Solutions to 18.781 Problem Set 3 - Fall 2008

Due Tuesday, Sep. 30 at 1:00

1. (Niven 2.3.3) Solve the congruences $x \equiv 1 \pmod 4, x \equiv 0 \pmod 3, x \equiv 5 \pmod 7$.

   First we note that 4, 3, and 7 are pairwise relatively prime, so there is a unique solution in the modulus $4 \cdot 3 \cdot 7 = 84$, by the Chinese Remainder Theorem. By inspection, the first two congruences imply that $x \equiv 9 \pmod{12}$. So we need to solve

   $$9 + 12y = 5 + 7z$$

   for integers y, z. Solving the Diophantine equation in the usual way, we find that one solution is $(y, z) = (3, 4)$, and this gives our final result, that

   $$x \equiv 33 \pmod{84}.$$

2. (Niven 2.3.8) Find the smallest positive integer whose remainder is $1, 2, 3, 4$, and 5 when divided by $3, 5, 7, 9$, and 11, respectively. What is the second smallest such integer?

   This problem is straightforward... the smallest positive integer giving any particular (postive) remainder is just the solution to the simultaneous congruences implied by the remainders. This will use CRT, but first we want to check all the moduli to make sure they are pairwise relatively prime. The only pair that are not are 3 and 9, but the two related congruences are

   $$x \equiv 1 \pmod 3 \text{ and } x \equiv 4 \pmod 9.$$

   It is easy to see that the second congruence implies the first; that is, any x giving 4 as a remainder when divided by 9 must give the remainder 1 when divided by 3. So we can ignore the first congruence, and the remaining 4 congruences can be solved using the iterative method discussed in problem 4.

   We start with the list $a_1, m_1, a_2, m_1, a_3, m_3, a_4, m_4 = 2, 5, 3, 7, 4, 9, 5, 11$. The first step replaces the first 4 terms with $a' = 2 + (3 - 2)3 \cdot 5 = 17$ and $m' = 5 \cdot 7 = 35$, so we are left with the reordered list $4, 9, 5, 11, 17, 35$.

   Now we replace the first 4 terms with $a' = 4 + (5 - 4)5 \cdot 9 = 49$ and $m' = 9 \cdot 11 = 99$. So this gives us the list $17, 35, 49, 99$. We finally have to solve this pair of congruences, and so using the Euclidean algorithm we can find that $x \equiv 17 \pmod{35}$ and $x \equiv 49 \pmod{99}$ gives that

   $$x \equiv 1732 \pmod{3465}.$$

   So the smallest postive number giving all of the requested remainders is 1732. The next smallest number is just $1732 + 3465 = 5197$.

3. (Niven 2.3.18) For any $k \geq 1$, prove that there exist k consecutive positive integers that are each divisible by a square number. For example, the sequence $\{48, 49, 50\}$ works for $k = 3$.

   We have to prove this for any arbitrary $k \in \mathbb{Z}$, so fix such a k. The problem is to find an N such that the set of integers $\{N - k + 1, N - k + 2, \dots, N\}$ contains only integers that are divisible by squares. We use our knowledge of modular arithmetic to find such an N. Consider the first k primes, call them $p_1 = 2, p_2 = 3, \ldots, p_k$. These primes are clearly all pairwise relatively prime, since they are distinct primes. In fact, the list of their squares, $4, 9, 25, \ldots, p_k^2$, are also pairwise relatively prime, since no pair of them share a prime factor. Then there is always a unique solution to the simultaneous congruence

$$\begin{aligned} x &\equiv a_1 \pmod{4}, \\ x &\equiv a_2 \pmod{9}, \\ &\vdots \\ x &\equiv a_k \pmod{p_k^2}, \end{aligned}$$

by the Chinese Remainder Theorem. Let $a_i = i - 1$ for all $1 \le i \le k$. Then we have a solution $x \in \mathbb{Z}$ with $x \equiv i - 1 \pmod{p_i^2}$ for all $1 \le i \le k$ This congruence is equivalent to

$$p_i^2 | (x - (i - 1)) \text{ for all } i \in \{1, 2, \ldots, k\}.$$

Letting i run over the k values, we get that the integers from $x - k + 1$ to x are each divisible by a square of a prime. Thus x is exactly the N for which we were looking.

