MATH 152 Problem set 3 solutions

As usual, p denotes a prime number.

1. Since g is a primitive root mod p, as i runs through 1, 2, ..., $p-1$, g^i takes each value 1, 2, ..., $p-1$ exactly once, possibly in a different order. This gives $(p-1)! \equiv g \cdot g^2 \cdot \ldots \cdot g^{p-1}$ (mod p). Also, by the identity $1+2+\ldots+p-1 = p(p-1)/2$, we have $g \cdot g^2 \cdot \ldots \cdot g^{p-1} \equiv g^{p(p-1)/2}$ (mod p).

Wilson's theorem follows if we show that $g^{p(p-1)/2} \equiv -1$ (mod p). When $p = 2$, this is trivial. When p is odd, $g^{p(p-1)/2} \equiv g^{(p-1)/2}$, and it follows that this equals -1, since it squares to 1 and there are only two numbers mod p that squares to 1 (because $x^2 - 1 \equiv 0$ (mod p) has at most two solutions, no other numbers than 1 and -1 square to 1).

2. If $k = 1$ the result is trivial so assume $k \geq 2$.

$(a, a^k - 1) = 1$, so a is contained in the reduced residue class (mod $a^k - 1$). (For those of you who have group theory background, $a \in (\mathbb{Z}/(a^k-1)\mathbb{Z})^*$.) Obviously $a^k - 1 \equiv 0 \Rightarrow a^k \equiv 1$ (mod $a^k - 1$), so the order of a divides k. However, any smaller power of a is strictly smaller than $a^k - 1$ and hence cannot be 1 mod $a^k - 1$. Therefore the order of a is precisely k. By Lagrange's theorem, $k \mid \phi(a^k - 1)$.

3. First suppose that $(p-1) \mid k$ i.e. $k = c(p-1)$ for some integer c. Then for every nonzero $n \in \mathbb{Z}/p\mathbb{Z}$ we have $n^k \equiv n^{c(p-1)} \equiv 1$ (mod p) by Fermat's little theorem. Therefore $\sum_{n=1}^{p-1} n^k \equiv -1$ (mod p).

Next suppose $(p-1) \nmid k$. Recall that there exists a primitive root g mod p, and that as i runs through 1, 2, ..., $p-1$, g^i assumes each of 1, 2, ..., $p-1$ exactly once. Therefore $\sum_{n=1}^{p-1} n^k \equiv g^k + g^{2k} + \ldots + g^{(p-1)k}$ (mod p). Note that $(g^k + g^{2k} + \ldots + g^{(p-1)k})(1 - g^k) \equiv 0$ (mod p). But then $1 - g^k \not\equiv 0$ (mod p) by our assumption on k. Therefore $g^k + g^{2k} + \ldots + g^{(p-1)k} \equiv 0$ (mod p).

4. The idea is to consider the Taylor expansion of $f(x)$ around $x = a$:

$$f(x) = f(a) + f'(a)(x-a) + f''(a)(x-a)^2/2! + \ldots + f^{(d)}(a)(x-a)^d/d!.$$

In each of the sub-problems, our goal is to find $0 \leq t < p$ such that

$$f(a+tp) = f(a) + f'(a)tp + f''(a)t^2p^2/2! + \ldots + f^{(d)}(a)t^dp^d/d!$$

is an integer multiple of p^2. (We're restricting the possible value of t here because $a+tp$ and $a+(t+Cp)p = a+tp+Cp^2$ are considered the same mod p^2.

As a lemma, we claim that for $n \geq 2$, $f^{(n)}(a)/n!$ is an integer. Write $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1 x + c_0$. Then

$$f^{(n)}(x) = d(d-1)\ldots(d-n+1)x^{d-n} + c_{d-1}(d-1)\ldots(d-1-n+1)x_+^{d-1-n}\ldots + c_n n!,$$

and $n!$ divides all the coefficients of $f^{(n)}(x)$ since $n!$ divides any product of n consecutive integers. Therefore our lemma is established, which immediately implies

$$f(a+tp) \equiv f(a) + f'(a)tp \pmod{p^2}.$$

We use this identity to solve the problem. We already have that $f(a) \equiv 0 \pmod p$, i.e. $f(a) = Cp$ for some integer C.

(i) If $f'(a) \not\equiv 0 \pmod p$: then $f(a) + f'(a)tp = p(C + f'(a)t)$, and since $f'(a)$ is not a multiple of p, we can find exactly one $t \in \{0, 1, \ldots, p-1\}$ such that $C + f'(a)t$ is a multiple of p. For this t we have $f(a+tp) \equiv 0 \pmod{p^2}$.

