WRITTEN HW #7 SOLUTIONS

(1) (10 points) Find all solutions to $x^2 + 3x + 3 \equiv 0 \bmod 7^3$. All calculations should be done by hand.

Solution. Because of the hand calculation restriction, we will start by looking for solutions to $x^2 + 3x + 3 \equiv 0 \bmod 7$ and then use Hensel's Lemma. Trial and error on $x^2 + 3x + 3 \equiv 0 \bmod 7$ yield solutions of $x \equiv 1, 3 \bmod 7$. Notice that once you discover these two roots you can stop, because you know that quadratic polynomials always have at most 2 roots mod primes p.

Now we apply Hensel's Lemma. First, if $f(x) = x^2 + 3x + 3$, then $f'(x) = 2x + 3$. Notice that $f'(1) = 5, f'(3) = 9$ are both not divisible by 7, so $1, 3 \bmod 7$ will each lift to a unique solution mod $7^3 = 343$. We can either use brute force, or think about solving a linear congruence. Let us take the latter approach.

From the proof of Hensel's Lemma, we want to try to solve $q + f'(1)k \equiv 0 \bmod p$, where $p = 7, f(1) = q \cdot 7$, and k is the variable, if we want to lift $1 \bmod 7$ to a solution $\bmod 7^2$. Recall that with this solution k, the lift of $x_1 = 1$ that solves $f(x) \equiv 0 \bmod 7^2$ is given by $x_2 = x_1 + k \cdot 7^1$. Since $f(1) = 7, q = 1$, and the linear equation we want to solve is $1 + 5k \equiv 0 \bmod 7$, so $k = 4$. This means that $x_2 = 1 + 4 \cdot 7 = 29$ is the lift of $1 \bmod 7$ to integers mod 49 which solves $f(x) \equiv 0 \bmod 7^2$.

We repeat the procedure again, with $f(29) = 931 = 7^2 \cdot 19$. This time, $q = 19 \equiv 5 \bmod 7$, so the linear congruence we want to solve is $5 + 5k \equiv 0 \bmod 7$, which has solution $k \equiv -1 \equiv 6 \bmod 7$. Therefore $x_3 = 29 - 49 = -20$ is the lift of 29 mod 49 which solves $f(x) \equiv 0 \bmod 7^3$. As a matter of fact, one can check that $f(-20) = 7^3$.

For $x \equiv 3 \bmod 7$, since $f(3) = 21 = 7 \cdot 3$, the first congruence we solve is $3 + 2k \equiv 0 \bmod 7$, so $k = 2$, and $x_2 = 3 + 2 \cdot 7 = 17$. As a matter of fact, one calculates that $f(17) = 343 = 7^3$, so this is also a solution to $f(x) \equiv 0 \bmod 7^3$; Hensel's Lemma guarantees that it is the unique lift of $3 \bmod 7$ which solves this polynomial congruence.

In summary, the solutions to this polynomial congruence are $x \equiv -20, 17 \bmod 343$. $\square$

(2) (10 points) Show that $x^3 \equiv 9 \bmod 11^n$ always has a solution if $n \geq 1$.

Solution. This is another problem which uses Hensel's Lemma. We will solve this problem by induction. First, we show this congruence has a solution mod 11. Trial and error shows that $x \equiv 4 \bmod 11$ solves $x^3 \equiv 9 \bmod 11$. Let $f(x) = x^3 - 9$. Notice that $f'(4) = 3(4)^2 = 48$ is not divisible by 11. Therefore, $x_1 = 4$ lifts to a solution $x_2 \bmod 11^2$ which solves $f(x) \equiv 0 \bmod 11^2$.

Suppose we know that $f(x) \equiv 0 \bmod 11^n$ has a solution x_n which is a lift of $x_1 = 4$ (ie, $x_n \equiv 4 \bmod 11$). Then $f'(x_n) \equiv f'(x_1) \bmod 11$, so in particular

$11 \nmid f'(x_n)$. Then we can apply Hensel's Lemma to conclude that there exists an x_{n+1} which solves $f(x) \equiv 0 \bmod 11^{n+1}$ and $x_{n+1} \equiv x_n \equiv x_1 \bmod 11$.

By induction, we can find an infinite sequence of integers $x_1, x_2 \ldots$, such that $x_n \equiv 4 \bmod 11$, and $f(x_n) \equiv 0 \bmod 11^n$. □

(3) (10 points) Suppose G is a cyclic group of order n with generator g. Recall that the order of every element in G divides n. Suppose $d \mid n, d \geq 1$. How many elements of G have order d? What are they, in terms of g?

