Homework 10 Solutions

Written Part

4. This problem goes hand in hand with Problem 3 in the impelementation part of this assignment. We describe how (the abstact version of) Pollard's ρ method can be used to factor large numbers N relatively quickly. It works best when N has a relatively small prime factor p. We first describe the method. Suppose you have a mixing function:

$$f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}.$$

Let $x_0 = y_0 \in \mathbb{Z}/N\mathbb{Z}$, and compute $x_{i+1} = f(x_i)$ and $y_{i+1} = f(f(y_i))$. At each step compute:

$$g_i = \gcd(|x_i - y_i|, N).$$

(a) Suppose f is sufficiently random and let p be the smallest prime divisor of N. Show that with high probability we find some $g_k = p$ for $k = \mathcal{O}(\sqrt{p})$.

Proof. We will assume that the mixing function f is a polynomial like in each case that we run it. Let p be the smallest prime dividing N, and denote by $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ that takes an element of $\mathbb{Z}/N\mathbb{Z}$ to its residue modulo p by $x \mapsto \overline{x}$. Since f is a polynomial one can define a it on $\mathbb{Z}/p\mathbb{Z}$ as well by the same rule (we will call this $\overline{f}$), and since reduction modulo p respects algebraic manipulation (HW1 Problem 8), we see that $\overline{f}(\overline{x}) = \overline{f(x)}$. In particular, we get a mixing function on $\mathbb{Z}/p\mathbb{Z}$ which is compatible with the mixing function on $\mathbb{Z}/N\mathbb{Z}$. We depict this via the following diagram:

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/N\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \xrightarrow{\overline{f}} & \mathbb{Z}/p\mathbb{Z}. \end{array}$$

We apply (the abstract version formulation of) Pollard's rho method to the mixing function $\overline{f}$, and starting point $\overline{x}_0 = \overline{y}_0 \in \mathbb{Z}/p\mathbb{Z}$. Then pollards rho method says we will find a collision $\overline{x}_k = \overline{y}_k$ for $k = \mathcal{O}(\sqrt{p})$. But if $\overline{x}_k = \overline{y}_k$, this says $x_k \equiv y_k \mod p$, so in particular p divides $|x_k - y_k|$. Therefore p divides $g = \gcd(|x_k - y_k|, N)$ as desired.

In fact, one might worry that $g = N$ and we didn't in fact find a nontrivial divisor. This would imply that in fact $x_k = y_k$. By (the abstract formulation of) Pollard's rho method applied to f we see that this is expected for $k = \mathcal{O}(\sqrt{N})$. If $\sqrt{p} < \sqrt{N}$, we'd likely stumble upon a pair congruent mod p before one congruent mod N. (Notice that this didn't happen every time, and sometimes one had to modify the mixing function and starting point in order to make this happen). □

(b) Compare what happened in 3(b) and 3(c). Did one have a faster run time? Why?
For me it seemed like they were comprable. $x^2 + 1$ was much faster for 2201 but $x^2 + 2$ was faster in the other two cases (in particular it was much faster fo 9409613). I suppose it comes down to how 'random' f is modulo the various primes.

(c) Explain what happened in 3(d) when the mixing function was $f(x) = x^2$.
x^2 was much solwer especially for larger values of N. This makes sense because x^2 is not particularly random, especially at the beginning, in fact up until $x = \sqrt{N}$ it behaves very predictably.

(d) Explain what happened in 3(e) when the mixing function was $f(x) = x^2 - 2$. With starting point 2, $x^2 - 2 = 2$ so that $x_i = y_i$ for every i, and in particular the gcd found is N itself. Once I switched the starting point to 3 it worked, but much much more slowly. (For $N = 1782886219$ it to 1080 steps, compared to 660 for x^2 and 68 for $x^2 + 2$). This is actually slightly perplexing for me.

(e) Explain what happened in 3(f) when N was prime. It can only return p, and does so in about $\mathcal{O}(\sqrt{p})$ as expected.

In class we stated and proved the forward direction of the following theorem.

Theorem 1. *Fix a cryptosystem with $\#\mathcal{M} = \#\mathcal{C} = \#\mathcal{K}$. The system has perfect secrecy if and only if the following two conditions hold.*

(1) Each key $k \in \mathcal{K}$ is used with equal probability.

