MATH 289, PROBLEM SET 7
DUE: 10/27/2004

HARM DERKSEN

Hand in solutions to 4 problems from the following list of problems: Larson, 3.2.11***, 3.2.12***, 3.2.14***, 3.2.15***, 3.2.16***, 3.2.17***, 3.2.18***, 3.2.19***, 3.2.20***, 3.2.21*, 3.2.22*, 3.2.23*, 3.2.24*, 3.2.25*, 3.4.7***, 3.4.8***, 3.4.9***, 3.4.10***, 3.4.11**. You may also choose problems from below.

1. The Chinese Remainder Theorem

Suppose that \( m \) is an integer. We say that \( a \) is congruent to \( b \) modulo \( m \) if \( m \) divides the difference \( a - b \). The notation we use is

\[
a \equiv b \pmod{m}.
\]

Notice that if \( a_1 \equiv b_1 \pmod{m} \) and \( a_2 \equiv b_2 \pmod{m} \) then

\[
a_1 + a_2 \equiv b_1 + b_2 \pmod{m}
\]

and

\[
a_1a_2 \equiv b_1b_2 \pmod{m}.
\]

Theorem 1. Suppose that \( m \) and \( n \) are positive integers such that \( \gcd(m, n) = 1 \). Suppose that \( a \) and \( b \) are integers. Then there is a unique integer \( c \) with \( 0 \leq c < mn \) such that

\[
c \equiv a \pmod{m}
\]

and

\[
c \equiv b \pmod{n}
\]

Proof. We find can find integers \( x, y \in \mathbb{Z} \) such that \( xm + yn = 1 \). Note that \( xm \equiv 1 \pmod{n} \) and \( yn \equiv 1 \pmod{m} \). Consider \( d = bxm + ayn \). We can write

\[
d = qmn + c \text{ with } 0 \leq c < mn.
\]

Then

\[
c \equiv d \equiv ayn \equiv a \pmod{m}
\]

and

\[
c \equiv d \equiv bxm \equiv b \pmod{n}.
\]

This shows the existence of \( c \). Suppose that \( c' \) is another integer with \( c' \equiv a \pmod{m} \), \( c \equiv b \pmod{n} \) and \( 0 \leq c' < mn \). Then \( c - c' \) is divisible by \( m \) and by

\[Date: Winter 2004.\]
Because \( \gcd(m, n) = 1 \), \( c - c' \) is divisible by \( mn \). Since \( |c - c'| < mn \) we must have that \( c = c' \). □

The previous theorem easily can be generalized as follows.

**Theorem 2.** Suppose that \( m_1, m_2, \ldots, m_k \) are pairwise relatively prime positive integers (so \( \gcd(m_i, m_j) = 1 \) for \( i \neq j \)). Suppose that \( a_1, a_2, \ldots, a_k \) are integers. Then there is a unique integer \( c \) with \( 0 \leq c < m_1 m_2 \cdots m_k \) such that

\[
c \equiv a_i \pmod{m_i}
\]

for \( i = 1, 2, \ldots, k \).

**Example 1.** Show that the difference of two consecutive prime numbers can be arbitrarily large.

**Discussion.** We want to show that for every \( m \) there exists an \( n \) such that \( n + 1, n + 2, \ldots, n + m \) are not prime. Let us assume that \( n + 1 \) is divisible by 2 and that \( n > 2 \). Then \( n + 1 \) is not a prime number. Now \( n + 2 \) is not divisible by 2. However, we could assume that \( n + 2 \) is divisible by 3 and \( n + 2 > 3 \). Then \( n + 2 \) is certainly not a prime either. Similarly we could assume that \( n + 3 \) is divisible by 5 and \( n + 3 > 5 \). The Chinese Remainder Theorem comes to the rescue.

**Proof.** Let \( p_1, p_2, \ldots, p_m \) be the first \( m \) prime numbers. Using the Chinese Remainder theorem we can find an integer \( c \) such that

\[
n \equiv -i \pmod{p_i}
\]

for \( i = 1, 2, \ldots, m \). Without loss of generality we may assume that \( n > p_i \) for all \( i \) (otherwise we may add a multiple of \( p_1 p_2 \cdots p_m \) to \( n \)). For every \( i \) in \( \{1, 2, \ldots, m\} \) we see that \( p_i \) divides \( n + i \) but \( c + i > p_i \). This shows that \( c + i \) is not a prime number.

