Modular Arithmetic

Kieran Cooney - kieran.cooney@hotmail.com

February 18, 2016

Sums and products in modular arithmetic

Almost all of elementary number theory follows from one very basic theorem:

Theorem. *Division Theorem*
Given the integers m and n with $n > 0$, then there exist unique integers k and r such that

$$m = nk + r$$

with $0 \leq r < n$.

This theorem simply states that we can divide the number m by n. It is sometimes said that n divides into m k times with *remainder* r. k is called the *quotient* of m with respect to n. As an example, take m and n to be 107 and 13 respectively. This is equivalent to dividing 107 by 13 so that $107 = 8 * 13 + 4$, with k and r equalling 8 and 4 respectively. If $r = 0$, then $m = nk$ and we say that n divides m, which we write as $n|m$.

Suppose that we want to divide two seperate numbers by n, say m_1 and m_2. Then $m_1 = k_1 n + r_1$ and $m_2 = k_2 n + r_2$. The sum of both of these equations is

$$m_1 + m_2 = k_1 n + r_1 + k_2 n + r_2 = (k_1 + k_2)n + r_1 + r_2$$

Notice that this equation is in exactly the same form as the divison theorem, with a quotient $k_1 + k_2$ and remainder $r_1 + r_2$. Thus, we might be tempted to suggest that with respect to a given divisor, the quotient and remainder of the sum of two numbers is just the sum of the quotients and remainders of those same two numbers. However in the definition we have presented, this is not quite true; it is quite possible that $r_1 + r_2 > n$. For example, suppose we wish to divide both 17 and 35 by 9. Then $16 = 1 * 9 + 7$, $35 = 3 * 9 + 8$ and $35 + 16 = 4 * 9 + 17$. But if I divide $35 + 16 = 51$ by 9, I get $51 = 5 * 9 + 6$.

To ammend for this, we introduce *modular arithmetic*.

Definition. Modular Equivalence
Two integers m_1 and m_2 are said to be *congruent modulo* n if their difference is divisible by n. This is written as

$$m_1 \equiv m_2 (mod\, n) \Rightarrow n | (m_1 - m_2)$$

Example. The following examples briefly illustrate this notation.

1. If we perform division on m with respect to n, then $m = nk + r \Rightarrow (m - r) = nk \Rightarrow (m - r)|n \Rightarrow m \equiv r\, (mod\, n)$. Thus any number is congruent modulo n to its remainder upon division by n.

2. If m is divisble by n, then $m = nk$ and $m \equiv 0\, (mod\, n)$. Thus, if we are trying to deduce if a number is divisble n or not, working modulo n is almost always the best way to go.

3. As $m - m = 0$ is divisble by n $(0 = 0 * n)$, then $m \equiv m\, (mod\, n)$.

4. Given integers m and n with $n > 0$, we can lazily divide m into n so that $m = nk + r$ without enforcing that $0 \leq r < n$. There are infinitely many ways to perform lazy division, e.g. $107 = 5 * 13 + 42$ and $107 = 3 * 13 + 68$ are examples of lazily dividing 107 by 13. However as $(m - r) = nk$, $m \equiv r\, (mod\, n)$. In other words, the lazy remainder r is always congruent to m modulo n. In fact, these lazy remainders correspond to all possible numbers x such that $m \equiv x\, (mod\, n)$. Thus, working modulo n is the same as working with lazy remainders.

We are now in a situation to precisely state what we observed before. If $m_1 \equiv r_1 \,(mod\, n)$ and $m_2 \equiv r_2 \,(mod\, n)$, then $m_1 + m_2 \equiv r_1 + r_2 \,(mod\, n)$. This is the sum rule of modulo arithmetic

