SOME ADDITIONAL ILLUSTRATIONS ON CONGRUENCES

To reduce large numbers (mod n, for a given n) the following result is very useful. Recall that \(a \equiv b \text{ (mod n)}\) is read “a congruent to b modulo n” or “a congruent to b mod n” And is equivalent to “n divides \(b-a\)” and also equivalent to \(a \text{ (mod n)} = b \text{ (mod n)}\)

**Theorem.** If \(a \equiv b \text{ (mod n)}\) and \(c \equiv d \text{ (mod n)}\) then

1) \(a+c \equiv b+d \text{ (mod n)}\)
2) \(a-c \equiv b-d \text{ (mod n)}\)
3) \(a \cdot c \equiv b \cdot d \text{ (mod n)}\)
4) \(a^k \equiv b^k \text{ (mod n)}\) for any \(k > 0\).

**Proof:** each statement is of the form “if A then B”

1) By hypothesis, \(a-b = n \cdot t\) for some integer \(t\). Also, \(c-d = n \cdot k\) for some integer \(k\). (Note: I cannot use the same letter \(t\).) To prove that \(a+c \equiv b+d \text{ (mod n)}\) we need to show (see definition) that \(n\) divides \((a+c)-(b+d)\), that is, that \((a+c)-(b+d)\) is a multiple of \(n\). But \((a+c)-(b+d) = a+c-b-d = a-b+c-d = n \cdot t + n \cdot k = n(t+k) = n \cdot z\) with \(z\) an integer. Hence \(a+c \equiv b+d \text{ (mod n)}\).

2) Similarly.

3) This requires some non-straightforward step. We need to show that \(n\) divides \(a \cdot c - b \cdot d\). Write \(a \cdot c - b \cdot d = a(c-d)+b \cdot d = a(c-d) + a \cdot d - b \cdot d = a(c-d) + d \cdot (a-b) = a(nk) + d(n \cdot t) = n(ak + dt) = n \cdot w\), with \(w\) an integer. So \(n\) divides \(a \cdot c - b \cdot d\), that is, \(a \cdot c \equiv b \cdot d \text{ (mod n)}\).

4) Just apply 3) to \(a \equiv b \text{ (mod n)}\) and \(a \equiv b \text{ (mod n)}\) several times.

The proof has been completed.

**Remark.** This theorem says that except for “division” we can operate algebraically with \(\equiv\) in a manner totally similar to =

**Warning:** As to dividing a congruence (both sides) by a number, things break down. For instance it is clear that \(6 \equiv 2 \text{ (mod 4)}\) but if we try to “divide by 2 both sides” we would get \(3 \equiv 1 \text{ (mod 4)}\) which is false. The reason is that to “divide by 2” means to multiply by the inverse of 2. However, we know that 2 is not invertible in \(Z_4\). (See your class notes)

**APPLICATIONS**

For simplicity, to avoid dragging the \(n\) along, in each case \(\equiv\) will indicate \(\equiv \text{ (mod n)}\) for the corresponding \(n\). Recall that the answer **must be a number in the set \(\{0,1,2, ..., n-1\}\)**

1) Reduce \(8^{243} \text{ mod 9}\).
   **Solution:** \(8 \equiv -1\) so \(8^{243} \equiv (-1)^{243} \equiv -1 \equiv 8\)

2) Reduce \(75^{86} \text{ mod 4}\)
Solution: \(75 \equiv 3 \equiv -1\) so \(75^{86} \equiv (-1)^{86} \equiv 1\) (mod 4)

3) Reduce \(75^{32} \mod 7\)

Solution: \(75 \equiv 5\) so \(75^{32} \equiv 5^{32} \equiv (5^2)^{16} \equiv (25)^{16} \equiv (4)^{16} \equiv (2)^{8} \equiv (2)^2 \equiv 4\) (mod 7)

4) Reduce \((5^{17})^{23} \mod 6\)

Solution: Since 2 and 3 divide 708, they both appear in the factorization of 708 into a product of primes. Therefore, 6 divides 708. Hence, \(708 \equiv 0\) and thus \((5^{17})^{23} \equiv 0\) (mod 6)

Notice that in class we proved the following statement by induction. Now, we will produce a totally different proof.

5) Prove that for every natural number \(n\), 7 divides \(8^n - 1\).

Proof: We must see that \(8^n - 1 \equiv 0\) (mod 7). It is very simple: in fact, \(8 \equiv 1\) (mod 7) so \(8^n \equiv 1^n \equiv 1\). We are done.

Next we will see some computations involving the use of Fermat’s Little Theorem, which states: if \(p\) is prime then \(a^p \equiv a\) (mod \(p\)).

