M328K Homework 4 – due Tuesday, Oct 19, 2010

1. Find all solutions to the following systems of equations:

(a) $x \equiv 3 \pmod 7$ and $x \equiv 7 \pmod 3$

(b) $x \equiv 5 \pmod{14}$ and $x \equiv 20 \pmod{21}$

(c) $x \equiv 5 \pmod{14}$ and $x \equiv 19 \pmod{21}$

2. The leader of an island tribe wanted to divide their pile of coconuts equally among the 10 inhabitants (including himself). When he discovered that there would be 9 coconuts left over, he reasoned (incorrectly) that if he expelled one member from the tribe, he would then be able to split the whole pile equally among the remaining members. Unfortunately when he re-divided the pile among the 9, there were now 8 coconuts left over, so he tried again to expel one person and split the pile among the remaining 8 people. This pattern continued: when he divided the pile evenly among 8 people there were 7 remaining coconuts, etc., until even when he split the pile among just 2 people, there was 1 coconut remaining. The only satisfactory solution, therefore, was to take all the coconuts himself! (Indeed, N divided by 1 leaves no remainder!)

How many coconuts were in the pile?

3. The Chinese Remainder Theorem merely asserts that something exists, but we can actually give a formula for it. Suppose that a and b are coprime; then we know that there exist integers u and v with $au + bv = 1$. Show that if we are given a and b *and* are given u and v as well, then for any two integers r and s, the integer $x = aus + bvr$ satisfies $x \equiv r \pmod a$ and $x \equiv s \pmod b$.

4. There is a tool that people use to check their arithmetic, called "casting out nines". This is illustrated by the following example: if we need to compute $(12 \times 34) + 56$ we may do so longhand; I get $408 + 56 = 464$. In order to check this, we instead replace every integer encountered by the sum of its digits, replacing 12 by $1 + 2 = 3$, 34 by 7, and 56 first by 11 and then by $1 + 1 = 2$; this gives us a simpler computation to do: $(3 \times 7) + 2 = 21 + 2 \longrightarrow 3 + 2 = 5$ This is to be compared to the digit-sum for our proposed answer: $464 \longrightarrow 14 \longrightarrow 5$. The fact that we got the same single digit (namely 5) in both cases is a corroboration that we probably did not make any mistakes.

(a) Show by example that this technique can fail to catch some errors in addition.

(b) Explain why the technique does work, that is, if for every integer n we let $D(n)$ be the sum of the digits of n (written in base-10 notation) and let $E(n)$ be the result of applying D repeatedly until only a single digit remains, then show $E(n + m) = E(E(n) + E(m))$ and $E(n \times m) = E(E(n) \times E(m))$. (*Hint:* $10^k \equiv 1 \pmod 9$ for every positive integer k. Now think about what "base-10 notation" means)

5. Recall that our *definition* of the Euler ϕ-function is that $\phi(n)$ is the number of integers in $\{0, 1, \ldots, n-1\}$ which are coprime to n. Use this definition to show that $\phi(n)$ is even for every integer $n > 2$.

6. We have proved the $\phi(nm) = \phi(n)\phi(m)$ when $a \perp b$, and we have also observed (from the definition of ϕ) that $\phi(p^k) = p^k - p^{k-1}$ when p is prime. Use these facts to show there is no integer n with $\phi(n) = 14$.

Remark It is clear from the definition of ϕ that $\phi(n) < n$, that is, if the value $m = \phi(n)$ is given, but n is not, then n must be larger than m. But how much larger? The answer is that there is no universal upper bound on n/m, that is, for every real number r there exist integers n with $n/\phi(n) > r$; similarly there are integers n with $n - \phi(n) > r$. So in question 5 you must provide some evidence that you have looked through all possible candidates n; saying you couldn't find any after checking all "small" n is not enough.

7. Show that if $m|n$ then $\phi(m)|\phi(n)$.

8. Show that if p and q are distinct primes, then

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

9. Fermat's theorem asserts that if p is prime and does not divide a then $F(a) = (a^p - 1)/p$ is an integer. Show that

$$F(a \cdot b) = F(a) + F(b) \pmod{p}$$

(Thus F is a kind of "discrete logarithm". Such functions are of great interest in computational number theory.)

Remark If $a \equiv 1 \pmod{p}$ then of course $F(a) = 0 \pmod{p}$. But there are other examples where $F(a) = 0 \pmod{p}$, for example $3^{10} - 1$ is a multiple of 11^2. An open question is whether there are other primes p with $2^p \equiv 1 \pmod{p^2}$, besides the two examples known ($p = 1093$ and $p = 3511$).