What about multiplication? If $m_1 = k_1 n + r_1$ and $m_2 = k_2 n + r_2$, then

$$m_1 m_2 = (k_1 n + r_1)(k_2 n + r_2) = k_1 n k_2 n + k_1 n r_2 + r_1 k_2 n + r_1 r_2 = (k_1 k_2 n + k_1 r_2 + k_2 r_1) n + r_1 r_2$$

$$\Rightarrow m_1 m_2 - r_1 r_2 = n(k_1 k_2 n + k_1 r_2 + k_2 r_1)$$

$$\Rightarrow m_1 m_2 \equiv r_1 r_2 \,(mod\, n)$$

We have just proven the product rule for modulo arithmetic. Note that for both the product and sum rules, I did not use anywhere that $0 \leq r_1 < n$ and $0 \leq r_2 < n$. It is enough that $m_1 \equiv r_1 \,(mod\, n)$ and $m_2 \equiv r_2 \,(mod\, n)$.

Theorem. *Sum and product ruleS for modular arithmetic*
Given the integers a_1, a_2, b_1, b_2, n with $a_1 \equiv b_1 \,(mod\, n)$ and $a_2 \equiv b_2 \,(mod\, n)$, then

$$a_1 + a_2 \equiv b_1 + b_2 \,(mod\, n)$$

$$a_1 a_2 \equiv b_1 b_2 \,(mod\, n)$$

Both the sum and product rule can be used repeatedly with each other to make short work of remainder calculations.

Example. Suppose I wish to find the remainder of 1011 upon division by 7. I write 1011 as $1000 + 11 = 10^3 + 11$. $10 \equiv 3 \,(mod\, 7)$ so by the product rule $10^3 = 10 * 10 * 10 \equiv 3 * 3 * 3 \,(mod\, 7)$. Then $3 * 3 * 3 = 27 \equiv 6 \,(mod\, 7)$. A common trick in modular arithmetic is to use negative numbers if it makes the computation simpler, for instance $6 \equiv 6 - 7 \equiv -1 \,(mod\, 7)$. $11 \equiv 4 \,(mod\, 7)$ so by the sum rule $1011 \equiv -1 + 4 \equiv 3 \,(mod\, 7)$.

Written out in this way, this method of finding remianders seems longer than just using standard long division. However with some practice you should be able to calculate complicated remainders in no time.

Example. We wish to evaluate the remainder of 2^{100} upon division by 13. 2^{100} has at least 30 digits, so it seems entirely unplausable to perform long division. On the other hand, modular arithmetic makes quick work of this type of problem. Let's take successive powers of 2, and evaluate them $(mod\, 13)$. $2^4 = 16 \equiv 3 \,(mod\, 13)$, so $2^6 = 2^2 2^4 \equiv 4 * (3) \equiv -1 \,(mod\, 13)$ and therefore $2^{12} \equiv 2^6 2^6 \equiv (-1)(-1) \equiv 1 \,(mod\, 13)$. Now we have that $2^{24} \equiv 2^{12} 2^{12} \equiv 1 * 1 \equiv 1 \,(mod\, 13)$, and we also see that any power of 2^{12} must be congruent to 1 modulo 13. $96 = 8 * 12$, thus $2^{96} = \left(2^{12}\right)^8 \equiv 1^8 \equiv 1 \,(mod\, 13)$. Finally, $2^{100} = 2^4 2^{96} \equiv 2^4 * 1 \equiv 16 \equiv 3 \,(mod\, 13)$.

Division in modular arithmetic and Euclid's algorithm

So far, we have shown how we can multiply and add in modular arithmetic. We can subtract as well, by combining these two rules: $a - b = a + (-1) * b \equiv a + (-1) * b \equiv a - b \,(mod\, n)$, which in hindsight was rather obvious. The next obvious step is to examine the division of numbers. Unlike the previous operations, it is not clear how to define this for modular arithmetic. After all, $\frac{a}{b}$ need not be an integer, yet modular arithmetic consists only of integers.

