Math 302 **Modern Algebra** **Spring 2009**

Exam 1 Solutions

1. (16 points) Prove Theorem 1.10 for positive integers: Every positive integer greater than 1 is the product of primes.

This has symbolic form

$$(\forall n > 1)\,[n \text{ is a product of primes}].$$

Note that a product of primes may include a single factor, so when we say "n is a product of primes," it includes the case that n is itself a prime.

Proof: Use a proof by contradiction. Suppose the statement is false, so the negation is true. The negation is

$$(\exists n > 1)\,[n \text{ is not a product of primes}].$$

Suppose then there exists a positive integer greater than 1 that is not the product of primes. We then need to obtain a contradiction.

Let S be the set of all positive integers greater than 1 that are not the product of primes, so

$$S = \{n > 1 \mid n \text{ is not a product of primes}\}.$$

Since we are supposing there exists a positive integer greater than 1 that is not the product of primes, then the set S is not empty. The Well Odering Axiom then implies S has a smallest element n_0. Since $n_0 \in S$, then $n_0 > 1$ and n_0 is not the product of primes. Since n_0 is not the product of primes, then n_0 is not itself a prime. Therefore n_0 is composite. This implies

$$n_0 = ab \qquad \text{for some integers } a \text{ and } b, \text{ with } 1 < a, b < m.$$

Since both a and b are less than n_0 and greater than 1 and n_0 is the smallest element of S, then $a \notin S$ and $b \notin S$. Therefore both a and b must be products of primes

$$a = p_1 p_2 \cdots p_s \qquad \text{and} \qquad b = q_1 q_2 \cdots q_t,$$

for some primes $p_1, p_2, \ldots, p_s, q_1, q_2, \ldots, q_t$. But then $n_0 = ab$ implies

$$n_0 = (p_1 p_2 \cdots p_s)(q_1 q_2 \cdots q_t).$$

This implies n_0 is a product of primes. This is a contradiction since $n_0 \in S$. Thus the result is true, so every positive integer greater than 1 is a product of primes.

2. (20 points)

(a) Find the greatest common divisor of 92 and 135 using the Euclidean Algorithm.

Start by dividing 135 by 92. At each step, divide the preceding step's remainder into the preceding step's divisor.

$$\begin{aligned} 135 &= 1(92) + 43 \\ 92 &= 2(43) + 6 \\ 43 &= 7(6) + 1 \\ 6 &= 6(1) + 0 \end{aligned}$$

The greatest common divisor is the last nonzero remainder. Therefore $(135, 92) = 1$.

(b) Use your work from part (a) to write the greatest common divisor as a linear combination of 92 and 135.

Back-substituting for the remainder in each step, we obtain

$$\begin{aligned} 1 &= 43 - 7(6) = 43 - 7[92 - 2(43)] \\ &= 15(43) - 7(92) = 15[135 - 1(92)] - 7(92) \\ &= 15(135) - 22(92) \end{aligned}$$

(c) Solve the equation $135x = 17$ in $\mathbb{Z}_{92}$.

Since $(135, 92) = 1$, then the equation has a unique solution by Corollary 2.10. From part (b), we have $135(15) - 92(22) = 1$, which implies

$$135(15) = 1 + 92(22) \equiv 1 \pmod{92}.$$

Multiplying by 17, we obtain

$$135(15 \cdot 17) \equiv 17 \pmod{92}.$$

Therefore $15 \cdot 17 = 255 \equiv 71 \pmod{92}$ is a solution to the equation in $\mathbb{Z}_{92}$.

3. (32 points) Let p be an integer other than 0, ± 1. Prove that p is prime if and only if it has the following property:

For all integers r and s, if $p = rs$, then $r = \pm 1$ or $s = \pm 1$.

This has symbolic form

$$(\forall p)\left[(p \text{ is prime}) \leftrightarrow (\forall r \in \mathbb{Z})\,(\forall s \in \mathbb{Z})\,[p = rs \rightarrow (r = \pm 1 \vee s = \pm 1)\right].$$

Proof:

Forward Direction. Suppose p is a prime. We need to show that the given property holds. That is, we need to show

$$(\forall r \in \mathbb{Z})\,(\forall s \in \mathbb{Z})\,[p = rs \rightarrow (r = \pm 1 \vee s = \pm 1).$$

Suppose r and s are arbitrary integers. Suppose

$$p = rs.$$

We need to show that

$$r = \pm 1 \qquad \text{or} \qquad s = \pm 1.$$

Since $p = rs$, then $p|rs$. Theorem 1.8 then implies that $p|r$ or $p|s$. This gives two cases. In each case, we need to show $r = \pm 1$ or $s = \pm 1$.

Case 1. Suppose $p|r$. Since $p = rs$, then $r|p$ also. Then $p|r$ and $r|p$ imply $p = \pm r$. Substituting into the equation $p = rs$, we obtain $\pm r = rs$ and therefore $s = \pm 1$, as required.

