CS 70 Discrete Mathematics and Probability Theory
Spring 2016 Rao and Walrand HW 4

Due Thursday 18th at 10PM

1. **Amaze your friends!**

   (a) You want to trick your friends into thinking you can perform mental arithmetic with very large numbers What are the last digits of the following numbers?

   i. 11^{2014}

   ii. 9^{10001}

   iii. $3^{987654321}$

   (b) You know that you can quickly tell a number n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. Prove that you can use this trick to quickly calculate if a number is divisible by 9.

   Answer:

   Motivation for Problem: This problem causes students to start recognizing tricks regarding modular arithmetic. This lays the ground later for proving properties of modular arithmetic.

   Solutions:

   (a) i. 11 is always 1 mod 10 therefore the answer to (a) is 1.

   ii. 9 is its own inverse mod 10, therefore, if 9 is raised to an odd power, the number will be 9 mod 10. So the answer is 9

   iii. $3^4 = 9^2 = 1$ mod 10. We see that the exponent $987654321 = 1$ mod 4 so the answer is 3.

   (b) Let n be written as $a_k a_{k-1} \cdots a_1 a_0$ where the a_i are digits, base-10. We can write $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10 a_1 + a_0 = (10^k - 1) a_k + (10^{k-1} - 1) a_{k-1} + \cdots + (10-1) a_1 + \sum_{i=0}^{k} a_i$

   The first few terms are all divisible 9; they're all of the form $99 \cdots 99 \cdot a_i$. So if the sum at the end is divisible by 9, then n is too and vice versa.

2. **Short Answer: Modular Arithmetic**

   (a) What is the multiplicative inverse of $3 \pmod 7$?

   Answer: $5 \pmod 7$.
   $(3)(5) = 15 = 1 \pmod 7$

   (b) What is the multiplicative inverse of $n-1$ modulo n? (An expression that may involve n. Simplicity matters.)

   Answer: $n-1 \pmod n$.
   Its $-1 \pmod n$! Or $(n-1)(n-1) = n^2 - 2n + 1 = 1 \pmod n$.

(c) What is the solution to the equation $3x = 6 \pmod{17}$? (A number in $\{0,\dots,16\}$ or "No solution".)

Answer: 2.
Muliply both sides by 6 the multiplicative inverse of 3 and reduce.

(d) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n = 2 \pmod{3}$ for $n \geq 1$? (True or False)

Answer: True.
Take the recursive formula modulo 3. This is a warmup question for the next problem.

(e) Given that $extended-gcd(53,m) = (1,7,-1)$, that is $(7)(53)+(-1)m = 1$, what is the solution to $53x+3 = 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consists of fractions.)

Answer: $x = 49 \pmod{m}$
Follows from 7 being multiplicative inverse of $53 \pmod{m}$.

3. **(Combining moduli)** Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5,8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod{5}$ and $c \pmod{8}$.

(a) What is $8 \pmod{5}$ and $8 \pmod{8}$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod{5}$ and $a \equiv 0 \pmod{8}$.

Answer: $8 \equiv 3 (\bmod 5)$ and $8 \equiv 0 (\bmod 8)$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 (\bmod 5)$. Therefore 16 satisfies both conditions.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod{5}$ and $b \equiv 1 \pmod{8}$.

Answer: We can find such a number by considering multiples of 5,i.e.0,5,10,15,20,25,30,35, and find that if $b = 25$, $25 \equiv 1 (\bmod 8)$, so it satisfies both conditions.

(c) Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod{5}$ and $c \equiv 5 \pmod{8}$. Find c by expressing it in terms of a and b.

Answer: We claim $c \equiv 2a+5b \equiv 37 (\bmod 40)$. To see that $c \equiv 2 (\bmod 5)$, we note that $b \equiv 0 (\bmod 5)$ and $a \equiv 1 (\bmod 5)$. So $c \equiv 2a \equiv 2 (\bmod 5)$. Similarly $c \equiv 5b \equiv 5 (\bmod 8)$.

(d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod{5}$ and $d \equiv 4 \pmod{8}$.

Answer: We can repeat the same procedure as above, and find that $d = 3a+4b \equiv 28 (\bmod 40)$.