To remedy this situation, let's investigate these four basic operations a bit more. Subtraction is defined as the opposite of addition, in the sense that for any integers a and b, $(a + b) - b = a$. In other words, *subtraction undoes addition.* Another way to define subtraction is to consider the *additive inverse* of a number a, which we call $-a$, so that $a + (-a) = 0$. Then we can define $a - b$ as $a + (-b)$. Here, we are using $-$ to mean two different things: the subtraction operation and the negative of a number. There is no real ambiguity here, as the net result is the same. Such a situation in mathematics is called an *abuse of notation.*

We are also familiar with the opposite of multiplcation, which we call division. As $a \div b$ is not always an integer, we will consider rational numbers instead of integers. Given two rational numbers x and $y \neq 0$, then division is defined so that $(x * y) \div y = x$. *Division undoes multiplication.* We may also define the *multiplicative inverse* of a number y which we call y^{-1}, such that $y * (y^{-1}) = 1$. Then dividing by y is the same as multiplying by y^{-1}; $x \div y = xy^{-1}$. Equivalently, $y * y^{-1} = 1$. From every day arithmetic, we know that if $y = \frac{p}{q}$ where p and q are integers then $y^{-1} = \frac{q}{p}$.

Now that we have the pedantics out of the way, can we apply this line of thinking to modular arithmetic? Given integers a and $n > 0$, we define the *multiplicative inverse* of a modulo n as the integer a^{-1}such that $a * a^{-1} \equiv 1 \,(mod\, n)$.

Example. Find 5^{-1} modulo 9.

At the moment, the only way we have of working this is out is trial and error. Thankfully, we don't have to look far: $5 * 2 = 10 \equiv 1 \,(mod\, 9)$. Thus, $5^{-1} \equiv 2 \,(mod\, 9)$.

Note that it is incorrect to say that $5^{-1} = 2$ modulo 9, as it is not the only solution to the problem. By using the sum and product rule, we may add on or subtract any multiple of 9 to 2 and it will still be a multiplicative inverse of 5. E.g., $5 * 11 \equiv 5 * 2 \equiv 5 * (-7) \equiv 1 \,(mod\, 9)$. To account for this, we may use modular arithmetic again and say that $5^{-1} \equiv 2 \,(mod\, 9)$, which includes all possible solutions for 5^{-1} modulo 9.

Example. Find 6^{-1} modulo 9.

This is a trick question; there is no multiplicative inverse of 6 modulo 9. This can easily be seen by multiplying 6 by the numbers 1 to 8 and checking their remainder $(mod\, 9)$. The reason why is that 6 and 9 share a common divisor, 3. By multiplying 6 by some number, the resulting remainder modulo 9 must be a multiple of 3 which cannot possibly be congruent to 1 modulo 9.

This is closely related to the fact that 6 is a zero divisor modulo 9, i.e. there exists an integer x with $x \not\equiv 0 \,(mod\, 9)$ such that $6 * x \equiv 0 \,(mod\, 9)$. In this case, we could take $x \equiv 3$ or $x \equiv 6$ modulo 9 as $6 * 3 \equiv 6 * 6 \equiv 0 \,(mod\, 9)$. This is a very peculiar property for a number to have. Suppose that 6^{-1} exists, then $6^{-1} * 6 * x \equiv 6^{-1} * 0 \,(mod\, 9) \Rightarrow x \equiv 0 \,(mod\, 9)$, which is a contradiction. Given a modulo n, either a^{-1} exists or a is a zero divisor; it is impossible for both statements to be true.

The above two examples illustrate the two main problems with multiplicative inverses in modulo arithmetic; how do I know if a multiplicative inverse exists, and if it does, how do I find said inverse?

To answer these questions, let us try and attack this problem systematically. Given integers a and $n > 0$, I wish to find the multiplicative inverse of a modulo n, which I call x. Then $ax \equiv 1 \,(mod\, n)$. From the definition of modular arithmetic, this implies that $n|ax - 1$, which further implies that $ax - 1 = kn \Rightarrow ax - kn = 1$ for some integer k. So far, k is arbitrary. Thus I will change the sign of k to get the equation

$$ax + kn = 1$$

Thus our goal is to solve this equation for k and x given a and n. Suppose that a and n have a common divisor greater than 1, say $d > 1$. Then $d|(ax + kn) \Rightarrow d|1$, which is clearly impossible. Recall that the greatest common divisor of two integers a and b is simply the largest integer dividing both a and b. This is usually denoted by $gcd(a, b)$, e.g. $gcd\,(36, 24) = 12$. Thus, if $gcd\,(a, n) > 1$, then the above equation will not have solutions and a^{-1} does not exist modulo n.

