Notes for Recitation 4

1 The Pulverizer

We saw in lecture that the greatest common divisor (GCD) of two numbers can be written as a linear combination of them.[1] That is, no matter which pair of integers a and b we are given, there is always a pair of integer coefficients s and t such that

$$\gcd(a, b) = sa + tb.$$

However, the proof was *nonconstructive*: it didn't suggest a way for finding such s and t.

That job is tackled by a mathematical tool that dates to sixth-century India, where it was called *kuttak*, which means "The Pulverizer". Today, the Pulverizer is more commonly known as "the extended Euclidean GCD algorithm", but that's lame. We're sticking with "Pulverizer".

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{ rem }(a, b))$$

which was proved in lecture (see the notes "Number Theory I"). For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{array}{rcll} \gcd(259, 70) & = & \gcd(70, 49) & \text{since } \text{rem }(259, 70) = 49 \\ & = & \gcd(49, 21) & \text{since } \text{rem }(70, 49) = 21 \\ & = & \gcd(21, 7) & \text{since } \text{rem }(49, 21) = 7 \\ & = & \gcd(7, 0) & \text{since } \text{rem }(21, 7) = 0 \\ & = & 7. & \end{array}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear

[1] In fact, we proved that among all positive linear combinations of the numbers their GCD is the smallest.

combination). For our example, here is this extra bookkeeping:

x	y	$(\operatorname{rem}(x,y))$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\operatorname{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

2 Problem: The Pulverizer!

There is a pond. Inside the pond there are n pebbles, arranged in a cycle. A frog is sitting on one of the pebbles. Whenever he jumps, he lands exactly k pebbles away in the clockwise direction, where $0 < k < n$. The frog's meal, a delicious worm, lies on the pebble right next to his, in the clockwise direction.

(a) Describe a situation where the frog can't reach the worm.

Solution. If $k \mid n$ (say $k = 3$ and $n = 6$), then no number of jumps will lead the frog to the worm, as the frog will be returning to his original pebble ad infinitum. ■

(b) In a situation where the frog can actually reach the worm, explain how to use the Pulverizer to find how many jumps the frog will need.

Solution. Suppose the frog can reach the worm. When he actually reaches it, he has jumped a number of times, say j, and he has travelled around the cycle a number of times, call it c. Then, the distance that the frog has covered is both $j \cdot k$ and $c \cdot n + 1$, so that

$$jk = cn + 1.$$

But this means that 1 can be written as a *linear combination* of n and k:

$$(-c)n + jk = 1.$$

Since 1 is positive, we conclude that it is a *positive linear combination* of n and k. And since it is the smallest positive integer, we also conclude that it is the *smallest positive linear combination* of n and k. But we have proved in lecture that the smallest positive linear combination of two integers is their GCD. So, the GCD of n and k is 1:

$$\gcd(n, k) = 1$$

and we can use the Pulverizer to find $-c$ and j. ■

(c) Compute the number of jumps if $n = 50$ and $k = 21$. Anything strange? Can you fix it?

Solution. We go through the steps as described in Section 1 (see the table below) to get that $1 = 8 \cdot 50 - 19 \cdot 21$, or $1 = -(-8) \cdot 50 + (-19) \cdot 21$. Hence, $c = -8$ and $j = -19$, which makes little sense. What does it mean for the frog to make -19 jumps?

The point is that the Pulverizer is guaranteed to give us the integer coefficients of a linear combination that equals the GCD, but it promises nothing about the signs of those coefficients (in this case we wanted them to be $-$ and $+$). To get coefficients of the desired sign, we have to think more.

One way to fix it is as explained in lecture. That is, subtract 21 from 8 and add 50 to -19.

Here is another way: We know $1 = 8 \cdot 50 - 19 \cdot 21$. Or, to obtain meaningful signs for the numbers, $19 \cdot 21 = 8 \cdot 50 - 1$. That is, after 19 jumps the frog will land 1 pebble short of

8 full cycles. So, he will be right next to his original pebble, but in the counter-clockwise direction. Given this, how can he reach the pebble he is after?

Well, if he makes 19 more jumps, he will land 2 pebbles away from his original position in the counter-clockwise direction. Another 19 jumps will lead him 3 pebbles away, and so on. After a total of 49 sets of 19 jumps, he will be 49 pebbles away from its original position in the counter-clockwise direction, which is of course the worm's pebble. Then, the frog will have made $49 * 19 = 931$ jumps.