(2) For each plaintext $m \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$ there exists a unique key $k \in \mathcal{K}$ with $e_k(m) = c$.

5. Complete the proof of Theorem 1 by proving the *only if* direction. That is, assuming conditions (1) and (2) hold, show the system has perfect secrecy.

Proof. We define the probability space $\Omega = \mathcal{M} \times \mathcal{C} \times \mathcal{K}$¡ and define the random variables M, C, K as the coordinate projections

$$M : \Omega \to \mathcal{M} \qquad C : \Omega \to \mathcal{C} \qquad K : \Omega \to \mathcal{K}.$$

As usual we let f_M, f_C, f_K be the associated density functions. We will prove 3 lemmas which together imply the result.

Lemma 1. *For all $c \in \mathcal{C}$, we have:*

$$\sum_{k \in \mathcal{K}} f_M(d_k(c)) = 1.$$

Proof of Lemma 1. By condition (2) we have a equality of sets

$$\{d_k(c) | k \in \mathcal{K}\} = \{m | m \in \mathcal{M}\}.$$

which makes the following equality tautological.

$$\sum_{k \in \mathcal{K}} f_M(d_k(c)) = \sum_{m \in \mathcal{M}} f_M(m).$$

For different values $m, m' \in \mathcal{M}$ the events $(M = m)$ and $(M = m')$ are disjoint. Therefore by Homework 8 4(e) we have:

$$\sum_{m \in \mathcal{M}} f_M(m) = \sum_{m \in \mathcal{M}} Pr(M = m) = Pr(\bigcup_{m \in \mathcal{M}} (M = m)).$$

But the latter is just $Pr(\Omega) = 1$ as desired. □

Lemma 2. *For all $c \in C$, we have:*

$$f_C(c) = \frac{1}{\#\mathcal{K}}.$$

Proof of Lemma 2. At the end of the November 10'th lecture we showed the identity:

$$f_C(c) = \sum_k \in \mathcal{K} f_K(k) f_M(d_K(c)). \tag{1}$$

We review the proof briefly (since it was rushed at the end of class). By HW 8 Problem Problem 5(c) we have the identity:

$$f_C(c) = Pr(C = c) = \sum_{k \in \mathcal{K}} Pr(C = c | K = k) Pr(K = k) = \sum_{k \in \mathcal{K}} f_{C|K}(c|k) f_K(k).$$

Then one observes that fixing k, we know that $C = c$ if and only if $M = d_k(c)$. Furthemore, as c is fixed, if $M = d_k(c)$ then $K = k$ (by assumption (2)), so that:

$$f_{C|K}(c|k) = Pr(C = c|K = k) = Pr(M = d_k(c)) = f_M(d_k(c)).$$

This completes the proof of Equation 1. By assumption (1) we know that $f_K(k) = 1/\#\mathcal{K}$, so that:

$$\begin{aligned} \sum_k \in \mathcal{K} f_K(k) f_M(d_K(c)) &= \sum_k \in \mathcal{K} \frac{1}{\#\mathcal{K}} f_M(d_K(c)) \\ &= \frac{1}{\#\mathcal{K}} \sum_{k \in \mathcal{K}} f_M(d_K(c)) \\ &= \frac{1}{\#\mathcal{K}} \end{aligned}$$

where the last step is Lemma 1, completing the proof. □

Lemma 3. *For all $c \in \mathbb{C}$ and $m \in \mathcal{M}$, we have:*

$$f_{C|M}(c|m) = \frac{1}{\#\mathcal{C}}.$$

Proof of Lemma 3. Once m is fixed, each value of c arises exactly once (for each value of k, this is assumption (2)). As each k arises with equal probability, therefore so does each c, completing the proof. □

Now we may prove the main result. Since $\#\mathcal{C} = \#\mathcal{K}$, we have $\frac{1}{\#\mathcal{C}} = \frac{1}{\#\mathcal{K}}$. Therefore by Lemmas 2 and 3, we have for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$ the identity $f_{C|M}(c|m) = f_C(c)$ which is the definition of perfect secrecy. □

6. Prove the following identities for binomial coefficients. (Parts (c) and (d) generalize computations in HW8 Problems 3(e) and 3(f)).
There are tons of lovely ways to prove these results, combinatorially, algebraically, numerically, and even with analysis of pascal's triangle. I will give what I think are rather slick algebraic proofs.

