Canada/USA Mathcamp
Background for the 2014 Qualifying Quiz

Number of paths through a grid (Problem #6)

As stated in Problem #6, the number of monotonic paths from the bottom left to the top right corner of an $m \times n$ grid is

$$\binom{m+n}{m}, \text{ which is the same as } \binom{m+n}{n}.$$

If you are unfamiliar with this notation, $\binom{r}{k}$ is the number of ways of choosing k different objects out of a set of r objects. Sometimes, instead of $\binom{r}{k}$, people write $C(r,k)$ or ${}_rC_k$; these are all just different notations for the same thing. For instance, there are 6 ways of choosing 2 letters from the word MATH (assuming the order does not matter): MA, MT, MH, AT, AH, and TH. Thus $\binom{4}{2} = 6$.

The general formula for $\binom{r}{k}$ is

$$\binom{r}{k} = \frac{r!}{k!(r-k)!}.$$

If you are unfamiliar with this formula, there are many places on the Web where you can learn about it. One good place to start is *The Art of Problem Solving* (www.artofproblemsolving.com). Go to their "Videos" section, look for the collection of videos on "Counting and Probability", and watch the videos for Sections 4.2 - 4.3. If you've already seen the concept and formula for $\binom{r}{k}$, but don't understand what this has to do with counting monotonic paths on a grid, watch the video for Section 5.2.

Basic number theory

Congruence modulo n

Let n be a positive integer. We say that two integers a and b are *congruent modulo n* if a and b differ by some multiple of n. We write this as $a \equiv b \pmod{n}$. Thus, for instance:

- $3 \equiv 8 \equiv -2 \pmod{5}$
- All even integers are congruent to 0 modulo 2; all odd integers are congruent to 1 modulo 2.

All the integers that are congruent to each other modulo n are said to be in the same *congruence class modulo n*; clearly, all of them have the same remainder when you divide them by n. Since the possible remainders after division by n are $0, 1, \ldots, n-1$, we can split all the integers into exactly n different congruence classes modulo n. For example, the five congruence classes modulo 5 are:

- Integers congruent to 0 modulo 5: $\{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$
- Integers congruent to 1 modulo 5: $\{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$
- Integers congruent to 2 modulo 5: $\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$
- Integers congruent to 3 modulo 5: $\{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$
- Integers congruent to 4 modulo 5: $\{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

If a is any integer, we denote the congruence class of a modulo n by $[a]_n$. Note that if b is another integer in the same congruence class, then $[a]_n = [b]_n$. For instance, $[2014]_2$ is the same as $[0]_2$ and $[2]_2$ and $[-1000]_2$: these are all different ways of referring to the same congruence class modulo 2 (the set of all even integers). Similarly,

$$[2014]_5 = [4]_5 = [-1]_5 = \{\ldots, -11, -6, -1, 4, 9, 14, \ldots\}.$$

Modular Arithmetic

In arithmetic modulo n (also known as *modular arithmetic*), we are interested not in the integers themselves, but in their congruence classes modulo n. For instance, in arithmetic modulo 2, we only care if an integer is even or odd; we are interested in facts like “the sum of two odd integers is always even” or “the product of two odd integers is always odd”. In arithmetic modulo 10, we are care only about the last digit of a number in base 10; we are interested in facts like “if you multiply a number that ends in 3 by a number that ends in 4, the last digit of the result will always be 2.”

The following general theorem is easy to prove, but very important. It says that when you are working modulo n, you can replace any integer in your calculations by any other integer in the same congruence class, and the final answer will be the same.

Theorem 1: If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $a + b \equiv c + d \pmod{n}$ and $ab \equiv cd \pmod{n}$.

Proof: Since $a \equiv c \pmod{n}$, we know that a and c differ by some multiple of n. In other words, there exists an integer r such that $a = c + rn$. Similarly, there exists an integer s such that $b = d + sn$. Then

$$\begin{aligned} a + b &= (c + rn) + (d + sn) = c + d + (r + s)n \\ ab &= (c + rn)(d + sn) = cd + csn + drn + rsn^2 = cd + (cs + dr + rsn)n \end{aligned}$$

Thus $a + b$ and $c + d$ differ from each other by a multiple of n, so $a + b \equiv c + d \pmod{n}$; similarly, $ab \equiv cd \pmod{n}$. QED.

Theorem 1 allows us to think of modular arithmetic in a subtly different way. Originally, when we said, e.g., “$3 \times 5 \equiv 1 \pmod{7}$”, we simply meant: “The integer 3×5 (i.e. 15) and the integer 1 are congruent modulo 7 (i.e. they differ by a multiple of 7).” But now that we have Theorem 1, the statement “$3 \times 5 \equiv 1 \pmod{7}$” becomes a much stronger assertion. It says: “Any integer from the congruence class of 3 times any integer from the congruence class of 5 gives you an integer from the congruence class of 1 modulo 7”.

Example 1: What is the remainder of 7^{1000} when divided by 8?

