Mathematics 243, section 3 – Algebraic Structures
Problem Set 6
due: October 26, 2012

'A' Section

1. Solve each of the following congruences for $x \in \mathbb{Z}$, with $0 \leq x < n$. Note that in each case it is possible to rewrite the given congruence in the form $ax \equiv b \pmod{n}$ with $\gcd(a, n) = 1$.

   a. $7x \equiv 13 \pmod{24}$

   Solution: Since $\gcd(7, 24) = 1$, there exist integers m, n such that $7m + 24n = 1$. Applying the Generalized Euclidean Algorithm, the smallest pair m, n that works here is $m = 7$ and $n = 2$. This says that $7 \cdot 7 \equiv 1 \pmod{24}$. So multiplying both sides of the congruence by 7, we get $x \equiv 91 \equiv 19 \pmod{24}$. The solution with $0 \leq x < 24$ is $x = 19$.

   b. $14x + 25 \equiv 3 \pmod{393}$

   Solution: The congruence can be rewritten as $14x \equiv -22 \pmod{393} \equiv 371 \pmod{393}$ Since $\gcd(14, 393) = 1$, there exist integers m, n such that $14m + 393n = 1$. Applying the Generalized Euclidean Algorithm, the smallest pair m, n that works here is $m = -28$ and $n = 1$. This says that $14 \cdot -28 \equiv 1 \pmod{393}$. So multiplying both sides of the congruence $14x \equiv -22 \pmod{393}$ by -28, we get $x \equiv 616 \equiv 223 \pmod{393}$. The solution with $0 \leq x < 393$ is $x = 223$.

2. What is the ones digit in 43^{15}? Hint: consider $43^{15} \pmod{10}$ and use Theorem 2.22 in the text, or problem B 4 below.

   Solution: We have $43 \equiv 3 \pmod{10}$, and computing using Theorem 2.22 or problem B 4 below we see

   $$43^2 \equiv 3^2 \equiv 9 \pmod{10} 43^3 \equiv 3^3 \equiv 7 \pmod{10} 43^4 \equiv 3^4 \equiv 1 \pmod{10}$$

   Hence the ones digits of the powers of 43 form a cycle of length 4: $3, 9, 7, 1, 3, 9, 7, 1, \cdots$. After 15 terms we will have gone through three full cycles and 3 more terms in the fourth cycle, so

   $$43^{15} \equiv 3^{15} \equiv 3^{15 \pmod{4}} \pmod{10} \equiv 3^3 \pmod{10} \equiv 7 \pmod{10}.$$

3. Find a positive integer x that satisfies the two simultaneous congruences

   $$\begin{aligned} 2x + 1 &\equiv 5 \pmod{9} \\ 3x + 4 &\equiv 8 \pmod{10} \end{aligned}$$

   Explain your method.

4. Proceeding as in question 1 above (but omitting the calculations which are much simpler), we see that x satisfies the first congruence if $2x \equiv 4 \pmod{9}$. Since $2 \cdot 5 \equiv 1 \pmod{9}$, we have $x \equiv 2 \pmod{9}$. This says that $x = 2 + 9k$ for some $k \in \mathbb{Z}$. Similarly, the second congruence says $3x \equiv 4 \pmod{10}$, and $3 \cdot 7 \equiv 1 \pmod{10}$, so $x \equiv 8 \pmod{10}$, so $x = 6 + 10\ell$ for some $\ell \in \mathbb{Z}$. Among the integers $x = 2, 11, 20, 29, 38, 47, 56, \cdots$, satisfying the first congruence, we see that $x = 38$ also satisfies the second. Note that any $x = 38 + 90m$ is another solution.

'B' Section

1. A *least common multiple*, or *lcm*, of two nonzero integers a, b is a positive integer m such that

   - $a|m$ and $b|m$, and
   - $a|c$ and $b|c$ imply $m|c$.

   Part a below will show that lcm's always exist, and part b asks you to derive a method for computing them via prime factorizations.

   a. Show that if $a, b > 0$, and $d = \gcd(a, b)$ with $a = da_0$ and $b = db_0$, then $m = da_0b_0$ is a least common multiple of a, b.

