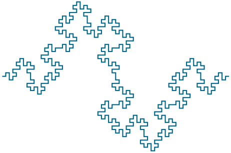
Cryptographic Mathematics I
Week 3

Dr. Eberhard Mayerhofer

University of Limerick



Semester I 2016/7

Pierre de Fermat lived in France in the 17th century before Newton. He was a jurist and only dabbled in mathematics in his spare time. He stated what has become known as Fermat's Little Theorem in a letter but gave no proof. Leibniz provided the first proof of the result. To see the result emerging, let us examine the following tables of powers modulo 3, 5 and 7.

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

mod 3

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

mod 5

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

mod 7

We can see that in each table there is a column with a zero at the top and all the other entries equal to 1. In particular, if $a \not\equiv 0$, then $a^2 \equiv 1 \mod 3$, $a^4 \equiv 1 \mod 5$ and $a^6 \equiv 1 \mod 7$. These observations lead to the conjecture $a^{p-1} \equiv 1 \mod p$ for $1 \leq a < p$. The result will also be true if $a > p$ and is not a multiple of p.

Fermat's Little Theorem

Theorem

Let p be a prime number and let a be any number which is not a multiple of p. Then

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

Fermat's Little Theorem is very useful in simplifying calculations. Fermat's theorem tells us that $9^{30} \equiv 1 \mod 31$. Without using the theorem we would have to work out $9^{30} - 1$ and then divide:

$$\begin{aligned} 9^{30} - 1 &= 42391158275216203514294433200 \\ &= 31 \cdot 1367456718555361403686917200 \end{aligned}$$

To get ready for the proof, let us first look at the special case $a = 3$ and $p = 11$. Examine the table below where calculations are carried out $\mod 11$.

m	1	2	3	4	5	6	7	8	9	10
$3m$	3	6	9	1	4	7	10	2	5	8

Each of the numbers $1, 2, \ldots, 10$ appears in the second row exactly once. Thus the product of the numbers on the top row equals the product of the numbers on the bottom row. Recalling that $10! = 1 \cdot 2 \cdot 3 \cdots 9 \cdot 10$ (factorial), we can express the product of the numbers in the second row in two ways and obtain this equality:

$$(3 \cdot 1)(3 \cdot 2) \cdots (3 \cdot 10) = 3^{10} 10! \equiv 10! \mod 11\,.$$

But, because 11 is a prime, $\gcd(10!, 11) = 1$. Hence $3^{10} \equiv 1 \mod 11$. The same idea works in the general case.

Proof of Fermat's Little Theorem.

Given a prime number p and an integer a that is not divisible by p, we claim that $a, 2a, 3a, \dots, (p-1)a$ are all different mod p. If this was not the case, for some i, j with $i \neq j$ we would have $ia \equiv ja \mod p$. But then $p \mid (i-j)a$. As p is prime, by Euclid's Lemma, $p \mid (i-j)$ or $p \mid a$. This is impossible as p divides no non-zero positive number less than p.
Taking products as before we have

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

Because $\gcd(p, (p-1)!) = 1$, we can conclude that $a^{p-1} \equiv 1 \mod p$. □

One application of Fermat's Little Theorem is in proving that a number is not prime. For example

$2^{220} = 1684996666696914987166688442938726917102321526408785780068975$

and we find $2^{220} \equiv 16 \mod 221$. If 221 was a prime, we should have found that 2^{220} is congruent to $1 \mod 221$. Thus 221 is not prime. In fact we can easily find $221 = 13 \cdot 17$.
How to calculate We can determine that $2^{220} \equiv 16 \mod 221$ without doing too many calculations and without getting very large numbers. How this can be done will be explained later. We will then see how Fermat's Little Theorem can be used to test if very large numbers are prime or not.

EULER'S FORMULA

Fermat's Little Theorem requires our modulus to be prime. If the modulus is not prime we need an alternative formula. This is given by a formula of Euler, an 18th century Swiss Mathematician. Firstly we define what we call the **Euler φ function**.