(e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod{5}$, and $c \times d \equiv 5 \times 4 \pmod{8}$?

Answer: $c \times d = 37 \times 28 \equiv 36 \pmod{40}$. Note that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a \times c \equiv b \times d \pmod{n}$.Therefore we can multiply $c \equiv 2 \pmod{5}$ and $d \equiv 3 \pmod{5}$ to get

$c \times d \equiv 2 \times 3 \pmod 5$. Similarly we can multiply these equations (mod 8) and get $c \times d = 5 \times 4 \pmod 8$.

4. **(The last digit)**
Let a be a positive integer. Consider the following sequence of numbers x defined by:

$$\begin{aligned} x_0 &= a \\ x_n &= x_{n-1}^2 + x_{n-1} + 1 \text{ if } n > 0 \end{aligned}$$

(a) Show that if the last digit of a is 3 or 7, then for every n, the last digit of x_n is respectively 3 or 7.

Answer: To answer this question, we can study how the last digit of x_n changes from n to $n+1$. We have the following table:

x_n mod 10	x_{n+1} mod 10
0	1
1	3
2	7
3	3
4	1
5	1
6	3
7	7
8	3
9	1

(b) Show that there exist $k > 0$ such that the last digit of x_n for $n \geq k$ is constant. Give the smallest possible k,
no matter what a is. **Answer:** 3 and 7 appear as our fixed points. Once we reach one of these, we stay there for all the following iterations by the previous question. But it is not immediate that we always reach one of the fixed points, and this is what we need to prove. Let's unroll each of the 10 cases for a for a few iterations and verify that we always reach 3 or 7.

a mod 10	$x_1, x_2, \ldots$ mod 10
0	1, 3, 3, 3, ...
1	3, 3, 3, ...
2	7, 7, 7, ...
3	3, 3, 3, ...
4	1, 3, 3, 3, ...
5	1, 3, 3, 3, ...
6	3, 3, 3, 3, ...
7	7, 7, 7, 7, ...
8	3, 3, 3, 3, ...
9	1, 3, 3, 3, ...

This case-splitting proves the claim. We can see from the table that $k = 2$ is the smallest constant such that the last digit of x_n is constant for $n \geq k$.

5. (a) Compute the inverse of 37 modulo 64 using Euclid's extended GCD algorithm.

Answer:

We can use the following form to find the inverse using Euclid's extended GCD algorithm, and the x,y for this case would be 64 and 37 since we need to have $x \geq y \geq 0$;

x,y	d	a,b
64, 37	1	11, -19
37, 27	1	-8, 11
27, 10	1	3, -8
10, 7	1	-2, 3
7, 3	1	1, -2
3, 1	1	0, 1
1, 0	1	1, 0

Here's how to read the chart:
The LHS top down is just the standard GCD algorithm, the last row indicates where we find the GCD for 64 and 37, which is 1. Then the RHS (including the middle column) bottom up is the recursive return value for extended GCD algorithm. Finally, the a,b value (11,-19) in the top row will be the return value for extended-gcd(64,37). We can check that this pair is indeed the value we are looking for by calculating $11*64-19*37=1$ i.e. $a*x+b*y=1$
Therefore, the inverse of 37 modulo 64 is -19.

(b) Prove that $gcd(F_n, F_{n-1}) = 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

Answer: We prove this by induction.

In the base case, we have $gcd(F_1, F_0) = gcd(1,0) = 1$, which is trivially true.
Inductive hypothesis: Assume we have $gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$
Inductive steps: Now we need to show that $gcd(F_{k+1}, F_k) = 1$ as well.
We can show that:
$gcd(F_{k+1}, F_k) = gcd(F_k + F_{k-1}, F_k) = gcd(F_k, (F_k + F_{k-1}) - F_k) = gcd(F_k, F_{k-1}) = 1$
Therefore the statement is also true for $n = k+1$.
By the rule of induction, we can conclude that $gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$ where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

6. **Bijections**

Let n be an odd number. Let $f(x)$ be a function from $\{0, 1, \ldots, n-1\}$ to $\{0, 1, \ldots, n-1\}$. In each of these cases say whether or not $f(x)$ is a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

Answer: Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$ (See Lemma 7.1 from Lecture note 7). Since n is odd, $gcd(2, n) = 1$, so the multiplicative inverse of 2 exists (See Theorem 6.2 from Lecture note 6).