   Proof: Note that $d > 0$ by definition. Since $a, b > 0$, then it is clear that $a_0, b_0 > 0$ too, so $da_0b_0 > 0$ is also true. We have $m = (da_0)b_0 = ab_0$ so $a|m$. Similarly, by commutativity and associativity of multiplication in $\mathbb{Z}$, $m = (db_0)a_0 = ba_0$. Hence $b|m$. Finally, we must show that if $a|c$ and $b|c$, then $(da_0b_0)|c$. It will be convenient to state and prove the following special case of what we are trying to prove first:

   Lemma 1 *Let* $\gcd(a_0, b_0) = 1$ *and assume that* $a_0|c$ *and* $b_0|c$. *Then* $(a_0b_0)|c$.

   The proof of the lemma is as follows: Since $a_0|c$ and $b_0|c$, we have $c = a_0q = b_0q'$ for some integers q, q'. Since $\gcd(a_0, b_0) = 1$, we have $1 = \ell a_0 + kb_0$ for some integers ℓ, k. But then multiplying both sides of the last equation by q, we have $q = \ell a_0q + kb_0q$, so

   $$q = \ell c + kb_0q = \ell b_0q' + kb_0q = b_0(\ell q' + kq)$$

   This shows that $b_0|q$. Hence $(a_0b_0)|c$.//

   Now we return to the main statement to be proved. Since $d = \gcd(a, b)$, in the factorizations $a = da_0$ and $b = db_0$, it must be the case that $\gcd(a_0, b_0) = 1$ (do you see why?) To apply the lemma, we can argue as follows. If $a|c$ and $b|c$, then $d|c$ as well, so $c = da_0q = db_0q'$ for some integers q, q'. By cancellation, this implies $a_0q = b_0q' = c' = c/d$. By the lemma, $(a_0b_0)|c'$. Hence $(da_0b_0)|c$.

   b. Deduce from part a that $md = ab$.

   Proof: This follows immediately since by commutativity and associativity of multiplication, $md = (da_0b_0)d = (a_0d)(b_0d) = ab$.

c. Describe a method for computing a least common multiple of a, b from their standard form factorizations as on page 92 of the text.

Proof: Suppose that $p_1, \ldots, p_k$ are all the primes appearing in the standard form factorizations of a or b or both. Then $a = \pm p_1^{e_1} \cdots p_k^{e_k}$ and $b = \pm p_1^{f_1} \cdots p_k^{f_k}$ for some exponents $e_i, f_i \geq 0$. The lcm of a, b is the integer with standard form factorization

$$\operatorname{lcm}(a, b) = p_1^{M_1} \cdots p_k^{M_k}$$

where $M_i = \max(e_i, f_i)$ for each $1 \leq i \leq k$.

2. In this problem, you will derive another result first found by the Pythagorean philosophers in ancient Greece. Let a, b be relatively prime integers.

a. Arguing by contradiction, use the fact that 2 is a prime number and Euclid's Lemma to show that it is never the case that $a^2 = 2b^2$.

Proof: By Euclid's Lemma, since $2|(2b^2)$, we have $2|a$, or $a = 2q$ for some integer q. But then $4|a^2$, so we have an equation $4q^2 = 2b^2$. By the cancellation law in $\mathbb{Z}$, we can write $2q^2 = b^2$. Now we repeat the same argument. Since $2|b^2$, it must be true that $2|b$ by Euclid's Lemma. But then $2|a$ and $2|b$ so a, b cannot be relatively prime. This contradiction shows that there is no equation $a^2 = 2b^2$ with $a, b \in \mathbb{Z}$.

b. Explain why the result of part a shows that $\sqrt{2} \in \mathbb{R}$ is *not a rational number.*

Proof: If $\sqrt{2} \in \mathbb{Q}$, then we would have an equation $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Moreover, recall that by cancelling common factors between the numerator and denominator, any rational number can be written as a fraction *in lowest terms.* So we can assume $\gcd(a, b) = 1$. But then squaring both sides and multiplying by b^2 would give $2b^2 = a^2$. This is not possible by part a. Therefore, $\sqrt{2} \notin \mathbb{Q}$.

