COMS10003 Workshop Sheet 8 - outline solutions.

Julian Gough 2014-11-20

1. Use the Euclid algorithm to find x and y, integers, so that $9 = 945x + 2421y$. **Solution:** So the idea is that first of all you use Euclid to show $(2431, 945) = 9$ and then go back up through the calculation to find x and y. So in one big glob the Euclid part is

$$\begin{aligned} 2421 &= 2 \cdot 945 + 531 \\ 945 &= 531 + 414 \\ 531 &= 414 + 117 \\ 414 &= 3 \cdot 117 + 63 \\ 117 &= 63 + 54 \\ 63 &= 54 + 9 \end{aligned} \tag{1}$$

   and $9|54$ so $(2421, 945) = 9$. Working backwards $9 = 63 - 54$ and so

$$\begin{aligned} 9 &= 63 - (117 - 63) = -117 + 2 \cdot 63 = -117 + 2 \cdot (414 - 3 \cdot 117) = -7 \cdot 117 + 2 \cdot 414 \\ &= 2 \cdot 414 - 7 \cdot (531 - 414) = 9 \cdot 414 - 7 \cdot 531 \\ &= -7 \cdot 531 + 9 \cdot (945 - 531) = -16 \cdot 531 + 9 \cdot 945 \\ &= 9 \cdot 945 - 16 \cdot (2421 - 2 \cdot 945) = 41 \cdot 945 - 16 \cdot 2421 \end{aligned} \tag{2}$$

   and you can check that's true.

2. Prove that congruence is an equivalence relation. That is show

   (a) Reflexivity: $x \equiv x \pmod{m}$.

   (b) Symmetry: if $x \equiv y \pmod{m}$ then $y \equiv x \pmod{m}$.

   (c) Transitivity: if $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$.

   Solution: So $m|0$ hence $m|x-x$, if $m|x-y$ then clearly $m|y-x$, that is, if $x-y = km$ then $y - x = -km$. Finally if $x - y = xm$ for some x and $y - z = ym$ for some y then $x - z = x - y + (y - z) = xm + ym = (x + y)m$.

3. Consider the set of all well-defined functions $f(x)$ where x is a real number. Now define $f(x) \sim g(x)$ if $f(0) = g(0)$. Prove this is an equivalence relation. **Solution:** So $f(0) = f(0)$ so $f(x) \sim f(x)$, if $f(0) = g(0)$ then $g(0) = f(0)$ so $f(x) \sim g(x)$ implies $g(x) \sim f(x)$ and if $f(0) = g(0)$ and $g(0) = h(0)$ then $f(0) = h(0)$ and so $f(x) \sim g(x)$ and $g(x) \sim h(x)$ implies $f(x) \sim h(x)$ and the property follows.

4. Prove the individual properties of congruences. If a, b, c, d are integers and m a positive integer then

(a) $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{m}$.

(b) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$.

(c) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.

(d) $a \equiv b \pmod{m}$ implies $a^k \equiv b^k \pmod{m}$ for positive integers k.

(e) $a \equiv b \pmod{m}$ and $d|m$ for some d a positive integer then $a \equiv b \pmod{d}$.

(f) $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m/(c,m)}$.

Solution: So if $a \equiv b \pmod{m}$ then $a - b = km$ for some k, multiply both sides by c and we get $ac - bc = kcm$ so $ac \equiv bc \pmod{m}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a - b = xm$ and $c - d = ym$ for some x and y; hence $(a + c) - (b + d) = (x + y)m$ and $a + c \equiv b + d \pmod{m}$ and since $c = d + ym$ and $a = b + xm$ we have $ac = bd + xmd + ymb + xym^2$ or $ac - bd = (xd + yb + xym)m$ so $ac \equiv bd \pmod{m}$. The next one follows by induction on the previous or by writing $a = b + xm$ and noticing

$$a^k = (b + xm)^k = b^k + \text{terms with } k\text{'s in them} \tag{3}$$

For the next one we have $a - b = km$ and $d|m$ means $d|(a - b)$ so $a \equiv b \pmod{d}$. Finally, let $(c, m) = d$, if $ac \equiv bc \pmod{m}$ then $ac - bc = km$. Now $d = (c, m)$ implies $c = c'd$ and $m = m'd$ where $(c', m') = 1$. Now $ac'd - bc'd = km'd$ or $ac' - bc' = km'$ and since $(m', c') = 1$ and m' divides the right hand side, it must divide $a - b$, hence $a \equiv b \pmod{m'}$.

5. Is -2 congruent to 31 modulo 11? **Solution:** keep adding 11 so

$$-2 \equiv 9 \equiv 20 \equiv 31 \pmod{11} \tag{4}$$

and there you go.