Solution. We claim that there are $\phi(d)$ elements of order d, and that they are $g^{k\frac{n}{d}}$, where k is an integer satisfying $1 \leq k \leq d, \gcd(k,d) = 1$. (Obviously, there are exactly $\phi(d)$ possible values of k.)

First, notice all of these elements of G really do have order d. Indeed, raising them to the dth power gives $g^{kn} = e$ (e is the identity element of G). On the other hand, no smaller power will give e, because if $1 \leq i < d$, then $(g^{kn/d})^i = g^{ikn/d}$, and since $\gcd(k,d) = 1$, the number ik/d is not an integer (if it were, then $d \mid ik \Rightarrow d \mid i$, a contradiction). Therefore, $n \nmid (ikn/d)$, so $g^{ikn/d} \neq e$.

Now we show that these are all the elements of order d. Since G is cyclic of order n with generator g, we can write every element of G uniquely as g^a, where $1 \leq a \leq n$. Suppose g^a has order d. Then $g^{ad} = e$, so $n \mid ad$, which means that we can find an integer k such that $ad = nk$. However, this implies that $a = k(n/d)$. Furthermore, because $1 \leq a \leq n$, $1 \leq k \leq d$. Therefore our element can be written in the form $g^{kn/d}$. All that remains is to show that if this element has order d, then $\gcd(k,d) = 1$. Notice that $g^{kn/d}$ has order $\leq d/\gcd(k,d)$. Indeed, raising $g^{kn/d}$ to the $d/\gcd(k,d)$ power yields

$$g^{\frac{kn}{d} \cdot \frac{d}{\gcd(k,d)}} = g^{kn/\gcd(k,d)} = e,$$

where the last equality is true because $k/\gcd(k,d)$ is an integer. Therefore, the only way $g^{kn/d}$ can possibly have order actually equal to d is if $\gcd(k,d) = 1$, as desired. □

(4) (10 points) Suppose $g_1 \in G_1$ has order n_1 and $g_2 \in G_2$ has order n_2. What is the order of $(g_1, g_2) \in G_1 \times G_2$, in terms of n_1, n_2?

Solution. We claim that the order of (g_1, g_2) is equal to $\operatorname{lcm}(n_1, n_2)$. Indeed, suppose that d is a positive integer with $(g_1, g_2)^d = (e_1, e_2)$. Then this means that $g_1^d = e_1, g_2^d = e_2$, so in particular $n_1, n_2 \mid d$. In other words, d is a common multiple of n_1, n_2. If we want d to be as small as possible, then $d = \operatorname{lcm}(n_1, n_2)$, by the definition of least common multiple. □

(5) (10 points) Show that each of the following groups is isomorphic to $\mathbb{Z}/n\mathbb{Z}$:

- The nth roots of unity; ie, the complex roots of $x^n = 1$, under multiplication.
- The rotational symmetries of the regular n-gon, under composition.

Solution. Because we know that every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, it suffices to show that these two examples are both cyclic of order n.

The nth roots of unity can be described by the complex numbers

$$e^{2\pi ik/n} = \cos(2\pi k/n) + i\sin(2\pi k/n),$$

where $1 \leq k \leq n$. These points form the vertices of a regular n-gon, found on the unit circle, in the complex plane. We can quickly check that the nth roots of unity form a group. Indeed, the identity is just the number 1, which is an nth root of unity, the product of two roots of unity is clearly still a root of unity, and the inverse of $e^{2\pi ik/n}$ is $e^{2\pi i(n-k)/n}$.

Let $\zeta_n = e^{2\pi i/n}$. Then clearly every nth root of unity has the form ζ_n^k, for some $1 \leq k \leq n$, and the order of ζ_n is n, because if $\zeta_n^d = 1$, then $e^{2\pi id/n} = 1$, which implies that d/n is an integer, or that $n \mid d$.

The second part is actually more or less identical to the first. Given a regular n-gon, there are apparently n different rotational symmetries, given by rotation about the origin by $2\pi k/n$ radians, where $1 \leq k \leq n$. These symmetries form a group, because the identity is just the identity map, and the inverse of rotation through $2\pi k/n$ radians is just rotation through $2\pi(n-k)/n$ radians. Again, the group is cyclic of order n, because it is generated by the single rotation through $2\pi/n$ radians. $\square$