Comments:

i. Here's an example of a lowest terms fraction. We have $\frac{240}{1600} = \frac{3}{20}$ in lowest terms, since $240 = 3 \cdot 80$ and $1600 = 20 \cdot 80$.

ii. A possibly fictional story runs that Hippasus of Metapontum (one of the Pythagoreans) was murdered by his colleagues for divulging this terrible secret(!) At the time, only rational numbers were accepted as valid objects for mathematical reasoning.

3. Let $b > 1$ be an integer. Show that every nonnegative integer n can be written in the form

$$n = d_0 + d_1 b + d_2 b^2 + \cdots + d_m b^m$$

where $0 \leq d_i < b$ for all i. (The resulting expansion is called the *base-b expansion* of n, and the d_i are called the base-b digits of n. The usual choice for us is $b = 10$, but any other base $b > 1$ works just as well.) Hints: Let m be the largest non-negative integer such that $b^m \leq n$, and divide b^m into n. If you are clever you can then apply an induction hypothesis to finish the proof.

Proof: We use the method of Proof by Complete Induction (see page 75 in the text). For the base case $n = 0$, we have $0 = 0 + 0 \cdot b + \cdots$, which has the required form. (In other words, all the digits are 0.) Now assume that the statement has been proved for all integers $n < k$ and consider $n = k$. Since $b > 1$, the powers b^ℓ for $\ell \in \mathbb{Z}^+$ grow without any bound. Hence there will be some $\ell = m$ such that

$$b^m \leq k < b^{m+1}. \tag{1}$$

Apply the division algorithm to divide k by b^m. We get

$$k = qb^m + r$$

where $0 \leq r < b^m$. Moreover, by (1), $1 \leq q < b$, so $q = d_m$ will be one of our base b digits. Finally since $r < b^m \leq k$, we can also apply our induction hypothesis to r, and write $r = d_0 + d_1 b + \cdots + d_{m-1} b^{m-1}$. Therefore

$$k = r + qb^m = d_0 + d_1 b + \cdots + d_{m-1} b^{m-1} + d_m b^m$$

as required. (Note that since $r < b^m$, in its base b expansion, only powers of b up to b^m can appear. Moreover,

$$(b-1) + (b-1)b + \cdots + (b-1)b^{m-1} = (b-1)(1 + b + \cdots + b^{m-1}) = b^m - 1$$

so no number $\geq b^m$ can be written using only powers b^{m-1} and smaller.)

4. Give a direct proof (i.e. one *not* appealing to Theorem 2.22 in the text) of the following statements: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

   Proof: The given information is equivalent to saying $a = b + kn$ and $c = d + \ell n$ for some integers k, ℓ. Therefore $a + c = b + d + (k + \ell)n$, so $(a + c) - (b + d) = (k + \ell)n$. Hence by definition, $a + c \equiv b + d \pmod{n}$. Similarly

   $$ac = (b + kn)(d + \ell n) = bd + n(b\ell + dk + nk\ell).$$

   This implies $ac - bd = n(b\ell + dk + nk\ell)$. By definition, $ac \equiv bd \pmod{n}$.

5. Show that if m is any integer, then exactly one of the following statements is true: $m^2 \equiv 0 \pmod{8}$, $m^2 \equiv 1 \pmod{8}$, or $m^2 \equiv 4 \pmod{8}$.

   Proof: Every integer m satisfies one of the congruences $m \equiv k \pmod{8}$ for $k = 0, 1, 2, 3, 4, 5, 6$, or 7. By Exercise B 4 above, then, $m^2 \equiv k^2 \pmod{8}$. If $k \equiv 0, 4$, then $k^2 \equiv 0 \pmod{8}$. (For instance, if $k \equiv 4 \pmod{8}$, then $k = 8\ell + 4$ for some integer ℓ. But then

   $$k^2 = 64\ell^2 + 64\ell + 16 = 8(8\ell^2 + 8\ell + 2) \equiv 0 \pmod{8}.0$$

   Similarly, if $k \equiv 1, 3, 5, 7$, then $k^2 \equiv 1 \pmod{8}$. Finally, if $k \equiv 2, 6$, then $k^2 \equiv 4 \pmod{8}$.