4. This problem presents an iterative approach to solving the simultaneous congruences $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots x \equiv a_k \pmod{m_k}$, where all of the m_i are coprime (thereby proving CRT). This technique is especially useful when the a_i are all relatively close in value. The algorithm follows:

   (i) Given $a_1, m_1, a_2, m_2, \ldots, a_k, m_k$, re-number indices so that $a_1 \le a_2 \cdots \le a_k$.
   (ii) Use the Euclidean algorithm to find y such that $ym_1 \equiv 1 \pmod{m_2}$.
   (iii) Set $a' := a_1 + (a_2 - a_1)ym_1 \pmod{m'}$, where $m' = m_1 m_2$.
   (iv) If $k \ge 3$, return to step (ii) with $a', m', a_3, m_3, \ldots, a_k, m_k$.

   (a) Prove that the algorithm works by showing that the final output a' is the unique solution x modulo $m_1 m_2 \cdots m_k$ (the main details to verify are in (iii)).
   (b) Solve the congruences $x \equiv 4 \pmod{5}, x \equiv 5 \pmod{7}, x \equiv 6 \pmod{11}$.

   (a) To show that the method works, we only have to show that each step can be done, and that each step preserves the set of solutions. The first one is easy to check for each of the four steps:

   (i) Clearly no problem here, you can always order integers from least to greatest.
   (ii) Here we need to be able to find a multiplicative inverse to m_1 mod m_2, but this is guaranteed as long as the m_i's are pairwise coprime.
   (iii) This step is no problem, we are just setting a' and m' equal to values, and clearly m' will still be coprime to the remaining m_i's since m_1 and m_2 were.
   (iv) This just returns to a previous step, so will never fail.

   So the steps will always be executable. Now to show that the original set of congruences is equivalent to the set with a_1, m_1, a_2, m_2 replaced with a', m'. We have that if $x \equiv a' \pmod{m'}$, then

$$\begin{aligned} x &\equiv a_1 + (a_2 - a_1)ym_1 \equiv a_1 \pmod{m_1}, \\ x &\equiv a_1 + (a_2 - a_1)ym_1 \equiv a_1 + (a_2 - a_1) \cdot 1 \equiv a_2 \pmod{m_2}. \end{aligned}$$

So if x a solution to the second (primed) set of equivalence classes, then it is a solution to the first. Now we would like to show that it is the unique solution. So say we had another solution, x', which satisfies the first set of equalities. Then we know that $x' \equiv x \pmod{m_i}$ for every i. But this implies that m_1 and m_2 both divide $x - x'$, and since they are coprime, their product must divide this difference. Thus $x' \equiv x \pmod{m'}$. This shows that x satisfies the first set of solutions if and only if it satisfies the second set of solutions, and so the iterative process works in every step.

So by induction, the final solution, which is just a congruence class modulo the product of the m_i's, is the unique solution of the set of congruences in the beginning.

(b) We start with $x \equiv 4 \pmod 5, x \equiv 5 \pmod 7, x \equiv 6 \pmod{11}$. Since $5 \cdot 3 \equiv 1 \pmod 7$, we get the set of equivalences

$$x \equiv 4 + (5-4)3 \cdot 5 \equiv 19 \pmod{5 \cdot 7 = 35} \text{ and } x \equiv 6 \pmod{11}.$$

Now, $35 \cdot 6 = 210 \equiv 1 \pmod{11}$, so we finally have

$$x \equiv 19 + (6-19)6 \cdot 35 \equiv -2711 \equiv 369 \pmod{385}.$$

5. (Niven 2.3.20) Prove that there is a simultaneous solution of $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ iff $a_1 \equiv a_2 \pmod{(m_1, m_2)}$. Prove that the solution is unique modulo $[m_1, m_2]$.

