ASSIGNMENT 4: SOLUTIONS

Question 1. Note: The question incorrectly states that there is a unique $\log_4 7 \in \mathbb{Z}/\phi(3^{54})\mathbb{Z}$.

Solution. Observe that 2 is a primitive root modulo 3^{54}, so there exists a unique solution $v \in \mathbb{Z}/\phi(3^{54})\mathbb{Z}$ to the equation

$$2^v \equiv 7 \pmod{3^{54}}.$$

If we can show that v is even, setting $t = v/2$ gives a desired solution. Now v is even since reducing mod 3 gives $2^v \equiv 1 \pmod 3$, and hence $v \equiv 0 \pmod 2$. Therefore a solution exists.

In order to find such a t, we can use truncated power series expansions of 3-adic logarithms. If we were looking for a solution for t in $\mathbb{Z}_3$, then

$$t = \frac{\log 7}{\log 4} = \frac{\log 1 + 6}{\log 1 + 3} = \frac{\sum_n (-1)^{n+1} 6^n/n}{\sum_n (-1)^{n+1} 3^n/n} = \frac{-a}{-b}.$$

But for now we only care about a solution to the equation modulo 3^{53}, so we can truncate the power series expansions of a and b for some n large enough, giving

$$a = \sum_{n=1}^{54} (-6)^n/n = 2865882868371128162622680907416091692987349267176203980845 04/17282129495479569175$$

$$b = \sum_{n=1}^{54} (-3)^n/n = 489013981719330526620480881276993586399952616 1/6083309582408808349600.$$

It follows that

$$t \equiv ab^{-1} \equiv 11914814460539851947621494 \pmod{3^{53}}.$$

Since we are looking for solutions modulo $\phi(3^{54}) = 2 \cdot 3^{53}$, we use the fact that $t \equiv 0, 1 \pmod 2$ (using solutions to the equation reduced modulo 3: $4^t \equiv 7 \pmod 3$) to lift to the desired solution using CRT.

The solutions are then

$$t \equiv 11914814460539851947621494, 31298060128219871844418217 \pmod{2 \cdot 3^{53}}.$$

□

Question 2.

Solution. Let $m > n$ be positive integers.

$$a_m - a_n = a^{p^m} - a^{p^n} = a^{p^n} \left(a^{p^n (p^{m-n} - 1)} - 1) \right).$$

But $p - 1 \mid p^{m-n} - 1$ (we took $m > n$) so by Fermat's little theorem, $a^{p^{m-n}-1} \equiv 1 \pmod p$ and hence

$$a^{p^n (p^{m-n} - 1)} \equiv 1 \pmod{p^{n+1}}.$$

It follows immediately that $a_m - a_n \equiv 0 \pmod{p^{n+1}}$, and setting $n = 0$, we get that $a_m - a \equiv 0 \pmod p$ for all $m > 0$.

Let $\varepsilon > 0$, and take N such that $p^{-N} < \varepsilon$. Consider $a_m - a_n$ for $m > n > N$.

$$|a_m - a_n|_p < p^{-N} < \varepsilon,$$

thus confirming that our sequence is Cauchy.

To show that (a_n) converges to a $(p-1)^{th}$ root of unity μ in $\mathbb{Z}_p$, notice that $a_n^{p-1} = (a^{p-1})^{p^n} \equiv 1 \pmod{p^n}$ since $a^{p-1} \equiv 1 \pmod p$. Therefore,

$$|a_n^{p-1} - 1| < p^{-n}$$

and $(a_n)^{p-1}$ converges to 1. Since $a_m - a \equiv 0 \pmod p$ for all $m > 0$, $\mu \equiv a \pmod p$. □

Question 3.

Solution. This is clear from counting arguments. Question 2 gives us $p - 1$ distinct roots of the polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p$, each one corresponding to a choice of an equivalence class modulo p. Since there are at most $p - 1$ roots of $x^{p-1} - 1$, all the roots can be obtained in this way and the roots can be distinguished by their equivalence classes. □

Question 4.

Solution. We show that such an x exists by showing there exists a sequence $(a_1, a_2, \ldots)$ where $a_i \in \{0, \ldots, p^i - 1\}$, such that

$$a_i \equiv a_j \pmod{p^i} \; \forall i \leq j$$

and

$$a_i \not\equiv x_i \pmod{p^i} \; \forall i.$$

First, choose any $a_1 \in \{0, \ldots, p-1\}$ such that $a_1 \not\equiv x_1 \pmod{p}$. Now, suppose that we have a sequence $(a_1, \ldots, a_n)$ satisfying the desired property. Then there are $\frac{\phi(p^{n+1})}{p^n} + 1 = p$ choices for an $a_{n+1} \in \{0, \ldots, p^{n+1} - 1\}$ such that $a_n \equiv a_{n+1} \pmod{p^n}$. Since $p \geq 2$ for all p prime, we can choose a_{n+1} such that $a_n \equiv a_{n+1} \pmod{p^n}$ but $a_{n+1} \not\equiv x_{n+1} \pmod{p^{n+1}}$. Thus, setting $x = (a_1, a_2, \ldots)$ gives the desired x.