For any positive integer m, $\varphi(m)$ is defined to be the number of integers between 1 and m inclusive which are coprime to m. The values of $\varphi(m)$ for small values of m are given in the table below.

m	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4

Note that $\varphi(p) = p - 1$ if p is prime. Euler's formula is that if $\gcd(a, m) = 1$ then

$$a^{\varphi(m)} \equiv 1 \mod m.$$

In the case of a prime this just reduces to Fermat's Little Theorem. The proof of Euler's formula is similar to that of Fermat's Little Theorem. We list the $\varphi(m)$ numbers between 1 and m which are coprime to m,

$$1 = b_1 < b_2 < \ldots < b_{\varphi(m)} < m.$$

Now multiply each number by $a \mod m$. We obtain the same numbers but in a different order. Thus the product of the two sets of numbers is the same $\mod m$. This leads to

$$a^{\varphi(m)} B \equiv B \mod m$$

where $B = b_1 \cdot b_2 \cdots b_{\varphi(m)}$. Clearly $\gcd(B, m) = 1$ hence we obtain Euler's formula.

Having established Euler's formula we see that it is important to be able to calculate $\varphi(m)$. We know $\varphi(p) = p - 1$ if p is a prime number. More generally, for $k \geq 1$ we have $\varphi(p^k) = p^k - p^{k-1}$ as any number of the form ap with $1 \leq a \leq p^{k-1}$ has a common factor with p^k.
Let us now look at $\varphi(p_1 p_2)$ where p_1 and p_2 are different primes. There are p_2 multiples of p_1 which are not coprime to $p_1 p_2$ and there are p_1 multiples of p_2 which are not coprime to $p_1 p_2$. However $p_1 p_2$ is in both lists. Thus

$$\varphi(p_1 p_2) = p_1 p_2 - p_1 - p_2 + 1 = (p_1 - 1)(p_2 - 1) = \varphi(p_1)\varphi(p_2).$$

Investigating further we can find out that $\varphi(p_1^r p_2^s) = \varphi(p_1^r)\varphi(p_2^s)$.

This is not quite enough to enable us to calculate $\varphi(m)$ once we know the prime factorisation of m. We need the following result.

$$\text{If} \quad \gcd(m,n) = 1 \quad \text{then} \quad \varphi(mn) = \varphi(m)\varphi(n).$$

A function satisfying this property is called **multiplicative**. Let us see how we can use this property to calculate $\varphi(m)$ in general. Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

be the prime factorisation of m, then

$$\begin{aligned}
\varphi(m) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) \\
&= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) \\
&= m \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

Example

$\varphi(2000) = \varphi(2^4 \cdot 5^3) = \varphi(2^4)\varphi(5^3) = (16 - 8)(125 - 25) = 800$

Example

$\varphi(2008) = \varphi(8)\varphi(251) = (8 - 4)(251 - 1) = 1000$

The proof of the multiplicative property of the function φ will be given in the next section in which we look at a result known as the Chinese Remainder Theorem.

Sun Zi who lived about 2000 years ago is thought to have discovered what is known as the Chinese Remainder Theorem. In his Mathematical Manual he posed the problem of finding the smallest solution of the system of congruences

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 2 \mod 7\,. \end{aligned}$$

In the original the problem is expressed as follows:

> *We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives we have three left over. If we count them by sevens there are two left over. How many things are there?*

Theorem (Chinese Remainder Theorem (simplest version))

Let m and n be integers with $\gcd(m,n) = 1$ and let a and b be integers. Then the system of congruences

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}$$

has exactly one solution c with $0 \leq c < mn$.

Proof.

Assume that $0 \leq a < m$ and $0 \leq b < n$. Solving the first congruence we obtain $x = a + my$ for some y. Substituting into the second congruence we have $my \equiv b - a \mod n$. Given that $\gcd(m, n) = 1$ we know (why?) there is exactly one solution y with $0 \leq y < n$. Then $c = my + a$ will be a solution of both congruences and $0 \leq c < mn$.