Solution: This is the same as asking: “What is the congruence class of 7^{1000} modulo 8?” By the theorem, since $7 \equiv -1 \pmod{8}$, we can immediately conclude that $7^{1000} \equiv (-1)^{1000} \pmod{8}$. But $(-1)^{1000}$ is just 1. Thus the answer is 1.

Example 2: Show that an even number that is not divisible by 4 cannot be a perfect square.

Solution: If k is an even number that is not divisible by 4, then $k \equiv 2 \pmod{4}$. Thus we simply need to show that the equation $x^2 \equiv 2 \pmod{4}$ has no solutions. Since there are only four congruence classes modulo 4, Theorem 1 tells us that we only need to check four cases: $x = 0$, $x = 1$, $x = 2$, and $x = 3$. (Make sure you understand why the theorem implies this.) Since

$$0^2 \equiv 2^2 \equiv 0 \pmod{4} \text{ and } 1^2 \equiv 3^2 \equiv 1 \pmod{4},$$

we conclude that $x^2 \equiv 2 \pmod{4}$ has no solutions.

Division modulo n, Part I

So far, modular arithmetic as we’ve described it is just a convenient notational tool for solving problems in regular arithmetic. Both of our example problems were about integers, and we could have solved them without using the word “modulo”, just by working with remainders.

But once you spend some time working modulo n, you get the sense that you’re actually dealing with a new kind of arithmetic. For instance, if you’re working modulo 5, you start feeling that you’re in a world in which there are only 5 numbers (0,1,2,3 and 4), and these numbers have funny properties, like $4 + 2 = 1$ and $2 = -3$ and $2 \times 3 = 1$. You are tempted to say things like, “Well, if 2×3 is 1, then shouldn’t 1/3 be 2?” And then you get confused, because it is certainly not the case that $1/3 \equiv 2 \pmod{5}$: congruence mod 5 isn’t even defined for fractions like 1/3, and anyway, the rational numbers 2 and 1/3 don’t differ by a multiple of 5.

The way out of the confusion is to realize that what we really want to add and multiply are not *integers* but *congruence classes of integers modulo n*. So let’s go ahead and define addition and multiplication of congruence classes in the natural way:

$$[a]_n + [b]_n = [a+b]_n \text{ and } [a]_n[b]_n = [ab]_n.$$

Notice that for this definition to make any sense, we need Theorem 1. If one congruence class contains a and c and another class contains b and d, then the sum and product of these two classes shouldn't depend on whether we call the first one $[a]_n$ or $[c]_n$ and the second one $[b]_n$ or $[d]_n$. In other words, if $[a]_n = [c]_n$ and $[b]_n = [d]_n$, we need to be sure that $[a+b]_n = [c+d]_n$ and $[ab]_n = [cd]_n$. This is exactly what Theorem 1 guarantees.

Now that we know what we mean by addition and multiplication of congruence classes mod n, we need to check a few routine things to make sure that our new $+$ and $\times$ work the way we expect them to. They are, after all, brand new operations, which we've just made up from scratch! So to justify calling them $+$and $\times$, we need to check that they satisfy all the usual properties like commutativity, associativity, and distributivity; that $[0]_n$ is an additive identity (adding it to any congruence class doesn't change the congruence class); that $[1]_n$ is a multiplicative identity; etc. We're not going to check all of that here; you can do it yourself (it's pretty straightforward) or you can just take it on faith that everything works out right.

Now, finally, we can write things like $[2]_5 + [4]_5 = [1]_5$ and $[2]_5 \times [3]_5 = [1]_5$. And now it makes perfect sense to write $[1]_5/[3]_5 = [2]_5$. We just have to remember that what we mean is division of congruence classes, not numbers; it is the inverse operation to multiplication of congruence classes.

If you found all of this abstraction a bit confusing, don't worry too much. (You'll definitely understand it all after you go to Mathcamp.) The point is simply that you *are* allowed to divide 1 by 3 modulo 5, though you have to change you theoretical framework in order to justify this rigorously.

In fact, it turns out that x/y is defined for any two congruence classes x and y modulo 5, unless $y = [0]_5$. (Division by zero is still not allowed.) To see this, let's write down the multiplication table for congruence classes modulo 5. (For better legibility, we have omitted the subscript "5" from the table; we'll do this from now on when the context is clear.)

×	[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]

Note that every non-zero row and column contains each congruence class modulo 5 exactly once. Thus, for any two congruence classes x and y with $y \neq [0]_5$, we can simply look for the entry x in the y column. If this entry is in row z then $x = yz$, i.e. $z = x/y$.

On the other hand, consider the multiplication table modulo 8:

×	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Note that there is no congruence class which, when multiplied by [2], gives [1] (or [3] or [5] or [7]). On the other hand, there are multiple classes which, when multiplied by 2, give [0] (or [2] or [4] or [6]). Thus, however you try, division by [2] is not defined. The same problem exists with division by [4] and [6]. On the other hand, the table shows that division by [3], [5], and [7] works fine.

