6. Euler Phi Function and digital signatures

Two integers m and n are said to be *coprime* if $gcd(m,n) = 1$. For example, the integers 30 and 77 are coprime. The integers 6 and 21 are not coprime. A integer $p \geq 2$ is *prime* if it is coprime to all integers other than itself.

We have seen that on an m-hour clock, an integer n has an inverse n^{-1} if and only if n is coprime to m. For this reason and other reasons we are interested in the following definition.

Definition 6.0.1 *Euler's Phi function* $\phi(m)$ is defined for any positive integer m as

$$\phi(m) = \text{ the number of integers in the range } 1,2,\ldots,m-1 \text{ that are coprime to } m \text{ .}$$

To calculate $\phi(8)$ we could use the table

$n =$	1	2	3	4	5	6	7
$gcd(n,8) = 1$	true	false	true	false	true	false	true

to obtain $\phi(8) = 4$. To calculate $\phi(6)$ we could use the table

$n =$	1	2	3	4	5
$gcd(n,6) = 1$	true	false	false	false	true

to obtain $\phi(6) = 2$.

This tabular approach to calculating $\phi(m)$ is not so practical when n is large. For some large numbers, such as $m = 107$, the calculation of $\phi(107)$ is very straightforward: $\phi(107) = 106$. The thinking underlying this calculation generalizes to the following.

Proposition 6.0.1 If p is a prime number then $\phi(p) = p - 1$.

6.1 What is a proposition?

Mathematicians use the term *theorem* to refer to a mathematical statement that they know is true. They may be able to explain why it is true, or they may just be aware that there exists an explanation

in some book or academic paper of why it is true and that this explanation has convinced many mathematicians and no credible mathematician doubts it. (An explanation of the term *credible mathematician* is beyond the scope of this book.) So a *theorem* is a mathematical statement that has a convincing explanation which meets the rigorous requirements of the mathematical community. We refer to such an explanation as a *proof*. The term *theorem* is only ever used in a mathematical context.

What then is a *proposition*? This term is used in many non-mathematical contexts. It could refer to a suggestion offered in a night club. Or a suggestion offered by a property developer to a banker. But what does the word mean when used by a mathematician?

A *proposition* is a mathematical statement that has a convincing explanation that meets the rigorous requirements of the mathematical community.

So what is the difference between a *theorem* and a *proposition*? The difference is analogous to that between a *city* and a *town*. Cities tend to be a bit larger than towns. Cities tend to be a bit higher in the unofficial hierarchy of housed communities; both cities and towns tend to be regarded as a bit more important than villages. The choice between the terms *city*, *town* and *village* is definitely country dependent. I live in a town in the West of Ireland – Oughterard – consiting of 800 inhabitants. I grew up in North Wales where we have a village – Llanfairpwllgwyngyll-gogerychwyrndrobwllllantysiliogogogoch – consisting of over 3000 inhabitants. However you measure it, the Welsh village is bigger than the Irish town.

Theorems tend to be a bit more substantial and more noteworthy than propositions. This is a subjective difference. What one mathematician might call a *theorem* another might call a *proposition*.

But what of mathematical villages? The term *lemma* is used to refer to these.

Having given a straighforward definition of the term *proposition*, let us now muddy the waters. In one branch of mathematics known as *mathematical logic* the term *proposition* just refers to any clear mathematical statement, and in this branch one allows the notion of propositions that are false as well as propositions that are true. Mathematical logic is a very specialized, though also very important, branch of mathematics. In all other branches of mathematics the above definition of *proposition* is the accepted one.

Occasionaly a proof establishing a result that has been accepted as a theorem is found to contain an error. In this case the mathematics community deals with the situation in the same way as the Catholic Church deals with broken marriage. The theorem is annuled – it is deemed never to have been a theorem.

6.2 Two more propositions

A little experimentation leads to further propositions. For instance, the easy calculations

$$\phi(2^2) = 2 \tag{6.1}$$
$$\phi(3^2) = 3 \tag{6.2}$$
$$\phi(5^2) = 20 \tag{6.3}$$
$$\phi(2^3) = 4 \tag{6.4}$$
$$\phi(2^4) = 8 \tag{6.5}$$
$$\phi(3^3) = 18 \tag{6.6}$$

might suggest a pattern. Namely, the pattern $\phi(p^k) = p^k - p^{k-1}$ when p is prime. To convert this apparent pattern into a proposition we need a convincing explanation. Here goes.

Suppose that $1 \leq n < p^k$. Then $gcd(n, p^k) > 1$ if and only if $n = pa$ with a any integer $1 \leq a \leq p^{n-1}$. There are p^{n-1} such integers a. So there are $p^n - p^{n-1}$ integers in the range $1, \ldots, p^n$ that are coprime to p^n. This establishes the following.