If c' was another solution of both congruences, than $c' - c$ would be divisible by m and by n. As $\gcd(m, n) = 1$, we would get $c' \equiv c \mod mn$. This shows that c is unique (it is the remainder on division by mn of each solution). $\square$

Example

Solution of Sun Zi's problem. We can list all solutions of the first congruence $x \equiv 2 \mod 3$

$$\{\dots, -7, -4, -1, 2, 5, 8, 11, 14, 17, 20, 23, \dots\}.$$

Now pick out those from this list which are congruent to 3 mod 5, this gives

$$\{\dots, -7, 8, 23, \dots\}.$$

These are the numbers $\equiv 8 \mod 15$. Now apply the Chinese remainder theorem to

$$\begin{aligned} x &\equiv 8 \mod 15 \\ x &\equiv 2 \mod 7\,. \end{aligned}$$

We see that a solution to Sun Zi's problem is 23. But 128 is also a solution. The general solution is $x \equiv 23 \mod 105$.

PROOF

We are now ready to prove that the Euler φ function is multiplicative. Let

$$A = \{x : \gcd(x, m) = 1 \text{ and } 1 \leq x < m\}$$

and let

$$B = \{x : \gcd(x, n) = 1 \text{ and } 1 \leq x < n\}$$

where $\gcd(m, n) = 1$. Then $|A| = \varphi(m)$ and $|B| = \varphi(n)$, where $|A|$ denotes the number of elements in the set A. Let

$$C = \{x : \gcd(x, mn) = 1 \text{ and } 1 \leq x < mn\}.$$

We need to show that $|C| = |A| \cdot |B|$.

Let $a \in A$ and $b \in B$. By the Chinese Remainder theorem we can associate with any ordered pair $(a, b) \in A \times B$ the unique c satisfying $1 \leq c \leq mn$ and

$$c \equiv a \mod m \quad \text{and} \quad c \equiv b \mod n.$$

These congruences and $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$ imply that $\gcd(c, m) = \gcd(c, n) = 1$. From this we get $\gcd(c, mn) = 1$, thus $c \in C$. Conversely, if $\gcd(c, mn) = 1$ then $\gcd(c, m) = 1$ and $\gcd(c, n) = 1$. This shows that we have a one-to-one relationship between pairs $(a, b) \in A \times B$ and the elements of C, thus $|C| = |A| \cdot |B|$ and we have shown that the Euler φ function is multiplicative.

Example

Let $m = 12$ and $n = 5$. The residues coprime to 12 and to 5 are:

$$A = \{1, 5, 7, 11\}, \quad B = \{1, 2, 3, 4\}.$$

The residues coprime to $mn = 60$ are

$$C = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}.$$

The correspondence between ordered pairs (a, b) and elements of C is as follows.

$(1, 1)$	1	$(5, 1)$	41	$(7, 1)$	31	$(11, 1)$	11
$(1, 2)$	37	$(5, 2)$	17	$(7, 2)$	7	$(11, 2)$	47
$(1, 3)$	13	$(5, 3)$	53	$(7, 3)$	43	$(11, 3)$	23
$(1, 4)$	49	$(5, 4)$	29	$(7, 4)$	19	$(11, 4)$	59

Example

Find the unique 3-digit number satisfying

$$\begin{aligned} x &\equiv 4 \mod 7 \\ x &\equiv 8 \mod 11 \\ x &\equiv 10 \mod 13 \end{aligned}$$

For a slick solution we observe that the congruences can be rewritten in the form

$$\begin{aligned} x &\equiv -3 \mod 7 \\ x &\equiv -3 \mod 11 \\ x &\equiv -3 \mod 13. \end{aligned}$$

Thus the solution of the system of congruences is $x \equiv -3 \mod 1001$ and so the only 3-digit solution is $-3 + 1001 = 998$. Check: $998 = 7 \cdot 142 + 4 = 11 \cdot 90 + 8 = 13 \cdot 76 + 10$.

Example

Find the smallest positive integer satisfying

$$\begin{aligned} 3x &\equiv 5 \mod 8 \\ 7x &\equiv 9 \mod 17 \\ 11x &\equiv 17 \mod 25 \end{aligned}$$

Whiteboard!