# Lecture 3: Fermat and Euler

## 3.1 Multiplying the first row mod 7

We will work out the $\times$ table for mod 7. [CLASS WORK] The first non-zero row is

$$\mathbf{0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6}$$

What is the product of the (non-zero) entries of this row? That is, what is $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$? I want to multiply mod 7. Or, if you know the notation, what is 6!, mod 7? This computation can be done several ways.

**Direct computation** is one way. $6! = 720$, and we can discard the 700 immediately. Then 20 is one away from 21, so the answer is $-1$ or 6 mod 7.

**Some thought** Maybe a little bit of information about the answer is enough. Actually, all we'll need is that 6! is *not zero* mod 7. I can conclude this almost immediately by "pure thought". The numbers I'm multiplying are all not zero. Since 7 is prime, there are no "interior" zeros in the multiplication table for 7. So the product, whatever it is, will be obtained by repeatedly looking up numbers inside the table, and it can't be zero.

**Even more thought** Here's a slightly stronger version of the pure thought argument, which gives the actual value. Remember that every non-zero number in $\{1, 2, 3, 4, 5, 6\}$ actually has a multiplicative inverse. Let's pair up the inverses: 2 and 4 are inverses; 3 and 5 are inverses. 1 and 6 are slightly different. Each of 1 and 6 are their own multiplicative inverses. That's because these are the solutions of $x^2 = 1$ mod 7. The solutions of $x^2 - 1 = 0$ can be gotten by factoring: $x^2 - 1 = (x - 1)(x + 1)$. The only $x$'s solving this are gotten either by setting $x - 1 = 0$ or $x + 1 = 0$ (this is again because the multiplication table has no interior zeros). So $x = 1$ or $x = -1$. The latter means $x = 6$, of course. Now consider the product $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ again. The inside numbers from 2 to 5 all cancel out, since we can pair up the pairs of numbers and multiplicative inverses. What's left? Only 1 and 6. So the product is 6.

## 3.2 Multiplying more rows: some theorems

Exactly the same approach will work with any prime number, $P$. The product of the non-zero numbers in the first row is $(P - 1)!$ and the mod $P$ value of this product can be exactly computed by realizing that almost all of the numbers can be matched up with their multiplicative inverses. The only ones which can't be canceled are 1 and $P - 1$. Discard the 1, since it doesn't effect the answer. And we now know $(P - 1)!$ is $-1$ mod $P$. This is called Wilson's Theorem, and is about 250 years old. It is nice to note that Wilson's Theorem was first proved by Lagrange. In my own career, I am trying to write as many theorems as possible, and hoping other people then will prove them so many "Greenfield's Theorem" citations will occur. By the way, the converse is true: if $N$ is an integer so that $(N-1)!$ is $-1$ mod $N$, then $N$ must be prime. It isn't practical to use this characterization of prime numbers since many multiplications must be done to compute the factorial.

What we'll need is merely that $(P - 1)!$ isn't 0 mod $P$. Understanding that is easy, as remarked above. But what about the other rows in the mod 7 table? For example, the row attached to 4 is the following:

**0 4 1 5 2 6 3**

What is the product of the non-zero entries of this row? I'll bet it is 6! because multiplication is commutative. But, wait, notice that the first non-zero entry is $4 \cdot 1$, the second is $4 \cdot 2$, the third is $4 \cdot 3$, the fourth is $4 \cdot 4$, the fifth is $4 \cdot 5$, and the sixth is $4 \cdot 6$. If we organize the computation effectively, remembering how to manipulate exponents* then the result is $4^6 \cdot 6!$. But now we see that $4^6 \cdot 6! = 6!$ mod 7. Since 6! isn't 0 mod 7 we can divide by it (I'm supposed to write: multiply by its multiplicative inverse). This is why I wanted to know 6! wasn't 0 mod 7, so I can conclude $4^6 = 1$ mod 7. By the way, $4^6$ in usual arithmetic is 4096. You can divide by 7 and verify that the result is 585, with remainder **1**, exactly as predicted.

### 3.3 Fermat's Little Theorem

> The result described here is called Fermat's Little Theorem because it was first written on the head of a pin, and smuggled out of France in a tailor's sewing kit. Results derived from it were used to win the war for England against France ...

Well, that's all ludicrous, but in fact cryptography, which we're edging closer and closer to, became extremely important during the Second World War. The clever use of information derived from making and breaking secure communications systems has become exceedingly important. More later about this, but here is a result from the year 1640:

**Fermat's Little Theorem**

If $P$ is prime, and $a$ is an integer between 0 and $P$, then $a^{P-1} = 1 \bmod P$.

It is called the *Little* Theorem to contrast it with the famous *Last* Theorem, proven quite recently after many people worked on it for many years.

If you followed the discussion above, you can see we have proved this result. The $a$'s row of the mod $P$ multiplication table is a rearrangement of the first row. The non-zero entries in each row therefore have a non-zero product which is the same, but the entries differ by $P - 1$ multiplications of $a$, so that must mean that multiplication by $a^{P-1}$ mod $P$ doesn't do much. It just multiplies by 1.

### 3.4 Crypto dreams ...

One cryptographic goal is to send information secretly using a channel that is assumed to be available to the opponent. We will in fact meet the most common personifications of this soon: Alice and Bob trying to communicate securely, and Eve, trying to untangle their disguises.

