Geoffrey Parker - grp352
HW 3: 1.21-1.23, 1.25-1.28
M328K
January 26th, 2012

1.21 Theorem. *Let a natural number n be expressed in base 10 as*

$$n = a_k a_{k-1} \dots a_1 a_0.$$

(Note that what we mean by this notation is that each a_i is a digit of a regular base 10 number, not that the a_i's are being multiplied together.) If $m = a_k + a_{k-1} + \dots + a_1 + a_0$, then $n \equiv m \pmod 3$.

Proof. Let a natural number n be expressed in base 10 as $n = a_k a_{k-1} \dots a_1 a_0$. Let m be the sum of these digits, that is $m = a_k + a_{k-1} + \dots + a_1 + a_0$. We will show that $n \equiv m \pmod 3$. First, note that because n is in base 10, in can be expressed like such:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

So if we compute $n - m$, we get:

$$n - m = a_k \cdot 10^k - a_k + a_{k-1} \cdot 10^{k-1} - a_{k-1} + \dots + a_1 \cdot 10^1 - a_1 + a_0 \cdot 10^0 - a_0$$

Combining terms, we see that:

$$n - m = a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \dots + a_1(10^1 - 1)$$

Next we see that for any integer j, $10^j - 1$ will be $9(10^{j-1}) + 9(10^{j-2} + \dots + 9(10^1) + 9(10^0)$, that is $999 \dots 99$, with the number of nines equal to 10^{j-1}. We can also see that this must be equal to $3 \times (3(10^{j-1}) + 3(10^{j-2}) + \dots + 3(10^1) + 3(10^0))$, because each term in the nines series is three times the corresponding term in the threes series. Therefore 3 must divide $10^k - 1$, $10^{k-1} - 1$, $\dots$, and $10^1 - 1$. So by theorem 1.3, 3 divides each term in the $n - m$ series. This means, by theorem 1.1, that 3 divides the entire series, and thus $n - m$. Since $3 \mid (n - m)$, by definition of congruence mod n $n \equiv m \pmod 3$, which is what we set out to prove. $\square$

1.22 Theorem. *If a natural number is divisible by* 3*, then, when expressed in base* 10*, the sum of its digits is divisible by* 3*.*

Proof. Let n be a natural number such that $3 \mid n$. We will show that, when expressed in base 10, 3 also divides the sum of its digits. First, let n be expressed as:

$$n = a_k = ja_{j-1} \ldots a_1 a_0$$

where each a_k is a base 10 digit of n. Then n can be rewritten:

$$n = a_j \cdot 10^j + a_{j-1} \cdot 10^{j-1} + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

Since, by the definition of divides there exists some integer k such that $n = 3k$:

$$3k = a_j \cdot 10^j + a_{j-1} \cdot 10^{j-1} + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

□

1.23 Theorem. *If the sum of the digits of a natural number expressed in base* 10 *is divisible by* 3*, then the number is divible by* 3 *as well.*

Proof. Type your proof here! □

1.25 Exercise. *Illustrate the Division Algorithm for:*

(1) $m = 25$, $n = 7$.

Solution. $m = n \times 3 + 4$ □

(2) $m = 277$, $n = 4$.

Solution. $m = n \times 69 + 1$ □

(3) $m = 33$, $n = 11$.

Solution. $m = n \times 11 + 0$ □

(4) $m = 33$, $n = 45$.

Solution. $m = n \times 0 + 33$ □

1.26 Theorem. *Prove the existence part of the Division Algorithm. (Hint: Given n and m, how will you define q? Once you choose this q, then how is r chosen? Then show that $0 \leq r \leq n-1$.)*

Proof. Let n and m be natural numbers. Let S be the set of natural numbers of the form $m - nk + 1$ for some integer k. Since m is a natural number, S always has at least one member, $m - n0 + 1$. Therefore by the Well-Ordering Axiom for the natural numbers, there exists a smallest element of the set S. Let q be an integer such that $m - nq + 1$ is this smallest element. Let $r = m - nq$. So $m = nq + r$. Now we will show that $0 \leq r \leq n-1$. Since r is defined to be drawn from a subset of the natural numbers, $r \geq 0$. Assume by way of contradiction that $r \geq n$. This would mean that $m - nq \geq n$, or $m - nq - n \geq 0$. So $m - n(q+1) \geq 0$, which makes $m - n(q+1) + 1$ an element of S. But $m - n(q+1) + 1 < m - nq + 1$, which is a contradiction, since $m - nq + 1$ is the smallest element of S. Therefore $r < n$, or, since r and n are integers, $r \leq n-1$. So we have proved that $0 \leq r \leq n-1$. □

NOTE TO READER: The well ordering axiom we have is only defined on the natural numbers, which is why there are +1's every time S is mentioned.

1.27 Theorem. *Prove the uniqueness part of the Division Algorithm.*

(Hint: If $nq + r = nq' + r'$, then $nq - nq' = r' - r$. Use what you know about r and r' as part of your argument that $q = q'$.)

Proof. Let there be integers $m,\ n,\ q,\ r,\ q',\ r'$ such that $m = nq + r$, $m = nq' + r'$, $0 \leq r \leq n$, and $0 \leq r' \leq n$. Given this, $nq+r = nq'+r'$, or $r-r' = nq'-nq = n(q'-q')$, which means that $n \mid (r-r')$. So by the definition of divides, there exists some integer k such that $nk = r - r'$. However, $\leq r \leq n$ and $0 \leq r' \leq n$, so $-n < r - r' < n$, which means that k must be 0 and $r - r'$ must be 0. Therefore $r = r'$. Going back to $r - r' = n(q' - q')$, we can say that $n(q' - q') = 0$. Since n is a natural number, and thus not 0, $q' - q$ must be 0. Therefore $q = q'$. □

1.28 Theorem. *Let a, b, and n be integers with $n > 0$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if and only if when $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$, then $r_1 = r_2$.*

Proof. Let a, b, and n be integers with $n > 0$. This will be a two part proof.

First, assume $a \equiv b \pmod{n}$. By definition of congruence mod n, this means that there exists some integer k such that $kn = a - b$, giving $a = kn + b$ and $b = -kn + a$. By the Division Algorithm, there exist integers $q_1,\ r_1,\ q_2,\ r_2$ with $0 \leq r_1 \leq n-1$ and $0 \leq r_2 \leq n-1$ such that $a = nq_1 + r_1$ and $b = nq_2 + r_2$ $\square$