(b) $f(x) = 5x \pmod{n}$.

Answer: Not a bijection. For example, $n = 5, f(0) = f(1) = 0$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ x^{-1} \pmod{n} & \text{if } x \neq 0 \end{cases}$$

Answer: Bijection, because the multiplicative inverse is unique (Theorem 6.2).

(d) n is prime and $f(x) = x^2 \pmod{n}$.

Answer: Not a bijection. For example, if n = 3, f (1) = f (2) = 1.

7. Using RSA (8 points, 5/3)

Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

(a) Assuming $p = 3$, $q = 11$, and $e = 7$, what is d? Calculate the exact value.

Answer: $(3-1)(11-1) = 20$, so d is the multiplicative inverse of 7 mod 20. Run egcd$(20,7)$ and get $1 = (-1) \times 20 + (3) \times 7$, so $d = 3$.

Note: You can also try $d = 1, 2, 3, \ldots$ and get $d = 3$.

(b) Following Part (a), what is the original message if Bob receives 4? Calculate the exact value.

Answer: $N = 3 \times 11 = 33$. $4^d = 4^3 = 64 \equiv 31 \pmod{33}$.

8. Tweaking RSA

(This problem will not be graded, the solution will be posted on the problem thread on piazza.)

(a) You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$. Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

Answer: Choose e such that it is coprime with $p-1$, and choose $d \equiv e^{-1} \pmod{p-1}$.
We want to show x is recovered by $E(x)$ and $D(y)$, such that $D(E(x)) = x$.
In other words, $x^{ed} \equiv x \pmod{p}$ $\forall x \in \{0, 1, \ldots, N-1\}$.
Proof: By construction of d, we know that $ed \equiv 1 \pmod{p-1}$. This means we can write $ed = k(p-1) + 1$, for some integer k, and $x^{ed} = x^{k(p-1)+1}$.

- x is a multiple of p: Then this means $x = 0$, and indeed, $x^{ed} \equiv 0 \pmod{p}$.
- x is not a multiple of p: Then $x^{ed} \equiv x^{k(p-1)+1} \equiv x^{k(p-1)}x \equiv 1^k x \equiv x \pmod{p}$, by using FLT.

And for both cases, we have shown that x is recovered by $E(D(y))$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

Answer: Since Eve knows $N = p$, and $d \equiv e^{-1} \pmod{p-1}$, now she can compute d using EGCD.

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so.

Answer: Let e be co-prime with $(p-1)(q-1)(r-1)$. Give the public key: (N, e) and calculate $d = e^{-1} \bmod (p-1)(q-1)(r-1)$. People who wish to send me a secret, x, send $y = x^e \bmod N$. We decrypt an incoming message, y, by calculating $y^d \bmod N$.

Does this work? We prove that $x^{ed} - x \equiv 0 \bmod N$, and thus $x^{ed} = x \bmod N$.
To prove that $x^{ed} - x \equiv 0 \bmod N$, we factor out the x to get
$x \cdot (x^{ed-1} - 1) = x \cdot (x^{k(p-1)(q-1)(r-1)+1-1} - 1)$ because $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$.

We now show that $x \cdot (x^{k(p-1)(q-1)(r-1)} - 1)$ is divisible by p, q, and r. Thus, it is divisible by N, and $x^{ed} - x \equiv 0 \bmod N$.

To prove that it is divisible by p:

- if x is divisible by p, then the entire thing is divisible by p.
- if x is not divisible by p, then that means we can use FLT on the inside to show that $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod p$. Thus it is divisible by p.

To prove that it is divisible by q:

- if x is divisible by q, then the entire thing is divisible by q.
- if x is not divisible by q, then that means we can use FLT on the inside to show that $(x^{q-1})^{k(p-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod q$. Thus it is divisible by q.

To prove that it is divisible by r:

- if x is divisible by r, then the entire thing is divisible by r.
- if x is not divisible by r, then that means we can use FLT on the inside to show that $(x^{r-1})^{k(p-1)(q-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod r$. Thus it is divisible by r.