

## Homework 8

Due Saturday, November 7

Since we haven't introduced any new algorithms this week, there will be no implementation part.

## Written Part

1. In Hw 7 problem 7c you described an algorithm that recovered the first  $k$  bits of the discrete log modulo  $p$ , assuming that  $p - 1$  is divisible by  $2^k$ . Prove the correctness of this algorithm. In particular, there is some ambiguity when you take the square root in last week's algorithm. Why does the assumption that  $p - 1$  is divisible by  $2^k$  alleviate this ambiguity?
2. We've given several proofs of Fermat's Little Theorem. This exercise outlines another one that is of a very different flavor. Throughout we fix a prime number  $p$ .
  - (a) Let  $j$  be an integer with  $1 \leq j \leq p - 1$ . Prove that  $\binom{j}{p}$  is divisible by  $p$ .
  - (b) For any integers  $a, b$ , show that:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

(This identity is often called the *freshman's dream* by jaded calculus professors).

- (c) Prove Fermat's Little Theorem:  $a^p \equiv a \pmod{p}$  by induction on  $a$  using part (b) with  $b = 1$ .
3. Suppose we flip a coin times. Compute the probability of the following event.
  - (a) The probability that the first and last coins are both heads.
  - (b) The probability that at least one of the first and last coins is heads.
  - (c) The probability that exactly 5 coin tosses are heads.
  - (d) The probability that exactly  $k$  coin tosses are heads.
  - (e) The probability that an even number of coin tosses are heads.
  - (f) The probability that an odd number of coin tosses are heads.
4. We let  $Pr : \Omega \rightarrow \mathbb{R}$  be a probability theory.
  - (a) Let  $E$  be an event, and  $E^c$  its complement. Prove  $Pr(E^c) = 1 - Pr(E)$ .
  - (b) Let  $E$  and  $F$  be disjoint events. Prove that

$$Pr(E \cup F) = Pr(E) + Pr(F).$$

- (c) Let  $E$  and  $F$  be any two events (not necessarily disjoint). Prove that

$$Pr(E \cup F) = Pr(E) + Pr(F) - Pr(E \cap F).$$

- (d) Let  $E_1, E_2$ , and  $E_3$  be events. Prove that:

$$\begin{aligned} Pr(E_1 \cup E_2 \cup E_3) = & Pr(E_1) + Pr(E_2) + Pr(E_3) - Pr(E_1 \cap E_2) - Pr(E_1 \cap E_3) \\ & - Pr(E_2 \cap E_3) + Pr(E_1 \cap E_2 \cap E_3). \end{aligned}$$

- (e) Let  $E_1, E_2, \dots, E_n$  be  $n$  events. We say that the events are *pairwise disjoint* if  $E_i \cap E_j = \emptyset$  for all  $i \neq j$ . Show that if the events are pairwise disjoint then:

$$Pr(E_1 \cup E_2 \cup \dots \cup E_n) = Pr(E_1) + Pr(E_2) + \dots + Pr(E_n).$$

- (f) Let  $E_1, \dots, E_n$  be  $n$  (not necessarily disjoint) events. Conjecture a general formula for  $Pr(E_1 \cup E_2 \cup \dots \cup E_n)$  in terms of the probability of the  $E_i$  and their various intersections. This is called the *inclusion-exclusion* principle.

5. Let  $E, F$  be events.

- (a) Show that  $Pr(E|E) = 1$ . Explain in words why this is reasonable.  
 (b) Suppose that  $E$  and  $F$  are disjoint. Show that  $Pr(E|F) = 0$ . Explain in words why this is reasonable.  
 (c) Let  $F_1, \dots, F_n$  be pairwise disjoint and suppose  $F_1 \cup \dots \cup F_n = \Omega$ . Prove the following decomposition formula:

$$Pr(E) = \sum_{i=1}^n Pr(E|F_i)Pr(F_i).$$

- (d) Prove the following general version of Bayes' formula:

$$Pr(F_i|E) = \frac{Pr(E|F_i)Pr(F_i)}{\sum_{j=1}^n Pr(E|F_j)Pr(F_j)}.$$

6. This is the famous *Monty Hall Problem*. Ralph is on a game show, and Monty Hall gives Ralph the choice of a prize, behind one of 3 closed doors. Monty tell's Ralph that behind 2 of the doors are goats, and behind the third is a new car. Ralph chooses a door, and then Monty opens one of the remaining 2 doors revealing a goat! Monty then asks Ralph: *would you rather stick to the door you chose? Or switch to the other closed door?*

- (a) If Ralph always sticks with the same closed door, what are his chances of winning a car? What about if Ralph always switches? What is Ralph's best strategy?  
 (b) More generally, suppose that there are  $N$  doors,  $M$  cars, and Monty hall reveals  $K$  goats after Ralphs first choice. Compute the probabilities:

$$Pr(\text{Ralph wins a car} \mid \text{Ralph sticks}),$$

$$Pr(\text{Ralph wins a car} \mid \text{Ralph switches}).$$

Which is the better strategy? (Letting  $N = 1000, M = 1, K = 998$  makes the solution to part (a) seem less paradoxical).

7. In this exercise we study the probability of success of a Monte Carlo algorithm in quite a bit more generality than we considered in class. Let  $\mathcal{S}$  be a set (of integers), and  $\mathcal{A}$  an interesting property of elements of  $\mathcal{S}$ . Suppose that:

$$Pr(x \in \mathcal{S} \text{ is not } \mathcal{A}) = \delta.$$

Suppose that you have a Monte-Carlo algorithm that takes as input a random number  $r$  and some  $m \in \mathcal{S}$  and returns **Yes** or **No** satisfying:

- (1) If the algorithm returns **Yes**  $m$  is *definitely*  $\mathcal{A}$ .
  - (2) If  $m$  has  $A$ , then the property that the algorithm returns **Yes** is at least  $P$ .
    - (a) Express conditions (1) and (2) as conditional probabilities
    - (b) Suppose we run the algorithm  $N$  times on a fixed  $m \in \mathcal{S}$ , and the algorithm returns **No** each time. Derive a lower bound in terms of  $\delta, P$  and  $N$  for the probability that  $m$  is *not*  $\mathcal{A}$ . (In class we did this for  $\delta = .01$  and  $P = 1/2$ . Here you will have to be more careful about distinguishing  $P$  and  $1 - P$ .)
8. We can now compute the probability of correctness for **probablyPrime**. Recall that if  $n$  is a composite number, then 75% of integers between 2 and  $n - 1$  are Miller-Rabin witnesses to the compositeness of  $n$ . You will also need the prime number theorem, which we interpret as saying the probability of an integer  $n$  being prime is approximately  $\ln(n)/n$ .
- (a) Suppose **probablyPrime**( $n$ ) returns **True**. Compute the probability that  $n$  is prime.
  - (b) Suppose instead of running the Miller-Rabin test on 20 potential witnesses, **probablyPrime** runs the test on  $N$  potential witnesses. If **probablyPrime**( $n$ ) returns **True**, compute the probability that  $n$  is prime in terms of  $N$ .