Grade 11/12 Math Circles

Cryptography, Part 2 - Problem Set

1. Which of the following numbers are prime? For the ones that aren't prime, factor them as a product of primes.
   (a) 101
   (b) 119
   (c) 127
2. (a) For any positive integer a, what is $\gcd(a, 0)$ equal to?
   (b) Calculate $\gcd(15, 27)$ using the Euclidean algorithm.
   (c) Calculate $\gcd(61783, 4019881)$ using the Euclidean algorithm.
3. Find integers x and y solving the following equations.
   (a) $15x + 27y = 3$. (**Hint:** We've done half the work in the previous question.)
   (b) $17x + 31y = 1$.
   (c) $17x + 31y = 4$. (**Hint:** This requires a little more than just the Extended Euclidean algorithm. How can you work with the answer obtained in part (b) to get an answer here?)
4. Compute the following values of the Euler phi function.
   (a) $\phi(7)$
   (b) $\phi(15)$
   (c) $\phi(27)$
   (d) $\phi(30)$
   (e) $\phi(p^k)$, where p is a prime number and k is a positive integer.
5. Modular arithmetic is good for much more than RSA. If an equation is true in the integers, we can "reduce it mod n" to get a congruence mod n that is also true. This is more useful in the other direction: if we start with an equation and prove it has no solutions mod n for some choice of n, then there are no integer solutions. This helps because we can exhaustively try every possibility for the variables mod n – there are only n different choices for each variable that would give a distinct result.

   Prove that each of the following equations has no integer solution by showing each one has no solutions mod n for a small choice of n (in each case, you can take $n \leq 5$.)

(a) $6x + 21y = 2$

(b) $5y = x^2 + 2$

(c) $x^2 + y^2 = 31$

6. In RSA, Nick is not supposed to reveal $\phi(N)$, because knowing it allows everybody to calculate Nick's private key. It's time to put on our cryptanalysis hats and try to break the system. If we know p and q, the two factors of N, it becomes easy to calculate $\phi(N)$. However, as we know, finding those factors is really hard. Maybe there's an easier way to calculate $\phi(N)$? We're going to see the answer is no.

   (a) Suppose you have a magic machine that takes N and instantly calculates $\phi(N)$. How can you use the values of N and $\phi(N)$ to calculate $p + q$?

   (b) Once you know both $p + q$ and $N = pq$, how can you calculate both p and q? (**Hint:** Consider the quadratic formula applied to the polynomial $x^2 - (p + q)x + pq$.)

   What this means is that an efficient way for calculating $\phi(N)$ leads to an efficient way of factoring N, and everyone believes that factorization is really hard.

7. Like any cryptosystem, the security of RSA can be compromised if used incorrectly. Suppose Nick and Bahaa have the same value of N, but different encryption exponents e_1 and e_2.

   (a) Explain how Nick and Bahaa can work out each other's private keys, and therefore read each other's encrypted messages.

   (b) Suppose Shefaza comes along and sends the same message M to both Nick and Bahaa (maybe it's Shefaza's credit card number). Suppose also that $\gcd(e_1, e_2) = 1$. Now, let's say Diana comes along and reads the ciphertexts that Shefaza sent to Nick and Bahaa, say $C_1 \equiv M^{e_1} \pmod{N}$ and $C_2 \equiv M^{e_2} \pmod{N}$.

   Explain how Diana can use this information to recover Shefaza's plaintext M.

   Hint: Running the Extended Euclidean algorithm on e_1 and e_2 allows Diana to find integers x and y such that $e_1x + e_2y = 1$. How can this information help her recover M?