An excerpt from the book *Love and Math* by Edward Frenkel[*]

When we talked about rotations of the circle, we saw that the addition of angles was done "modulo 360." That is to say, if the result of addition of two angles is greater than 360 degrees, we subtract from it 360 to bring it into the range from 0 to 360. For example, rotation by 450 degrees is the same as rotation by 90 degrees, because $450-360=90$.

We also encounter this arithmetic when we use the clock. If we start working at 10 o'clock in the morning and work for 8 hours, when do we finish? Well, $10+8=18$, so a natural thing to say would be: "We finish at 18 o'clock." This would be perfectly fine to say in France where they record hours as numbers from 0 to 24. But in the U.S. we say: "We finish at 6 pm." How do we get 6 out of 18? We subtract 12 from it: $18-12=6$.

So we use the same idea with hours as we do with angles. In the first case, we do addition "modulo 360." In the second case, we do addition "modulo 12."

Likewise, we can do addition modulo any natural number N. Consider the set of all consecutive whole numbers between 0 and $N-1$,

$$\{0,1,2,\ldots,N-2,N-1\}.$$

If $N=12$, this is the set of possible hours. In general, the role of 12 is played by number N, so that it's not 12 that takes us back to 0, but N.

We define addition on the set of these numbers in the same way as for the hours. Given any two numbers from this set, we add them up, and if the result is greater than N, we subtract N from it to get a number from the same set. The operation

[*] To be published by Basic Books in October 2013. Available on Amazon.com at http://www.amazon.com/gp/product/0465050743/

of addition modulo N makes this set into a group. Recall that a group is a set with an operation that assigns an element of the set to any pair of elements and satisfies certain properties (identity element, inverse elements, and associativity). In our case these properties are as follows. The identity element is the number 0: adding it to any other number does not change it. Indeed, we have $n+0=n$ for any number n from our set. And for any n, its "additive inverse" is $N-n$, because $n+(N-n)=N$, which is the same as 0 according to our rules. (The associativity property also holds.)

For example, let's take $N=3$. Then we have the set $\{0,1,2\}$ and addition modulo 3. For example, we have

$$2+2=1 \qquad \text{modulo} \quad 3$$

in this system, because $2+2=4$, but since $4=3+1$, the number 4 is equal to 1 modulo 3.

So if someone says to you: "2 plus 2 equals 4" to indicate a well-established fact, you can now say (with a condescending smile if you like): "Well, actually, that's not always true." And if they ask you to explain what you mean, you can tell them, "If you do addition modulo 3, then 2 plus 2 is equal to 1."

Given any two numbers from the above set, we can also multiply them. The result may not be between 0 and $N-1$, but there will be a unique number in this range which will differ from the result of multiplication by something divisible by N. However, in general, the set $\{1,2,...,N-1\}$ is not a group with respect to multiplication. We do have the identity element: number 1. But not every element has the multiplicative inverse modulo N. This happens if and only if N is a *prime number*, that is, a number that is not divisible by any other natural number other than 1 and itself.

For each prime number p, the set of p elements: $\{0,1,2,...,p-1\}$ is a numerical system with operations of addition, subtraction, multiplication, and division modulo p, which obey the same rules as the corresponding operations on the rational and real numbers.

There is also something special about this numerical system. If you take any element of the finite field $\{0,1,2,...,p-1\}$ and raise it to pth power – in the sense of the arithmetic modulo p – you will get back the same number! In other words,

$$a^p = a \quad \text{modulo} \quad p.$$

This formula was proved by Pierre Fermat, the mathematician who came up with Fermat's Last Theorem. Unlike the proof of the latter, though, the proof of the above formula is fairly simple. The idea is to view it from the point of view of group theory. Consider the non-zero elements of the finite field: $1, 2, ..., p-1$. They form a group with respect to multiplication. Indeed, the identity element with respect to multiplication is the number 1: if we multiply any element a by 1, we get back a. And each element has an inverse: for any a in $\{1, 2, ..., p-1\}$, there is an element b such that $a \cdot b = 1$ modulo p.

