Lecture 9 notes

Puzzler:

Last time, Alice and Bob wanted to exchange messages, but the only time they met was in a class where Carl sat between them. Everything they exchanged had to go through Carl. To prevent him from reading their notes, they devised a scheme of using both of their locks on the outside of the suitcase.

But a problem happened: To all appearances, the locks seem identical. In other words, Alice can't see whether or not a lock on the suitcase is really Bob's. She suspects that Carl has been switching suitcases, and the locks that she assumed were Bob's were actually Carl's! It looks like some of the notes she received weren't actually from Bob, but maybe from Carl instead!

In order to circumvent the process, Bob goes to the key and lock store and buys a new, second lock and gets some extra copies of his new key. He also buys a new briefcase that is smaller and can fit inside the original one. How can he use these to securely send un-forgeable messages?

Review of modular arithmetic concepts

We noticed last time that we could treat the concept of even and odd as if they were a number system in themselves. That is, if E stands for the concept of even number and O stands for the concept of odd number, then we have

$$E+E=E, E+O=O, O+O=E, E\times E=E, E\times O=E, O\times O=O$$

Alternately, and with an eye towards generalizations, we use the notation

$[0]_2$ instead of E and $[1]_2$ instead of O. These are supposed to signify a "type of number" which gives a remainder of 0 when divided by 2 and a type of number which

has a remainder of 1 when divided by 2.

Recall we did the same thing with 10 and noticed we could do this for any base.

Do the following base 10 and provide some examples.

In other words, can write $[7]_{10} + [9]_{10} = [6]_{10}$ more intuitively as $[7]_1 0 + [9]_{10} = [16]_{10} = [6]_{10}$

Base 2:

Our rules then say that $[0]_2 + [0]_2 = [0]_2$ etc. We can make things like $[1]_2 + [1]_2 = [0]_2$ a bit more intuitive by extending this notation a bit. To express the concept 11 is odd, we write $[11]_2 = [1]_2$, which we can think of as saying that 11 and 1 give the same remainder when divided by 2.

Recall the division algorithm:

Given integers n, d with $d > 0$, there exist unique integers q, r with $0 \leq r < |d|$ such that $n = dq + r$.

Proof: (in the case that $n, d > 0$, other cases are similar)

Let $Q = \{s \in \mathbb{N} \mid sd > n\}$. Notice that $0 \notin Q$ since $0 \cdot d = 0 < n$. Therefore $s \geq 1$ for all $s \in Q$. Since Q is a subset of $\mathbb{N}$ it has a smallest element q'. Let $q = q' - 1$. Notice that $q \geq 0$ since $q' \geq 1$. Since q' is the smallest element of Q, we know $q \notin Q$ and therefore $qd \leq n$. Let $r = n - qd \geq 0$ (by the above inequality). Since $q' = q + 1 \in Q$ we know $qd + d > n$ and so $d > n - qd = r$ as claimed. This shows that q, r exist as in the statement of the algorithm.

For uniqueness, suppose that $n = dq + r = dq' + r'$. Either $q = q'$ or not. If they are equal then $dq = dq'$ and so subtracting this off, we find $r = r'$. If they aren't equal then one is larger, say $q > q'$. In this case, $0 < d(q - q') = r' - r$ and so $r' - r$ is a positive multiple of d. In other words $r' = r + d \cdot m$ for some $m \geq 1$. But $0 \leq r <$

$|d| = d$ (note that we assumed $$d > 0$) tells us that $r' \geq d \cdot m \geq d$. Therefore r' isn't less than d contradicting our hypothesis.

Lemma: n and m have the same remainder when divided by d if and only if $n - m$ is a multiple of d.

I'll prove one direction and leave the other for the homework:

Suppose n, m have the same remainder when divided by d. Then $n = dq + r$ and $m = dq' + r$(same r). Therefore $n - m = dq - dq' = d(q - q')$.

So we find $[a]_d = [b]_d$ can be interpreted as saying that either a and b have the same remainder when divided by d or that $b - a$ is a multiple of d.