Here is the table produced by the Pulverizer:

x	y	$(\operatorname{rem}(x,y))$	$=$	$x - q \cdot y$
50	21	8	$=$	$50 - 2 \cdot 21$
21	8	5	$=$	$21 - 2 \cdot 8$
			$=$	$21 - 2 \cdot (50 - 2 \cdot 21)$
			$=$	$-2 \cdot 50 + 5 \cdot 21$
8	5	3	$=$	$8 - 1 \cdot 5$
			$=$	$(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$
			$=$	$3 \cdot 50 - 7 \cdot 21$
5	3	2	$=$	$5 - 1 \cdot 3$
			$=$	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			$=$	$-5 \cdot 50 + 12 \cdot 21$
3	2	1	$=$	$3 - 1 \cdot 2$
			$=$	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			$=$	$\boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0		

■

3 Problem: The Fibonacci numbers.

The Fibonacci numbers are defined as follows:

$$F_0 = 0 \qquad F_1 = 1 \qquad F_n = F_{n-1} + F_{n-2} \quad (\text{for } n \geq 2).$$

Give an inductive proof that the Fibonacci numbers F_n and F_{n+1} are relatively prime for all $n \geq 0$.

Solution. We use induction on n. Let $P(n)$ be the proposition that F_n and F_{n+1} are relatively prime.

Base case: $P(0)$ is true because $F_0 = 0$ and $F_1 = 1$ are relatively prime.

Inductive step: We show that, for all $n \geq 0$, $P(n)$ implies $P(n+1)$. So, fix some $n \geq 0$ and assume that $P(n)$ is true, that is, F_n and F_{n+1} are relatively prime. We will show that F_{n+1} and F_{n+2} are relatively prime as well. We will do this by contradiction.

Suppose F_{n+1} and F_{n+2} are not relatively prime. Then they have a common divisor $d > 1$. But then d also divides the linear combination $F_{n+2} - F_{n+1}$, which actually equals F_n. Hence, $d > 1$ divides both F_n and F_{n+1}. Which implies F_n, F_{n+1} are not relatively prime, a contradiction to the inductive hypothesis.

Therefore, F_{n+1} and F_{n+2} are relatively prime. That is, $P(n+1)$ is true.

The theorem follows by induction. ■

4 Extra Problem: The power of 3.[2]

Let N be a number whose decimal expansion consists of 3^n identical digits. Show by induction that $3^n \mid N$. For example:

$$3^2 \mid \underbrace{777777777}_{3^2 = 9 \text{ digits}}$$

Recall that 3 divides a number iff it divides the sum of its digits.

Solution. We proceed by induction on n. Let $P(n)$ be the proposition that $3^n \mid N$, where the decimal expansion of N consists of 3^n identical digits.

Base case. $P(0)$ is true because $3^0 = 1$ divides every number.

Inductive step. Now we show that, for all $n \geq 0$, $P(n)$ implies $P(n+1)$. Fix any $n \geq 0$ and assume $P(n)$ is true. Consider a number whose decimal expansion consists of 3^{n+1} copies of the digit a:

$$\begin{aligned}\underbrace{aaaaaa\ldots aaaaaa}_{3^{n+1} \text{ digits}} &= \underbrace{aaa\ldots aaa}_{3^n \text{ digits}}\underbrace{aaa\ldots aaa}_{3^n \text{ digits}}\underbrace{aaa\ldots aaa}_{3^n \text{ digits}} \\ &= \underbrace{aaa\ldots aaa}_{3^n \text{ digits}} \cdot 1\underbrace{000\ldots001}_{3^n \text{ digits}}\underbrace{000\ldots001}_{3^n \text{ digits}}\end{aligned}$$

Now 3^n divides the first term by the assumption $P(n)$, and 3 divides the second term since the digits sum to 3. Therefore, the whole expression is divisible by 3^{n+1}. This proves $P(n+1)$.

By the principle of induction $P(n)$ is true for all $n \geq 0$. ■

[2] Try this if you have time!

6.042J / 18.062J Mathematics for Computer Science
Fall 2010