We can prove this if and only if statement with a string of equivalences. We start with the left side of the equation:

$$\begin{gathered} \exists x \in \mathbb{Z} \text{ s.t. } x \equiv a_i \pmod{m_i} \text{ for } i \in \{1,2\} \\ \Leftrightarrow \exists n_i \in \mathbb{Z} \text{ s.t. } a_1 + m_1 n_1 = a_2 + m_2 n_2 \\ \Leftrightarrow \exists n_i \in \mathbb{Z} \text{ s.t. } m_1 n_1 - m_2 n_2 = a_2 - a_1. \end{gathered}$$

So the left side of the iff is equivalent to the solution in integers x, y of an equation of the form $ax + by = c$. We know that this is solvable exactly when $(a,b)|c$. So we have:

$$\begin{gathered} \Leftrightarrow (m_1, m_2)|(a_2 - a_1) \\ \Leftrightarrow a_1 \equiv a_2 \pmod{(m_1, m_2)}. \end{gathered}$$

6. (Niven 2.3.25) Prove that the number of integers $1 \leq n \leq mk$ that satisfy $(n,m) = 1$ is $k\phi(m)$.

With $k = 1$, this is just exactly the definition of the ϕ function. Now lets assume that the equation holds for some k, and try to prove it for $k+1$.

The number of integers $1 \leq n \leq m(k+1)$ that satisfy $(n,m) = 1$ is the sum of the following:

$$\#\{1 \leq n \leq mk \mid (n,m) = 1\} + \#\{mk + 1 \leq n \leq m(k+1) \mid (n,m) = 1\}.$$

By our inductive hypothesis, the first summand is $k\phi(m)$. Now to compute the second summand. For any n such that $mk + 1 \leq n \leq m(k+1)$, we have that $(n,m) =$

$(n-mk, m)$, since any common factor of n and m must divide $n-mk$, and any common factor of $n-mk$ and m must divide $n-mk+mk=n$. Therefore,

$$n \in \{mk+1 \leq n \leq m(k+1) \mid (n,m)=1\} \Leftrightarrow n-mk \in \{1 \leq n \leq m \mid (n,m)=1\}$$

Since the size of the right set is by definition $\phi(m)$, so is the size of the left set. Therefore, the above sum is $k\phi(m)+\phi(m)=(k+1)\phi(m)$, and the inductive step is complete!

7. (Niven 2.3.26) Prove that $\phi(nm)=n\phi(m)$ if every prime divisor of n also divides m.

   By definition,
   $$\phi(nm)=\#\{1 \leq t \leq nm \mid (t,nm)=1\}.$$
   Now, saying $(t,nm)=1$ is the same as saying t and nm share no prime divisors. But every prime dividing n also divides m, so the set of primes dividing nm is the exact set of primes that divide m. Therefore, $(t,nm)=1 \Leftrightarrow (t,m)=1$. So we get
   $$\phi(nm)=\#\{1 \leq t \leq nm \mid (t,m)=1\}=n\phi(m),$$
   where the last equality is known from the previous problem.

8. (Niven 4.2.4) Find the smallest m for which there exists another $n \neq m$ with $\sigma(m)=\sigma(n)$.

   This is a problem of simple computation:

n	$\sigma(n)$
1	1
2	3
3	4
4	7
5	6
6	12
7	8
8	15
9	13
10	18
11	12

   So six is the least number such that there exists another integer with the same sum of divisors (clearly no integer greater than 11 can have a sigma that is less than eight).

9. (Niven 4.2.5) Prove that
   $$\prod_{d|n} d = n^{d(n)/2}.$$
   Consider the square of the left side of the equation. We can shuffle this product as follows:
   $$\left(\prod_{d|n} d\right)^2 = \left(\prod_{de=n} d\right)\left(\prod_{de=n} e\right) = \prod_{de=n} de = \prod_{de=n} n = \prod_{d|n} n = n^{d(n)}.$$
   Since the square of the left side equals the square of the right, and they are both obviously positive, the sides are equal.

10. (Niven 4.2.9) Suppose that $f(n)$ and $g(n)$ are multiplicative.

    (a) Prove that $F(n) := f(n)g(n)$ is also multiplicative.
    Let $a, b \in \mathbb{Z}$ be such that $(a, b) = 1$. Then we have that

    $$F(ab) = f(ab)g(ab) = (f(a)f(b))(g(a)g(b)) = (f(a)g(a))(f(b)g(b)) = F(a)F(b).$$

    (b) If $g(n) \neq 0$ for all n, prove that $G(n) := f(n)/g(n)$ is multiplicative.
    Once again, we assume a and b are coprime. Then

    $$G(ab) = \frac{f(ab)}{g(ab)} = \frac{f(a)f(b)}{g(a)g(b)} = \frac{f(a)}{g(a)} \cdot \frac{f(b)}{g(b)} = G(a)G(b).$$

    We note that all fractions are well defined since $g(n) \neq 0$ for all $n \in \mathbb{Z}$.