Proposition 6.2.1 For any prime p wnd integer $k \geq 1$ we have

$$\phi(p^k) = p^k - p^{k-1} .$$

More experimentation leads to further propositions. For instance, the calculations

$$\phi(15) = 8 \tag{6.7}$$
$$\phi(3) = 2 \tag{6.8}$$
$$\phi(5) = 4 \tag{6.9}$$

show that $\phi(3 \times 5) = \phi(3)\phi(5)$. On the other hand the calculations

$$\phi(24) = 8 \tag{6.10}$$
$$\phi(4) = 2 \tag{6.11}$$
$$\phi(6) = 2 \tag{6.12}$$

show that $\phi(4 \times 6) \neq \phi(4)\phi(6)$. The mathematical literature contains an abundance of proofs of the following proposition. It is a worthwhile excercise figuring out a proof without recourse to the literature.

Proposition 6.2.2 For any pair of coprime integers m and n the equality

$$\phi(mn) = \phi(m)\phi(n)$$

holds.

We are now in a position to quickly calculate the Euler Phi function of larger integers. For example:

$$\phi(440) = \phi(2^3 \times 3 \times 5) \tag{6.13}$$
$$= \phi(2^3)\phi(3)\phi(5) \tag{6.14}$$
$$= (2^3 - 2^2)(3-1)(5-1) \tag{6.15}$$
$$= 160 \tag{6.16}$$

6.3 Public Key Cryptography

A cryptosystem requires an enciphering key and a deciphering key. The keys need to be changed on a regular basis to maintain security. But how should sender and receiver agree on new keys? There is little point using the existing keys to encrypt and send new keys! One possibility is to pre-arrange which keys to use at given times and to record these arrangement in a codebook. The risk is that the codebook may fall into the hands of an adversary. The German Navy used this method in World War II and, sure enough, on 30 October 1942 the Allies captured the codebook. The submarine $U-559$ was spotted at around 5am by an RAF Sunderland. Allied destroyers hunted her with depth charges for 16 hours. She was eventually damaged, and the crew had to abort the vessel. But they failed to destroy the codebbook before leaving, and it was retrieved from the sinking U-boat by three Royal Navy sailors.

In 1976 Whitfield Diffie and Martin Hellma published a paper in which they proposed the following.

Definition 6.3.1 — Diffie & Hellman. A *public key cryptosystem* is a cryptosystem with the property that someone who knows only the enciphering key can not, without a prohibitively large effort, determine how to decipher.

The idea had in fact been invented five years earlier, independently and under the name *non-secret encryption*, by James Ellis who worked for the British Govenrment Communications Headquarters (GCHQ) – an organization not so eager to publicize its work!

The affine cryptosystem described in Chapter 3 is not public key. Formulae (3.13) and (3.14) allow one to quickly compute the deciphering key from a knowledge of the enciphering key.

A cryptosystem satisfying the definition of a public key cryptosystem was invented and publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. Rivest was a mathematics graduate from Yale, Shamir a mathematics graduate from Tel Aviv, and Adleman a mathematics graduate from Berkeley. The system has become known as *RSA cryptography* and is widely used on a daily basis by those sending messages or buying goods over the internet. It is based on properties of Euler's Phi function.

The problem of constructing a public key encryption system had in fact been given to a new recruit to GCHQ – Clifford Cocks – in 1973. Cocks had studied mathematics as an undergraduate at Cambridge and as a postgraduate at Oxford. Within a day at GCHQ he had invented what is essentially the RSA algorithm, a full four years before Rivest, Shamir and Adleman published their public key cryptosystem. This history became known only in 1997 when GCHQ declassified his invention.

6.4 Digital signatures

Before describing the RSA example of public key cryptography, we explain how any public key system

$$\text{plaintext} \underset{f_D}{\overset{f_E}{\rightleftarrows}} \text{ciphertext}$$

can allow a bank customer to remotely sign papers for a transaction.

The customer first needs to create an enciphering key E and deciphering key D for the cryptosystem. The customer's enciphering key E is registered with the bank, and can be made public by the customer if desired. For instance, E could be placed on a public web page. The deciphering key D is kept sercret by the customer – not even the bank is given any knowledge of D.

When the customer emails the bank asking it to send €10 000 to a supplier of goods, the bank first needs to confirm that it is indeed the customer and not some adversary who has emailed them. To confirm this, the bank generates some random message such as

$$\text{Cymru\_am\_byth}$$

and sends the enciphered message $f_E(\text{Cymru\_am\_byth})$ to the customer. The bank then asks the customer for details of the random message. The customer calculates

$$f_D(f_E(\text{Cymru\_am\_byth})) = \text{Cymru\_am\_byth}$$

and is able to send the random message back to the bank. Only this customer is able to do this as only the customer knows the deciphering key D.

6.5 A puzzle

Mary and Joseph have fallen in love, and Joseph wishes to send her a ring via mail. Unfortunately they live in Kleptopia where anything sent by mail will be stolen unless it is in a padlocked box.

The two of them have many padlocks, but none to which the other has a key. How can Joseph mail the ring safely to Mary?