6. Is 77 congruent to 5 modulo 12? **Solution:** Well $77 = 6 \cdot 12 + 5$ so yes.

7. Find the inverse of 67 modulo 119 and the inverse of 119 modulo 67. **Solution:** Again with the Euclid:

$$\begin{aligned} 119 &= 67 + 52 \\ 67 &= 52 + 15 \\ 52 &= 3 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \end{aligned} \tag{5}$$

So

$$1 = 15 - 2 \cdot 7 = 15 - 2(52 - 3 \cdot 15) = 7 \cdot 15 - 2 \cdot 52 \tag{6}$$

and, deep breath,

$$1 = -2 \cdot 52 + 7(67 - 52) = -9 \cdot 52 + 7 \cdot 67 = 7 \cdot 67 - 9(119 - 67) \tag{7}$$

so $1 = 16 \cdot 67 - 9 \cdot 119$. Hence $67^{-1} \equiv 16 \pmod{119}$ and $119^{-1} \equiv -9 \equiv 58 \pmod{67}$ where we have used $67 - 9 = 58 \equiv -9 \pmod{67}$.

8. By looking at all the possibilities, show that 12 has no inverse modulo 18. **Solution:** Well this is boring

$$\begin{aligned} 2 \cdot 12 = 24 &\equiv 6 \\ 3 \cdot 12 = 36 &\equiv 0 \\ 4 \cdot 12 = 48 &\equiv 12 \\ 5 \cdot 12 = 60 &\equiv 6 \end{aligned} \tag{8}$$

and so on, all modulo 18.

9. Solve $11x \equiv 28 \pmod{37}$. **Solution:** So this is another Euclid algorithm because we need to invert eleven and multiply both sides by 11^{-1}. Now

$$\begin{aligned} 37 &= 3 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 3 + 1 \end{aligned} \tag{9}$$

and hence

$$1 = 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = -11 + 3 \cdot (37 - 3 \cdot 11) = -10 \cdot 11 + 3 \cdot 37 \tag{10}$$

so $11^{-1} \equiv -10 \equiv 27 \pmod{37}$. Now this means $x \equiv 27 \cdot 28 \pmod{37}$. This can be simplified,

$$27 \cdot 28 \equiv 54 \cdot 14 \equiv 17 \cdot 14 \equiv 16 \pmod{37} \tag{11}$$

10. Consider $(p-1)! = (p-1) \cdot (p-2) \ldots 1$ where p is an odd prime. Now modulo p only one and $p - 1 \equiv -1 \pmod{p}$ are their own inverse; every other element has a unique inverse different from itself. Now by pairing each element with its inverse show that $(p-1)! \equiv -1 \pmod{p}$. This is known as Wilson's Theorem. **Solution:** The hint basically solves it, every element has it an inverse except $p - 1$ and 1 and multiplying them gives -1.

    The next few problems are about cryptography, this is in preparation for next week when we will look at RSA. The cryptography schemes here are simpler and don't really rely on the number theory we have been doing.

11. The key idea behind cryptography is to keep messages secret. One of the most widely known cryptography techniques is called Caesar's cipher. The idea behind this is to shift all the letters a fixed amount down the alphabet. See if you can work out how this works and decipher these texts, each has a different shift.

    (a) Aqwtg iqppc pggf c dkiigt dqcv

    (b) Vlr hklt elt ql tefpqib, alkq vlr, Pqbsb? Vlr grpq mrq vlro ifmp qldbqebo xka yilt.

    (c) Rpyewpxpy, jzf nlye qtrse ty spcp. Estd td esp Hlc Czzx.

Solution: Youre gonna need a bigger boat - forward by two, You know how to whistle, dont you, Steve? You just put your lips together and blow - forward by 23 and Gentlemen, you cant fight in here. this is the War Room, forward by 11.

12. One problem with Caesar's cipher is that you can just try every shift until you find one that makes sense. There are ways to make this harder, but many schemes are vulnerable to frequency analysis, for example, for Caesar's cipher, if you have lots of text you can just guess the most common letter is coding 'e' and use that to calculate the shift and more complicated versions of this apply to more complicated ciphers. Vigenère's cipher is designed to combat this. In this cipher you do modular arithmetic on letters, so for simplicity ignore the space and punctuation and number the letters zero through to 25. Now, to add two letters add the corresponding numbers modulo 26. Hence a+b=b, b+b=c and c+c=e. Now to use Vigenère's cipher choose a code key, say 'casablanca' and to encode 'tomorrowisanotherday' you add c to t, a to o, s to m, a to o, b to r, l to r, a to o, n to w, c to i and a to s. At this points you have run out of letters in casablanca, so you start again, c to a, a to n and so on. Work out the Vigenère cipher of 'tomorrowisanotherday' using 'casablanca' and the cipher of 'bondjamesbond' using 'drno'. **Solution:** voeoscojkscngtiprqcy and ecarmozsvpbbg.

13. Decode 'ihczsfmkoyysexgpwkqwmumiwrvlqeqa' with the key 'maewest'. **Solution:** whydontyoucomeupsometimeandseeme