In the text this is also written as $a \equiv b \pmod{d}$. This means the same thing as $[a]_d = [b]_d$.

Rules of modular arithmetic. The punchline: it doesn't matter which representative you use!

Examples: $([4]_{10})^{42}$ can be worked out as follows: $4^2 = 16$ so 6 base 10. 4^3 is then like $6 \times 4 = 24 = 4$ base 10. But now this says $([4]_{10})^3 = [4]_{10}$. So

$([4]_{10})^{42} = ([4]_{10})^{3 \times 14} = ([4]_{10})^{14} = ([4]_{10})^{3^3+3+2} = [4]_{10} \cdot [4]_{10} \cdot ([4]_{10})^2 = ([4]_{10})^4 = ([4]_{10})^{3+1} = ([4]_1 0)^2 = ([16]_{10}) = [6]_{10}$

Probably could have been more slick, but this is a reasonable example. There are lots of ways to try and simplify these things!

So, if we take 4^{42}, the last digit will be 6.

Quiz: What's the last digit of 9^{50}?

Answer: $([9]_{10})^2 = [81]_{10} = [1]_{10}$. Consequently, $([9]_{10})^5 0 = (([9]_{10})^2)^{25} = ([1]_{10})^{25} = [1]_{10}$ and so the last digit is 1.

How about using this for divisibility? How do we check the divisibility of a number represented in base 10 by 2?

well, if we have a decimal representation, for example 2341, we think of this as $2 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 1$ and so we have $[2341]_2 = [2]_2 \times ([10]_2)^3 + [3]_2 \times ([10]_2)^2 + [4]_2 \times [10]_2 + [1]_2$, and since $[10]_2 = 0$, we get this is all the same as $[1]_2$.

More abstractly, if we write $n = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots a_r \times 10^r$ (so that each a_i stands for one of the decimal digits — in the previous example we'd have $a_0 = 1, a_1 = 4, a_2 = 3, a_4 = 2$ (we're writing in reverse order here for convenience)), we then find that since $$[10]_2 = 0$$, we have $[n]_2 = \cdots = [a_0]_2$. In other words, a number is even exactly when its last digit it even, and moreover, the remainder you get when dividing by 2 is exactly the same as the reminder you'd get when dividing the last digit by 2.

How about 9?

This is a bit more interesting. If we write $n = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots a_r \times 10^r$ again, this time we'd get $[n]_9 = [a_0]_9 + [a_1]_9 \times [10]_9 + [a_2]_9 \times ([10]_9)^2 + \cdots + [a_r] \times ([10]_9)^r$. But notice: $[10]_9 = [1]_9$! This means that $[n]_9 = [a_0]_9 + [a_1]_9 \times [1]_9 + [a_2]_9 \times ([1]_9)^2 + \cdots + [a_r] \times ([1]_9)^r$ which is equal to $[a_0 + a_1 + \cdots + a_r]_9$. In other words, you can just add up the digits and see whether a number is divisible by 9. This also computes the remainder when you divide by 9.

Example: is 51913 divisible by 9? If not, what is its remainder when you divide it by 9? What about 50913?

How about 11? Here's an interesting thing we can take advantage of: we can use both positive and negative numbers in our representations. This is because the division algorithm works just as well for positive as for negative numbers. So we can use the equation $[10]_1 1 = [-1]_{11}$ and find that therefore $[10^r]_{11} = ([10]_{11})^r = ([-1]_{11})^r = [(-1)^r]_{11}$ which is 1 or -1 depending on whether r is even or odd. So, for example:

$[1253]_{11} = [1]_{11} \times [10^3]_{11} + [2]_{11} \times [10^2]_{11} + [5]_{11} \times [10]_{11} + [3]_{11} = -[1]_{11} + [2]_{11} - [5]_{11} + [3]_{11} = [3 - 5 + 2 - 1]_{11} = [-1]_{11} = [10]_{11}$

so we find that 1253 has a remainder of 10 when divided by 11. Therefore in particular it isn't divisible by 11.