CONGRUENCES

As will be known, when we write $12 \equiv 7$ (modulo 5) we are expressing the fact that both 12 and 7 have the same remainder when divided by 5. Alternatively, the statement means that 12-7 is an exact multiple of 5. Indeed we can also write it as $12-7 \equiv 0 \pmod 5$. We also, of course, can write $12 \equiv 12 \pmod 5$, $12 \equiv 17 \pmod 5$ and $12 \equiv 2 \pmod 5$ and so on.

The real interest comes from the fact that if we let "a" stand for any number congruent to 12 modulo 5 and "b" represent any number congruent to 9 modulo 5 we find that (i) $a + b \equiv 21 = 12 + 9 \pmod 5$ (ii) $a - b \equiv 3 = 12-9 \pmod 5$ (iii) $a.b \equiv 108 = 12.9 \pmod 5$. We can of course prove this by showing that as $12 \equiv 5m + a$ and $9 = 5n + b$, $12 + 9 = 5(m + n) + a + b \equiv a + b \pmod 5$, $12 - 9 = 5(m - n) + a - b \equiv a - b \pmod 5$ and $12.9 = 5(mn + an + bm) + a.b \equiv a.b \pmod 5$. In other words, the operations of addition, subtraction and multiplication commute with the operation of "taking remainders"; it doesn't matter which we do first. So we can do three arithmetic processes using the congruence sign (modulo the same integer of course) instead of the equals sign.

Let us now cut out some alternatives by taking our "a"'s and "b"'s from only the numbers 0, 1, 2, 3, 4 or, more generally, where we are taking congruences modulo m we will allow only the values 0, 1, 2, ... , m-1 for "a" and "b". We will call these values "least residues"; should we want to revert to our earlier viewpoint and talk of any remainder, we will use the term residues. Thus 17, 7, 2 and 12 itself are all residues, modulo 5, but 2 is the least residue. We thus have a new sort of arithmetic using only the least residues

$0, 1, \dots, m-1$ with the knowledge that if we get the result $a \equiv b \pmod{m}$ then a actually equals b, is b; for we can never get $2 \equiv 7 \pmod{5}$ as a result of our calculations, as 7 is not a least residue. As will be known, we can draw up addition and multiplication tables, modulo 5, using only least residues.

Addition:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is comforting to note that (iv) $a + 0 \equiv a \pmod{5}$ (v) $a.0 \equiv 0 \pmod{5}$ and (vi) $a.1 \equiv a \pmod{5}$.

Because, in "ordinary" arithmetic we deduce from the statement $f + g = h$ that $f = h - g$, we can do the same for congruences, modulo m, and thus obtain from $3 + 4 \equiv 2 \pmod{5}$ that $3 \equiv 2 - 4 \pmod{5}$. Looking at the addition table, modulo 5, we see that no number appears more than once in any row or column; indeed, each least residue appears exactly once in each case. It follows that we always get exactly one solution for x in each of the equations (vii) $a + x \equiv c \pmod{5}$ (viii) $x + b \equiv c \pmod{5}$ (ix) $a + b \equiv x \pmod{5}$. Consequently the same statement will be true for the equations (xii) $a \equiv c - x \pmod 5$ (xiii) $x \equiv c - b \pmod 5$ (xiv) $a \equiv x - b \pmod 5$. Thus (xiii) guarantees that we may do subtraction of least residues, modulo 5, and always get a precise answer. I leave you to prove that all this will be true for any positive integer m instead of 5; you will need to show mainly, that each least residue appears exactly once in each row and column of the addition table.

You will notice that we had $2 - 4 \equiv 3 \pmod 5$; should we not have written $2 - 4 \equiv -2 \pmod 5$? Certainly -2 is a residue, but it is not a least residue, so that we choose 3 which is. It is, however, instructive to remember that a property of "ordinary" negative integers such as -8 is that $(-8) + (8) = 0$; it follows from this that $m - 1 \equiv -1 \pmod m$, $m - 2 \equiv -2 \pmod m$ and so on because $(m - a) + a \equiv 0 \pmod m$. For congruences, then, we have no need to invent negative integers to ensure that equations (vii) to (xiv) always have a solution. On the other hand, we do lose something we have in ordinary arithmetic, because there we could state that (xv) $a > b$ if and only if $a - b$ is positive (xvi) $a = b$ if and only if $a - b = 0$ (xvii) $a < b$ if and only if $a - b$ is negative. For congruences we can only use (xvi) because our least residues are both positive and negative; talking about least residues being greater or less than one another is meaningless.

