CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

DIS 2B

1 Touring Hypercube

In the lecture, you have seen that if G is a hypercube of dimension n, then

- The vertices of G are the binary strings of length n.
- u and v are connected by an edge if they differ in exactly one bit location.

A *Hamiltonian tour* of a graph is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that:

- Each vertex appears exactly once in the sequence.
- Each pair of consecutive vertices is connected by an edge.
- v_0 and v_k are connected by an edge.

(a) Show that a hypercube has an Eulerian tour if and only if n is even. (*Hint: Euler's theorem*)

(b) Show that every hypercube has a Hamiltonian tour.

Solution:

(a) In the n-dimensional hypercube, every vertex has degree n. If n is odd, then by Euler's Theorem there can be no Eulerian tour. On the other hand, the hypercube is connected: we can get from any one bit-string x to any other y by flipping the bits they differ in one at a time. Therefore, when n is even, since every vertex has even degree and the graph is connected, there is an Eulerian tour.

(b) By induction on n. When $n = 1$, there are two vertices connected by an edge; we can form a Hamiltonian tour by walking from one to the other and then back.

Let $n \geq 1$ and suppose the n-dimensional hypercube has a Hamiltonian tour. Let H be the $n+1$-dimensional hypercube, and let H_b be the n-dimensional subcube consisting of those strings with initial bit b.

By the inductive hypothesis, there is some Hamiltonian tour T on the n-dimensional hypercube. Now consider the following tour in H. Start at an arbitrary vertex x_0 in H_0, and follow the tour T except for the very last step to vertex y_0 (so that the next step would bring us back to x_0). Next take the edge from y_0 to y_1 to enter cube H_1. Next, follow the tour T in H_1 backwards from y_1, except the very last step, to arrive at x_1. Finally, take the step from x_1 to x_0 to complete

the tour. By assumption, the tour T visits each vertex in each subcube exactly once, so our complete tour visits each vertex in the whole cube exactly once.

To build some intuition, here are the first few cases:

- $n = 1$: 0, 1
- $n = 2$: 00, 01, 11, 10 [Take the $n = 1$ tour in the 0-subcube (vertices with a 0 in front), move to the 1-subcube (vertices with 1 in front), then take the tour backwards. We know 10 connects to 00 to complete the tour.]
- $n = 3$: 000, 001, 011, 010, 110, 111, 101, 100 [Take the $n = 2$ tour in the 0-subcube, move to the 1-subcube, then take the tour backwards. We know 100 connects to 000 to complete the tour.]

The sequence produced with this method is known as a Gray code.

2 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, we can prove both directions of the implication at once. Take n, which has k digits.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = \sum_{i=0}^{k-1} 10^i n_i$$

We can take $n \pmod 4$ and see that all terms n_2 up to n_{k-1} drop out since $10^2, 10^3, \ldots, 10^{k-1}$ are all divisible by 4.

$$n \equiv n_0 + 10n_1 \pmod 4$$

$n_0 + 10n_1$ 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. We know that the number will thus have the following value, for some k-digit number.

$$n = n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1}$$

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 $n_3, \ldots, n_{k-1}$. 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 $n = 4l$ for some integer l. We wish to prove that this implies the last two digits are divisible by 4. We see

$$n_0 + 10n_1 + 10^2 n_2 + 10^3 n_3 + \cdots + 10^{k-1} n_{k-1} = 4l.$$

Re-arrange, and we have

$$\frac{n_0 + 10n_1}{4} + 25n_2 + 250n_3 + \cdots + 25 \cdot 10^{k-3} n_{k-1} = l.$$

Since l is an integer, and all values after the first two terms are integers, we have that $(n_0 + 10n_1)/4$ 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 condition that n is divisible by 3 is equivalent to condition that the sum of n's digits is divisible by 3.

Consider the following expression for n.

$$n = \sum_{i=0}^{k-1} 10^i n_i \pmod 3$$

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

$$n \equiv \sum_{i=0}^{k-1} n_i \pmod 3.$$

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.

3 Modular Practice

(a) Calculate $72^{316} \bmod 7$.

(b) Solve the following system for x:

$$\begin{aligned} 3x &\equiv 4+y \pmod 5 \\ 2(x-1) &\equiv 2y \pmod 5 \end{aligned}$$

(c) If it exists, find the multiplicative inverse of 31 mod 23 and 23 mod 31.

