18.781 Problem Set 4 part 1

Thursday March 15, with the rest of Problem Set 4.
Collaboration is allowed and encouraged. However, your writeups should be your own, and you must note on the front the names of the students you worked with.
Extensions will only be given for extenuating circumstances.
For problems 2 and 3, turn in a printout of your gp code as well.

1. (a) Show that the only cube roots of 1 modulo 1024 is 1.
   (b) Find all the cube roots of -3 modulo 1024. (Hint: use Hensel's Lemma, but you might want to start with a high enough power of 2 which is 3 away from a cube).
   (c) Solve $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$.

2. Write a gp program to implement Pollard rho: given N start with $x_0 = 1$ and let $x_{n+1} = x_n^2 + 1$. Evaluate $\gcd(x_{2n} - x_n, N)$ till you find a factor. Use it to find a prime factor of $2^{1231} - 1$.

3. Suppose that $N = pq$ is the product of two primes. Suppose in addition to knowing N, we also know $M = \phi(N)$. Describe how to obtain p and q from this information. Use your method to factor the number

$$N = 27606985387162255149739023449107931668458716142620601169954803000803329$$

which is a product of two primes, given that

$$\phi(N) = 27606985387162255149739023449107761527112996396559656119259509106409476.$$

4. Suppose that $f(a) \equiv 0 \pmod{p^j}$ and that $f'(a) \not\equiv 0 \pmod{p}$. Let $\overline{f'(a)}$ be an integer chosen so that $f'(a)\overline{f'(a)} \equiv 1 \pmod{p^{2j}}$, and set $b = a - f(a)\overline{f'(a)}$. Show that $f(b) \equiv 0 \pmod{p^{2j}}$. Note: this is the p-adic Newton's method, and it differs from the Hensel's lemma formula in that $\overline{f'(a)}$ is an inverse of $f'(a)$ modulo p^{2j}, not just modulo p.

5. Let p be a prime. Let $\sigma_1, \sigma_2, \ldots, \sigma_{p-1}$ be the elementary symmetric polynomials in $1, 2, \ldots, p-1$, as in class (i.e. σ_k is the sum of products of k of these numbers). We showed that $(-1)^{p-1}\sigma_{p-1} = (p-1)! \equiv -1 \pmod{p}$.
   (a) Show that $\sigma_1, \ldots, \sigma_{p-2}$ are all congruent to $0 \pmod{p}$ (Hint: use the polynomial congruence from class).
   (b) For $p \geq 5$, show that $\sigma_{p-2} \equiv 0 \pmod{p^2}$. (Hint: plug in $x = p$ in the equation $(x-1)(x-2)\ldots(x-p+1) = x^{p-1} - \sigma_1 x^{p-2} + \cdots + \sigma_{p-1}$.)

6. Let p be a prime, and g a primitive root modulo p. Show that $1, g, g^2, \ldots, g^{p-2}$ are all the nonzero residue classes mod p. For a positive integer k, let $S_k = 1^k + 2^k + \ldots (p-1)^k$. Compute the value of S_k modulo p in closed form, as a function of k.

7. (Bonus) Let p be an odd prime.

   (a) Let $x_1, \ldots, x_n$ be variables, and for $1 \leq k \leq n$, let $\sigma_k(x_1, \ldots, x_n)$ is the k'th elementary symmetric polynomial in the x_i's as in class (i.e. the sum of all products of k distinct x_i's). For instance,

   $$\sigma_1 = x_1 + \cdots + x_n$$
   $$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \ldots x_{n-1}x_n$$

   and so on. Note that

   $$\prod_{i=1}^{n}(y - x_i) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} + \cdots + (-1)^n \sigma_n$$

   On the other hand, let S_k be the power sum

   $$S_k = x_1^k + \cdots + x_n^k$$

   Newton's identities relate the power sums and the elementary symmetric polynomials:

   $$k\sigma_k = S_1\sigma_{k-1} - S_2\sigma_{k-2} + \ldots (-1)^{k-2}S_{k-1}\sigma_1 + (-1)^{k-1}S_k$$

   for $1 \leq k \leq n$. Now let p be a prime and let $x_1, \ldots x_p$ be $0, 1, \ldots, p-1$. Use Newton's identities (and the result of Problem 5 (a)) to calculate the power sums $S_1, \ldots, S_{p-2}, S_{p-1}$ modulo p.

   (b) Let $f(x)$ be a polynomial in n variables, of degree $d < n$. Show that the number of zeros of f modulo p is divisible by p. In particular, if f has no constant term, then show that $f(x) \equiv 0 \pmod{p}$ has a nonzero solution $(a_1, \ldots, a_n)$ (i.e. not all the a_i are 0 mod p). [Hint: Consider the polynomial $g(x) = (1 - f(x))^{p-1}$. What are the possible values of $g(a_1, \ldots, a_n)$ mod p? Compute the sum

   $$\sum_{a_1,\ldots,a_n} g(a_1, \ldots, a_n)$$

   modulo p, where $a_1, \ldots, a_n$ take all p^n possible values modulo p.]

MIT OpenCourseWare
http://ocw.mit.edu

18.781 Theory of Numbers
Spring 2012

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.