18.781 Solutions to Problem Set 4, Part 1

1. (a) If x is a cube root of 1 then $x^3 \equiv 1 \pmod{1024}$. Obviously x must be coprime to 1024, so $x^{\phi(1024)} = x^{512} \equiv 1 \pmod{1024}$ by Fermat. Since 3 and 512 are coprime, and the order of x mod 1024 divides both, it must be 1. Therefore $x \equiv 1 \pmod{1024}$.

   (b) By part (a), if a cube root of -3 exists, it must be unique (if x, y are both cube roots of -3 mod 1024, then $(xy^{-1})^3 \equiv 1 \pmod{1024}$ so $x \equiv y$). Now $5^3 = 125 \equiv -3 \pmod{128}$. Note that the derivative of $x^3 + 3$ is $3x^2$, and $3 \cdot 5^2 \not\equiv 0 \pmod{2}$. We have $\overline{f(5)} = (3 \cdot 5^2)^{-1} \equiv 1 \pmod{2}$.
   Lifting to a cube root mod 256, we get $5 - 128 \equiv 5 + 128 \equiv 133 \pmod{256}$. Now

   $$133^3 = (5+128)^3 \equiv 5^3 + 3 \cdot 5^2 \cdot 128 \equiv -3 + 76 \cdot 128 \equiv -3 \pmod{512},$$

   so we don't need to modify 133 mod 512.
   Mod 1024, we have

   $$133^3 \equiv -3 + 76 \cdot 128 \equiv -3 + 39 \cdot 512 \equiv -3 + 512 \pmod{1024},$$

   so the solution is $133 - 512 \equiv 133 + 512 \equiv 645 \pmod{1024}$.

   (c) First, working mod 3, it's easy to see that the only solution is $x \equiv 1 \pmod{3}$. Now $f'(1) = 5 + 4 \equiv 0 \pmod{3}$, so it's not a nonsingular solution and we can't apply Hensel's lemma. But the proof of Hensel's lemma (by Taylor series expansion) tells us that mod 9, all the lifts of 1 (i.e., 1, 4, 7) will have the same value when plugged into f mod 9. We also know that any solution mod 9 must be a solution mod 3. Since $f(1) = 3 \not\equiv 0 \pmod{9}$, there is no solution mod 9, and thus none mod 81.

2. See gp file for the code. The factor 531793 is found. (Some other factors obtained from running Pollard rho on the quotient are 5684759 and 18207494497.)

3. If we know $N = pq$ and $\phi(N) = (p-1)(q-1)$, then we know $p + q = N - \phi(N) - 1$. So p and q are the roots of $x^2 - Mx + N$ for some integer M, which we can solve by the quadratic formula.

4. Let $f(a) = tp^j$ where t is an integer. Then, by the Taylor series expansion,

   $$\begin{aligned} f(b) &= f(a - tp^j \overline{f'(a)}) \\ &= f(a) - tp^j \overline{f'(a)} f'(a) + \frac{f''(a)}{2} (tp^j \overline{f'(a)})^2 + \cdots \end{aligned}$$

   Since the coefficients $f''(a)/2$, etc. are all integers,

   $$\begin{aligned} f(b) &\equiv f(a) - tp^j \overline{f'(a)} f'(a) \\ &\equiv tp^j - tp^j \overline{f'(a)} f'(a) \\ &\equiv tp^j (1 - \overline{f'(a)} f'(a)) \pmod{p^{2j}}. \end{aligned}$$

   Now by definition, $\overline{f'(a)} f'(a) \equiv 1 \pmod{p^j}$. So the product on the RHS is divisible by p^{2j}. Therefore $f(b) \equiv 0 \pmod{p^{2j}}$, as desired.

5. (a) Remember that we have

$$\begin{aligned} x^{p-1} - 1 &\equiv (x-1)(x-2)\cdots(x-p+1) \pmod p \\ &= x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} - \cdots - \sigma_{p-2}x + \sigma_{p-1}. \end{aligned}$$

So since the coefficients of $x, x^2, \ldots, x^{p-2}$ on the LHS are all 0, we must have that $\sigma_1, \sigma_2, \ldots, \sigma_{p-2}$ are all congruent to 0 mod p.

(b) Plugging $x = p$ into

$$(x-1)\cdots(x-p+1) = x^{p-1} - \sigma_1 x^{p-2} + \cdots + \sigma_{p-1},$$

we get $(p-1)! = p^{p-1} - \sigma_1 p^{p-2} + \cdots + \sigma_{p-3}p^2 - \sigma_{p-2}p + \sigma_{p-1}$. Now $\sigma_{p-1} = (p-1)!$, the product of the roots. So we cancel it with the $(p-1)!$ from the LHS and divide by p to get

$$0 = p^{p-2} - \sigma_1 p^{p-3} + \cdots + \sigma_{p-3}p - \sigma_{p-2}.$$

Since $p \geq 5$ and $\sigma_1, \ldots, \sigma_{p-3}$ are all divisible by p by part (a), we see that p^2 divides all the terms on the RHS except possibly σ_{p-2}. But since the terms sum to zero, it follows that p^2 divides σ_{p-2} as well.

