Solutions to non-text problems in Assignment #9

I-3: I hope Diffie-Hellman worked for you. Remember, the mathematical ideas are that

- $(g^a)^b = g^{ab} = (g^b)^a$,
- if the prime p is huge, there is no known reasonably fast way of finding a given g^a or b given g^b

and the cryptological ideas are that

- one person knows g^a and b,
- one person knows g^b and a,
- someone intercepting the messages instead sees only g^a and g^b.

(Comments:

The problem of finding a from g^a is called the "discrete log problem"—"log", because for ordinary numbers to get from g^a to a you take $\log_g$, and "discrete" as a contrast to "continuous". (The real numbers are "continuous" while finite fields are "discrete", meaning that there is no concept of elements being arbitrarily close to one another.)

The reason that $p = 14737727$ is a "toy" example, even though it seems large by ordinary standards, is that on current computers it would be easy to find a from g^a just by trying all 14737726 possible values of a and seeing which one gives the desired g^a.

There is also the issue mentioned in class, that this basic version of Diffie-Hellman is susceptible to the "man-in-the-middle" attack, where someone gets in the communication stream between Alice and Bob and to Alice pretends to be Bob and to Bob pretends to be Alice. This intruder then ends up sharing a secret key with Alice and another secret key with Bob and can read and relay messages between them without their realizing it. So to use Diffie-Hellman in practice it is desirable to make modifications to get around this problem.)

M-7: See the solution already given.

O-1: Including α^7 as a check to make sure it's 1, we get

$$\begin{array}{rcccccc}
1 & = & 1 & & & & \\
\alpha & = & & & \alpha & & \\
\alpha^2 & = & & & & & \alpha^2 \\
\alpha^3 & = & 1 & + & \alpha & & \\
\alpha^4 & = & & & \alpha & + & \alpha^2 \\
\alpha^5 & = & 1 & + & \alpha & + & \alpha^2 \\
\alpha^6 & = & 1 & & & & \alpha^2 \\
\hline
\alpha^7 & = & 1 & & & &
\end{array}$$

Here $\alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3 = \alpha^2 + (1 + \alpha) = 1 + \alpha + \alpha^2$, etc.

O-2: (a) The usual, except that we can't write "$1, 2, \ldots$" for the nonzero elements. Instead, just call them $r_1, r_2, r_3, \ldots, r_{p^k-1}$. For any nonzero a in F, multiply these all by a to get $ar_1, ar_2, ar_3, \ldots, ar_{p^k-1}$. We know that no two elements in this list are equal since if $ar_i = ar_j$ we could cancel a to get $r_i = r_j$. So $ar_1, \ldots, ar_{p^k-1}$ must be all the nonzero elements again. Therefore their product is same as the product P of all the nonzero elements. So $P = (ar_1)\ldots(ar_{p^k-1}) = a^{p^k-1} r_1 \ldots r_{p^k-1} = a^{p^k-1} P$. Canceling P (which is nonzero) we get $a^{p^k-1} = 1$.

(b) For any nonzero element a, take the result of part (a) and multiply through by a. On the other hand, if $a = 0$ then $a^{p^k} = a$ anyway.

(c) Notice that ϕ here is not the Euler ϕ-function! Rather, $\phi(a)$ means a^p. So $\phi(\phi(a)) = (a^p)^p = a^{p^2}$, $\phi(\phi(\phi(a))) = ((a^p)^p)^p = a^{p^3}$, and so on, until $\phi(\ldots(\phi(a))\ldots)$ (k times) is a^{p^k}, which by part (b) we know is a again.

O-3: (i) says $(ab)^p = a^p b^p$, which is true (by commutativity and associativity).

(ii) $\phi(a + b) = \phi(a) + \phi(b)$ sounds strange. But notice that $(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ and we also know that since p is prime, each binomial coefficient except the 0-th and last is divisible by p and so is 0 in a field of characteristic p. Therefore $(a + b)^p = a^p + b^p$ as required.

(iii) By **O-2** we know that $\phi(\phi(\ldots(\phi(a))\ldots)) = a$ for all a. If $\phi(a) = \phi(b)$, then applying ϕ to both sides $p - 1$ more times we get $a = b$, so ϕ can't take different elements to the same element, i.e., ϕ is one-to-one. Also to show that ϕ is "onto", either remark that a one-to-one function on a finite set must be onto, or else notice that $\phi(a) = b$ has the solution $a = \phi(\phi(\ldots(\phi(b))\ldots))$ (with $p - 1$ applications of ϕ).

O-4: In this kind of problem, start by making yourself some simple examples. For example, if a has order 12, then a^3 has order 4, because $(a^3)^4 = 1$ and

yet no smaller power of a^3 is 1. To emphasize the 4, we can say $a^{12/4}$ has order 4. Now you're ready to try the official version.

