Solutions to 18.781 Problem Set 2 - Fall 2008

Due Tuesday, Sep. 23 at 1:00

1. (Niven 1.3.39) Prove that

$$1-\frac{1}{2}+\frac{1}{3}-\cdots+\frac{1}{2007}-\frac{1}{2008}=\frac{1}{1005}+\frac{1}{1006}+\cdots+\frac{1}{2008}.$$

You may find it easier to prove a general statement!

This problem hints at a general statement, with 2008 replaced by any (even) integer:

$$1-\frac{1}{2}+\frac{1}{3}-\cdots+\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}.$$

We can prove this using induction on n. For the base case, $n=1$, we just have $1-\frac{1}{2}=\frac{1}{2}$, which is clear enough. Now let's assume the equation for some fixed n. Then we can add $\frac{1}{2n+1}-\frac{1}{2n+2}$ to each side:

$$\begin{aligned}1-\frac{1}{2}+\cdots-\frac{1}{2n}+\frac{1}{2n+1}-\frac{1}{2n+2}&=\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}+\frac{1}{2n+1}-\frac{1}{2n+2}\\&=\frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+1}+\left(\frac{1}{n+1}-\frac{1}{2n+2}\right)\\&=\frac{1}{n+2}+\frac{1}{n+3}+\cdots+\frac{1}{2n+1}+\frac{1}{2n+2}.\end{aligned}$$

This shows that assuming the formula for n implies the formula holds for $n+1$, thus the inductive hypothesis is true for all positive n.

2. (Niven 1.3.4, 1.3.5, and 1.3.8) Write $n=a_m a_{m-1}\ldots a_1 a_0$ in decimal digits, so that $n=a_m 10^m+a_{m-1}10^{m-1}+\cdots+a_1 10+a_0$.

   (a) Prove that n is divisible by 3 if and only if $a_m+a_{m-1}+\cdots+a_0$ is divisible by 3.
   We can rewrite n in the following way:

$$\begin{aligned}n&=(a_m 10^m+a_{m-1}10^{m-1}+\cdots+a_1 10+a_0)\\&=a_m(10^m-1)+a_{m-1}(10^{m-1}-1)+\cdots+a_1(10-1)+a_m+a_{m-1}+\cdots+a_1+a_0)\end{aligned}$$

   Now note that since $10\equiv 1 \pmod 3$, $10^k\equiv 1^k\equiv 1 \pmod 3$. Thus $3|(10^k-1)$ for any $k\in\mathbb{Z}^+$. Therefore all the summands before a_m are divisible by 3, so

$$3|n \Leftrightarrow 3|(a_m+a_{m-1}+\cdots+a_1+a_0).$$

   (b) Prove that n is divisible by 9 if and only if $a_m+a_{m-1}+\cdots+a_0$ is divisible by 9.
   This solution is virtually identical to the above one, with 3 replaced by 9. Note the crucial property of 3 that was used is $10\equiv 1 \pmod 3$. Since this also holds mod 9, the proof works here.

(c) Prove that n is divisible by 11 if and only if

$$a_m - a_{m-1} + a_{m-2} - \cdots + (-1)^{m-1}a_1 + (-1)^m a_0$$

is divisible by 11.

Once again a similar solution is employed. But here we have $10 \equiv -1 \pmod{11}$. Thus we get

$$\begin{aligned} n &\equiv a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_m(-1)^m + a_{m-1}(-1)^{m-1} + \cdots - a_1 + a_0 \pmod{11} \end{aligned}$$

Since divisibility by 11 depends only on whether $n \equiv 0 \pmod{11}$, we can multiply by $(-1)^m$ to get that

$$11|n \Leftrightarrow 11|(a_m - a_{m-1} + a_{m-2} - \cdots + (-1)^{m-1}a_1 + (-1)^m a_0).$$

(d) Prove that n is divisible by 7 if and only if $n' - 2a_0$ is divisible by 7, where $n' = (n - a_0)/10$. Explain how this can be iterated to give a divisibility test for 7 and use it on $n = 39333$.