Case 2. Suppose $p|s$. Since $p = rs$, then $s|p$ also. Then $p|s$ and $s|p$ imply $p = \pm s$. Substituting into $p = rs$, we obtain $\pm s = rs$ and therefore $r = \pm 1$, as required.

This proves the forward direction.

Backward Direction. Now suppose the property holds:

For all integers r and s, if $p = rs$, then $r = \pm 1$ or $s = \pm 1$.

We need to show

p is prime.

Using the definition, to show that p is prime, we need to show that the only divisors of p are ± 1 and $\pm p$. Suppose then that d is an arbitrary divisor of p. We need to show $d = \pm 1$ or $d = \pm p$.

Since $d|p$, then there exists an integer c such that $p = cd$. By the property, it follows that $c = \pm 1$ or $d = \pm 1$. This gives two cases. In each case, we need to show $d = \pm 1$ or $d = \pm p$.

Case 1. Suppose $d = \pm 1$. There's nothing to show in this case.

Case 2. Suppose $c = \pm 1$. Then $p = cd = \pm d$ so $d = \pm p$.

This shows that the only divisors of p are ± 1 or $\pm p$. Thus p is prime. This proves the backward direction.

4. (20 points)

(a) Prove: For all nonnegative integers k, $10^k \equiv (-1)^k \pmod{11}$.

Suppose k is an arbitrary nonnegative integer. We need to show that $10^k \equiv (-1)^k \pmod{11}$. First note that

$$10^0 = 1 \equiv (-1)^0 \pmod{11}$$

so the result holds when $k = 0$. Next,

$$10^1 \equiv (-1)^1 \pmod{11}$$

since $11|\big(10 - (-1)\big) = 11$. According to Theorem 2.2(b), we can multiply this congruence by itself to obtain the congruence

$$10^2 \equiv (-1)^2 \pmod{11}.$$

We can then multiply the original congruence times this congruence to obtain

$$10^3 \equiv (-1)^3 \pmod{11}.$$

Continuing this procedure, we obtain the required result

$$10^k \equiv (-1)^k \pmod{11}.$$

(b) Prove: For all positive integers n, if n has decimal representation $n = a_t a_{t-1} \cdots a_1 a_0$, then

$$n \equiv a_0 - a_1 + a_2 - a_3 + a_4 - \cdots + (-1)^t a_t \pmod{11}.$$

Suppose n is a positive integer with decimal representation $n = a_t a_{t-1} \cdots a_2 a_1 a_0$. This means

$$n = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + a_4 10^4 + \cdots + a_t 10^t.$$

By part (a), since $10^k \equiv (-1)^k \pmod{11}$ for each positive integer k, then Theorem 2.2(b) implies

$$a_k 10^k \equiv (-1)^k a_k \pmod{11} \qquad \text{for each } k = 1, 2, \ldots, t.$$

Theorem 2.2(a) then implies

$$\begin{aligned} n &= a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + a_4 10^4 + \cdots + a_t 10^t \\ &\equiv a_0 + a_1(-1)^1 + a_2(-1)^2 + a_3(-1)^3 + a_4(-1)^4 + \cdots + a_t(-1)^t \pmod{11} \\ &\equiv a_0 - a_1 + a_2 - a_3 + a_4 - \cdots + (-1)^t a_t \pmod{11} \end{aligned}$$

(c) Use the result of part (b) to show that 11|646,173.

According to the result of part (b),

$$\begin{aligned} 646{,}173 &\equiv 3 - 7 + 1 - 6 + 4 - 6 \pmod{11} \\ &\equiv -11 \pmod{11} \\ &\equiv 0 \pmod{11} \end{aligned}$$

This implies 11|646,173.

5. (18 points) Prove: For all integers a, b, and c, and all positive integers n, if $[a] \odot [b] = [a] \odot [c]$ in $\mathbb{Z}_n$ and $(a, n) = 1$, then $[b] = [c]$ in $\mathbb{Z}_n$.

This has symbolic form

$$(\forall a \in \mathbb{Z})\,(\forall b \in \mathbb{Z})\,(\forall c \in \mathbb{Z})\,(\forall n \in \mathbb{N})\,\big[[a] \odot [b] = [a] \odot [c] \wedge (a, n) = 1 \rightarrow [b] = [c]\big].$$

Proof: Suppose a, b, and c are arbitrary integers and n is an arbitrary positive integer. Suppose

$$[a] \odot [b] = [a] \odot [c] \quad \text{in } \mathbb{Z}_n$$

and

$$(a, n) = 1.$$

We need to show that

$$[b] = [c] \quad \text{in } \mathbb{Z}_n.$$

Since $[a] \odot [b] = [a] \odot [c]$, then $[ab] = [ac]$ in $\mathbb{Z}_n$, which implies

$$ab \equiv ac \pmod{n}.$$

This implies $n|ab - ac = a(b - c)$. Since $(a, n) = 1$, this implies $n|(b - c)$ by Theorem 1.5. Therefore

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

which then implies

$$[b] = [c] \quad \text{in } \mathbb{Z}_n$$

as required.