Now, suppose that $\mathbb{Z}_p$ is countable. Then there exists a sequence of elements in $\mathbb{Z}_p$ enumerating the elements of $\mathbb{Z}_p$. However, by our above construction we can find an element of $\mathbb{Z}_p$ not in our sequence. Therefore $\mathbb{Z}_p$ and hence $\mathbb{Q}_p$ are uncountable. □

Question 5.

Solution. Consider the group homomorphism

$$\phi : \mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times$$
$$a \mapsto a^t.$$

Since 0 always has a unique t^{th} root (itself), we see that every element of $\mathbb{Z}/p\mathbb{Z}$ has a unique t^{th} root if and only if ϕ is an isomorphism if and only if ϕ is injective (since $\mathbb{Z}/p\mathbb{Z}^\times$ is finite).

But $\ker(\phi) = \{a \mid a^t \equiv 1 \pmod{p}\}$ and by Fermat's little theorem (and the existence of primitive roots), if $(t, p-1) = 1$, $|\ker(\phi)| = 1$. On the other hand, if $(t, p-1) = c \neq 1$, then $g^{\frac{p-1}{c}}$ is a non-trivial element of $\ker(\phi)$ for any choice of g a primitive root modulo p. Thus ϕ is an isomorphism if and only if $(t, p-1) = 1$. □

Question 6.

Solution. Not much to say here. By construction, $\frac{1+(p-1)e}{t} \in \mathbb{N}$, and $(p-1)e \equiv 1 \pmod{\phi(p) = p-1}$, so $b^t \equiv a \pmod{p}$. Thus we can find a t^{th} root of a:

- Run the Euclidean algorithm to obtain v such that $e(p-1) + vt = 1$.
- Return $a^v \pmod{p}$.

To see the output of this algorithm is correct, note that $vt = 1 - (p-1)e$, so $v = \frac{1-(p-1)e}{t}$. □

Question 7.

Solution. We have that 503 is prime, $777 = 3 \cdot 7 \cdot 37$ and $501 = 3 \cdot 167$. Immediately we see that $\left(\frac{501}{777}\right) = 0$ as $(501, 777) = 3 \neq 1$. In the other case we get (via quadratic reciprocity):

$$\begin{aligned}
\left(\frac{503}{777}\right) &= \left(\frac{777}{503}\right) = \left(\frac{274}{503}\right) = \left(\frac{2}{503}\right)\left(\frac{137}{503}\right) \\
&= (1)\left(\frac{503}{137}\right) = \left(\frac{92}{137}\right) = \left(\frac{2^2}{137}\right)\left(\frac{23}{137}\right) \\
&= \left(\frac{137}{23}\right) = \left(\frac{22}{23}\right) = \left(\frac{-1}{23}\right) \\
&= (-1)^{\frac{23-1}{2}} = -1
\end{aligned}$$

□

Question 8. Note: This wasn't marked.

Solution. The proof of Hensel's lemma still works if we replace polynomials with power series. We now apply Hensel's lemma to the power series in quesion. To find a solution we observe that 1 is a root mod 3, as

$$f(x) = x \log x - 3 = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{x(x-1)^j}{j} - 3$$

and hence

$$f(1) = 0 - 3 \equiv 0 \pmod{3}.$$

Furthermore,

$$f'(x) = 2x - 1 + \sum_{j=2}^{\infty} (-1)^{j+1} \frac{(x-1)^{j-1}((j+1)x - 1)}{j} = 1 + \log x$$

so

$$f'(1) = 1 \neq 0 \pmod{3}.$$

This means that we can obtain a root modulo 3^{40} by finding a 3-adic root with precision $O(3^{40})$. We now apply Hensel's lemma (Newton iteration) using $a_0 = 1$ and

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} = a_n - \frac{a_n \log a_n - 3}{1 + \log a_n}.$$

Since there are nice built in functions for the p-adic logarithm, all it takes is a little for loop to obtain a root for $f(x)$ of our desired precision:

$$\begin{aligned} &1 + 3 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 2 \cdot 3^9 + 2 \cdot 3^{10} // \\ &+ 2 \cdot 3^{11} + 2 \cdot 3^{12} + 2 \cdot 3^{14} + 2 \cdot 3^{16} + 3^{17} + 2 \cdot 3^{19} + 3^{20} // \\ &+ 3^{21} + 3^{22} + 3^{24} + 2 \cdot 3^{26} + 2 \cdot 3^{27} + 3^{28} + 2 \cdot 3^{29} + 2 \cdot 3^{30} // \\ &+ 3^{32} + 3^{33} + 3^{34} + 3^{35} + 3^{36} + 3^{37} + 3^{38} + 2 \cdot 3^{39} + O(3^{40}) \end{aligned}$$

(this result can be obtained after only the 5^{th} iteration, so it is a very small for loop). Thus, the desired root is $10131053957499665308 \pmod{3^{40}}$. □