This is equation is a *linear Diophantine equation.* Fortunately, there is a well known algorithm for solving equations of this type., It is called Euclid's algorithm, and is generally used to find $gcd\,(a, b)$. We will not go through the details here, but Euclid's algorithm guarantess that if $gcd(a, n) = 1$ then $ax + kn = 1$ will have infinitely many solutions for x and k. What's more, all the solutions for x will be congruent modulo n, and thus $x = a^{-1}$ exists and is unique modulo n.

Let's put Euclid's algorithm to the test. Let's try to find 11^{-1} modulo 28. The first part of Euclid's algorithm is a repeated use of the division theorem. I will divide 28 by 11 to get remainder 6, I will then divide 11 by 6 to get remainder 5 etc.

$$28 - 2 * 11 = 6$$

$$\Rightarrow 11 - 1 * 6 = 5$$

$$\Rightarrow 6 - 1 * 5 = 1$$

and the first part of Euclid's algorithm is done. The fact that we finished on a 1 and not a 0 means that $gcd(11, 28) = 1$ and $11^{-1} \,(mod\, 28)$ exists. Next, we begin the roll back procedure by subbing in equations into each other, starting from the bottom up.

$$6 - 1 * 5 = 1$$

$$\Rightarrow 11 - 1 * 6 = 5 = (6 - 1) \Rightarrow 2 * 6 - 11 = 1$$

$$\Rightarrow 2 * (28 - 2 * 11) = 2 * 6 = 1 + 11 \Rightarrow 2 * 28 - 5 * 11 = 1$$

Thus, $(-5) * 11 \equiv 1 \,(mod\, 28)$ and $11^{-1} \equiv -5 \equiv 23 \,(mod\, 28)$.

Now that we can construct a^{-1}, we can also contruct a^{-m} quite easily too as $a^{-m} = \left(a^{-1}\right)^m$.

Modular arithmetic with prime numbers

One of the appeals of the rational numbers is that every non zero rational number has a unique additive and multiplicative inverse. This is a property that the integers do not have, e.g. $2^{-1} = \frac{1}{2}$ is not an integer. Can we a find an integer n such that working modulo n has this property? Finding additive inverses is no problem, but for a^{-1} to exist we require that $gcd\,(a, n) = 1$. Is there an n such that if $a \not\equiv 0\,(mod\, n)$, then $gcd(a, n) = 1$? There are many such n in fact, what we require is that n be a prime number.

A *prime number* p is any integer greater than 1 such that it's only divisors are 1 and itself. We will not pursue prime numbers much here, but they are extremely useful and pervasive in number theory due to the *fundamental theorem of arithmetic*. The first 10 prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23$ and 29. If $0 < a < p$, then $gcd(a, p) = 1$. If this wasn't true, then there would have to be some number dividing p. Thus working modulo p has the very important property that if $a \not\equiv 0\,(mod\, p)$, then a^{-1} exists.

There are some really nice consequences of this. For instance, given a prime number p, line up all the numbers modulo p excluding 0: $(1, 2, 3, \ldots, p-2, p-1)$. Now pick any number from this set, say a, then multiply each of these numbers by a to get $(a*1, a*2, a*3, \ldots, a*(p-1))$. Can we say anything about this new set? Let's examine the case $p = 11$ and $a = 7$. Then

$$(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \to (7, 3, 10, 6, 2, 9, 5, 1, 8, 4)$$

What's curious about this is that multiplying by 7 has just shuffled around the numbers modulo p. This is always true for p a prime and $a \not\equiv 0\,(mod\, p)$, and is not too hard to show. Take two numbers x and y modulo p. Is it possible that $a*x$ and $a*y$ are the same? In that case, $a*x \equiv a*y\,(mod\, p) \Rightarrow a^{-1}*a*x \equiv a^{-1}*a*y\,(mod\, p) \Rightarrow x \equiv y\,(mod\, p)$. This implies that when I multiply these $p-1$ numbers by a they must all be different, completing the argument.