We have yet to look at the fourth operation of arithmetic: division. Just as subtraction is invented from addition, or is the operation inverse to addition which restores the status quo, so is division invented from multiplication i.e. from $96 = 12.8$ we get $96 \div 12 = 8$ or $96 \div 8 = 12$. Seeking to apply this to congruences, modulo m, our first requirement must be, as in (vii), (viii) and (ix) with subtraction, that there shall always be one, but no more than one, solution to every equation (xviii) $a.x \equiv c \pmod{m}$ (xix) $x.b \equiv c \pmod{m}$ (xx) $a.b \equiv x \pmod{m}$.

Let us look at the multiplication table for congruences modulo 6.

Multiplication:

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Clearly this does not match up to our requirements: $2.1 \equiv 2 \pmod{6}$ and $2.4 \equiv 2 \pmod{6}$; yet we do get unique solutions for (xviii), (xix), (xx) when we work modulo 5, provided neither a nor b is zero in (xviii) and (xix) as can be verified from the multiplication table modulo 5. Why this difference? Why are there two or more solutions for $a.x \equiv b \pmod{m}$ for some values of m? Well, we know that $a.x \equiv b \pmod{m}$ if and only if $ax - b$ is divisible by m. Consider $a = 2$, $b = 2$, $m = 6$ again. We will have to find x so that $2(x - 1)$ is divisible by 6 in ordinary arithmetic. But this will be so if $x - 1$ is divisible by 3 and this certainly happens if $x = 1$, as $3 \times 0 = 0$, and also if $x = 4$ as $3 \times 1 = 3$. It is also true for an infinite number of other integers too, but remember that we want x to be a least residue, to have a value between 0 and 5. The "more than one solution" result, $x = 1$ or 4, arose because 2 was a factor of a, b and m. Now we can see that, whenever m has two factors each different from 1, this situation will arise for some a and b. Thus, $m = r.s$, $r \neq 1$, $s \neq 1$, $m \neq 0$, will always yield at least the two solutions $x = 1$, $x = s + 1$ as solutions to $rx \equiv r \pmod{m}$. The only times this sort of situation cannot arise is when m is a prime number p because we can then only have

$r = p$, $s = 1$ or vice versa. So (xviii), (xix), (xx) are uniquely solvable modulo a prime when $a \not\equiv 0 \pmod{p}$ in (xviii) and $b / 0 \pmod{p}$ in (xix). This means that $x \equiv c \div a \pmod{p}$ and $x \equiv c \div b \pmod{p}$ always have exactly one answer, from (xviii) and (xix). Incidentally, (xx) just shows that multiplication modulo <u>any</u> m always yields a precise answer.

We are now in the position where we know that the arithmetic of least residues, modulo a prime p, behaves just like our ordinary arithmetic of positive, negative and zero fractions (i.e. rational numbers); we can divide any one by any other except that we are forbidden to divide by zero. (Can you see why this is logically necessary?) Once we introduce division, our least residues are no longer like ordinary integers, because, for instance, you can't divide 3 by 2 and get an integer answer. One might be tempted to think that least residues modulo a non-prime number like 6 might behave like integers in ordinary arithmetic with respect to the four rules of arithmetic, but of course they don't, because in ordinary arithmetic we get one or no answer to the problem $c \div a = x$ whereas, modulo 6, we get two answers sometimes, and sometimes none.

If least residues, modulo a prime, behave like rational numbers, can we write them in the same way as rational numbers if we want? Let's look at ordinary arithmetic. $\frac{2}{3} = 2.3^{-1}$ where 3^{-1} is the solution to $1 \div 3 = x$. We might try the same definition for $\frac{2}{3}$ modulo 5. $\frac{2}{3} \equiv 2.3^{-1} \pmod{5}$ where 3^{-1} is the solution to $1 \div 3 = x \pmod{5}$. Of course, we don't mean "two-thirds" in the usual sense here, and of course $1 \div 3 \equiv 2 \pmod{5}$ so that we obtain $\frac{2}{3} \equiv 2.3^{-1} \equiv 2.2 \equiv 4 \pmod{5}$. Similarly, we get $\frac{1}{4} \equiv 4 \pmod{5}$, $\frac{3}{2} \equiv 4 \pmod{5}$ etc. It would be intriguing to see if we can add, subtract, multiply and divide our new "fractions" in the same way as ordinary fractions.