This group has $p-1$ elements. There is a general fact that holds for *any* finite group G with M elements: the Mth power of each element a of this group is equal to the identity element (which we will denote by 1):

$$a^M = 1.$$

To prove this, consider the following elements in the group G: $1, a, a^2, ...$ Because the group G is finite, these elements cannot all be distinct. There have to be repetitions. Let k be the smallest natural number such that a^k is equal to 1 or a^j for some $j = 1, ..., k-1$. Suppose that the latter is the case. Let a^{-1} denote the inverse of a, so that $a \cdot a^{-1} = 1$ and take its jth power $(a^{-1})^j$. Multiply both sides of the equation $a^k = a^j$ with $(a^{-1})^j$ on the right. Each time we encounter $a \cdot a^{-1}$ we replace it by 1. Multiplying by 1 does not change the result, so we can always remove 1 from the product. We see then that each a^{-1} will cancel one of the a's. Hence, the left-hand side will be equal to a^{k-j}, and the right-hand side will be equal to 1. We obtain that $a^{k-j} = 1$. But $k - j$ is smaller than k, and this contradicts our choice of k. Therefore, the first repetition on our list will necessarily have the form $a^k = 1$, so that the elements $1, a, a^2, ..., a^{k-1}$ are all distinct. This means that they form a group of k elements: $\{1, a, a^2, ..., a^{k-1}\}$. It is a subgroup of our original group G of M elements, in the sense that it is a subset of elements of G such that the result of multiplication of any two elements of this subset is again an element of the subset, this subset contains the identity element of G, and this subset contains the inverse of each of its elements.

Now, it is known that the number of elements of any subgroup always divides the number of elements of the group. This statement is called the Lagrange theorem. I'll leave it for you to prove (or you may Google it).

Applying the Lagrange theorem to the subgroup $\{1, a, a^2, \ldots, a^{k-1}\}$, which has k elements, we find that k must divide M, the number of elements of the group G. Thus, $M = kl$ for some natural number l. But since $a^k = 1$, we obtain that

$$a^M = (a^k) \cdot (a^k) \cdot \ldots \cdot (a^k) = 1 \cdot 1 \cdot \ldots \cdot 1 = 1,$$

which is what we wanted to prove.

Let's go back to the group $\{1, 2, \ldots, p-1\}$ with respect to multiplication. It has $p-1$ elements. This is our group G, so our M is equal to $p-1$. Applying the general result in this case, we find that $a^{p-1} = 1$ modulo p for all a in $\{1, 2, \ldots, p-1\}$. But then

$$a^p = a \cdot a^{p-1} = a \cdot 1 = a \quad \text{modulo} \quad p.$$

It is easy to see that the last formula actually holds for all integers. This is the statement of Fermat's little theorem. To distinguish this result from Fermat's Last Theorem (sometimes also referred as Fermat's Great Theorem), it is called Fermat's little theorem.

For example, set $p = 5$. Then our finite field is $\{0, 1, 2, 3, 4\}$. Let's raise each of them to the 5th power. Surely, 0 to any power is 0, and 1 to any power is 1, so no surprises here. Next, let's raise 2 to the 5th power: we then get 32. But $32 = 2 + 5 \cdot 6$, so modulo 5 this is 2 – we get back 2, as promised. Let's take the 5th power of 3: we get 243, but this is $3 + 5 \cdot 48$, so it is 3 modulo 5. Again, we get back the number we started with. And finally, let's try the same with 4: its 5th power is 1024, which is 4 modulo 5. Bingo! I encourage you to check that $a^3 = a$ modulo 3, and $a^7 = a$ modulo 7 (for larger primes you might need a calculator to verify Fermat's little theorem).