6. Consider the $p-1$ congruence classes $1, g, \ldots, g^{p-2}$ mod p. These are all distinct, or else we would have $g^i \equiv g^j$ for some $0 \leq i < j \leq p-2$ and then $g^{j-i} \equiv 1 \pmod p$, contradicting the fact that g is a primitive root. Furthermore, they are all coprime to p. So they must be $1, 2, \ldots, p-1$ in some order. Therefore

$$S_k = 1^k + \cdots + (p-1)^k = 1^k + g^k + g^{2k} + \cdots + g^{(p-2)k}.$$

If $p-1$ divides k then each term is congruent to 1, so the sum is congruent to $p-1$. Otherwise

$$S_k = \frac{g^{(p-1)k} - 1}{g^k - 1} \equiv 0 \pmod p,$$

since the numerator is $g^{(p-1)k} - 1 \equiv 1^k - 1 \equiv 0 \pmod p$, but the denominator is $g^k - 1 \not\equiv 0 \pmod p$, since g has order $p-1$ and by assumption $p-1 \nmid k$. So

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} -1 & \text{if } p-1 | k \\ 0 & \text{if } p-1 \nmid k. \end{cases}$$

7. (a) We know

$$x^p - x \equiv x(x-1)\cdots(x-p+1) \pmod p,$$

so $\sigma_1, \ldots, \sigma_{p-2}, \sigma_p \equiv 0 \pmod p$ while $\sigma_{p-1} \equiv -1 \pmod p$. It can be easily shown by induction that for $k = 1, \ldots, p-2$, $S_k \equiv 0 \pmod p$. (The inductive step is using Newton's identity $k\sigma_k = S_1\sigma_{k-1} - S_2\sigma_{k-2} + \cdots + (-1)^{k-2}S_{k-1}\sigma_1 + (-1)^k S_k$ and noting that all terms on the LHS and RHS except for $(-1)^k S_k$ are congruent to 0). Then, for $k = p-1$, we get $(p-1)\sigma_{p-1} \equiv 0 + \cdots + 0 + (-1)^{p-2}S_{p-1}$, so $S_{p-1} \equiv -1 \pmod p$. Indeed, this checks with Fermat since

$$\begin{aligned} 0^{p-1} + 1^{p-1} + \cdots + (p-1)^{p-1} &\equiv 0 + \underbrace{1 + \cdots + 1}_{p-1 \text{ times}} \\ &\equiv p - 1 \\ &\equiv -1 \pmod p. \end{aligned}$$

Finally, for $k = p$, we get

$$p\sigma_p = S_1\sigma_{p-1} + 0 + \cdots + 0 + (-1)^{p-1}S_p.$$

So $S_p \equiv 0 \pmod p$ as well. These results agree with Problem 6.

(b) Let $x_1, \ldots, x_n$ be the n variables. Suppose that for some values of $x_1, \ldots, x_n$, we have $f(x_1, \ldots, x_n) \equiv 0$. Then $1 - f(x_1, \ldots, x_n)^p \equiv 1 \pmod{p}$. On the other hand, if $f(x_1, \ldots, x_n) \not\equiv 0 \pmod{p}$, then by Fermat's Little Theorem $f(x_1, \ldots, x_n)^{p-1} \equiv 1 \pmod{p}$, so $1 - f(x_1, \ldots, x_n)^{p-1} \equiv 0 \pmod{p}$. Therefore, the function $1 - f(x)^{p-1}$ equals 1 if x is a root, 0 mod p if x is not a root. So the number of roots, mod p, is

$$\begin{aligned} \sum_{a_1,\ldots,a_n} [1 - f(a_1, \ldots, a_n)^{p-1}] &= p^n - \sum_{a_1,\ldots,a_n} f(a_1, \ldots, a_n)^{p-1} \\ &\equiv - \sum_{a_1,\ldots,a_n} f(a_1, \ldots, a_n)^{p-1} \pmod{p}. \end{aligned}$$

To show that the number of roots is equivalent to $0 \pmod{p}$, it's enough to see that this sum $\sum f(a_1, \ldots, a_n)^{p-1}$ vanishes mod p. Now f has total degree $d < n$, i.e., each monomial of f has degree $d < n$. So for each monomial $x_1^{e_1} \cdots x_n^{e_n}$ of f^{p-1}, we have $e_1 + \cdots + e_n < (p-1)n$. This implies that some e_i must be less than $p - 1$. Now, if we can show that for any monomial M appearing in f^{p-1},

$$\sum_{a_1,\ldots,a_n} M(a_1, \ldots, a_n) \equiv 0 \pmod{p},$$

then we're done by linearity. But we have

$$\begin{aligned} \sum_{a_1,\ldots,a_n} M(a_1, \ldots, a_n) &= \sum_{a_1,\ldots,a_n} a_1^{e_1} \cdots a_n^{e_n} \\ &= \prod_{i=1}^{n} \left(\sum_{a_i} a_i^{e_i} \right), \end{aligned}$$

where the sum runs from 0 through $p - 1$ for each i. Now if some $e_i < p - 1$ then by Problem 6, $\sum a_i^{e_i} \equiv 0 \pmod{p}$. Therefore $\prod(\sum a_i^{e_i}) \equiv 0 \pmod{p}$ for every monomial, proving our result.

When f has no constant term, the number of roots is a multiple of p, and it is positive since $(0, \ldots, 0)$ is a root. So there are at least p roots. This implies there must be a nontrivial root as well.

18.781 Theory of Numbers
Spring 2012