First, it is clear that n' is an integer, because $n - a_0$ is divisible by 10. So we have

$$n' - 2a_0 = \frac{n - a_0}{10} - 2a_0 = \frac{n - 21a_0}{10}$$

This gives that

$$7|(n' - 2a_0) \Leftrightarrow 7|\frac{n - 21a_0}{10} \Leftrightarrow 7|(n - 21a_0) \Leftrightarrow 7|n.$$

So we can iterate this method, and each step reduces the number of digits of n by one, so it rapidly becomes a one-digit number. The final number is 0 or ± 7 if and only if the n we started with is divisble by 7. Using this on 39333:

$$\begin{aligned} n_0 = 39333 \Leftarrow n_1 = 3933 - 2(3) = 3927 \Leftarrow n_2 = 392 - 2(7) = 378 \\ \Leftarrow n_3 = 37 - 2(8) = 21 \Leftarrow n_4 = 2 - 2(1) = 0. \end{aligned}$$

So $7|39333$.

(Bonus) For any prime $p > 5$, use the fact that there exists a solution to $xp \equiv 1 \pmod{10}$ to devise a divisibility test.

3. (Niven 1.3.10 and 1.3.26)

(a) Prove that any number of the form $3k + 2$ has a prime factor of the same form. Do the same for numbers of the form $4k + 3$ and $6k + 5$.

Consider some $n \equiv 2 \pmod{3}$. We know that we can write the integer n as a product of primes $p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$. Now assume none of the primes that divide n is of the form $3k + 2$. Then each p_i is congruent to 0 or 1 mod 3. But a product of 0's and 1's is either 0 or 1, so that implies $n \not\equiv 2 \pmod{3}$. This is a contradiction, so our assumption must be false, so there is some $p_i \equiv 2 \pmod{3}$.

The proofs for the forms $4k+3$ and $6k+5$ are quite similar, but you look mod 4 (and mod 6, respectively). Also, here you need to argue that any product of any integers congruent to 0,1,2 (respectively 0,1,2,3,4) cannot generate an integer congruent to 3 (5). This is done by showing that if 2 (respectively 2,3, or 4) occurs in a product, then the product must be divisible by 2 (respectively 2 or 3) and thus cannot be in the prescribed form.

(b) Prove that there are infinitely many primes of the form $3k+2, 4k+3$, and $6k+5$. We can once again prove all three with the same method. I'll illustrate the technique with the case $4k+3$. Assume, for the sake of a contradiction, that there is a finite list of primes of the form $4k+3$, say $\{p_1, p_2, \ldots, p_N\}$. Then let

$$A = 4p_1p_2\cdots p_N - 1 \equiv 3 \pmod 4.$$

By the above argument, there is some prime of the form $4k+3$ that divides A, but it obviously isn't in our list, since all of the primes there divide $A+1$. Thus there is a prime that we left out of our finite list, and this contradiction proves there are infinitely many in that form.

4. (Niven 1.3.21) Prove that for positive integers a, b, c,

$$[a,b,c](ab,bc,ca) = abc.$$

On page 25 of Niven, we find a formula for the lcm and gcd of two integers using the prime factorizations of the integers. These formulae can actually be extended to more than two integers in the following way. If $f(n,p)$ is the power of prime p that occurs in the prime factorization of n, we have:

$$f([n_1,\ldots,n_r],p) = \max_i(f(n_i,p)) \text{ and } f((n_1,\ldots,n_r),p) = \min_i(f(n_i,p)).$$

This generalization was covered in class, so I won't explain it here. Now we use these formulae to show that the two sides of the equation we are to prove have the same prime factorizations. Choose any prime p. Then we want to show

$$f([a,b,c](ab,bc,ca),p) = f(abc,p).$$

The right side is simple to compute: since it is just a product, we add the exponents of each prime, so

$$f(abc,p) = f(a,p) + f(b,p) + f(c,p).$$

On the left, we also have a product, and then using the formulae we get

$$\begin{aligned} f([a,b,c](ab,bc,ca),p) &= f([a,b,c],p) + f((ab,bc,ca),p) \\ &= \max(f(a,p),f(b,p),f(c,p)) + \min(f(ab,p),f(bc,p),f(ca,p)) \\ = \max(f(a,p),f(b,p),f(c,p)) &+ \min(f(a,p)+f(b,p), f(b,p)+f(c,p), f(c,p)+f(a,p). \end{aligned}$$