Suppose we want to reduce \(8^{20} \mod 20\). (Observe that the exponent coincides with \(n\)) We proceed as before: \(8^{20} \equiv 64^{10} \equiv 4^{10} \equiv 16^5 \equiv 16 \cdot 16^2 \equiv 16^3 \equiv 16^5 \equiv 16 \cdot 16^2 \equiv 16\). So after all these calculations, we have that \(8^{20} \equiv 16\) (mod 20).

Conclusion: we needed these computations because 20 is not a prime number! When dealing with congruences mod \(p\), with \(p\) prime, we must use Fermat’s Little Theorem to simplify the procedure considerably. (Make sure you know how to work with exponents before proceeding!)

Examples: \(3^5 \equiv 3\) (mod 5) and \(10^7 \equiv 10\) (mod 7) \(\equiv 3\) (mod 7) (No further calculations necessary)

6) Reduce \(213^{271} \mod 5\)

Solution: since 5 is a prime number we use Fermat’s result. We must accommodate the exponent to produce multiples of 5 (look again at Fermat’s statement!) To begin with, \(213 \equiv 3\) (mod 5) and so we need to reduce \(3^{271}\) (mod 5)
By the Integer Division Algorithm, $271 = (5)(54) + 1$. Thus, $3^{271} \equiv 3^{(5)(54)+1} \equiv 3^{54} \equiv (3^5)^{11} \equiv (by\ Fermat) \equiv 3^{11} \equiv 3 \cdot 3^5 \cdot 3^5 = (by\ Fermat) \equiv 3 \cdot 3 \cdot 3 \equiv 27 \equiv 2 (mod \ 5)$

Likewise, it can be shown that $39^{268} \ (mod \ 17) = 4 \ (Exercise)$

Let us illustrate how to solve some congruences and systems of congruences next. “To solve” means to find all the integer solutions. In general, for a and n fixed, the set of all the integer solutions of $x \equiv c \ (mod \ n)$ is $\{c + nt, (t \ integer)\}$.

a) Find all the integer solutions to $x \equiv 3 (mod \ 4)$

Solution: 4 must divide $x - 3$, for an integer. Therefore, $x = 3 + 4t$, with t an arbitrary integer (called a parameter), gives all the integer solutions. If you wish to exhibit some of them, just give the parameter t some values. So we have, 3, 7, 11, -1, 31, are some of the solutions. Solutions in the interval $11 < x < 24$? Only 15, 19, 23

Recall that a is invertible in $Z_n$ if and only if gcd (a, n) = 1.

b) Find all the integer solutions to $3x \equiv 12 \ (mod \ 14)$

Solution: since 3 is invertible mod 14 we multiply both sides of the equation by the inverse of 3. Since $3 \otimes 5 = 1$ in $Z_{14}$ the inverse of 3 is 5. Then, we obtain $x \equiv 60 \ (mod \ 14) \equiv 4 \ (mod \ 14)$. Therefore we must solve (as in a) $x \equiv 4 \ (mod \ 14)$. The solutions are $x = 4 + 14t$ with t an integer.

Conclusion: whenever we deal with $ax \equiv b \ (mod \ n)$, if a is invertible (mod n) we multiply both sides of the equation by the inverse of a and the equation reduces to one of the form $x \equiv c \ (mod \ n)$; thus the solutions are $c + nt$, with t arbitrary integer. Of course, if gcd(a, n) ≠ 1 we can not do this. Moreover, in this case there may or may not be any solution. For instance, $2x \equiv 1 \ (mod \ 6)$ has no solution, but $2x \equiv 0 \ (mod \ 6)$ has infinitely many: all the multiples of 3.

c) Find all the integer solutions of $3x - 5 \equiv 6x + 11 \ (mod \ 14)$

Solution: we have, equivalently, $3x \equiv -16 \ (mod \ 14) \equiv -2 \ (mod \ 14) \equiv 12 \ (mod \ 14)$. Thus $3x \equiv 12 \ (mod \ 14)$. By b) above, we know that $x = 4 + 14t$ with t an integer gives all the integer solutions.

When solving a system of two congruences, both of the type $x \equiv c \ (mod \ n)$, we use the Chinese Remainder Theorem: the system $x \equiv a \ (mod \ n)$ and $x \equiv b \ (mod \ m)$ where gcd(m, n) = 1 has

a) only one solution $x_0$ in $\{0, 1, 2, \ldots, mn - 1\} = Z_{mn}$, and
b) all the integer solutions are given by \( x_0 + (m n) t \), with \( t \) an arbitrary integer.