(a) Taking powers of $a^{r/r'}$, we have $1, a^{r/r'}, a^{2r/r'}, \ldots$, returning to 1 only for $a^{r'r/r'}$, so the order of $a^{r/r'}$ is r'.

(b) Here an example would be $\text{lcm}(12, 15) = 60$ and $4 \cdot 15 = 60$. Another choice would be $12 \cdot 5 = 60$.

For an official version, as suggested write

$$\begin{aligned} r &= p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \\ s &= p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k} \\ \ell &= p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} \end{aligned} .$$

Here $g_i = \max(e_i, f_i)$ for each i. We are supposed to make ℓ out of coprime divisors r' of r and s' of s. So let's go through the primes one by one, throwing a power of it into r' or s' but not both: If $e_i > f_i$, put $p_i^{e_i}$ into r'. If $e_i < f_i$, put $p_i^{f_i}$ into s'. If $e_i = f_i$ we have a choice but let's say put $p_i^{e_i}$ into r'. Then each prime-power factor of ℓ is in exactly one of r' and s', which gives $\ell = r's'$ and also r', s' are coprime.

(c) If a has order r and b has order s, let $\ell = \text{lcm}(r, s)$. By (b) we can find coprime r', s' with $r'|r$, $s'|s$. Let $a' = a^{r/r'}$ and let $a' = b^{s/s'}$. By (a) we know a' has order r' and b' has order s'. And since r', s' are coprime, by N-3 we know $a'b'$ has order $r's'$, which is ℓ. So we do have an element whose order is the lcm of the orders of a and b.

(d) If r is the maximum possible order of a unit, and s is the order of some other unit, then by (c) there is an element of order $\text{lcm}(r, s)$. This is at least as large as r but can't be larger, since r was already the largest possible order. Then $\text{lcm}(r, s) = r$, which is a fancy way of saying that $s|r$.

O-5: As suggested, let r be the maximum possible order of a unit (nonzero element). Then by **O-4**(d), if a is *any* unit, the order of a divides r, so that $a^r = 1$. Now we use a fact about fields: A polynomial of degree n has at most n roots. Where is the polynomial? $a^r = 1$ says that a is a root of $x^r - 1$. So every nonzero element of F is a root of $x^r - 1$. If the field has $q = p^k$ elements, then $x^r - 1$ has $q - 1$ roots and so $r \geq q - 1$. Also r, being the order of an element, can't be larger then $q - 1$, so $r = q - 1$. Therefore there *is* an element of order $q - 1$, or in other words, a generator (since it has $q - 1$ different powers)..

P-1: These are just to get an intuitive feel for the complex numbers and complex series. These demos will not be covered on the final exam.

(a) The straight line segments represent the terms $1, z, z^2, z^3, \ldots$ that are to be added together to make a geometric series. When $|z| \geq 1$, the absolute

value of these powers is always 1 or more, so there is no convergence. On the other hand, you can see from experimenting that for $|z| < 1$ the geometric series does converge. (The sum is $\frac{1}{1-z}$ for any z, the same formula as for real z.)

(b) The sum goes around the circle, because you are computing $e^{i\theta}$ for various numbers $i\theta$ on the imaginary axis.

Note: This demo also shows a couple of interesting things even for real z. Compare, say, e^{10} and e^{-10} as computed by series:

$$\begin{aligned} e^{10} &= 1 + 10 + \tfrac{1}{2}10^2 + \tfrac{1}{10!}10^3 + \dots \\ e^{-10} &= 1 - 10 + \tfrac{1}{2}10^2 - \tfrac{1}{10!}10^3 + \dots \end{aligned}$$

The first interesting thing is that the terms get large in absolute value before starting to get small and tending towards 0. For example, the term with exponent 10 is $\frac{1}{10!}10^{10} \approx 2755.73$. Of course, it makes sense to have some large terms since e^{10} is also large, ≈ 22026.5.

The second interesting thing, though, is that these same terms with alternating signs add up to e^{-10}, which is extremely small, ≈ 0.000045. So they come very close to canceling each other out.

To see this happening in the demo, move the pointer to the the left end of the real axis (which is about -3). The yellow dot shows that the sum is just about 0. Now move the pointer upwards a bit so you can see some terms separately; they make zigzag lines indicating lots of big terms adding up to about 0, but not quite.

(c) The "spotlight" shows part of a grid in the domain and its corresponding image. The polynomial function you are seeing is $f(z) = z^2 + 1$. The two dots on the imaginary axis are the roots, which are $\pm i$.

The reason for showing a spotlighted portion of the grid in the domain instead of the whole grid is simply that the whole grid gives too confusing an image.

