Please write your hackerrank username somewhere on your problem set.
Written problems are due at the beginning of class on Friday, November 20.
Programming problems are not due until 10:50am on Wednesday, November 25. The submission page for the programming questions is the following.

`https://www.hackerrank.com/math158-problem-set-8/`

Written problems

1. Textbook exercise 4.7.
2. Textbook exercise 5.24.
3. Textbook exercise 5.28.
4. Textbook exercise 5.29.
5. Textbook exercise 5.39.
6. Suppose that n is an odd integer greater than 1, and that we are selecting an element $a \in \mathbf{Z}/n$ uniformly at random. This problem will investigate the probability that a is a unit. Let $p_1, p_2, \cdots, p_\ell$ be the distinct prime factors of n (e.g. if $n = 45$, $\ell = 2$ and the primes are 3 and 5; note that 3 occurs only once in the list even though 3^2 divides n).
   (a) Let E_i denote the event that p_i does not divide a, and let F denote the event that a is a unit modulo n. Prove that $F = E_1 \cap E_2 \cap \cdots \cap E_\ell$.
   (b) Prove that the probability of F is equal to the product of the probabilities of the E_i (a stronger fact is that the events E_i are independent events, which is one way to prove this).
   (c) Compute the probability of E_i and deduce a formula for the probability of F.
   (d) Use this formula to deduce a formula for $\phi(n)$ in terms of n and the primes p_i.

   Remark. At various times while discussing RSA, we allowed ourselves to assume that the message transmited is a unit modulo N. Part (c) of this problem justifies why this is a reasonable assumption, given the size of the primes in RSA.
7. Suppose that n and p_i are as in the previous problem. Suppose that we are choosing an integer a uniformly at random from the unit group $(\mathbf{Z}/n)^\times$. This problem will investigate the probability that a is a square, i.e. that $x^2 \equiv a \pmod{n}$ has a solution.
   (a) Let E_i denote the event that $x^2 \equiv a \pmod{p_i}$ has a solution and let F denote the event that $x^2 \equiv a \pmod{n}$ has a solution. Prove that $F \subseteq E_1 \cap \cdots \cap E_\ell$. (*Note.* In fact, these events are identical, so we could write $=$ instead of $\subseteq$, but this is more difficult to prove.)

(b) Assume that the probability of E_i is $\frac{1}{2}$ (I encourage you to try to prove it, but you are free to assume it without proof). Prove that

$$\Pr(F) \leq \frac{1}{2^\ell}.$$

(you should proceed in a similar manner as in the previous problem).

Remark. We discussed a collision algorithm in class that can factor n if two different integers a, b are found such that $a^2 \equiv b^2 \pmod{n}$. This algorithm is more likely to succeed if there are relatively few squares modulo n (hence greater odds of a collision). This problem shows that this algorithm is most effective when n has many distinct prime factors, since a smaller fraction of the units are squares. In particular, this algorithm poses little danger to RSA keys.

8. Suppose that p, q are two prime numbers such that $p \equiv 1 \pmod{q}$. Suppose that we choose an element a from $(\mathbf{Z}/p)^\times$ uniformly at random.

   (a) What is the probability that $\mathrm{ord}_p(a) = q$?

   (b) What is the probability that $\mathrm{ord}_p(a^{(p-1)/q}) = q$?

   Remark. This shows why the suggested approach to finding DSA parameters (as in PSet 6 number 12) is better than choosing a at random until you find one that is order q.

9. Suppose that Samantha signs M different documents with the same DSA public key. Suppose the number of possible ephemeral keys is N. We have seen that she must be sure not to use the same ephemeral key twice.

   (a) Suppose that $k_1, \cdots, k_M$ are the ephemeral keys that Samantha chooses. Assume that each was chosen uniformly at random from all N possible choices. Calculate the expected value of the number of pairs $\{i, j\}$ of two distinct indices such that $k_i = k_j$.

   (b) Prove that the probability that *some two* keys are the same is less than your answer from part (a).

   (c) Suppose that $M = 2^{32}$ (this is what M would be if Samantha signs one document per second for 120 years). Suppose that the parameters (p, q) used for DSA are such that p is 512 bits long and q is 160 bits long (as in the original DSA standard from 1991). Show that the probability that Samantha ever chooses the same ephemeral key twice is less than $\frac{1}{2^{96}}$.

   Remark. These odds are a lot worse for Samantha if she doesn't choose a good random number generator.

10. Textbook exercise 6.1.

11. Textbook exercise 6.2.

12. Textbook exercise 6.4. (You can use whatever computing equipment you wish to help sketch the pictures).

Programming problems

13. Given integers A, B, and p, and two points P, Q on the elliptic curve $Y^2 = X^3 + AX + B$ over $\mathbf{F}_p$, compute the sum $P \oplus Q$.

14. Given A, B, p as before, one point P on the elliptic curve, and an integer n (positive or negative), compute the point nP.

15. Given A, B, p as before, determine the number of points on the elliptic curve, and print the "trace of Frobenius" t_p, as defined on page 309 of the textbook.

    Remark. There are very efficient algorithms for this problem, sufficient for primes of the size needed for cryptography, but they are beyond the scope of this course. For this problem, p will be no more than 15 bits in length, and a more naive method will suffice. See the online problem statement for a further hint.

16. Given parameters p, q, g for DSA and a public key A, find a document D with a valid signature (S_1, S_2). Note that you will *not* be able to decide on D in advance (since DSA is secure, as far as we know), but instead compute it along with a signature. See exercise 4.7 in the textbook for a suggestion; you will need to adapt the method in that exercise from ElGamal to DSA.