(ii) If $f'(a) \equiv 0 \pmod p$ and $f(a) \not\equiv 0 \pmod{p^2}$: then $f(a)+f'(a)tp \not\equiv 0 \pmod{p^2}$ for any t, because by our assumptions $f'(a)tp$ is divisible by p^2 but $f(a)$ is not. Hence no solutions.

(iii) If $f'(a) \equiv 0 \pmod p$ and $f(a) \equiv 0 \pmod{p^2}$: then $f(a)+f'(a)tp \equiv 0 \pmod{p^2}$ for all $t \in \{0, 1, \ldots, p-1\}$. Therefore $a, a+p, \ldots, a+(p-1)p$ are all solutions to $f(x) \equiv 0 \pmod{p^2}$.

5. To prove the first statement, use induction on k.

Case $k = 0$: $5^{2^k} = 5 \equiv 1 \pmod{2^{k+2} = 4}$, and $5 \not\equiv 1 \pmod{2^{k+3} = 8}$ are all easily verified.

General case: assume the truth of the statement for $k-1$. We have $5^{2^{k-1}} = 1 + C \cdot 2^{k+1}$, $2 \nmid C$. Therefore $5^{2^k} = (5^{2^{k-1}})^2 = 1 + C \cdot 2^{k+2} + C^2 \cdot 2^{2k+2}$. Clearly this is congruent to 1 mod 2^{k+2}, but not to 1 mod 2^{k+3}, since $2 \nmid C$ (in fact, it is $1 + 2^{k+2}$ mod 2^{k+3}).

Next, the order of 5 (mod 2^α): by the above result, we know that $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. So the order of 5 divides $2^{\alpha-2}$. But it does not divide $2^{\alpha-3}$ since $5^{2^{\alpha-3}} \not\equiv 1 \pmod{2^\alpha}$. Therefore the order of 5 is precisely $2^{\alpha-2}$.

For the final part: there are $\phi(2^\alpha) = 2^{\alpha-1}$ reduced residue classes mod 2^α. The powers of 5 already accounts for $2^{\alpha-2}$ of them. To show that -1 and 5 generate all of the reduced residue classes—in the language of group theory, $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$—it suffices to show that -1 is not a power of 5. This is trivial when $\alpha = 2$, so assume $\alpha \geq 3$ (so as to avoid some tricky computational issues below).

Suppose by contradiction that $-1 \equiv 5^d \pmod{2^\alpha}$ for some $d < 2^{\alpha-2}$. Then $1 \equiv 5^{2d} \pmod{2^\alpha}$, so $2^{\alpha-2} \mid 2d \Rightarrow 2^{\alpha-3} \mid d$. This forces $d = 2^{\alpha-3}$.

Recall that $5^d = 5^{2^{\alpha-3}} \equiv 1 \pmod{2^{\alpha-1}}$ by what we proved above. Therefore

$$5^d = -1 + A \cdot 2^\alpha = 1 + B \cdot 2^{\alpha-1}$$

for some integers A, B. But then this implies $-1 \equiv 1 \pmod{2^{\alpha-1}}$, which is impossible since $\alpha \geq 3$. This proves that -1 is not a power of 5.

6. We will verify that the (least) period $l = p(p-1)$. (This conjecture is not totally out of the blue. One experiments on many values of n to see what n^n looks like, and finds that there's something special about the behavior p and $p-1$ with respect to the sequence n^n.)

First we show $(n+l)^{n+l} \equiv n^n \pmod p$ for all n: $(n+l)^{n+l} \equiv (n+p(p-1))^{n+p(p-1)} \equiv n^{n+p(p-1)} \equiv n^n n^{p(p-1)} \equiv n^n \pmod p$.

Next suppose l' is any number satisfying $(n+l')^{n+l'} \equiv n^n \pmod p$ for any n. We will show that $p \mid l'$ and $p-1 \mid l'$, thereby showing $l = p(p-1)$ is indeed the least value of l' satisfying the condition. For the former, let $n = 0$; then we have $l'^{l'} \equiv 0 \pmod p$. Therefore $p \mid l'$, and we can write $l' = pr$ for some r.[1] For the latter, note that our assumption on l' implies that, for all n, $(n+l')^{n+l'} \equiv (n+pr)^{n+pr} \equiv n^n n^r \equiv n^n \pmod p$. This implies that $n^r \equiv 1 \pmod p$ for every nonzero n. Exercise 3 in this problem set shows that this cannot be true unless $p-1 \mid r$. This completes the proof.

[1] If you insist that n has to start from 1, take $n = p$ and we will have the same conclusion.