In mathematics whenever we see two things that look different but are the same, we should always equate these two things to obtain an identity. In this case, let's multiply all the elements from $(1, 2, 3, \ldots, p-2, p-1)$ and $(a*1, a*2, a*3, \ldots, a*(p-1))$and equate them:

$$1*2*3*\ldots*(p-2)*(p-1) \equiv (a*1)*(a*2)*\ldots*(a*(p-1)) \equiv a^{p-1}(1*2*3*\ldots*(p-2)*(p-1))\,(mod\, p)$$

But p does not divide $1*2*3*\ldots*(p-2)*(p-1)$, so I can eliminate this from both sides of the equation. Thus $a^{p-1} \equiv 1\,(mod\, p)$, which is known as Fermat's little theorem.

Theorem. *Fermat's Little theorem*

For a prime number p and an integer a with $gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1\,(mod\, p)$$

If we do not assume that $gcd(a, p) = 1$, then it is true that $a^p \equiv a\,(mod\, p)$.

Fermat's little theorem can be incredibly practical for some calculations.

Example. Find the remainder of $56^{10^{10}}$ upon division by 101.

First we observe that 101 is a prime number. By Fermat's Little theorem, $56^{100} \equiv 1\,(mod\, 101)$. But $10^{10} = \left(10^2\right)^5 = 100^5$. Thus $56^{10^{10}} \equiv \left(56^{100}\right)^5 \equiv 1^5 \equiv 1\,(mod\, p)$.

Note that if $gcd(a, p) = 1$, then $a^{p-1} \equiv a^{p-2}a \equiv 1\,(mod\, p)$. Thus $a^{p-2} \equiv a^{-1}\,(mod\, p)$, which gives us a nice alternative formula for finding multiplicaitve inverse modulo p. More generally, given two integers b_1 and b_2:

$$b_1 \equiv b_2\,(mod\, p-1) \Rightarrow a^{b_1} \equiv a^{b_2}\,(mod\, p)$$

Thus if we are working modulo p, then we work in powers modulo $p-1$. The generalisation of these results for non prime integer is known as Euler's totient theorem.

Polynomials also behave nicely modulo p. Recall the fundamental theorem of algebra; a polynomial of $q(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$ of degree n has n roots in the complex numbers, counting multiplicities (roots appearing more than once, e.g. $q(z) = z^2$). Without counting multiplicities, we could say instead that a degree n polynomial has at most n solutions in the complex numbers. The same is true for polynomials modulo p.

Theorem. *Lagrange's Theorem*

If $q(x)$ is a polynomial of degree n with integer coefficients so that at least one coefficient is not divisible by the prime p, then $q(z) \equiv 0\,(mod\, p)$ has at most n roots modulo p.

We will not prove this theorem here. We require that at least one coefficient is not divisible by p, as otherwise every coefficient would be divisible by p, and then $q(x) \equiv 0 \,(mod\, p)$ for all x. This theorem does not guarantee that $q(x)$ has a solution, for instance take $q(x) = x^2 + x + 1$ modulo 2. Then $q(0) \equiv q(1) \equiv 1 \,(mod\, 2)$, and $q(x) \equiv 0 \,(mod\, 2)$ has no solutions.

There is a very nice corollary of Lagrange's theorem that ties in with Fermat's little theorem. In algebra we talk about the n-th roots of unity, the n solutions to $z^n = 1$ in the complex plane. These solutions may easily be found using de Moivre's theorem. This corollary is the appropriate modulo p analogy.