Just the multiplication table mod $P$ when $P$ is a "large" prime (9001?) already begins to look interesting. Why not take a message, and have the sender interchange the letters of the message according to a far-out row of the multiplication table, the row corresponding to multiplication by, say, 433. Then the receiver would decode by using the row corresponding to the multiplicative inverse of 433 mod 9001. What a great scheme! The Euclidean algorithm allows us to easily find the multiplicative inverse, and then there

* **OFFICIAL EXPONENT RULE 1:** $A^B \cdot A^C = A^{B+C}$.

would be no problem. Oops: the Euclidean algorithm *also* allows Eve to find the inverse rapidly. Part of our goal should not be to make the eavesdropper's work easier!

So equations like $433x = 1 \bmod P$ can be solved easily. But experimentally and theoretically, exponentiation seems much harder to undo. Look at Fermat's result again: $a^{P-1} = 1 \bmod P$ so $a^P = a \bmod P$. Somehow, $a$ gets fed into a messy exponential machine, and then magically (mod $P$!) the original information, $a$ comes right out:

$$a \to \overbrace{a^P}^{\textbf{!!!}} \to a$$

A mystery occurs at **!!!**. If we could stop the exponentiation *halfway through* – then we'd have a neat scheme. If somehow we could exponentiate twice, sending our message *between* the two exponentiations, then we'd have a candidate for a neat "cryptosystem". Repeated exponentiation* is certainly possible, but, darn it, the exponent here is a *prime* so that if $P$ is $BC$, one of $B$ and $C$ must be 1, so one of the exponentiations isn't doing much.

### 3.5 Euler's generalization of Fermat's result and some sociology

We will generalize Fermat's result in order to create a situation which is more useful for cryptography. So given an integer $N$, we want to find another integer, $\mathbf{magic}(N)$ (which may depend on $N$) so that for lots of integers, $a$, $a^{\mathbf{magic}(N)} = 1 \bmod N$. Euler thought of this. The useful generalization is to numbers which are the products of two distinct primes. Even here we must give up the freedom of choosing essentially any non-zero $a$. If $P = 3$ and $Q = 5$ and $a = 3$, then the powers of $a$ mod 15 are 3, 9, $9 \cdot 3 = 27 = 12$, $12 \cdot 3 = 36 = 6$, $6 \cdot 3 = 18 = 3$, etc. *None* of these powers are 1. More information is needed about $a$ in this case.

**Euler's Theorem**

If a is not divisible by $P$ or $Q$ then

$$a^{(P-1)(Q-1)} = 1 \bmod PQ.$$

In a lovely book called *A Mathematician's Apology*, G. H. Hardy, one of the great mathematicians of the last (twentieth!) century, asserted that he selected the mathematics he investigated solely because of its beauty. He stated with pride that almost nothing he had done had *any* use.† Much of Hardy's work during the first half of the twentieth century was in number theory, studying properties of prime numbers. Hardy's efforts are quite relevant to contemporary cryptography. Looking back at his comments one can see he was as foolish as people who want to do *only* work that has immediate applications, and who declare that theoretical work without applications is always unjustified. Perhaps neither

* **OFFICIAL EXPONENT RULE 2:** $\left(A^B\right)^C = A^{BC}$**.**

† He wrote: "... Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems very unlikely that anyone will do so for many years."

side of this discussion is always right, or even correct a great deal of the time. Both abstract and applied investigations seem to be important. And maybe human beings can't totally forecast the future.

An example for Euler's Theorem: suppose $P = 3$, $Q = 5$, and $a = 2$. Then $(P-1)(Q-1) = 2 \cdot 4 = 8$ and $2^8 = 256$. Since $256 = 255 + 1 = 15 \cdot 17 + 1$, $256 = 1 \bmod 15$. Of course, since powers of 1 are 1, we know that $256^{10} = 1^{10} = 1 \bmod 15$. `Maple` reports that $256^{10}$ is 12089 25819 61462 91747 06176. It is not immediately clear to me that the remainder resulting from dividing this number by 15 will be 1.

We will use the following equation repeatedly:

$$a^{(\text{any integer})(P-1)(Q-1)} = 1 \bmod PQ.$$

This follows from Euler's Theorem since $1^{\text{any integer}}$ is 1.

Euler's Theorem can be proved in a fashion similar to Fermat's result. The proof is more involved, since the multiplication table is more complicated: there *are* interior zeros.

### 3.6 Bibliography

Here are some upper-level undergraduate texts.

[1] Johannes A. Buchmann, *Introduction to Cryptography (Undergraduate Texts in Mathematics)*, Springer, 2001 ($40).

[2] Paul B. Garrett, *Making, Breaking Codes: Introduction to Cryptology*, Prentice Hall, 2000 ($70, about 525 pages).

[3] Richard Anthony Mollin, *An Introduction to Cryptography*, CRC Press, 2000 ($80, about 400 pages).

Here are some texts with prerequisites more suitable for high-school students.

[4] Albrecht Beutelspacher, *Cryptology (Spectrum Series)*, Mathematical Association of America, 1994 ($36, 156 pages).

[5] Thomas H. Barr, *Cryptology: the Science of Secret Writing*, 2002, Prentice-Hall ($70, 420 pages).

For people who want the computer programs, too, and other insights into implementation:

[6] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, second edition, 1995, John Wiley (a paperback 785 pages long, $55).