \mod m$ but $\varphi(n) = \varphi(p \cdot m) = \varphi(p)\varphi(m)$, so we have $p^{\varphi(n)} \equiv 1 \mod m$. Then

$$p^{\varphi(n)+1} \equiv p \mod mp$$

$$\equiv p \mod n.$$

We may generalize the previous conclusion to higher powers of p. We assume that p is a prime, $p^k|n$ but $p^{k+1} \not| n$. Let $n = p^k m$ where $(p, m) = 1$ then $p^{\varphi(m)} \equiv 1 \mod n$. But $\varphi(n) = \varphi(p^k m) = \varphi(p^k)\varphi(m)$, so $p^{\varphi(n)} \equiv 1 \mod m$. So

$$p^{\varphi(n)+k} \equiv p^k \mod m \cdot p^k$$

$$\equiv p^k \mod n.$$

10. (i) By assumption, $2^p \equiv 1 \mod q$. By Fermat's Theorem, $2^{q-1} \equiv 1 \mod q$. Let a be the order of 2 in $\mathbb{Z}_q$. It follows that $a|p$. But p is a prime, therefore $a = p$. Since we have also $a|q - 1$, we deduce $p|q - 1$.

(ii) Assume that q is a prime divisor of $2^{37} - 1$. By part (i), $37|q - 1$. So $q = 37k + 1$ for some k. Since $2^{37} - 1$ is odd, we deduce that k must be an even number. We write $k = 2t$, and then $q = 74t + 1$. Substituting $t = 1, 2, ...$, we get $75, 149, ...$ and test them if they divide $2^{37} - 1$. We find that $2^{37} - 1 = 223 \times 616318177$.