Assignment 1 Solution

July 7, 2006

Problem 1

We use proof by induction.

1. The base case works, because $1^3 = 1$, and $\frac{1^2(1+1)^2}{4} = 1$
2. Induction step:
   Assume $1^3+2^3+\ldots+k^3 = \frac{k^2(k+1)^2}{4}$ for some $k \in \mathbf{N}$. Then this implies:
   $$1^3+2^3+\ldots+k^3+(k+1)^3 = \frac{k^2(k+1)^2}{4}+(k+1)^3 = \frac{k^2(k+1)^2+4(k+1)^3}{4}$$
   $$= \frac{k^2(k+1)^2+(k+1)^2(4k+4)}{4} = \frac{(k+1)^2(k^2+4k+4}{4} = \frac{(k+1)^2(k+2)^2}{4}$$
   This is what we needed to show.

The base case works and the induction step works, so the theorem is proven for all $n \in \mathbf{N}$.

Problem 2

We use proof by induction.

1. The base case works, because $4 \cdot 10^2 + 9 \cdot 10^1 + 5 = 495 = 5 \cdot 99$
2. Induction step:
   Assume $4 \cdot 10^{2k} + 9 \cdot 10^{2k-1} + 5 = 99a$ for some a, $k \in \mathbf{N}$. Then this implies:
   $$4{\cdot}10^{2k+2}+9{\cdot}10^{2k+1}+5 = 100{\cdot}4{\cdot}10^{2k}+100{\cdot}9{\cdot}10^{2k-1}+5 = 99{\cdot}4{\cdot}10^{2k}+99{\cdot}9{\cdot}10^{2k-1}+99a$$
   All terms here are divisible by 99, so the entire RHS is divisible by 99. This is what we needed to show.

The base case works and the induction step works, so the theorem is proven for all $n \in \mathbf{N}$.

Problem 3

a) We use proof by induction.

1. For this problem, because f_n depends on f_{n-1} *and* f_{n-2}, we need to check 2 base cases: $n = 1$ and $n = 2$. These both work, because $1 < 2^1 = 2$ and $1 < 2^2 = 4$

2. Induction step:
   Assume $f_k < 2^k$ and $f_{k+1} < 2^{k+1}$ for some $k \in \mathbf{N}$. Then this implies

   $$f_{k+2} = f_{k+1} + f_k < 2^{k+1} + 2^k < 2^{k+1} + 2^{k+1} < 2 \cdot 2^{k+1} = 2^{k+2}$$

   This is what we needed to show.

The base case works and the induction step works, so the theorem is proven for all $n \in \mathbf{N}$.

b) We use induction again.

1. The base case $n = 2$ works, because $f_3 f_1 = 2 \cdot 1 = 2$ and $f_2^2 + (-1)^2 = 1 + 1 = 2$.

2. Induction step:
   Assume $f_{k+1} f_{k-1} = f_k^2 + (-1)^k$ for some $k \in \mathbf{N}$. Then this implies

   $$f_{k+2} f_k = (f_{k+1} + f_k) f_k = f_{k+1} f_k + f_k^2$$

   $$= f_{k+1} f_k + f_{k+1} f_{k-1} - (-1)^k = f_{k+1}(f_k + f_{k-1}) + (-1)^{k+1} = f_{k+1}^2 + (-1)^{k+1}$$

   This is what we needed to show.

The base case works and the induction step works, so the theorem is proven for all $n \in \mathbf{N}$.

c)We use induction again.

1. The base cases work, because $[(1+\sqrt{5})^1 - (1-\sqrt{5})^1]/(2\sqrt{5}) = 1$ and $[(1+\sqrt{5})^2 - (1-\sqrt{5})^2]/(4\sqrt{5}) = [1 + 2\sqrt{5} + 5 - 1 + 2\sqrt{5} - 5]/(4\sqrt{5}) = 1$