Up to now, we have considered the arithmetic modulo a prime number p. However, it turns out that there is a statement analogous to Fermat's little theorem in the arithmetic modulo any natural number N. To explain what it is, I need to recall the Euler function $\phi(N)$ equal to the number of natural numbers between 1 and $N-1$ which are relatively prime with N; that is, do not have common divisors with N (other than 1). For instance, if N is a prime, then all numbers between 1 and $N-1$ are relatively prime to n, and so $\phi(N) = N-1$.

Now, the analogue of the formula $a^{p-1} = 1$ modulo p that we discussed above is the formula

$$a^{\phi(N)} = 1 \quad \text{modulo} \quad N.$$

It holds for any natural number N and any natural number a that is relatively prime to N. It is proved in exactly the same way as before: We take the set of all natural numbers between 1 and $N-1$ that are relatively prime to n. There are $\phi(n)$ of them. It is easy to see that they form a group with respect to the operation of multiplication. Hence, by the Lagrange theorem, for any element of this group, its $\phi(N)$th power is equal to the identity element.

Consider, for example, the case that N is the product of two prime numbers. That is, $N = pq$, where p and q are two distinct prime numbers. In this case, the numbers that are not relatively prime to N are either divisible by p or by q. The former have the form pi, where $i = 1,\dots,q-1$ (there are $q-1$ of those), and the latter have the form qj, where $j = 1,\dots,p-1$ (there are $p-1$ of those). Hence we find that

$$\phi(N) = (N-1)-(q-1)-(p-1) = (p-1)(q-1).$$

Therefore we have

$$a^{(p-1)(q-1)} = 1 \quad \text{modulo} \quad pq$$

for any number a that is not divisible by p and q. But in fact, it is easy to see that the formula

$$a^{(p-1)(q-1)+1} = a \quad \text{modulo} \quad pq$$

is true for any natural number a.

This equation is the basis of one of the most widely used encryption algorithms, called RSA algorithm (after Ron Rivest, Adi Shamir, and Leonard Adleman, who described it in 1977). The idea is that we pick two primes p and q (there are various algorithms for generating them) and let N be the product pq. Number N is made public, but the primes p and q are not. Next, we pick a number r that is relatively prime to $(p-1)(q-1)$. This number is also made public.

The encryption process converts any number a (such as a credit card number) to a^r modulo N:

$$a \quad \mapsto \quad b = a^r \quad \text{modulo} \quad N.$$

It turns put that there is an efficient way to reconstruct a from a^r. Namely, we find a number s between 1 and $(p-1)(q-1)$ such that

$$rs = 1 \quad \text{modulo} \quad (p-1)(q-1).$$

In other words,

$$rs = 1 + m(p-1)(q-1)$$

for some natural number m. Then

$$\begin{aligned} a^{rs} \quad \text{modulo} \quad N &= a^{1+m(p-1)(q-1)} \quad \text{modulo} \quad N \\ &= a \cdot a^{m(p-1)(q-1)} \quad \text{modulo} \quad N \\ &= a \quad \text{modulo} \quad N \end{aligned}$$

because $a^{(p-1)(q-1)} = 1$ modulo N as we have seen above.

Therefore, given $b = a^r$, we can recover the original number a as follows:

$$b \quad \mapsto \quad b^s \quad \text{modulo} \quad N.$$

Let's summarize: we make the numbers N and r public, but keep s secret. The encryption is given by the formula

$$a \quad \mapsto \quad b = a^r \quad \text{modulo} \quad N.$$

Anyone can do it because r and N are publicly available.

The decryption is given by the formula

$$b \quad \mapsto \quad b^s \quad \text{modulo} \quad N.$$

Applied to a^r, it gives us back the original number a. But only those who know s can do this.

The reason why this is a good encryption scheme is that in order to find s, which enables one to reconstruct the numbers being encoded, we must know the value of $(p-1)(q-1)$. But for this we need to know what p and q are, which are the two prime divisors of n. Those are kept secret. For N sufficiently large, using known methods of prime factorization, it may take many months, even on a network of powerful computers, to find p and q. The RSA algorithm has many uses, and it is often used as one step in a multi-step encryption protocol.