Corollary. *Suppose p is a prime and $n|p-1$, . Then the equation $x^n \equiv 1 \,(mod\, p)$ has exactly n solutions.*

Again, we will not prove this here. As a brief example, consider $x^2 \equiv 1 \,(mod\, p)$. Then for $p > 2$, p must be odd and $p-1$ must be even. Then $2|p-1$ and we know that there are only two solutions to $x^2 \equiv 1 \,(mod\, p)$. In fact we know what these solutions are, $x \equiv 1$ and $x \equiv -1$ modulo p.

There is one last card up our sleeve. To prove Fermat's little theorem, we multiplied all the non-zero integers modulo p by a fixed number a and compared the products of the two results. This worked because multiplying by a shuffled the numbers modulo p. However there is another way to shuffle the numbers, by taking x to x^{-1}.

$$(1, 2, 3, \ldots, p-2, p-1) \,(mod\, p) \to \left(1^{-1}, 2^{-1}, 3^{-1}, \ldots, (p-1)^{-1}\right) \,(mod\, p)$$

If we multiply all the terms on the left, we get $(p-1)! \,(mod\, p)$. If we multiply all the terms on the right, I get $((p-1)!)^{-1} \,(mod\, p)$. Therefore, $(p-1)! \equiv ((p-1)!)^{-1} \,(mod\, p) \Rightarrow ((p-1)!)^2 \equiv 1 \,(mod\, p)$. We know that this equation has two solutions, thus $(p-1)! \equiv 1 \,(mod\, p)$ or $(p-1)! \equiv -1 \,(mod\, p)$.

To figure out which, we need to take a closer look at the numbers $(1, 2, 3, \ldots, p-2, p-1) \,(mod\, p)$. As the inverse of the inverse of a number is just the original number, $\left(x^{-1}\right)^{-1} \equiv x \,(mod\, p)$, multiplicative inverses come in pairs. For example, $3 * 5 \equiv 1 \,(mod\, 7)$. Thus $3^{-1} \equiv 5 \,(mod\, 7)$ and $5^{-1} \equiv 3 \,(mod\, 7)$. For $p > 2$ $p-1$ is even, thus I can split up these $p-1$ numbers into multiplicative inverse pairs. There is one snag however. The multiplicative inverse of 1 is always 1 modulo p, and similarly for -1. Thus, both 1 and -1 belong in a multiplicative "pair" on their own. Are these the only numbers with this property? Yes; if we try to find x such that $x \equiv x^{-1} \,(mod\, p)$ then $x^2 \equiv 1 \,(mod\, p)$ and x is congruent to 1 or -1 modulo p. So we can split up $(1, 2, 3, \ldots, p-2, p-1) \,(mod\, p)$ into 3 groups; the multiplicative inverse pairs, 1 and -1. The product of all these numbers is $(p-1)! \,(mod\, p)$. The product of the multiplicative inverses alone is 1, and thus when we include 1 and -1 we see that $(p-1)! \equiv -1 \,(mod\, p)$.

Theorem. *Wilson's Theorem*
For p a prime,

$$(p-1)! \equiv -1 \,(mod\, p)$$

There are many more useful benefits of working modulo p that we have not discussed here.

Some diophantine equations

In the following statements like $a \equiv b, c \,(mod\, n)$ mean a is congruent to b or c modulo n. Before introducing any new ideas, let us begin with an example.

Example. Find all integer solutions to $x^2 + y^2 = 103$.

The trick is to work modulo 4. $103 \equiv 3 \,(mod\, 4)$. As neither x or y are specified, we need to deduce all possible values that $x^2 + y^2$ could take. For $x \equiv 0, 2 \,(mod\, 4)$ then $x^2 \equiv 0 \,(mod\, 4)$, whereas if $x \equiv 1, 3 \,(mod\, 4)$ then $x^2 \equiv 1 \,(mod\, 4)$. Thus $x^2 \equiv 0, 1 \,(mod\, 4)$ and $x^2 + y^2 \equiv 0, 1, 2 \,(mod\, 4)$. But $0, 1, 2 \not\equiv 3 \,(mod\, 4)$. Thus there are no solutions to $x^2 + y^2 \equiv 103$.