11. (Niven 4.2.12) Prove that $\omega(n) = \#\{d \mid n\}$ is odd iff n is a square.

    Solution 1. Consider the set of divisors of n. Every element of this set pairs with another unique element of the set by the map $d \longleftarrow \frac{n}{d}$. The order of the pair doesn't matter. That is, if $x \longrightarrow y$ then $y \longrightarrow x$, because if we have $x \longrightarrow y \longrightarrow z$, then $xy = n = yz$ so $x = z$. So this relation pairs the divisors of n, and since all the divisors are paired uniquely, the parity of the number of elements in the set is equal to the parity of the number of elements that are mapped to themselves. So say there is some $x \longrightarrow x$. This implies that

    $$x = \frac{n}{x} \Longrightarrow x^2 = n.$$

    So clearly, the only time there is such an element, it is the unique square root of n. Thus $\omega(n)$ is odd exactly when n has an integral square root, that is, n is a square.

    Solution 2. Recall the divisor formula

    $$\omega(n) = \omega(p_1^{a_1} \cdots p_r^{a_r}) = (1 + a_1) \cdots (1 + a_r).$$

    This product is odd if and only if each term is odd, which means each a_i is even. But this means that $n = m^2$, with $m = p_1^{a_1/2} \cdots p_r^{a_r/2}$, which is guaranteed to be an integer due to the condition on the a_is.

12. (Niven 4.2.16 and 4.2.19) A positive integer n is a perfect number if $\sigma(n) = 2n$ (i.e., n is the sum of its proper divisors; for example, $6 = 1 + 2 + 3$ is perfect). Prove that if $2^m - 1 = p$ is prime, then $2^{m-1}p$ is perfect.

    So we have to calculate $\sigma(2^{m-1}p)$. We can certainly write out the divisors of this number, since we have its prime factorization. So

    $$\begin{aligned}\sigma(2^{m-1}p) &= 1 + 2 + 2^2 + \cdots + 2^{m-1} + p + 2p + 2^2p + \cdots + 2^{m-1}p \\ &= 1 + p + 2 + 2p + 2^2 + 2^2p + \cdots + 2^{m-1} + 2^{m-1}p \\ &= (1 + p)(1 + 2 + 2^2 + \cdots + 2^{m-1}) = (1 + p)(2^m - 1) \\ &= (1 + (2^m - 1))(2^m - 1) = 2^m(2^m - 1) = 2(2^{m-1}p).\end{aligned}$$

    So indeed, we have the $\sigma(n) = 2n$ for n of this form, and thus it is a perfect number.

(Bonus) Prove that every even perfect number has this form.

Remark: It is widely believed that there are no odd perfect numbers, although this is still an open conjecture!

13. (Niven 4.2.1) Find n such that $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.

    Since μ takes only the values $0, \pm 1$, it is clear that we need three consecutive integers with mu equalling positive one. For this, we need to avoid prime numbers, with a bit of checking the smallest such example is

    $$\mu(33) + \mu(34) + \mu(35) = \mu(3 \cdot 11) + \mu(2 \cdot 17) + \mu(5 \cdot 7) = 1 + 1 + 1 = 3.$$

14. (Niven 4.2.2) Prove that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$ for all n.

    Consider the four numbers $n, n+1, n+2, n+3$ mod 4. One of them must be congruent to zero mod 4. But this implies that four divides in, and so it is not squarefree. Therefore the μ of that number is zero, and so the product has one factor equal to zero. Thus the entire product is zero, so we are done.

(Bonus) (a) Prove that if f and g are multiplicative, then

$$F(n) := \sum_{d|n} f(d)g(n/d)$$

is multiplicative.

(b) Prove that if

$$F(n) = \sum d \mid nf(d),$$

then $f(n)$ is also multiplicative.

(c) Define

$$F(n) := \begin{cases} 1 & \text{if } n \text{ is square,} \\ 0 & \text{otherwise.} \end{cases}$$

Use Möbius inversion to find $f(n)$ such that

$$F(n) = \sum_{d|n} f(d).$$

Prove that f is multiplicative and find an explicit formula for $f(n)$.