(d) What theorem allows us to know of the existence of multiplicative inverses?

(e) Prove the theorem in part (d).
(Hint: Remember an iff needs to be proven both directions. The gcd cannot be 0 or negative.)

Solution:

(a) Notice that $72 \equiv 2 \pmod 7$. Also notice that $2^3 = 8 \equiv 1 \pmod 7$. Then

$$72^{316} \equiv 2^{316} \equiv 2 \cdot 2^{315} \equiv 2 \cdot (2^3)^{105} \equiv 2 \cdot 1^{105} \equiv 2 \pmod 7$$

(b) Solving the system we get $2x \equiv 3 \pmod 5$. At this point, the student must remember that he/she cannot divide by 2 and must find the inverse. We can multiply both sides by $2^{-1} \pmod 5$. Since $2 * 3 \equiv 1 \pmod 5$, we multiply 3 on both sides of the second equation to get $x - 1 \equiv 6y \pmod 5$, which can be simplified to $x - 1 \equiv y \pmod 5$. (Note that division by 2 in normal arithmetic is the same as multiplying by 2^{-1} in modular arithmetic.) Our final solution is $x = 4$.

(c)

31	23	-20	27	1
23	8	7	-20	1
8	7	-6	7	1
7	1	1	-6	1
1	0	1	1	1

The table above is running egcd algorithm. First apply the gcd on the left two columns. After confirming that the gcd is 1, we then start the process of finding the multiplicative inverse by using the egcd algorithm explained in the notes. (Remember that finding the multiplicative inverse for $a \pmod b$ is to find an x to fulfill $a * x \equiv 1 \mod b$.) Using this tabular form will speed up your process (compared to writing out equations each time).

$$31^{-1} \bmod 23 = 3 = -20$$
$$23^{-1} \bmod 31 = 27$$

(d) Let n, x be positive integers. Then x has a multiplicative inverse modulo n if and only if

$$\gcd(n, x) = 1.$$

(e) If x has a multiplicative inverse modulo n, then $\gcd(n,x) = 1$.

Given that x has a multiplicative inverse modulo n, we can proceed as follows:

Assume for the sake of contradiction that the gcd, d, is greater than 1.

$$\begin{aligned} xa &\equiv 1 \pmod{n} \\ xa &= bn + 1 \\ \frac{xa}{d} &= \frac{bn+1}{d} \\ \frac{xa}{d} &= \frac{bn}{d} + \frac{1}{d} \end{aligned}$$

We've reached a contradiction because xa/d and bn/d must both be integers, however, $1/d$ is not. Therefore we've reached a contradiction, and because the gcd cannot be 0 or negative, it must be 1.

If $\gcd(n,x) = 1$, then x has a multiplicative inverse modulo n. The proof is as follows:

We know $\exists\, a,b \in \mathbb{Z}$ such that

$$\begin{aligned} an + bx &= 1, \\ bx &\equiv 1 \pmod{n}. \end{aligned}$$

Thus, x has a multiplicative inverse b.

4 Modular Arithmetic Equations

Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $9x \equiv 1 \pmod{11}$.

(b) $3x + 15 \equiv 4 \pmod{21}$.

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

Solution:

(a) Multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get $x \equiv 5 \pmod{11}$.

(b) Subtract 15 from both sides to get $3x \equiv 10 \pmod{21}$. Now note that this implies $3x \equiv 1 \pmod{3}$, since 3 divides 21, and the latter equation has no solution, so the former cannot either.

We are using the fact that if $d \mid m$, then $x \equiv y \pmod{m}$ implies $x \equiv y \pmod{d}$ (but not necessarily the other way around). To see this, if $x \equiv y \pmod{m}$, then $m \mid x - y$ (by definition) and so $d \mid x - y$, and hence $x \equiv y \pmod{d}$.

(c) First, subtract the first equation from double the second equation to get $2(2x+y)-(3x+2y) \equiv x \equiv 1 \pmod 7$; now plug in to the second equation to get $2+y \equiv 4 \pmod 7$, so the system has the solution $x \equiv 1 \pmod 7$, $y \equiv 2 \pmod 7$.