An equation that needs to be solved in integers is called a *diophantine equation*. Modular arithmetic is a very neat tool for analysing diophantine equations, but it is not a universal method.

Example. Find all integer solutions to $x^2 = 1 + y^3$.

The first step with any diophantine equation should be to look for small non trivial solutions. In this instance, we see that $(x, y) = (3, 2)$ is a solution. This implies that using modular arithmetic is a bad idea. No matter what n we choose, working modulo n must always allow this small solution. The methods used to solve this equation are currently beyond us.

Modular arithmetic is not generally a constructive method, i.e. it will not deduce all solutions of a diophantine equation. There are various ways to do this, none of which we will do here.

Example. Find all integer solutions to $x^4 + y^4 = 5z^4$.

Note that $x^4 = (-x)^4$. Thus without loss of generality I may assume that x, y, z are all positive. By Fermat's little theorem we know that if $gcd(a, 5) = 1$ then $a^4 \equiv 1 \,(mod\, 5)$. As $5z^4 \equiv 0 \,(mod\, 5)$, then $x^4 + y^4 \equiv 0 \,(mod\, 5)$. The only way that this can happen is if both x and y are congruent to 0 modulo 5. Thus 5 divides both x and y, say $x = 5x'$ and $y = 5y'$. Plugging this back into the original equation: $625(x'^4 + y'^4) = 5z^4 \Rightarrow 125(x'^4 + y'^4) = z^4$. As before, $z^4 \equiv 0 \,(mod\, 5) \Rightarrow 5|z$ so $z = 5z'$. Thus $125(x'^4 + y'^4) = 625z'^4 \Rightarrow x'^4 + y'^4 = 5z'^4$. This equation is the same as the one we started with. What we have show is that if (x, y, z) is a solution to our diophantine equation, then $\left(\frac{x}{5}, \frac{y}{5}, \frac{z}{5}\right)$ is also a solution. But this makes no sense, how can I keep on dividing my solutions by 5 and get a new solution? That would mean that x (for example) would have to be divisible by 5 infinitely many times. This makes no sense.

To make this argument more formal, assuming that x, y, z are positive and that there are solutions, I know that there must be a solution with smallest x. (This property is known as the *least ordering principle*.) But I also know that there is a solution with $\frac{x}{5}$, which is smaller than my smallest solution. This is a contradiction, so x, y, z cannot be positive. The only solutions are $(x, y, z) = (0, 0, 0)$.

This problem exposed a few very important techniques. First, we used modular arithmetic to place restrictions on x, y and z. We could then substitute these restrictions back into our equation to get a new equation. Secondly, given a solution to the equation we generated a new solution. Finally, we showed that given a positive solution we could always construct a smaller positive solution, leading to a contradiction. This last technique is known as the *method of infinite descent*, first used by Fermat.

Fine, so modular arithmetic is useful. But if I decide to work modulo n, how do I pick n? There is trial and error; simply pick a few small n and see what works. There are also a few standard identities:

1. $m^2 \equiv 0, 1 \,(mod\, 3)$
2. $m^2 \equiv -1, 0, 1 \,(mod\, 5)$
3. $m^2 \equiv 0, 1, 4 \,(mod\, 8)$
4. $m^3 \equiv -1, 0, 1 \,(mod\, 9)$
5. $m^4 \equiv 0, 1 \,(mod\, 16)$

Gievn a polynomial $f(m)$, we will refer to all the possible values of $f(m)$ as m ranges over all the integers $(mod\, n)$ as the image of $f(m)$ modulo n. We could similarly define the image for a function with more than one argument, e.g. $f(x, y) = x^2 + y^2$ in the example above. We may rephrase the above identities in this language; the image of m^2 modulo 3 is $\{0, 1\}$ etc. These identities are useful because they take a function $f(m)$ and give an n for which the image of f modulo n is small. Our goal is thus to try and deduce an n that minimises the size of the image of f modulo n. Based on our previous work we will only consider n prime, even though the previous identities show that composite n is useful too. To examine composite n, the reader should investiagte the Chinese remainder theorem and Euler's totient theorem.