A slightly easier proof is the following.

**Proof.** For every \( n \), consider the numbers

\[
n! + 2, n! + 3, \ldots, n! + n.
\]

all these numbers are not prime numbers because \( n! + i \) is divisible by \( i \). ☺

**Problem 1.** ***[Gardner, M., *The Monkey and the Coconuts*, Ch. 9 in The Second Scientific American Book of Puzzles & Diversions: A New Selection. New York: Simon and Schuster, pp. 104-111, 1961.] Five sailors survive a shipwreck and swim to a tiny island where there is nothing but a coconut tree and a monkey. The sailors gather all the coconuts and put them in a big pile under the tree. Exhausted, they agree to go to wait until the next morning to divide up the coconuts.

At one o’clock in the morning, the first sailor wakes. He realizes that he can’t trust the others, and decides to take his share now. He divides the coconuts into
five equal piles, but there is one left over. He gives that coconut to the monkey, buries his coconuts, and puts the rest of the coconuts back under the tree. 

At two o’clock, the second sailor wakes up. Not realizing that the first sailor has already taken his share, he too divides the coconuts up into five piles, leaving one over which he gives to the monkey. He then hides his share, and piles the remainder back under the tree.

At three, four and five o’clock in the morning, the third, fourth and fifth sailors each wake up and carry out the same actions.

In the morning, all the sailors wake up, and try to look innocent. No one makes a remark about the diminished pile of coconuts, and no one decides to be honest and admit that they’ve already taken their share. Instead, they divide the pile up into five piles, for the sixth time, and find that there is yet again one coconut left over, which they give to the monkey.

How many coconuts were there originally? (Find the smallest number of coconuts that is consistent with this story.)

2. Euler’s Function

For an integer $n$ we define $\phi(n)$ as the number of elements in the set 
$$\{ a \in \mathbb{Z} \mid 1 \leq a \leq n, \gcd(a, n) = 1 \}$$
of all positive integers $a$ which are relatively prime to $n$.

**Lemma 1.** If $m$ and $n$ are positive integers then $\phi(mn) = \phi(m)\phi(n)$.

**Proof.** Given $c \in \{1, 2, \ldots, mn\}$ we can find unique $a \in \{1, 2, \ldots, n\}$ and $b \in \{1, 2, \ldots, m\}$ such that

$$c \equiv a \pmod{n}$$

and

$$c \equiv b \pmod{m}.$$ 

Conversely, given $a \in \{1, 2, \ldots, n\}$ and $b \in \{1, 2, \ldots, m\}$ there exists a unique $c \in \{1, 2, \ldots, mn\}$ such that (1) and (2) hold by the Chinese remainder theorem.

We have

$$\gcd(c, mn) = \gcd(c, m) \gcd(c, n) = \gcd(a, n) \gcd(b, m).$$

So $\gcd(c, mn) = 1$ if and only if $\gcd(a, n) = \gcd(b, m) = 1$. There are $\phi(n)$ choices for $a$ such that $\gcd(a, n) = 1$. There are $\phi(m)$ choices for $b$ such that $\gcd(a, m) = 1$. Therefore, there are $\phi(n)\phi(m)$ choices for $a$ and $b$ such that $\gcd(a, n) = \gcd(b, m) = 1$. So there are $\phi(m)\phi(n)$ choices for $c$ such that $\gcd(c, mn) = 1$. This shows that $\phi(mn) = \phi(m)\phi(n)$. 

**Lemma 2.** If $p$ is a prime number and $k$ is a positive integer then

$$\phi(p^k) = (p - 1)p^{k-1}.$$
Proof. The elements of
\[ \{1, 2, 3, \ldots, p^k\} \]
that are not relatively prime to \( p^k \) are exactly the \( p^{k-1} \) multiples of \( p \). This shows that
\[ \phi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}. \]
\[ \square \]

In general if \( n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \) is the prime factorization of \( n \), where \( p_1 < p_2 < \cdots < p_k \) are distinct prime numbers and \( a_1, a_2, \ldots, a_k \) are positive integers, then
\[ \phi(n) = (p_1 - 1)p_1^{a_1-1}(p_2 - 1)p_2^{a_2-1}\cdots(p_k - 1)p_k^{a_k-1}. \]

