CS 70 Discrete Mathematics and Probability Theory
Fall 2016 by Sinho Chewi, Jin Park, Alvin Wan, Davis Yang **Review**

1. **Divisible or Not**

   (a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, '23xx' is divisible by 4 if and only if the number 'xx' is divisible by 4.)

   (b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

Solution:

(a) Using modular arithmetic, the proof is simple. We can prove both directions of the implication at once. Take n, which has k digits.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 \dots 10^k n_k = \sum_{i=1}^{k} 10^i n_i$$

We can take $n(\bmod 4)$ and see that all terms n_2 up to n_k drop out since $10^2, 10^3 \dots 10^k$ are all divisible by 4.

$$n = n_0 + 10n_1 (\bmod 4)$$

$n_0 + 10n_1$ is 0 in mod 4 if and only if n is 0 in mod 4, proving that the number formed by the last digits is divisible by 4 if and only if the entire number n is divisible by 4.

Let us now consider the alternative solution, where we do not use modular arithmetic.

Alternative Solution

Let P be "the last two digits of n are divisible by 4", and Q be "n is divisible by 4."

Forward Direction: $P \implies Q$

Let us re-express any number n as a function of its digits. Let n_i be the ith digit of the number n. We know that the number will thus have the following value, for some k-digit number.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 \dots 10^k n_k$$

We know that since 10^2 is divisible by 4, $10^2 n_2$ is divisible by 4 for all possible values of n_2. This is true for all $n_3 \dots n_k$. Since the number formed by the first two digits $n_0 + 10n_1$ is divisible by 4, n is divisible by 4.

Reverse Direction: $Q \implies P$

If n is divisible by 4, we can re-express $n = 2k$ for some integer k. We wish to prove that this implies the first two digits are divisible by 4. We see

$$n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 \ldots 10^k n_k = 4k$$

Re-arrange, and we have

$$\frac{n_0 + 10n_1}{4} + 25n_2 + 250n_3 \ldots 25 * 10^{k-1} n_k = k$$

Since k is an integer, and all values after the first two terms are integers, we have that $\frac{n_0+10n_1}{4}$ is necessarily an integer. This implies that 4 divides $n_0 + 10n_1$.

(b) We will again use modular arithmetic to prove both directions of the implication at once. We will show that the sum of the digits is divisible by 3 is equal to condition that the sum of all the digits is divisible by 3.
Consider the following expression for n.

$$n = \sum_{i=1}^{k} 10^i n_i (\text{ mod } 3)$$

Note that in mod 3, $10 = 1$, so in mod 3, this is equivalent to

$$n = \sum_{i=1}^{k} n_i (\text{ mod } 3)$$

As it turns out, the latter expression is exactly the sum of all the digits in n. As a result, n is 0 in mod 3 if and only if the sum of all the digits is 0 in mod 3.

2. **Squared RSA**

(a) Prove the identity $a^{p(p-1)} \equiv 1 \pmod{p^2}$, where a is relatively prime to p and p is prime.

(b) Use the identity above to construct a RSA scheme. In other words, what is the public key and private key?

(c) Prove that your scheme is correct, i.e. $x^{ed} \equiv x \pmod{N}$.

(d) Prove that your scheme is unbreakable, i.e. your scheme is at least as difficult as ordinary RSA.

Solution:

(a) Consider the set S of all numbers between 1 and $p^2 - 1$ (inclusive) which are relatively prime to p. Consider the map $f(x) = ax$, and let T be the image of S, i.e. $T = f(S)$. Since a is relatively prime to p, and therefore relatively prime to p^2, we know that $a^{-1} \pmod{p^2}$ exists, modulo p^2. Since the inverse exists, we know that $f(x)$ has an inverse map, and is therefore a bijection: $|S| = |T|$. To show that $S = T$, it suffices to show that $T \subseteq S$. But if $t \in T$, then $t = as$ for some $s \in S$ with s relatively prime to p^2. Since a

is also relatively prime to p^2, then $as = t$ is also relatively prime to p^2. We have shown that $t \in T$ implies $t \in S$, so $T \subseteq S$ (and by the discussion above, $T = S$). Finally, observe that the product of the elements of S is the same as the product of the elements of T, so

$$\prod_{i=1}^{|S|}\{s : s \in S\} = \prod_{i=1}^{|S|}\{t : t \in S\} \pmod{p^2}$$
$$= a^{|S|}\prod_{i=1}^{|S|}\{s : s \in S\} \pmod{p^2}$$

so we can conclude that $a^{|S|} \equiv 1 \pmod{p^2}$. To conclude the argument, we show that $|S| = p(p-1)$. But there are p^2 numbers between 1 and p^2, and if we subtract the p multiples of p, we end up with $|S| = p^2 - p = p(p-1)$.