2. Induction step:
   Assume $f_n = [(1+\sqrt{5})^n - (1-\sqrt{5})^n]/(2^n\sqrt{5})$ for some $n = k$ and $n = k + 1$. Then this implies

   $$f_{k+2} = [(1+\sqrt{5})^k - (1-\sqrt{5})^k]/(2^k\sqrt{5}) + [(1+\sqrt{5})^{k+1} - (1-\sqrt{5})^{k+1}]/(2^{k+1}\sqrt{5})$$

$$= \frac{1}{2^k\sqrt{5}}[\frac{1}{2}((1+\sqrt{5})^k(1+\sqrt{5})-(1-\sqrt{5})^k(1-\sqrt{5}))+(1+\sqrt{5})^k-(1-\sqrt{5})^k]$$

$$= \frac{1}{2^k\sqrt{5}}[(1+\sqrt{5})^k(1+\frac{1}{2}(1+\sqrt{5}))-(1-\sqrt{5})^k(1+\frac{1}{2}(1-\sqrt{5}))]$$

$$= \frac{4}{2^{k+2}\sqrt{5}}[(1+\sqrt{5})^k(1+\frac{1}{2}(1+\sqrt{5}))-(1-\sqrt{5})^k(1+\frac{1}{2}(1-\sqrt{5}))]$$

$$= \frac{1}{2^{k+2}\sqrt{5}}[(1+\sqrt{5})^k(4+2+2\sqrt{5})-(1-\sqrt{5})^k(4+2-\sqrt{5})]$$

$$= \frac{1}{2^{k+2}\sqrt{5}}[(1+\sqrt{5})^k(1+\sqrt{5})^2-(1-\sqrt{5})^k(1-\sqrt{5})^2]$$

$$= [(1+\sqrt{5})^{k+2}-(1-\sqrt{5})^{k+2}]/(2^{k+2}\sqrt{5})$$

This is what we needed to show.

The base cases work and the induction step works, so the theorem is proven for all $n \in \mathbf{N}$.

d)Let $x = \lim_{n\to\infty} \frac{f_n}{f_{n+1}}$.
Then $x = \lim_{n\to\infty} \frac{f_n}{f_n+f_{n-1}}$
$\Rightarrow \frac{1}{x} = \lim_{n\to\infty} \frac{f_n+f_{n-1}}{f_n} = 1 + \lim_{n\to\infty} \frac{f_{n-1}}{f_n} = 1 + x$
So $x^2 + x - 1 = 0$. The solution is $x = \frac{-1\pm\sqrt{5}}{2}$. Since every number in the Fibonacci sequence is positive, we need to take the positive value, $x = \frac{\sqrt{5}-1}{2}$.

e)We use induction (I promise this is the last time!)

1. Base case: technically 1 is coprime with 1, so this works. But since this is sort of strange, you might also check that 1 and 2 are coprime, and that 2 and 3 are coprime.

2. Induction step:
   Assume that f_n and f_{n+1} are relatively prime. Then $\exists u, v \in \mathbf{Z}$ such that $uf_n + vf_{n+1} = 1$.
   $\Rightarrow uf_{n+1} + v(f_{n+2} - f_{n+1}) = 1$
   $\Rightarrow vf_{n+2} + (u - v)f_{n+1} = 1$
   $\Rightarrow f_{n+2}$ and f_{n+1} are relatively prime.

The base case works, and the induction step works, so f_n and f_{n+1} are relatively prime.

Problem 4

Adding the two equations, we get $2a^2 = r^2 + s^2$. This means that $r^2 + s^2$ must be even. So r^2 and s^2 must either be both even or both odd. Therefore r and s must either be both even or both odd. But if r and s were both even, then they would not be coprime, since they would both be multiples of 2. Therefore r and s are both odd.
Subtracting the second equation from the first, we get

$$2b^2 = r^2 - s^2 = (2k_r+1)^2 - (2k_s+1)^2 = 4k_r^2 + 4k_4 + 1 - 4k_s^2 - 4k_s - 1 = 4(k_r^2 + k_4 - k_s^2 - k_s)$$

$\Rightarrow b^2$ is even, and hence b is even.
Since b is even, a must be odd (a and b must be coprime).

Problem 5

Suppose a and b do not have a unique least common multiple; that is, suppose there are two integers m and n that satisfy the requirement. Then m and n are both multiples of a and b, so by definition of the lcm we must have $m|n$ and $n|m$ and hence $n = m$.