**Problem 2.** **** Find all integers \( n \) for which \( \phi(n) \) divides \( n \).

### 3. Fermat’s Theorem

**Theorem 3** (Fermat’s Theorem). If \( p \) is a prime number and \( a \) is an integer not divisible by \( p \), then
\[ a^{p-1} \equiv 1 \pmod p. \]

This is a special case of the Theorem 4

**Theorem 4.** If \( n \) is a positive integer and \( a \) is relatively prime to \( n \), then
\[ a^{\phi(n)} \equiv 1 \pmod n. \]

**Proof.** Let
\[ \{b_1, b_2, \ldots, b_{\phi(n)}\} \subset \{1, 2, \ldots, n\} \]
be the subset of elements that are relatively prime. For any \( i \), \( ab_i \) is again be relatively prime to \( \phi(n) \), because \( a \) and \( b_i \) are. Also if \( i \neq j \), then \( n \) does not divide \( b_i - b_j \). Since \( a \) is relatively prime to \( n \), \( n \) also does not divide \( a(b_i - b_j) = ab_i - ab_j \). This means that \( ab_i \) and \( ab_j \) are distinct modulo \( n \) if \( i \neq j \). Modulo \( n \),
\[ ab_1, ab_2, \ldots, ab_{\phi(n)} \]
is just a permutation of
\[ b_1, b_2, \ldots, b_{\phi(n)}. \]
In particular, their products are the same, so
\[ a^{\phi(n)}b_1b_2\cdots b_{\phi(n)} \equiv b_1b_2\cdots b_{\phi(n)} \pmod n \]
which means that \( n \) divides
\[ (a^{\phi(n)} - 1)b_1b_2\cdots b_{\phi(n)}. \]
Because all the \( b_i \) are relatively prime to \( n \), we get that \( n \) divides \( a^{\phi(n)} - 1 \) and we are done. \( \square \)
PROBLEM SET 7

PROBLEMS

Problem 3. ** Prove that a positive integer \( m \) is divisible by 11 if and only if the alternating sum of the digits of \( m \) is divisible by 11. (If \( m = a_n a_{n-1} \cdots a_0 \) then the alternating sum of the digits is \( a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \).) For example, 143 is divisible by 11 because \( 3 - 4 + 1 = 0 \).

Problem 4. * What is the remainder if we divide \( 2^{100} \) by 17.

Problem 5. * Show that

\[ x^2 + y^2 = 4k - 1 \]

has no integer solutions for \( x, y \) and \( k \).

Problem 6. ** Find the last 2 digits of \( 3^{1234} \). (Hint: Compute modulo 100)

Problem 7. (from Putnam)*** Let \( n \) be a positive integer such that \( n + 1 \) is divisible by 24. Prove that the sum of all the divisors of \( n \) is divisible by 24.

Problem 8. *** Assume that \( p \) is a prime number.

(a) Show that for any integer \( a \) with \( 1 \leq a \leq p - 1 \) there exists a unique integer \( b \) with \( 1 \leq b \leq p - 1 \) such that \( ab \equiv 1 \mod p \).

(b) Suppose that \( a^2 \equiv 1 \mod p \). Prove that \( a \equiv 1 \mod p \) or \( a \equiv -1 \mod p \).

(c) Prove Wilson’s Theorem:

\[ (p - 1)! \equiv -1 \mod p. \]

(Hint: Use (a) and (b).)

Problem 9. *** Let \( f(x) \) be a non-constant polynomial with integer coefficients. Prove that there exist infinitely many integers \( x \) such that \( f(x) \) is not a prime.

Problem 10. (from Putnam)**** The sequence \( (a_n)_{n \geq 1} \) is defined by \( a_1 = 1, \ a_2 = 2, \ a_3 = 24 \) and for \( n \geq 4, \)

\[ a_n = \frac{6a_{n-2}a_{n-3} - 8a_{n-1}a_{n-2}}{a_{n-2}a_{n-3}}. \]

Show that, for all \( n \), \( a_n \) is an integer multiple of \( n \).

Problem 11. (from Putnam)***** Show that if \( n \) is an integer greater than 1, then \( n \) does not divide \( 2^n - 1 \).