(b) We will let our public key be $(N = p^2q^2, e)$ for primes p and q, with e relatively prime to $p(p-1)q(q-1)$. We let our private key be $d = e^{-1} \pmod{p(p-1)q(q-1)}$.

(c) By the definition of d above, $ed = 1 + kp(p-1)q(q-1)$ for some k. Look at the equation $x^{ed} \equiv x \pmod{N}$ modulo p^2 first:

$$x^{ed} \equiv x^{1+kp(p-1)q(q-1)} \equiv x \cdot (x^{p(p-1)})^{kq(q-1)} \equiv x \pmod{p^2}$$

where we used the identity above. If we look at the equation modulo q^2, we obtain the same result. Hence, $x^{ed} \equiv x \pmod{p^2q^2}$.

(d) We consider the scheme to be broken if knowing p^2q^2 allows you to deduce $p(p-1)q(q-1)$. (Observe that knowing $p(p-1)q(q-1)$ is enough, because we can compute the private key with this information.) Suppose that the scheme can be broken; we will show how to break ordinary RSA. For an ordinary RSA public key $(N = pq, e)$, square N to get $N^2 = p^2q^2$. By our assumption that the squared RSA scheme can be broken, knowing p^2q^2 allows us to find $p(p-1)q(q-1)$. We can divide this by $N = pq$ to obtain $(p-1)(q-1)$, which breaks the ordinary RSA scheme. This proves that our scheme is at least as difficult as ordinary RSA.

Remark: The first part of the question mirrors the proof of Fermat's Little Theorem. The second and third parts of the question mirror the proof of correctness of RSA.

3. **Safety of Secret Sharing**

In class we derived the secret sharing scheme to protect a secret s among n people such that any group of $\geq k$ people could recover the secret, and any group of $< k$ people cannot. In this problem let's explore the safety of secret sharing from a probability point of view. Suppose that we are working in the finite field GF(p). Alice, Bob and Cathy share a secret s that can be recovered if and only if all of them come together. Now, suppose that only Alice and Bob come together. Show that the probability of them recovering the secret is as low as the probability of a random guess.

Solution:

Alice and Bob require 3 points to recover the polynomial, but between them, they only have 2 points. There are p possible choices for the third choice, and the true polynomial goes through one of them, so the probability that they can recover the polynomial is $1/p$. This is the same as the probability of randomly guessing the secret in the first place, since there were p possibilities for the secret.

4. **Berlekamp-Welch Algorithm with Fewer Errors**

In class we derived how Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors?

Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4,4,4)$ to Bob.

(a) Suppose Bob receives the message $(4,5,4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4,4,4)$. Show that the $Q(x), E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(c) Show that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(d) Suppose you're actually trying to decode the received message $(4,4,4)$. Based on what you showed in the previous two parts, can you predict what will happen during row reduction when you try to solve for the unknowns?

(e) As you showed in the previous part, when there are less than k errors and Bob actually receives $n+2k$ packets, there will be multiple possible $Q(x)$ and $E(x)$ polynomials. Prove that no matter what the solution of $Q(x)$ and $E(x)$ are, the recovered $P(x)$ will always be the same.

Solution:

(a) $E(x) = x - 1$ and $Q(x) = P(x)E(x) = 4x - 4$.

(b) This is true because there were no errors, so $P(i) = r_i$ for $i = 0,1,2$.

(c) Since $Q(x) = P(x)E(x)$ and $P(i) = r_i$ for $i = 0,1,2$, we must have $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(d) There are multiple solutions to the system of equations.

(e) If $Q(x)$ and $E(x)$ are solutions to the system of equations, then we know that $r_i E(i) = P(i)E(i) = Q(i)$ holds for $n+2k$ equations. Since $P(x)E(x) - Q(x)$ is a polynomial of degree at most $n+k-1$ that is 0 at $n+2k$ points, we know that it must be the zero polynomial, i.e. $P(x)E(x) = Q(x)$.

5. **Hotel Bert**

Hillbilly Bert has a hotel H that has infinite rooms R_i where $i \in \mathbb{N}$. Due to the popularity of the hotel, each room is filled with one person P_i. However, infinite rooms allows him to accomodate more guests. Prove, with bijection, that he can accomodate the following:

(a) One new guest G_1.

(b) Infinitely new guests G_j where $j \in \mathbb{N}$.

(c) Consider a car with infinite guests, $C_j = (G_{j1}, G_{j2}, ...)$ where $j \in \mathbb{N}$. How can he accommodate all guests in the infinite cars?

Solution:

(a) Move current people to the next room. Then, put the guest in the first room. In other words, $P_i \leftrightarrow R_{i+1}$, and $G_1 \leftrightarrow R_1$.