So this is the sum of the max of the set $\{f(a,p), f(b,p), f(c,p)\}$ and the min of the pairwise sums of the same set. This is obviously just the sum of the elements of the set. So we finally get

$$f([a,b,c](ab,bc,ca),p) = f(a,p) + f(b,p) + f(c,p) = f(abc,p).$$

Since every integer has a unique prime factorization, we have shown that, in fact,

$$[a, b, c](ab, bc, ca) = abc.$$

5. (a) Prove that there is not unique factorization in the set $\{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}$. We have the following two decompositions of the number 8 in this set:

$$2^3 = 8 = (1 + \sqrt{-7})(1 - \sqrt{-7}).$$

So if we can show that these factors don't reduce further, we have disproven unique factorization in this ring. It is easy to see that $2 \not| (1 \pm \sqrt{-7})$, since any number divisible by two has coefficients that are even. Finally, two can be shown to be irreducible, since it is smaller than any number that can be written as the product $(a + b\sqrt{-7})(a - b\sqrt{-7})$, and this is the only nontrivial product that could give a real prime number. Thus this ring does not have unique factorization.

(b) If D is an odd, positive integer that is not a square number, prove that there is not unique factorization in $\{a + b\sqrt{-D} \mid a, b \in \mathbb{Z}\}$.

This can be done by generalizing the above idea. First we note that the last argument holds to show that for any $D \geq 3$, two is irreducible in the ring of numbers of the form $a + b\sqrt{-D}$.

Using this, we can show that there will always be a number in the ring with two distinct decompositions. We know that D is odd, so we can write:

$$2k = D + 1 = (1 + \sqrt{-D})(1 - \sqrt{-D}).$$

Since 2 is irreducible, if this set of numbers had unique factorization, 2 would divide either $(1 + \sqrt{-D})$ or $(1 - \sqrt{-D})$. But it's obvious that 2 cannot divide either of these because any multiple of 2 has even coefficients:

$$2(a + b\sqrt{-D}) = 2a + 2b\sqrt{-D}.$$

This contradicts the assumption that this set has unique factorization, so it does not.

(Bonus) Consider the *Gaussian integers*, which is the set of "integer coordinate complexes": $\{a + bi \mid a, b \in \mathbb{Z}\}$. Prove that in this set, $p = 1 + i$ has the following property of prime numbers:
If $p \mid (a + bi)(c + di)$, then either $p \mid (a + bi)$ or $p \mid (c + di)$.

6. (Niven 2.1.7) Show that if $f(x)$ is a polynomial with integral coefficients and $f(a) \equiv k \bmod m$, then $f(a + tm) \equiv k \pmod m$ for any t.

Another way this problem can be phrased is

$$a \equiv b \pmod m \implies f(a) \equiv f(b) \pmod m.$$

This is simply the consequence of addition and multiplication being well defined. That is, we know that $a \equiv b$ and $c \equiv d \bmod m$ gives the congruences

$$a + c \equiv b + d;\ ac \equiv bd \pmod m.$$

Knowing this, since any polynomial is just a combination of additions and multiplications, we get that polynomials are also well defined mod m.

7. (Niven 2.1.20) Prove that $42 \mid (n^7 - n)$ for any n.

   Observe that we need to show that $2, 3$, and 7 all divide $(n^7 - n)$. But this is equivalent to showing

   $$n^7 \equiv n \pmod{a}$$

   for $n \in \mathbb{Z}$ and $a \in \{2, 3, 7\}$. Here, we can use Fermat's Little Theorem: in mod 7, for example, we know that $n^7 \equiv n$, so this holds. For the other two moduli, 2 and 3, the congruence we have from Fermat's Little Theorem implies the necessary equivalence, so we are done.

8. (Niven 2.1.25) Prove that $91 \mid (n^{12} - a^{12})$ for any a, n that are both coprime to 91. Give an counterexample showing that this condition is necessary.

   Note that $91 = 7 \cdot 13$, so we want to show that any two numbers that aren't divisble by 7 or 13 have equivalent twelfth powers mod 7 and mod 13. Once again, Fermat's Little Theorem can be used. In mod 7, we know for any $n \not\equiv 0$ we have $n^{7-1} \equiv n^6 \equiv 1 \pmod{7}$. Squaring this gives $n^{12} \equiv 1 \pmod{7}$, so all numbers not divisible by 7 have congruent twelfth powers mod 7.

   For Fermat's Little Theorem applied to the prime 13, we immediately get the congruence $n^{13-1} \equiv n^{12} \equiv 1 \pmod{13}$ for all n not divisible by 13. Thus we have shown that all n with $(91, n) = 1$ have equivalent twelfth powers mod 7 and mod 13, and thus they have equivalent twelfth powers mod 91.