It's not hard to guess the general pattern: working modulo n, you can divide by $[c]_n$ if and only if c is relatively prime to n, i.e. $\text{GCD}(c, n) = 1$. Before we can prove this, we first need a very important result about the GCD (greatest common divisor) of two integers, which at first glance seems completely unrelated to modular arithmetic.

An important property of the GCD

Theorem 2. Let m and n be any two integers. Then $\mathrm{GCD}(m, n)$ is the smallest positive integer that can be written as $am + bn$ for some integers a and b.

Example. The GCD of 6 and 10 is 2. The t states that 2 can be written as $10a + 6b$ for some integers a and b; indeed, $2 = 10 * 2 - 6 * 3$. Moreover, the theorem states that 2 is the smallest positive integer that can be written in this form; indeed, it obviously won't work for 1, since $10a + 6b$ will always be even, whereas 1 is odd.

Proof. Given integers m and n, consider the set of all integers of the form $am + bn$. Choose the smallest positive integer in this set, say $g = cm + dn$.

To prove that $g = \mathrm{GCD}(m, n)$, we need to show two things:

(i) That m is divisible by g (written $g|m$) and similarly that $g|n$ (i.e., g is a common divisor of m and n); and:

(ii) If $d|m$ and $d|n$ then $d|g$ (i.e. any other common divisor of m and n is smaller than g).

To show that $g|m$, let's try dividing m by g, possibly with a remainder. We obtain $m = qg + r$, where q is the quotient and r is the remainder, with $0 \leq r < g$. Our goal is to show that $r = 0$. Let's rewrite r as

$$r = m - qg = m - q(cm + dn) = (1 - qc)m - (qd)n.$$

We assumed that g was the smallest positive integer of the form $am + bn$, yet we now see that r is also of this form, and $r < g$. Thus we are forced to conclude that $r = 0$, so $g|m$. By exactly the same argument, $g|n$, so (i) is proved. To show (ii), suppose that $d|m$ and $d|n$. Then clearly $d|cm + dn$, so $d|g$. QED

Division modulo n, Part II

Theorem 2 is a very powerful result in its own right. (In fact, it's relevant for one of the Qualifying Quiz problems this year.) Let us now use it to prove our conjecture about division modulo n:

Theorem 3. Working modulo n, you can divide any congruence class $[a]_n$ by $[c]_n$ if and only if $\mathrm{GCD}(c, n) = 1$.

Note that to prove an "if and only" statement, we need to prove both directions of implication:

($\Rightarrow$) If you can divide any congruence class modulo n by $[c]_n$ then $\mathrm{GCD}(c, n) = 1$.

($\Leftarrow$) If $\mathrm{GCD}(c, n) = 1$, then you can divide any congruence class modulo n by $[c]_n$.

Proof.

($\Rightarrow$) If you can divide any congruence class by $[c]_n$, then, in particular, you can divide $[1]_n$ by $[c]_n$. Thus there exists an integer b such that $bc \equiv 1 \pmod{n}$. By the definition of congruence modulo n, this means that there exists an integer a such that $bc + an = 1$. By Theorem 2, this means that $\mathrm{GCD}(c, n) = 1$.

($\Leftarrow$) Suppose $\mathrm{GCD}(c, n) = 1$. Then, by Theorem 2, there exist integers a and b such that $bc + an = 1$. Then $bc \equiv 1 \pmod{n}$, so $[b]_n[c]_n = [1]_n$.

This is not quite enough to say that $[1]_n/[c]_n = [b]_n$; we also need to show that $[b]_n$ is the *only* congruence class satisfying $[b]_n[c]_n = [1]_n$. So suppose $[b']_n$ is another class such that $[b']_n[c]_n = [1]_n$. Then

$$[b]_n[c]_n - [b']_n[c]_n = [b - b']_n[c]_n = [0]_n,$$

which means that $(b - b')c$ is divisible by n. But since c and n are relatively prime, we conclude that $b - b'$ is itself divisible by n, i.e. $b \equiv b' \pmod{n}$ and $[b]_n = [b']_n$. This proves the uniqueness of $[b]_n$, so $[1]_n/[c]_n = [b]_n$.

Finally, if we want to divide any other congruence class $[a]_n$ by $[c]_n$, we note that

$$[ab]_n[c]_n = [a]_n[b]_n[c]_n = [a]_n \cdot [1]_n = [a]_n,$$

Uniqueness is proved exactly as above, so $[a]_n/[c]_n = [ab]_n$. Thus any congruence class $[a]_n$ can be divided by $[c]_n$. QED.

Corollary.[1] If q is prime, then we can divide by any congruence class modulo q except $[0]_q$. In other words, for any two integers a and c with c not divisible by q, the equation $cx \equiv a \pmod{q}$ has a unique solution modulo q.

[1] A corollary is what mathematicians call an easy consequence of a previously proved theorem.