(b) Move current people to every even room. Then, interweave the new guests in every odd room. In other words, $P_i \leftrightarrow R_{2i}$, and $G_i \leftrightarrow R_{2i-1}$.

(c) Notice that each guest has an "address": what car s/he is in and what seat number s/he is. In other words, $G_{ij} \in \mathbb{N}^2$. Through the spiral method, we know there is a bijection between $\mathbb{N}^2 \leftrightarrow \mathbb{N}$. This reduces to the same exact problem as part b! Therefore, we can accommodate these guests.

6. **Hello World!**

Determine the computability of the following tasks. If it's not computable, write a reduction or self-reference proof. If it is, write the program.

(a) You want to determine whether a program P on input x outputs "Hello World!". Is there a computer program that can perform this task? Justify your answer.

(b) You want to determine whether a program P prints "Hello World!" by a specific line k. Is there a computer program that can perform this task? Justify your answer.

(c) You want to determine whether a program P prints "Hello World!" in the first k lines of code run. Is there a computer program that can perform this task? Justify your answer.

Solution:

(a) Incomputable. We will reduce such computer program PrintsBoo(P, x) to TestHalt.

```
P'(x):
  run P(x) while suppressing print statements
  print("Hello World!")

TestHalt(P, x):
  if PrintsBoo(P', x):
    return true
```

```
else:
  return false
```

If PrintsBooo exists, TestHalt must also exist by this reduction. Since TestHalt cannot exist, PrintsBoo cannot exist.

(b) Incomputable. Reduce this program PrintsBooByK(P, x, k) to the PrintsBoo(P, x) in part a.

```
PrintsBoo(P, x):
  # Find all "return" statements in P and put these
  # line numbers in set S
  return_statements = []
  for i in range(len(P)):
    if isReturnStatement(i):
      return_statements.append(i)

  # For each "return" statement, check if "Hello World!"
  # is printed
  For r in return_statements:
    if PrintsBooByK(P, x, r):
      return true
  return false
```

(c) Computable. You can simply run the program until k lines are executed. If P has halted by then, return true. Else, return false.

7. **Montagues and Countulets!**

Two families, Montagues and Capulets, each have n men and n women. However, due to family rivalry, the Montagues and Capulets do not marry each other. Answer the following questions about marriage arrangements.

(a) How many ways marriage arrangements are there for just the Montague family?

(b) How many marriage arrangments are there for both the Montagues and Capulets?

(c) Now, say Romeo Montague and Juliet Capulet **can** (but not necessarily) get married. How many marriage arrangements are there for both families?

Solution:

(a) The first female has n options for a man. The next has $n-1$ and so on and so forth. Thus, there are $n!$ arrangements.

(b) We simply square the answer to part a. $(n!)^2$

(c) Consider the case where Romeo and Juliet are paired. Then, there is $n-1$ Capulet males left and n Capulet females. There is no arrangement that can be created since the number of men and women are mismatched within the Montagues (a similar argument

can be made for Capulets). Since there is no arrangement in which Romeo and Juliet are paired, the number of arrangements is equal to part b, $(n!)^2$.

8. **Presidential Election**

We want to determine which presidential candidate will win this coming election. There are two candidates, Clinton and Trump.

(a) For each state, Clinton has p chance of winning. What is the probability that Clinton will win exactly half the states (there are 50 states)?

(b) What is the probability that she will win at least one state?

(c) Say that $p = 0.25$ or $p = 0.75$ with equal chance. If Clinton wins every single state, what is the probability that $p = 0.75$? (Hint: Use Bayes Rule)

Solution:

(a) There are 50 choose 25 ways to choose 25 out of 50 states for Clinton to win. In this situation, there is p chance that Clinton will win each state, so the total probability she will win all 25 states is p^{25}. There is $(1-p)$ chance that Trump will win the other 25 states, so the total probability he will win the other 25 states is $(1-p)^{25}$. Combining these probabilities with the ways to choose 25 states yields $\binom{50}{25} p^{25}(1-p)^{25}$.

(b) We will compute the complement probability and then subtract from 1, since the complement is much easier to compute. The complement of Hilary winning at least one state is that she wins no states. This is equivalent to Trump winning all states, or $(1-p)^{50}$. Subtracting this from one yields $1-(1-p)^{50}$.

(c) Using Bayes Rule,

$$\begin{aligned} P(p=0.75|C) &= \frac{P(C|p=0.75)P(0.75)}{P(C)} \\ &= \frac{P(C|p=0.75)P(0.75)}{P(C|p=0.75)P(0.75)+P(C|p=0.25)P(0.25)} \\ &= \frac{(0.75^{50})(0.5)}{(0.75^{50})(0.5)+(0.25^{50})(0.5)} \\ &\approx 1 \end{aligned}$$