

Wednesday,  
April 17

Let's address some homework stuff before we begin.

Are we allowed to use  $f_0$  in Zeckendorf decomposition?

No! Why not? Well, the decomposition is supposed to be unique. If we allow  $f_0$ ,  $3 = f_3 = f_2 + f_0$ , so the decomposition is not unique.

Fun note: the ratio between consecutive ~~idea~~ Fibonacci numbers is approximately the ratio between miles and kilometers, so we can convert from miles to kilometers by moving to the next Fibonacci number (for instance,  $55 \text{ mph} \approx 89 \text{ km/h}$ ).

What if the number of miles per hour isn't a Fibonacci number? ZECKENDORF DECOMPOSITION! Just do the shift with the ~~m~~ Fibonacci numbers that comprise the number (for instance,  $65 \text{ mph} = 55 + 8 + 2 \text{ mph} \approx 89 + 13 + 3 \text{ km/h} = 105 \text{ km/h}$ ).

One problem on the homework requires a uniqueness proof. Let's do an example with binary.

Theorem: Every positive integer has a unique binary expansion.

Idea:  $75 = 64 + 8 + 2 + 1 = 2^6 + 2^3 + 2^1 + 2^0$ .

How did we get this? We took the largest power of 2 less than 75, then the largest power of 2 less than  $75 - 64$ , and so on. (This is called a greedy algorithm.)

If 64 weren't in our expansion, could we reach 75?

No! Why not? If we added  $2^7 = 128$ , we'd overshoot the goal, and  $2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 32 + 16 + 8 + 4 + 2 + 1 = 63 < 75$ , so we need 64.

Now let's prove it!

Proof of theorem:

Let  $m$  be the least positive integer that has multiple binary expansions, say  $m = 2^k + \text{smaller powers of } 2 = 2^l + \text{smaller powers of } 2$ .

Without loss of generality, say  $k \geq l$ .

If  $k \neq l$  (i.e.  $k > l$ ), then

$m = 2^l + \text{smaller powers of } 2 \leq 2^l + 2^{l-1} + 2^{l-2} + \dots + 2 + 1 = 2^{l+1} - 1 \leq 2^k - 1 < m$ . This is a contradiction, so  $k = l$ .

Since  $m$  is minimal,  $m - 2^k$  has a unique binary expansion.

Thus,  $m$  has a unique binary expansion.  $\blacksquare$

We're going to slightly modify notation from last time.

We wrote  $82 \equiv 5 \pmod{7}$ , but for now, we'll write

$82 \bmod 7 = 5$ . (This means  $82 \div 7$  has a remainder of 5,

or, equivalently,  $82 = 7 \times 11 + 5$ .)

Question: What time will it be ~~at 80~~ 80 hours from now?

Section 1: It's 10:00(ish). In 80 hours, it'll be 90:00(ish),

which doesn't make sense. ~~clocks~~ Clocks work mod 12, and

$90 \bmod 12 = 6$ , so in 80 hours, it'll be 6:00(ish).

Section 2: It's 11:00(ish). In 80 hours, it'll be 91:00(ish),

which doesn't make sense. Clocks work mod 12, and ~~clocks~~

$91 \bmod 12 = 7$ , so in 80 hours, it'll be 7:00(ish).

(Something to think about: Are those times am or pm? How could we figure that out?)

Definition: For  $a \in \mathbb{Z}$  and  $n \in \mathbb{Z}_{>0}$ , we can write  $a = qn + r$ , where  $q, r \in \mathbb{Z}$  and  $0 \leq r < n$ . Then  $a \pmod{n} = r$ .

We showed this  $a = qn + r$  business on the homework, but we didn't show that  $q$  and  $r$  were unique. What if there's some  $x$  such that  $x \pmod{7} = 3$  and  $x \pmod{7} = 5$ ?

Let's prove some stuff.

Theorem (quotient remainder theorem):

Given  $a \in \mathbb{Z}$ ,  $n \in \mathbb{Z}_{>0}$ ,  $\exists! q, r \in \mathbb{Z}$  s.t.  $a = qn + r$  and  $0 \leq r < n$ .

[Note:  $\exists!$  means "there exists a unique!"]

Existence of  $q$  and  $r$ :

Let  $q := \lfloor \frac{a}{n} \rfloor$ . Then  $q \leq \frac{a}{n} < q+1 \Rightarrow qn \leq a < (q+1)n \Rightarrow$

$0 \leq a - qn < n$ . Let  $r := a - qn$ . Thus,  $q$  and  $r$  exist.

Uniqueness of  $q$  and  $r$ :

Suppose  $a = qn + r = q'n + r'$  for some  $q, q', r, r' \in \mathbb{Z}$  with

$0 \leq r, r' < n$ . Then  $qn - q'n = r' - r \Rightarrow |(q - q')n| = |r' - r| \leq n - 1 \Rightarrow$

$|q - q'| \leq \frac{n-1}{n} < 1 \Rightarrow q - q' = 0 \Rightarrow q = q' \Rightarrow 0 = r' - r \Rightarrow r = r' \quad \square$