9. (Niven 2.1.27) Prove that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for any n.

   First, let's collect the fractions into one fraction with a common denominator:

   $$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = \frac{3n^5 + 5n^3 + 7n}{15}.$$

   So if we show that $15|(3n^5+5n^3+7n)$ for all $n \in \mathbb{Z}$, we are done. Being divisible by 15 is equivalent to being divisible by 3 and 5 simultaneously. Looking at $f(n) = 3n^5+5n^3+7n$ in these two moduli, we have

   $$f(n) \equiv 2n^3 + n \pmod{3} \text{ and } f(n) \equiv 3n^5 + 2n \pmod{5}.$$

   Now, Fermat's Little Theorem tells us that for any prime p and integer a,

   $$a^p \equiv a \pmod{p}.$$

   This makes these two congruences into:

   $$f(n) \equiv 2n + n \equiv 0 \pmod{3} \text{ and } f(n) \equiv 3n + 2n \equiv 0 \pmod{5}.$$

   So in fact, $f(n)$ is divisible by both 3 and 5 for every $n \in \mathbb{Z}$. Therefore $15|f(n)$ which implies that the original polynomial is an integer for every $n \in \mathbb{Z}$.

10. (Niven 2.2.2) Let $N(k)$ denote the number of solutions to $f(x) \equiv k \pmod{m}$. Prove using a simple counting argument that

    $$\sum_{k=1}^{m} N(k) = m.$$

This argument is actually quite straightforward. There are m numbers mod m. Any one of these numbers, call in a, is a solution to exactly one of the m equivalences $f(x) \equiv k \pmod{m}$, namely, when $k \equiv f(a) \pmod{m}$. Thus in the sum

$$\sum_{k=1}^{m} N(k)$$

each number mod m gets counted exactly once, and no number gets skipped, so the sum must equal m.

11. (Niven 2.2.5acd) Find *all* solutions of the congruences

    (a) $20x \equiv 4 \pmod{30}$,
    This congruence has no solutions. This is because the left side of the congruence can only be congruent to 0, 10, or 20. This is because 20 and 30 share the common factor 10.

    (b) $353x \equiv 254 \pmod{400}$,
    For this congruence, we can see that x needs to be even. Thus if we let $x = 2y$ then we are solving the reduced congruence $353k \equiv 127 \pmod{200}$. Now to find the inverse of $353 \equiv -47$, we use the Euclidean algorithm:

$$\begin{aligned} 200 &= 47(4) + 12 & & & 1 &= 12(1) + 11(-1) \\ 47 &= 12(3) + 11 & & \nearrow & 1 &= 12(4) + 47(-1) \\ 12 &= 11(1) + 1 & & & 1 &= 200(4) + 47(-17). \end{aligned}$$

    This shows that 17 is the inverse of (-47) $\pmod{200}$. Thus the solution to the reduced congruence is

$$k \equiv (17)(127) \equiv 2159 \equiv 159 \pmod{200}.$$

    Since $x = 2k$, $x = 318$. This solution is unique, mod 400, since $(353, 400) = 1$.

    (c) $57x \equiv 87 \pmod{105}$.
    We can reduce this congruence by dividing by 3:

$$19x \equiv 29 \pmod{35}.$$

    Now, since $(19, 35) = 1$, there will be exactly one solution to this congruence. Using the same method illustrated above, we find that $(31)(19) \equiv 29 \pmod{35}$. Now we move this solution up to mod 105, and we have to take care that it will split into 3 solutions, every number that is congruent to 31 mod 35. So the complete set of solutions is

$$x \equiv 31, 66, \text{ or } 101 \pmod{105}$$

(Bonus) *Postage stamp problem.* Since $(5, 12) = 1$, we know that the linear combination $5x + 12y = n$ can be solved for all n. However, consider the related problem of characterizing positive linear combinations, with $x, y \geq 0$ (this situation would arise if we had only 5 and 12 cent stamps). In that case, we cannot solve the cases $n = 1, 2, 3, 4, 6, \ldots$.

(a) Prove that there is some bound N such that $5x + 12y = n$ has solutions whenever $n \geq N$. List all of the n for which there is no solution - how many such n are there?

(b) Repeat part (a) for general $(a, b) = 1$: find a bound N such that $ax + by = n$ has solutions for $n \geq N$, and characterize and count the n for which there is no solution.