Can we deduce the size of the image of x^n modulo p? Yes, in the special case $n|p - 1$. If $x \equiv 0 \,(mod\, p)$, then $x^n \equiv 0 \,(mod\, p)$. Now take $gcd(x, p) = 1$. Suppose $\frac{p-1}{n} = k$. Then $(x^n)^k \equiv x^{p-1} \equiv 1 \,(mod\, p)$ by Fermat's Little theorem. Let $y = x^n$. Then x^n must be a solution to $y^k \equiv 1 \,(mod\, p)$. We know that there are exactly k solutions to this equation, thus x^n can take on at most k values. We won't prove it here, but x^n will take on all values of these k roots. For a proof, the reader should learn about primitive roots modulo p. Thus including the 0 solution also, x^n takes on $\frac{p-1}{n} + 1$ values modulo p, provided $n|p - 1$. We can use this fact solve diophantine equations.

Example. Find all integer solutions to $x^2 + y^5 = 29$.

To start with, note that both 2 and 5 divide 10. By Fermat's little theorem $a^{10} \equiv 1 \,(mod\, 11)$ if $gcd(a, 11) = 1$. Thus we will try working modulo 11: $x^2 + y^5 \equiv 7 \,(mod\, 11)$. I know that $\left(x^2\right)^5 \equiv 1 \,(mod\, 11)$, so there are exactly 5 solutions for x^2. In other words, x^2 will take on exactly 5 values provided $gcd(x, 11) = 1$. Thus, the image of x^2 modulo 11 should have 6 elements. The image of x^2 modulo 11 can be found very easily be squaring all of the numbers modulo 11. The image of x^2 is found to be $\{0, 1, 3, 4, 5, -2\}$, confirming our calculation. Similarly, the image of $y^5 \,(mod\, 11)$ is just $\{-1, 0, 1\}$ and has $2 + 1$ elements. To work out the image of $x^2 + y^5 \,(mod\, 11)$, we just form all possible sums between the two images. Thus the image of $x^2 + y^5 \,(mod\, 11)$ is $\{0, 1, 2, 3, 4, 5, 6, 8, 9, 10\}$. As 7 is not in the image of $x^2 + y^5 \,(mod\, 11)$, this diophantine equation has no solutions.

We see straight away from this example that things were set up. If some other number instead of 29 were chosen, $(mod\,11)$ probably would not have worked. That said, it was still a good idea to try applying modular arithmetic first before moving onto other solution methods.

Thus, a good motivation for working modulo p is to find a p such that the powers in the diophantine equation divide $p-1$.

Exercises

1. Given integers m and n with $n > 0$, prove rigorously that the set of solutions for x in the equation $m \equiv x\,(mod\,n)$ is exactly of the form $x = r + nk$, where k is some integer and r is the remainder of m upon divison by n.
2. Calculate 10^{-1} modulo 27.
3. Calculate 24^{-1} modulo 47.
4. Prove that $(xy)^{-1} \equiv x^{-1}y^{-1}\,(mod\,p)$.
5. Compute 2^{-1} and 3^{-1} modulo 107. Using the previous exercise, compute 72^{-1} modulo 107.
6. Find 2^{-1} modulo p.
7. Find the remainder of 5^{716} upon disivison by 43.
8. Given a polynomial $p(m)$ with integer coefficients, show that if $m_1 \equiv m_2\,(mod\,n)$ then $p\,(m_1) \equiv p\,(m_2)\ \ (mod\,n)$.
9. Find all solutions to $x^3 \equiv 1\,(mod\,31)$.
10. Find all solutions to $x^5 \equiv 1\,(mod\,11)$.
11. Find all integer solutions to $x^2 + y^2 = 3z^2$.
12. Find all integer solutions to $x^3 + y^4 = 20$.
13. Find all integer solutions to $x^2y^3 = 72$.
14. Find all integer solutions to $3x^4 + 5y^{11} = 15$.
15. Find all integer solutions to $x^2 + 20\,y^9 = 13$.