(a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Proof. By the binomial theorem:

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}.$$

But the left side is obviously 2^n. □

(b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

Proof. By the binomial theorem:

$$(-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

But the left side is obviously 0. □

(c) $\sum_{k \geq 0} \binom{n}{2k} = 2^{n-1}$

Proof. Adding together the formulas from part (a) and part (b) gives:

$$2^n + 0 = \sum_{k=0}^{n} \binom{n}{k} + (-1)^k \binom{n}{k} = \sum_{k \text{ even}} 2\binom{n}{k}.$$

Dividing by 2 gives the result. □

(d) $\sum_{k \geq 0} \binom{n}{2k+1} = 2^{n-1}$

Proof. Subtracting the formulas from part (a) and part (b) gives:

$$2^n - 0 = \sum_{k=0}^{n} \binom{n}{k} - (-1)^k \binom{n}{k} = \sum_{k \text{ odd}} 2\binom{n}{k}.$$

Dividing by 2 gives the result. □

7. Consider the elliptic curve E given by the equation $y^2 = x^3 - 2x + 4$. Let $P = (0, 2)$ and $Q = (3, -5)$.

(a) Show $P, Q \in E$.

Proof. Just plug and chug. For P:

$$2^2 = 4 \qquad 0^3 - 2 \cdot 0 + 4 = 4.$$

For Q:

$$(-5)^2 = 25 \qquad 3^3 - 2 \cdot 3 + 4 = 27 - 6 + 4 = 25.$$

□

(b) Compute $P \oplus Q$.

Proof. One first computes the line through P and Q. The slope is:

$$\frac{\Delta y}{\Delta x} = \frac{-5-2}{3-0} = -\frac{7}{3}.$$

Therefore the line is $y = -\frac{7}{3}x + 2$. We next intersect this with the curve. First square the y-coordinate:

$$\left(-\frac{7}{3}x + 2\right)^2 = \frac{49}{9}x^2 - \frac{28}{3}x + 4.$$

Subtracting this from the right hand side of the elliptic curve gives:

$$x^3 - \frac{49}{9}x^2 + \frac{56}{3}x = 0.$$

But we know this factors as:

$$(x-3)(x)(x-\alpha) = 0.$$

We want to find α. Expanding and considering coefficients of x^2 shows:

$$\alpha + 3 = \frac{49}{9},$$

so that $\alpha = \frac{22}{9}$. Plugging this back into the equation of the line gives:

$$\beta = -\frac{7}{3}\alpha + 2 = -\frac{100}{27}.$$

Therefore $P \oplus Q = (\alpha, -\beta) = \left(\frac{22}{9}, \frac{100}{27}\right)$. □

(c) Compute $P \oplus P$.

Proof. We first compute the tangent line to P. By implicit differentiation we have:

$$2y\frac{dy}{dx} = 3x^2 - 2,$$

so that

$$\frac{dy}{dx} = \frac{3x^2-2}{2y}.$$

Pluggin in P gives a slope:

$$\frac{dy}{dx}\Big|_{(0,2)} = \frac{-2}{4} = -1/2.$$

That way the tangent line is $y = -\frac{1}{2}x + 2$. Next intersect with the curve. As before we square the y coordinate

$$\left(-\frac{1}{2}x + 2\right)^2 = \frac{1}{4}x^2 - 2x + 4.$$

and subtract from the right side of the elliptic curve equation:

$$x^3 - \frac{1}{4}x^2 = 0.$$

We know this also factors as:

$$x^2(x-\alpha) = 0,$$

so that $\alpha = 1/4$. Plugging back into the equation of the line gives $\beta = 15/8$ so that we see that $2P = \left(\frac{1}{4}, -\frac{15}{8}\right)$. □

(d) Compute $P \oplus P \oplus P$.

Proof. The line between P and $2P$ is $y = -\frac{31}{2}x + 2$. Squaring and subtracting from the right side of the elliptic curve (of whom we know two roots) gives:

$$x^3 - \frac{961}{4}x^2 + 60x = 0 = (x)(x - 1/4)(x - \alpha).$$

Therefore $\alpha + 1/4 = 961/4$ so that $\alpha = 960/4 = 240$. Plugging back into the line and negating gives the point $(240, 3718)$. □