In ordinary arithmetic, $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ ($b \neq 0$, $d \neq 0$). Why? Because $\frac{a}{b} + \frac{c}{d} = a.b^{-1} + c.d^{-1} = ad.d^{-1}b^{-1} + c.bb^{-1}d^{-1} = (ad + bc)b^{-1}d^{-1}$. Clearly the same rule will hold for congruences. Thus: $\frac{2}{3} + \frac{3}{4} = 2.3^{-1} + 3.4^{-1} \equiv (2.4 + 3.3).4^{-1}.3^{-1} \equiv (3 + 4).(4.3)^{-1} \equiv 2.2^{-1} \equiv 2.3 \equiv 1 \pmod{5}$. (We could have left it as $\equiv \frac{2.4 + 3.3}{3.4}$.) Checking, we have $\frac{2}{3} \equiv 4 \pmod{5}$, $\frac{3}{4} \equiv 2 \pmod{5}$ and $4 + 2 \equiv 1 \pmod{5}$. Subtraction must work in the same way. For multiplication ordinary arithmetic goes $\frac{a}{b}.\frac{c}{d} = (a.b^{-1})(c.d^{-1}) = (a.c)(b.d)^{-1} = \frac{ac}{bd}$ while modulo 5 $\frac{2}{3}.\frac{1}{4} \equiv 2.3^{-1}.1.4^{-1} \equiv (2.1)(3.4)^{-1}$ $(\equiv \frac{2.1}{3.4})$ $\equiv 2.2^{-1} \equiv 2.3 \equiv 1 \pmod{5}$. A check yields $\frac{2}{3} \equiv 4 \pmod{5}$, $\frac{1}{4} \equiv 4 \pmod{5}$ and $4.4 \equiv 1 \pmod{5}$. Finally division in ordinary arithmetic, "invert and multiply", follows from $\frac{a}{b} \div \frac{c}{d} = (a.b^{-1})\ (c.d^{-1}) = (ab^{-1}).(cd^{-1})^{-1} = (a.b^{-1}).(c^{-1}d) = (ad)(b^{-1}c^{-1}) = \frac{ad}{bc}$. Modulo 5, $\frac{2}{3} \div \frac{3}{4} \equiv (2.3^{-1})(3.4^{-1}) \equiv (2.3^{-1}).(3.4^{-1})^{-1} \equiv (2.3^{-1})(3^{-1}.4) \equiv (2.4)(3^{-1}.3^{-1}) \equiv \frac{2.4}{3.3} \pmod{5}$ or $\equiv (2.4)(3.3)^{-1} \equiv (3)(4)^{-1} \equiv 3.4 \equiv 2 \pmod{5}$. Checking, $\frac{2}{3} \equiv 4 \pmod{5}$, $\frac{3}{4} \equiv 2 \pmod{5}$, $4 \div 2 \equiv 4.2^{-1} \equiv 4.3 \equiv 2 \pmod{5}$. Can you prove that we could rightly have said $4 \div 2 \equiv 2 \pmod{5}$ "by ordinary arithmetic"? Finally, can you prove that the cancellation law holds for our "fractions" modulo 5 just as it does with ordinary fractions?

Follow-up problems:

N.B.: p always represents a prime number; all letters that appear represent least residues.

1. Prove that the formula $x \equiv \frac{-b\pm\sqrt{b^2-4ac}}{2a} \pmod{p}$ will give the solutions to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$, where such solutions exist.

2. Show that the solutions of $3x^2 + 2x + 4 \equiv 0 \pmod{5}$ are also solutions of $x^2 + 4x + 3 \equiv 0 \pmod{5}$.

3. Show that the solutions of $ax^2 + bx + c \equiv 0 \pmod{p}$ must also satisfy a congruence of the form $x^2 + dx + e \equiv 0 \pmod{p}$.

4. (Hard) How many least residues, modulo p, are perfect squares modulo p? (Try it out with $p = 5$, $p = 7$ first.)

5. For which prime numbers less than 14 does the congruence $x^2 \equiv -1 \pmod{p}$ have a solution? Can you suggest a general rule for all prime numbers and not just those less than 14?

M. Greening.

THE QUARTZ TRACK

A man runs n times around a circular track of radius s miles and drinks t pints of some liquid (which will remain nameless) every miles. He only drinks one quart. Explain. (Hint: It is not because he gets giddy or drunk.) Answer page 36.