Problem 6

By definition of the gcd, we know that there exist integers q_a and q_b such that $a = q_a d$ and $b = q_b d$; furthermore q_a and q_b must be coprime (else there would be a greater common divisor of a and b). This means they must both be positive (else -1 would be a common divisor).
So we can write $|ab| = |q_a d q_b d| = |d^2||q_a q_b| = d^2 q_a q_b = d(d q_a q_b)$
We now need to show that $d q_a q_b = lcm(a, b)$. Since it's clearly a multiple of both a and b, all we now need to show is that any other multiple of a and b is also a multiple of $d q_a q_b$.

Consider x a multiple of a and b. There is some c_a and c_b such that $x = c_a a$ and $x = c_b b$. So we get

$$c_a a = c_b b$$

$$c_a q_a d = c_b q_b d$$

$$c_a q_a = c_b q_b$$

Since q_a and q_b are coprime, q_a must divide c_b and q_b must divide c_a. So c_a is a multiple of q_b, which implies that $c_a q_a d$ is a multiple of $d q_a q_a$. So x is a multiple of $d q_a q_a$. Hence $d q_a q_b = lcm(a, b)$.

Problem 7

This is a direct consequence of Problem 6. If $d = 1$, then a and b must both be positive, so we get $m = ab$. In the other direction, if $m = ab$, then the equation from Problem 6 becomes $dab = |ab|$. Since m is nonnegative by definition, ab is positive, so $|ab| = ab$ and we get $d = 1$.

Problem 8

Since this problem is featured on Problem Set 2, I'm not going to give you the solution here. Instead, here's a gigantic hint: for any x, the following is true:

$$x^n - 1 = (x - 1)(1 + x + x^2 + x^3 + ... + x^{n-1})$$

Problem 9

First notice that any integer can be written in one of the following forms: $a = 4n - 1$, $a = 4n$, $a = 4n + 1$ or $a = 4n + 2$. Now consider the following lemma:

Lemma. *A product of 2 integers of the form* $4n + 1$ *is another integer of the form* $4n + 1$.

Proof. Consider two integers $4n + 1$ and $4m + 1$.
$(4n + 1)(4m + 1) = 16mn + 4n + 4m + 1 = 4(4mn + n + m) + 1$ ☐

(If you've never seen a lemma before, it's basically just a "helper proof" we use on the way to proving a bigger theorem.)

Now suppose there was only a finite number n of primes of the form $q = 4n - 1$. Let $k = 4q_1q_2...q_n - 1$. k must have some prime factorization: $k = p_1p_2...p_m$. Now by definition it is clear that k is odd. So $p_i \neq 2\ \forall i$. So each p_i must be of the form $4n - 1$ or $4n + 1$. Furthermore, k is clearly of the form $4n - 1$, so k must have at least one prime factor that is of the form $4n - 1$, because if not then our lemma tells us that k would be of the form $4n + 1$.

Now this means that there is some x such that $4x - 1$ is prime and such that $4x - 1 | 4q_1q_2...q_n - 1$. By definition of k, $4x - 1$ must be one of the primes we started out with, so it divides $4q_1q_2...q_n$. So $4x - 1$ must also divide 1. This is not possible $\Rightarrow$ contradiction. So there must be infinitely many primes of the form $4n-1$.

Problem 10

Suppose there existed integers p and q such that $p^2 = 2q^2$. Using the Fundamental Theorem of Arithmetic, we can decompose p^2 and q^2 uniquely into prime factors. p^2 has the same prime factors as p, except that it has each one twice. (For example if $p = 10$: $10 = 2 \cdot 5$ whereas $10^2 = 100 = 2 \cdot 2 \cdot 5 \cdot 5$.) The same thing is true for q^2 and q. So p^2 has an even number of prime factors, and so does q^2. Then $2q^2$ has an odd number of prime factors, since 2 is prime. But if $p^2 = 2q^2$, then p^2 must have an odd number of prime factors, which is a contradiction.
We cannot find integers p and q such that $p^2 = 2q^2$, so we cannot write $2 = \frac{p^2}{q^2}$ and hence there are no integers p and q such that $\sqrt{2} = \frac{p}{q}$. Therefore $\sqrt{2}$ is irrational.

The Challenge Problem

I'm not giving you the solution to this one since it's being repeated on Problem Set 2.