Geoffrey Parker - grp352
HW 16: 3.13-3.17
M328K
March 22th, 2012

3.13 Theorem. *Suppose* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ *is a polynomial of degree* $n > 0$ *with integer coefficients. Then* $f(x)$ *is a composite number for infinitely many integers* x.

Proof. Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is a polynomial of degree $n > 0$ with integer coefficients and $a_n > 0$. We will show that $f(x)$ is a composite number for infinitely many integers x. Let S be the set of integers x such that $f(x)$ is composite and let T be the set of numbers $f(x)$ such that x is an element of S. Assume by way of contradiction that S is finite. Let m be an element of S such that $f(m)$ is the largest element of T. By theorem 3.12, there exists an integer k such that for all integers $j > k$, $f(j) > f(m)$. Now consider these two cases: $a_0 = 0$ and $a_0 \neq 0$.
In the case that $a_0 \neq 0$, let $y = (k+1)\,|a_0|$. Since $a_0 \neq 0$, y must be greater than k. Therefore $f(y) > f(m)$. Also, $a_0 \mid y$, so $y \equiv 0 \pmod{a_0}$. By theorem 3.8, this means that $f(y) \equiv f(0) \pmod{a_0}$, or equivalently, $a_0 \mid f(y) - a_0$. Then by theorem 1.1, $a_0 \mid f(y) - a_0 + a_0$, so $a_0 \mid f(y)$. This means that $f(y)$ is composite.
In the other case, $a_0 = 0$, let p be a natural number and let $y = kp$. This implies that $y > m$ and that $y \equiv 0 \pmod{p}$. By theorem 3.8, $f(y) \equiv f(0) \pmod{p}$, and since $a_0 = 0$, $f(y) \equiv 0 \pmod{p}$. Now we have that $p \mid f(y)$, so y is composite.
In either case, we have found an integer $y > m$ such that $f(y)$ is composite. By theorem 3.12, $f(y) > f(m)$. However, because $f(y)$ is composite, it must be an element of T and $f(m)$ is the largest element of T. Therefore we have contradicted our assumption and S must be infinite. $\square$

3.14 Theorem. *Given any integer a and any natural number n, there exists a unique integer t in the set $\{0, 1, 2, \ldots, n-1\}$ such that $a \equiv t \pmod{n}$.*

Proof. Let a be an integer and n be a natural number. Let S be the set $\{0, 1, 2, \ldots, n-1\}$. By the division algorithm there exist integers q and r such that $a = nq + r$ with $0 \leq r \leq n-1$. So $nq = a - r$, which by the definition of dividies means that $n \mid a - r$. By the definition of congruence mod n, $a \equiv r \pmod{n}$. Since $0 \leq r \leq n-1$, if we let $t = r$, we have shown that there exists an integer t element of S such that $a \equiv t \pmod{n}$. □

3.15 Exercise. *Find three complete residue systems modulo 4: the canonical complete residue system, one containing negative numbers, and one containing no two consecutive numbers.*

Solution. canonical complete: $\{0, 1, 2, 3\}$
negative: $\{-1, -2, -3, -4\}$
non-consecutive: $\{0, 2, 5, 7\}$ □

3.16 Theorem. *Let n be a natural number. Every complete residue system modulo n contains n elements.*

Proof. Let n be a natural number. Let S be any complete residue system modulo n. We will show that S contains n elements. Consider T, the set of integers $\{0, 1, \ldots, n-1\}$. Note that T is the canonical complete residue system modulo n and $|T| = n$. Since each element of T is congruent to itself modulo n and by definition of complete residue systems modulo n every integer is congruent modulo n to exactly one element of T, no element of T is congruent to another distinct element of T modulo n. Let a and b be any two distinct elements of T. We know by definition of complete residue systems modulo n again that a and b are congruent modulo n to exactly one element of S each. We will call these elements of S a' and b' respectively. We know that $a' \neq b'$ because if they were equal, then we would have $a \equiv a' \pmod{n}$ and $a' \equiv b \pmod{n}$ implying by theorem 1.11 that $a \equiv b \pmod{n}$, which we know is not true. Therefore every element of T coorespondes to a distinct element of S, meaning that $|S| \geq |T|$. Assume by way of contradiction that $|s| > n$. We know, since T is the canonical complete residue system modulo n, that every element of S is congruent modulo n to exactly one element of T. Because $|S| > |T|$, the pigeon hole principle implies that there must be at least two elements of S, call them x and y that are congruent modulo n to the same element of T, which we will call z. So $x \equiv z \pmod{n}$ and $y \equiv z \pmod{n}$, implying by theorem 1.11 that $x \equiv y \pmod{n}$. However, since all integers are congruent mod n to themselves, we now have that y is congruent mod n to two elements of S, contradicting it's definition as a canonical complete residue system modulo n. Therefore S contains exactly n elements. $\square$

3.17 Theorem. *Let n be a natural number. Any set of n integers $\{a_1, a_2, \ldots, a_n\}$ for which no two are congruent modulo n is a complete residue system modulo n.*

Proof. Let n be a natural number. Let S be a set of n integers $\{a_1, a_2, \ldots, a_n\}$ for which no two are congruent modulo n. Let T be the canonical complete residue system modulo n. Let x be an arbitrary integer. By definition of T, there must be some y which is an element of T such that $x \equiv y \pmod{n}$. Let z be an element of S such that $z \equiv y \pmod{n}$. We know that z exists because $|S| = |T|$ and every element of S is congruent modulo n to a different element of T. If there were two elements of S, j and k, that were congruent modulo n to the same element of T. then by theorem 1.11 we would have $j \equiv k \pmod{n}$, which contradicts the definition of S. Now by theorem 1.11 again, $x \equiv z \pmod{n}$. Let z' some element of S such that $x \equiv z' \pmod{n}$. By theorem 1.11, this means that $z \equiv z' \pmod{n}$, which contradicts the definition of S unless $z = z'$. Therefore, since x is arbitrary, every integer is congruent modulo n to exactly one element of S, which is the definition of a complete residue system modulo n. $\square$