An illustration: suppose there are a certain number \( x \) of persons in one room, and we know \( 250 < x < 300 \). Moreover, when asked to leave the room in groups of 7, two persons remain, and when they leave the room in groups of 10, six persons remain. How many people were in the room?

**Solution:** we translate the information into congruences, obtaining the following system,

\[
\begin{align*}
\text{Equation 1:} & \quad x \equiv 2 \pmod{7} \\
\text{Equation 2:} & \quad x \equiv 6 \pmod{10}
\end{align*}
\]

Here \( n=7, m=10 \) and \( \gcd(10,7) = 1 \). The Chinese Remainder Theorem tells us that there is only one solution \( x_0 \) in \( \{0,1,2,\ldots,69\} \) and once we find \( x_0 \) we obtain all the solutions by simply writing \( x_0 + 70t \).

From the first equation, we have \( x = 2 + 7t \) (\( t \) an integer). (*)

Plug this into the second equation, to have \( 2 + 7t \equiv 6 \pmod{10} \), so \( 7t \equiv 4 \pmod{10} \). Since 7 is invertible \( \pmod{10} \) with inverse 3 (because \( 3 \otimes 7 = 1 \) in \( Z_{10} \)), we multiply by 3 both sides, and get \( t \equiv 12 \pmod{10} \equiv 2 \pmod{10} \). Thus, \( t \equiv 2 \pmod{10} \). This implies that \( t = 2 + 10k \), \( k \) an arbitrary integer. We have solved for \( t \), so go back to (*) and replace, obtaining \( x = 2 + 7(2 + 10k) = 16 + 70k \), \( k \) an arbitrary integer. These are all the solutions to our system. Finally, for \( k = 4 \) we have the only solution (296) that satisfies \( 250 < x < 300 \). Thus, the answer: there were 296 persons in the room.

Observe how the Chinese Remainder Theorem has been illustrated: here, \( x_0 = 16 \) (only solution between 0 and 69) and \( mn=70 \).

Problem: A bus route follows a 21-mile loop through N.Y.City, where the top speed allowed is 40 m/h. A driver leaving his shift on a Friday observes that the last two digits of the odometer are 29. He returns two days later and observes that the last two digits of the odometer are 49. Find the number of loops that the bus has completed during the two days he was off.

**Solution:** call \( x \) the number of loops. Thus the bus traveled \( 21x \) miles. We know *(read the statement again, please!)* that \( 21x \equiv 20 \pmod{100} \). Since 21 is invertible mod 100, we apply the Euclidean Algorithm and find that its inverse is 81, so we multiply by 81 both sides, obtaining \( x \equiv (81)(20) \pmod{100} \equiv 1620 \pmod{100} \equiv 20 \pmod{100} \). All the integer solutions are \( 20 + 100t \), \( t \) an arbitrary integer. The number of loops (\( x \)) must be positive, clearly. So \( x \in \{20,120,220,320,\ldots\} \) Since 120 loops of 21 miles each amounts to 2520 miles (in 48 hours it means an average speed of over 50 m/h, which is not the case) the only feasible solution is **20 loops**.
Congruences are sometimes disguised as linear equations. Consider for instance the equation \(2x+3y=5\); we are interested in finding all the integer solutions \((x, y)\) that satisfy it. Observe that since \(\gcd(3, 2) = 1\) any multiple of 1 (in this case 5) can be written in the form \(2x+3y\). In other words we know there will be infinitely many solutions to our problem. To find them, reduce the equation mod 3 first, obtaining \(2x \equiv 5 \pmod{3} \equiv 2 \pmod{3}\).

We must thus solve \(2x \equiv 2 \pmod{3}\), something we know how to do. In fact, since 2 is invertible mod 3 (and its inverse is 2) we get \(x \equiv 1 \pmod{3}\), that is, \(x = 1 + 3t\), \(t\) an arbitrary integer.

Our original equation becomes now \(2(1+3t) + 3y = 5\), that is, \(2 + 6t + 3y = 5\), and so, \(6t + 3y = 3\). Equivalently, \(2t + y = 1\). Therefore, \(y = 1 - 2t\).

We have all the solutions: \(x = 1 + 3t\) \quad \(y = 1 - 2t\) \quad \text{\(t\) an arbitrary integer. By giving values to the parameter \(t\) we produce solutions to the equation. For instance, \((x, y) = (1, 1)\). Or \((x, y) = (-2, 3)\) (we took \(t = -1\)), etc.}

**Exercise:** solve a) \(3x + 7y = 2\), \(b) 17x + 8y = -4\)