For the related function z^2, if you walk around a circle in the domain then the image goes around a circle twice. With $f(z) = z^2 + 1$ (which is z^2 moved right by 1) the same is true; try dragging the spotlight around a circle in the domain, with the two roots inside.

The problem mentions "analytic" functions; that means differentiable. Complex analytic functions have the property that they are "conformal", meaning angle-preserving, wherever the derivative is not zero. For $f(z) = z^2 + 1$, the derivative is $2z$, so it's conformal except at the origin.

This demo is actually more elaborate; you can make different polynomials by dragging the roots around and you can even change the degree by dragging an additional root from the "root box" in the upper left corner.

P-2: The first part is just like N-2 but for any field $\mathbb{F}_q$ with $q = p^k$, instead of just for $\mathbb{F}_p$. But the reasoning is exactly the same; there are $q^3 - 1$ nonzero vectors and $q - 1$ nonzero vectors per 1-dimensional subspace, so there are $\frac{q^3-1}{q-1} = q^2 + q + 1$ one-dimensional subspaces.

How about 2-dimensional subspaces? We can use "overcounting" by counting their bases. (These are "ordered" bases, where v_1, v_2 is considered different from v_2, v_1.) To make a single 2-dimensional subspace, we need a basis of two vectors. The first is simply nonzero, so we have $q^3 - 1$ choices. The second is any vector not containing the span of the first; the span is 1-dimensional and so has q vectors (the number of scalars), so the number of choices for the second is $q^3 - q$. The number of bases of two vectors is therefore $(q^3-1)(q^3-2)$. Within a single 2-dimensional subspace, how many bases are there? A 2-dimensional subspace has q^2 elements, so in choosing a basis within it we have $q^2 - 1$ choices for the first vector and $q^2 - q$ choices for the second, making $(q^2 - 1)(q^2 - q)$ choices in all. Using the "overcounting" method, then, we get $\frac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} = \frac{(q-1)(q^2+q+1)q(q+1)(q-1)}{(q+1)(q-1)q(q-1)} = q^2 + q + 1$, the same as the number of 1-dimensional subspaces.

How many 1-dimensional subspaces are there within each 2-dimensional subspace? A 2-dimensional subspace has $q^2 - 1$ nonzero vectors, and each 1-dimensional subspace uses $q - 1$ of them, so there are $\frac{q^2-1}{q-1} = q + 1$ one-dimensional subspaces contained in each 2-dimensional subspace.

How many 2-dimensional subspaces are there containing a given 1-dimensional subspace? Let v_1 be a basis for the 1-dimensional subspace (i.e., any nonzero vector in the subspace). Let v_2 be any vector not in the 1-dimensional subspace; then v_1, v_2 are linearly independent and their span is a 2-dimensional subspace. There are $q^3 - q$ choices for v_2, but how many of these give the *same* 2-dimensional subspace? Notice that v_1, v_2' give the same subspace as v_1, v_2 when v_2' is in the span of v_1, v_2 but is not in the span of v_1. In other words, $v_2' = r_1 v_1 + r_2 v_2$ with $r_2 \neq 0$. There are q choices for r_1 and $q-1$ choices for r_2, so $q(q-1)$ choices in all. Then the number of 1-dimensional subspaces containing a given 1-dimensional subspace is $\frac{q^3-q}{q(q-1)} = \frac{q(q+1)(q-1)}{q(q-1)} = q+1$.

Conclusion: There are $q^2 + q + 1$ plants, $q^2 + q + 1$ blocks, $q + 1$ plants per block and $q + 1$ blocks per plant.

Notice that this checks with the case $q = 2$, where these numbers come out to be 7 and 3.

Note: N-2 might be on the final but P-2 won't be.

P-3: (Not on final) You have seen a description of $\mathbb{F}_8$ mentioning that it has a

generator α with $\alpha^3 = \alpha+1$, so α is a root of x^3+x+1. (As usual, signs don't matter with characteristic 2.) And this polynomial is indeed irreducible since a reducible polynomial of degree 3 would have a linear factor and so would have a root in $\mathbb{F}_2$, but this one does not (since 0 and 1 are not roots). So use "boxes modulo $x^3 + x + 1$" (or more officially, congruence classes). Just as boxes mod 7 correspond to the possible remainders on dividing by 7 (namely 0 through 6), the boxes for polynomials correspond to the possible remainders on dividing by x^3+x+1, which is anything of lower degree. So the boxes can be described as containing respectively $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x^1$ (eight boxes). Of these, α is the box of x. You can see that α is a root of $x^3 + x + 1$ since all multiples of that polynomial, including the polynomial itself, are in box 0.

P-4: